Name :باسم عادل الحسيني عبد الحليم

ID : 241

Group : 2

Section: 11

* mobile computing system

1. Home

    <div id="home">

        <P>

            Mobile computing is human–computer interaction in which a computer is expected to be transported during

            normal usage, which allows for the transmission of data, voice, and video. Mobile computing involves mobile

            communication, mobile hardware, and mobile software. Communication issues include ad hoc networks and

            infrastructure networks as well as communication properties, protocols, data formats, and concrete

            technologies. Hardware includes mobile devices or device components. Mobile software deals with the

            characteristics and requirements of mobile applications.

            Expandability, Replaceability and Modularity: In contrast to the common traditional motherboard-based PC the

            SoC architecture in which they are embedded makes impossible these features.

            Lack of a BIOS: As most smart devices lack a proper BIOS, their bootloading capabilities are limited as they

            can only boot into the single operative system with which it came, in contrast with the PC BIOS model.

            Range and bandwidth: Mobile Internet access is generally slower than direct cable connections, using

            technologies such as GPRS and EDGE, and more recently HSDPA, HSUPA, 3G and 4G networks and also the proposed

            5G network. These networks are usually available within a range of commercial cell phone towers. High-speed

            network wireless LANs are inexpensive but have a very limited range.

            Security standards: When working mobile, one is dependent on public networks, requiring careful use of VPN.

            Security is a major concern while concerning the mobile computing standards on the fleet. One can easily

            attack the VPN through a huge number of networks interconnected through the line.

            Power consumption: When a power outlet or portable generator is not available, mobile computers must rely

            entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually

            expensive batteries must be used to obtain the necessary battery life.

            Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere

            with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

            Potential health hazards: People who use mobile devices while driving are often distracted from driving and

            are thus assumed more likely to be involved in traffic accidents.[1] (While this may seem obvious, there is

            considerable discussion about whether banning mobile device use while driving reduces accidents.[2][3]) Cell

            phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health

            have been raised.

            Human interface with device: Screens and keyboards tend to be small, which may make them hard to use.

            Alternate input methods such as speech or handwriting recognition require training.

        </P>

    </div>

1. Devices

    <div id="Main principles">

        <p>

            Portability: Devices/nodes connected within the mobile computing system should facilitate mobility. These

            devices may have limited device capabilities and limited power supply but should have a sufficient

            processing capability and physical portability to operate in a movable environment.

            Connectivity: This defines the quality of service (QoS) of the network connectivity. In a mobile computing

            system, the network availability is expected to be maintained at a high level with a minimal amount of

            lag/downtime without being affected by the mobility of the connected nodes.

            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 often denote an individual;

            a mobile computing system should be able to adopt the technology to cater to the individual needs and also

            to obtain contextual information of each node.

            Wireless data connections used in mobile computing take three general forms.[11] Cellular data service uses

            technologies GSM, CDMA or GPRS, 3G networks such as W-CDMA, EDGE or CDMA2000.[12][13] and more recently 4G

            and 5G networks. These networks are usually available within range of commercial cell towers. Wi-Fi

            connections offer higher performance,[14] may be either on a private business network or accessed through

            public hotspots, and have a typical range of 100 feet indoors and up to 1000 feet outdoors.[15] Satellite

            Internet access covers areas where cellular and Wi-Fi are not available[16] and may be set up anywhere the

            user has a line of sight to the satellite's location,[17] which for satellites in geostationary orbit means

            having an unobstructed view of the southern sky.[11] Some enterprise deployments combine networks from

            multiple cellular networks or use a mix of cellular, Wi-Fi and satellite.[18] When using a mix of networks,

            a mobile virtual private network (mobile VPN) not only handles the security concerns, but also performs the

            multiple network logins automatically and keeps the application connections alive to prevent crashes or data

            loss during network transitions or coverage loss.

        </p>

        <!-- img of mobidic mobile -->

        <img

            src="data:image/jpeg;base64,">

    </div>

1. Classification

    <div id="classification">

        <table>

            <caption>classification of mobile communication</caption>

            <tr>

                <th> mobile communication </th>

            </tr>

            <tr>

                <th>infrascruted</th>

                <td>celluer</td>

            </tr>

            <tr>

                <th scope="row"> infrastructer less </th>

                <td>manet</td>

                <td>wsn</td>

            </tr>

        </table>

    </div>

1. In-vehicle computing

    <div id="Security">

        <p>

            Mobile security has become increasingly important in mobile computing. It is of particular concern as it

            relates to the security of personal information now stored on the smartphone. Mobile applications might copy

            user data from these devices to a remote server without the users’ permission and often without the users’

            consent.[4] The user profiles automatically created in the cloud for smartphone users raise privacy concerns

            on all major platforms, in terms of, including, but not limited to, location tracking[5] and personal data

            collection,[6] regardless of user settings on the device.[7]

            More and more users and businesses use smartphones as a means of planning and organizing their work and

            private life. Within companies, these technologies are causing profound changes in the organization of

            information systems and therefore they have become the source of new risks. Indeed, smartphones collect and

            compile an increasing amount of sensitive information to which access must be controlled to protect the

            privacy of the user and the intellectual property of the company.

            All smartphones are preferred targets of attacks. These attacks exploit weaknesses related to smartphones

            that can come from means of wireless telecommunication like WiFi networks and GSM. There are also attacks

            that exploit software vulnerabilities from both the web browser and operating system. Finally, there are

            forms of malicious software that rely on the weak knowledge of average users.

            Different security counter-measures are being developed and applied to smartphones, from security in

            different layers of software to the dissemination of information to end-users. There are good practices to

            be observed at all levels, from design to use, through the development of operating systems, software

            layers, and downloadable apps.

        </p>

    </div>

* This Html Document :

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>mobile computing</title>

</head>

<body>

    <p class="logo">mobile computing</p>

    <!-- list of anchor -->

    <ul>

        <li><a href="#home">home</a></li>

        <li><a href="#Main principles">Main principles</a></li>

        <li><a href="classification">classification</a></li>

        <li><a href="#Security">Security</a></li>

        <li><a href="#communication">communication</a></li>

    </ul>

    <div id="home">

        <P>

            Mobile computing is human–computer interaction in which a computer is expected to be transported during

            normal usage, which allows for the transmission of data, voice, and video. Mobile computing involves mobile

            communication, mobile hardware, and mobile software. Communication issues include ad hoc networks and

            infrastructure networks as well as communication properties, protocols, data formats, and concrete

            technologies. Hardware includes mobile devices or device components. Mobile software deals with the

            characteristics and requirements of mobile applications.

            Expandability, Replaceability and Modularity: In contrast to the common traditional motherboard-based PC the

            SoC architecture in which they are embedded makes impossible these features.

            Lack of a BIOS: As most smart devices lack a proper BIOS, their bootloading capabilities are limited as they

            can only boot into the single operative system with which it came, in contrast with the PC BIOS model.

            Range and bandwidth: Mobile Internet access is generally slower than direct cable connections, using

            technologies such as GPRS and EDGE, and more recently HSDPA, HSUPA, 3G and 4G networks and also the proposed

            5G network. These networks are usually available within a range of commercial cell phone towers. High-speed

            network wireless LANs are inexpensive but have a very limited range.

            Security standards: When working mobile, one is dependent on public networks, requiring careful use of VPN.

            Security is a major concern while concerning the mobile computing standards on the fleet. One can easily

            attack the VPN through a huge number of networks interconnected through the line.

            Power consumption: When a power outlet or portable generator is not available, mobile computers must rely

            entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually

            expensive batteries must be used to obtain the necessary battery life.

            Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere

            with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

            Potential health hazards: People who use mobile devices while driving are often distracted from driving and

            are thus assumed more likely to be involved in traffic accidents.[1] (While this may seem obvious, there is

            considerable discussion about whether banning mobile device use while driving reduces accidents.[2][3]) Cell

            phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health

            have been raised.

            Human interface with device: Screens and keyboards tend to be small, which may make them hard to use.

            Alternate input methods such as speech or handwriting recognition require training.

        </P>

    </div>

    <div id="Main principles">

        <p>

            Portability: Devices/nodes connected within the mobile computing system should facilitate mobility. These

            devices may have limited device capabilities and limited power supply but should have a sufficient

            processing capability and physical portability to operate in a movable environment.

            Connectivity: This defines the quality of service (QoS) of the network connectivity. In a mobile computing

            system, the network availability is expected to be maintained at a high level with a minimal amount of

            lag/downtime without being affected by the mobility of the connected nodes.

            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 often denote an individual;

            a mobile computing system should be able to adopt the technology to cater to the individual needs and also

            to obtain contextual information of each node.

            Wireless data connections used in mobile computing take three general forms.[11] Cellular data service uses

            technologies GSM, CDMA or GPRS, 3G networks such as W-CDMA, EDGE or CDMA2000.[12][13] and more recently 4G

            and 5G networks. These networks are usually available within range of commercial cell towers. Wi-Fi

            connections offer higher performance,[14] may be either on a private business network or accessed through

            public hotspots, and have a typical range of 100 feet indoors and up to 1000 feet outdoors.[15] Satellite

            Internet access covers areas where cellular and Wi-Fi are not available[16] and may be set up anywhere the

            user has a line of sight to the satellite's location,[17] which for satellites in geostationary orbit means

            having an unobstructed view of the southern sky.[11] Some enterprise deployments combine networks from

            multiple cellular networks or use a mix of cellular, Wi-Fi and satellite.[18] When using a mix of networks,

            a mobile virtual private network (mobile VPN) not only handles the security concerns, but also performs the

            multiple network logins automatically and keeps the application connections alive to prevent crashes or data

            loss during network transitions or coverage loss.

        </p>

        <!-- img of mobidic mobile -->

        <img

            src="data:image/jpeg;base64,">

    </div>

    <!-- table for classification of mobile communication-->

    <div id="classification">

        <table>

            <caption>classification of mobile communication</caption>

            <tr>

                <th> mobile communication </th>

            </tr>

            <tr>

                <th>infrascruted</th>

                <td>celluer</td>

            </tr>

            <tr>

                <th scope="row"> infrastructer less </th>

                <td>manet</td>

                <td>wsn</td>

            </tr>

        </table>

    </div>

    <div id="Security">

        <p>

            Mobile security has become increasingly important in mobile computing. It is of particular concern as it

            relates to the security of personal information now stored on the smartphone. Mobile applications might copy

            user data from these devices to a remote server without the users’ permission and often without the users’

            consent.[4] The user profiles automatically created in the cloud for smartphone users raise privacy concerns

            on all major platforms, in terms of, including, but not limited to, location tracking[5] and personal data

            collection,[6] regardless of user settings on the device.[7]

            More and more users and businesses use smartphones as a means of planning and organizing their work and

            private life. Within companies, these technologies are causing profound changes in the organization of

            information systems and therefore they have become the source of new risks. Indeed, smartphones collect and

            compile an increasing amount of sensitive information to which access must be controlled to protect the

            privacy of the user and the intellectual property of the company.

            All smartphones are preferred targets of attacks. These attacks exploit weaknesses related to smartphones

            that can come from means of wireless telecommunication like WiFi networks and GSM. There are also attacks

            that exploit software vulnerabilities from both the web browser and operating system. Finally, there are

            forms of malicious software that rely on the weak knowledge of average users.

            Different security counter-measures are being developed and applied to smartphones, from security in

            different layers of software to the dissemination of information to end-users. There are good practices to

            be observed at all levels, from design to use, through the development of operating systems, software

            layers, and downloadable apps.

        </p>

    </div>

    <div id="communication">

        Several categories of portable computing devices can run on batteries but are not usually classified as laptops:

        portable computers, PDAs, ultra mobile PCs (UMPCs), tablets, and smartphones.

        A portable computer (discontinued) is a general-purpose computer that can be easily moved from place to place,

        but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source. The

        most famous example is Osborne 1. Portable computers are also called a "transportable" or a "luggable" PC.

        A personal digital assistant (PDA) (discontinued) is a small, usually pocket-sized, computer with limited

        functionality. It is intended to supplement and to synchronize with a desktop computer, giving access to

        contacts, address book, notes, e-mail, and other features.

        A Palm TX PDA

        An ultra mobile PC (discontinued) is a full-featured, PDA-sized computer running a general-purpose operating

        system.

        Tablets/phones: a slate tablet is shaped like a paper notebook. Smartphones are the same devices as tablets,

        however, the only difference with smartphones is that they are much smaller and pocketable. Instead of a

        physical keyboard, these devices have a touchscreen including a combination of a virtual keyboard but can also

        link to a physical keyboard via wireless Bluetooth or USB. These devices include features other computer systems

        would not be able to incorporate, such as built-in cameras, because of their portability - although some laptops

        possess camera integration, and desktops and laptops can connect to a webcam by way of USB.

        A carputer is installed in an automobile. It operates as a wireless computer, sound system, GPS, and DVD player.

        It also contains word processing software and is Bluetooth compatible.[8]

        A Pentop (discontinued) is a computing device the size and shape of a pen. It functions as a writing utensil,

        MP3 player, language translator, digital storage device, and calculator.[9]

        An application-specific computer is one that is tailored to a particular application. For example, Ferranti

        introduced a handheld application-specific mobile computer (the MRT-100) in the form of a clipboard for

        conducting opinion polls.[10]

        Boundaries that separate these categories are blurry at times. For example, the OQO UMPC is also a PDA-sized

        tablet PC; the Apple eMate had the clamshell form factor of a laptop but ran PDA software. The HP Omnibook line

        of laptops included some devices small more enough to be called ultra mobile PCs. The hardware of the Nokia 770

        internet tablet is essentially the same as that of a PDA such as the Zaurus 6000; the only reason it's not

        called a PDA is that it does not have PIM software. On the other hand, both the 770 and the Zaurus can run some

        desktop Linux software, usually with modifications.

    </div>

</body>

</html>