Mobile technology and Security Issues

By – Parisha

G.C Bhiwani

Assistant Professor in Computer Science

ABSTRACT

In this abstract we will discuss Mobile Technology, its pros and cons and some security issues related to mobiles. Mobile Technology is the technology used for cellular communications .Mobile code division multiple access (CDMA) technology has evolved rapidly over the past few years Mobile technology includes general packet radio service (GPRS), multimedia messaging service (MMS), Bluetooth, 3G, wireless fidelity (Wi fi), global positioning system (GPS), CLI, wireless application protocol (WAP), and short message service (SMS).Here Mobile Networking refers to technology that support voice and data network connectivity using wireless via a radio transmission solution .The most common application of mobile networking is the mobile phone. There are different technologies evolved in mobile world .Today we all are familiar with 3G,4G technologies used in mobiles which have faster data transmission speed . These technology grew because previously wireless communication use circuit switching to carry over a network ,however ,more recently both voice and data are being transmitted over both circuit and packet switched networks .The mobile technology is portable and it can be carried from one place to another .The main disadvantage of mobile technology is some security issues like unauthorized person can access the important details and it should be kept safe .In mobile Technology 5G is going to be a new mobile revolution in mobile market .It has extra ordinary data capabilities and has ability to tie together unrestricted call volumes and infinite data broadcast within latest mobile operating system .It has bright future because it can handle best technologies .It would provide high connectivity and high resolution for cell phone users .It will provide 25Mbps connectivity speed . All features will provide enhanced capabilities of data transmission with effective speed .This technology will help a lot for cell phone user.

I. INTRODUCTION

Mobile technology is exactly what the name implies - technology that is portable. Examples of mobile IT devices include laptop, tablets and notebook computers ,smart phones ,global positioning system (GPS) devices ,wireless debit/credit card payment terminals .Mobile devices can be enabled to use a variety of communications technologies, including wireless fidelity (Wi-Fi) - a type of wireless local area network technology .Bluetooth - connects mobile devices wirelessly 'third generation' (3G), 'fourth generation' (4G), global system for mobile communications (GSM) and general packet radio service (GPRS) data services - data networking services for mobile phones dial-up services - data networking services using modems and telephone lines ,virtual private networks - secure access to a private network. It is therefore possible to network the mobile device to a home office or the internet while travelling .Mobile laptop and notebook computers can use one of two types of

wireless access services when away from the home or office. The most commonly used and least expensive is Wifi . Wifi uses radio waves to broadcast an Internet signal from a wireless router to the immediate surrounding area. If the wireless network is not encrypted, anyone can jump on. WiFi is commonly used in public places to create "hotspots."The drawback to WiFi is that you must locate a hotspot, then stay put within broadcasting range to use it. An alternative to WiFi is cellular broadband. This type of mobile computing technology utilizes a cellular modem to connect to tower. Small computers are some of the most versatile computing devices. Notebooks, or ultra-mobile PCs , include many different features, making them similar in functionality to an actual laptop. They may not be able to handle the games that a larger computer can, but they are designed to be convenient for browsing the Web, working in word processing or other office programs, and sending emails. For people who travel a lot and want a light yet functional computer, this type can be the best choice; they generally feature built-in Wi-Fi, or offer the option to add the feature when purchasing the computer.

II. MOBILE TECHNOLOGY 4G AND 5G

Fourth Generation (4G) mobile technology is a set of standards for providing broadband Internet access to devices like cell phones and tablets. Though it first became available in the US in 2009, no specific technologies were officially designated as 4G until 2011. Despite this, many devices were labeled as "4G" even though they did not meet the International Telecommunication Union's (ITU) standards for the technology. The main difference between it and previous standards is a big increase in data transfer speeds and the types of media people can access with it.

There are also a number of technical specifications, including things like the wireless standard, radio interface, and frequency spectrum used .The main difference between 4G mobile technology and the previous standard, 3G technology, in terms of end usage is the data transfer speeds provided. This means that users can access much more sophisticated data that requires a lot of bandwidth very quickly. Depending on the service provider, however, 4G mobile devices may be limited to specific zones for making phone calls that are generally smaller than the areas covered by 3G. This means that people trying to make a call would have their call dropped if they went outside the covered area. Some 4G phones also have much shorter battery life than most 3G phones.

5G will, however, make communications so fast they become almost real-time, putting mobile internet services on a par with office services. One of the Chinese telecoms giant that is a driving force behind 5G research, says 5G will allow any mobile app and any mobile service to connect to anything at any time, from people and communities to physical things, processes, content, working knowledge, timely pertinent information and goods of all sorts in entirely flexible, reliable and secure ways.

It will provide greater network stability to ensure that business-critical mobile functions do not go offline and the speed necessary to give employees a fully equipped virtual office almost anywhere. If broadband services do not experience significant uplifts in speed, 5G might even prove to be a cost-effective alternative to fixed-line services in ten years' time.

Mobile data could prove to be the answer for businesses that operate outside the reach of broadband networks or suffer from slow fixed-line service. Because the cost of putting up mobile data masts is far lower than installing

fibre optic cables, operators may well decide that 5G is speedy enough to be used to reach rural areas as an alternative to fixed lines.

III. ADVANTAGES OF MOBILE TECHNOLOGIES

Mobile computing can improve the service you offer your customers. For example, when meeting with customers, you could access your customer relationship management system - over the internet - allowing you to update customer details whilst away from the office you can enable customers to pay for services or goods without having to go to the till, example by using a wireless payment terminal diners can pay for their meal without leaving their table. Powerful solutions can link you directly into the office network while working off site. For example, we could remotely set up a new customer's account , check prices and stock availability and place an order online .The growth of cloud computing has also impacted positively on the use of mobile devices, supporting more flexible working practices by providing services over the internet.

IV. ACCESS

Access is the primary benefit of mobile technology. And what's even better is that there are thousands of applications and programs that can help you stay informed and relevant to your precious customers. For example, marketing automation and CRM coupled with mobile tech can tell you every detail regarding a lead anywhere at any time .When your prospects are ready to take action, mobile technology enables you to seize the moment making it easier to close a deal. Internet technology lets you strike while the iron is hot.

V. HIGHER EFFICIENCY

Whether you own a smart phone, tablet, computer or other technological contraption, you are using a device that has been designed to help you become more productive and efficient.

VI. REDUCED COST OF OPERATIONS

At a glance, it could seem that the cost of expanding technologies may cause a deficit in the company's expenses. However, the increased productivity can easily outweigh the minimal cost and effort it would take to implement a new technology. For example, if your company has 10 employees and each employee saves 1 hour or 60 minutes per week by implementing a new technology, you've just lowered your staff cost by over 500 hours per year.

VII. DISADVANTAGES OF MOBILE TECHNOLOGIES

There are costs involved in setting up the equipment and training required to make use of mobile devices. Mobile IT devices can expose valuable data to unauthorized people if the proper precautions are not taken to ensure that the devices, and the data they can access, are kept safe .There are number of other shortcomings in mobile technologies , like,

• Range and bandwidth: Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS , and more recently 3G and 4G networks and also the upcoming 5G network. These networks are usually available within range of commercial cell phone towers. High speed network wireless LANs are inexpensive but have 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.

• 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. Cell phones may interfere with sensitive medical devices.

VIII. MOBILE SECURITY

• Mobile security or mobile phone 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 smart phone.

• More and more users and businesses use smart phones as communication tools but also 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, smart phones 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 smart phones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smart phones that can come from means of communication like SMS, MMS, 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 smart phones, 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 .

IX. HOW SECURITY SHOULD BE DONE ON DEVICES

There are several simple ways to protect the information stored on your computer or device. Installing a physical lock on laptop and notebook computers and instructing employees to use them whenever the device is at risk is considered a best practice in mobile computing security. Notebook computers should also be secured by setting a Basic Input/Output System (BIOS) or hard drive password. If the device is used remotely from the network, install stand-alone anti-virus and malware software. Consider purchasing software that tracks mobile devices and reports their location when connected to the Internet, as some security software allows the drive on a stolen device to be erased remotely.

USB flash drives pose a serious risk to mobile computing security and all data placed on them should be encrypted. Anti-malware software will prevent placing infected files on the drive that may then infect your entire network. Use your computer operating system's permission management software to control who can read and write to specific files and folders. There are also port management tools that limit access to USB, FireWire, printer, and serial ports, as well as specific devices, such as CD-ROM drives.

Portable devices should be equipped with a personal firewall. Be aware, however, that they need to be carefully chosen and configured so as to not interfere with or prevent legitimate network connectivity. Portable firewalls are especially critical for personnel who connect to the network via a Virtual Private Network (VPN). Advanced firewall software provides other functions such as intrusion prevention, anti-phishing, spam blocking, and detection of software that scans devices seeking security vulnerabilities. Encryption using a protocol, such as Wi-Fi Protected Access 2 (WPA2), is also essential for protecting wireless transmission of data.

On the network level, software should be installed that protects it from malware infections picked up by mobile devices. Beyond hardware and software mobile computing security measures, it is recommended that organizations publish clear guidelines for employees. These should address what devices may be used beyond the network, the security measures personnel must follow, and also provide general advice on preventing security breaches.

X. CONCLUSION

There are many different types of mobile computing devices designed to make it easier to travel and conveniently access technology on the go. Notebooks are small laptop computers that typically feature built-in wireless networking, and are great choices for getting work done while traveling. Mobile computing devices with a smaller form factor, such as smart phones or tablet computers, are also quite popular, and often include many advanced features comparable to those found on a laptop computer. PDAs, though much less common, are another type of mobile computing device. Even simpler cell phones will frequently include Internet access, to allow users to check their email or to access instant messaging programs .Through this paper different mobile technologies have been discussed and different ways to keep our mobile secure so that unauthorized persons could not be able to access any ones private information . In this different pros and cons of mobile technology have been discussed and 4g technology provide high speed to the users and the new technology 5g which will provide more speed and communication at low cost in future is yet to come.

REFERENCES

[1.] David P. Helmbold, "A dynamic disk spin-down technique for mobile computing", citeseer.ist.psu.edu.

[2.] MH Repacholi, "health risks from the use of mobile phones", Toxicology Letters, 2001 - Elsevier

[3.] Landay, J.A. Kaufmann, T.R., "user interface issues in mobile computing", Workstation Operating Systems.

[4.] Imieliński, T.; Badrinath, B.R. (Oct 2001). "Mobile wireless computing, challenges in data management". Communications of the ACM: 18–28.

[5.] Imieliński, T.; Badrinath, B.R. (1992). "Querying in highly mobile distributed environments" (PDF). Proceedings VLDB '92: 41–52.

[6.] T. Imielinski; H.F. Korth (Eds.) (1996). Mobile Computing. Springer.