North Asian International Research Journal of Sciences, Engineering & I.T.

IRJIF. I.F. : 3.821

ISSN: 2454-7514 Vol. 7, Issue-4 April -2021

Index Copernicus Value: 52.88 Fulfill MCI Criteria Citation Index

A Peer Reviewed Refereed Journal

ANALYSIS OF FUTURE WIRELESS TECHNOLOGIES

ASHIQ MALIK & TURAB HYDER

INTRODUCTION

Within this report, the main objective is to convince Your company director of your opinion on available wireless technologies. The director is also wary of the security concerns of the wireless technologies as she/he has read on the technical magazines. Within this report contains the pros and cons of wireless technologies ,as well as examples of some cases to help convince the director whether or not wireless technologies are good for the company or not.

Pros and Cons of wireless Technologies

Wireless technology refers to the way that communication or transmission of data and information is transferred over distance whether it be large such as a WAN or a small network like LAN .The main objective is to eliminate the use of wires, cables and other electrical conducts that may be used in a wired connection. [1]

There are many different types and ways to use wireless communications in everyday life that are huge benefit to everyday life These include Satellite communications, Wireless networking ,WiMax,WI-FI , Bluetooth as well as many others . [1]

The pros of Wireless Technologies are that they are easy to set up, coverage and the amount of users is unlimited. [1]

SIMPLE TO SET UP

Remote systems are as simple to set up as wired systems, as is adding more PCs to the system. There is clearly no compelling reason to fix wires and clients can move around inside the sign range at their watchfulness. Cell phones, for example, telephones and iPads can likewise be effectively set up to interface with the system.[1]

COVERAGE

Remote coverage of wireless technologies have improved over the previous decade and great inclusion is accessible inside a predetermined range. You can also extend the range of the desired coverage by using a extender and booster to maximize the coverage of the wireless network. [1]

BOUNDLESS USERS

Wired switches will normally accompany three or four connection ports and require a switch for extra extension. With a remote system you can include more clients without the need to change equipment, however data transfer capacity and speed may turn into an issue if there are an excessive number of clients. If the routers aren't capable of all the data traffic. [1]

COST

Remote switches have turned out to be truly reasonable in the previous couple of years, so the expenses related with setting up a remote system won't really be restrictive. It might even be less expensive to introduce a remote system in certain circumstances. [1]

As well as there being pros of networking technologies there are also cons that relate to technology, These are security, speed and the signal strength . [1]

SECURITY

Remote systems are significantly more powerless against malicious assaults and data transmission robbery when in comparison to wired systems. As it is extremely simple to associate gadgets to a remote system, a few organizations may not know that workers have introduced remote gadgets and frameworks. [1]

SPEED

While remote systems are quicker than dial-up connections, the normal speed will be generally more slower than an Ethernet connection for the internet , this could be an issue to be considered on the off chance that you or your association will depend exclusively on a remote system ,especially if you are relying on a fast internet connection and to have a steady speed. [1]

SIGNAL STRENGTH

Users can experience black spots within the coverage range of the wireless signal, due to the internet signal having trouble passing through walls and other materials which may intrude the range or the signal strength of the connection. [1] There is also a case study which I've found to help develop an idea of whether it is a good or bad idea to change to a wireless connection. It is about all the different types of connections and the reasons as to why or why not to choose a wireless system.

OPERATIONAL MECHANISMS

Bluetooth

Bluetooth is an innovation standard for remotely trading information over short separations utilizing ultra high recurrence radio waves in the unlicensed or the free to use ISM band of 2.4 GHz recurrence. The use of bluetooth in a workplace is highly recommended, Bluetooth can possibly give staff a chance to utilize their cell phones as cordless telephones connected to the PBX, just as the first thought for Bluetooth of interfacing remote headsets. The key application for Bluetooth in organizations has been as an instrument for the business power, and not on the grounds that new enactment will stop sales reps utilizing telephones while driving. Bluetooth creates a good free hands unit, however it likewise gives a connection among workstations and cell phones. [2]

Due to Bluetooth technology this means salespeople can access there company network at any time without waiting to find a wired connection to access there documents or to come in range of a wireless Lan. Although some are using wired connections to link a mobile phone and a computer, this can allow there to be a low signal if the line is busy which may delay the phone call. [2]

One of the essential advantages of Bluetooth is that it enables gadgets to transmit information remotely. This bit of leeway means that is able to incorporate remotely associating or “blending” gadgets to make a remote individual Area network system or WPAN, remote Internet availability, and remote synchronization, just as advantageously sending or potentially getting documents without the inconvenience of conveying and utilizing links or other equipment such as the use of a USB standard or Thunderbolt innovation. [2]

WLAN

A WLAN is a wireless connection that allows there to be delivery of data which joins high-frequency radio devices. More often than not, those gadgets share a frequency with an Access point in order to create a small community connection with a confined geographical catchment region of internet data which is then used to connect all devices to, within the verified distance. Organizations with a WLAN are able to utilize a wide variation of devices. You must be connected to the web to enjoy full use of the majority card machines, industrial equipment, telephones and computer systems. WLANs are the cheapest and easiest way to connect to the internet. [3]

Security vulnerabilities and resolutions

There are security vulnerabilities in every network or new technology but due to Bluetooth being created in 1994 there has been many improvements. A few vulnerabilities still. Do occur due to the software always changing and updating and these vulnerabilities are No consumer authentication. At this stage of time the Bluetooth specification solely presents built-in machine authentication with doesn’t offer the highest security .But if you wish to have a higher degree of security, you must add security by the application developer. Another issue with Bluetooth is that Link keys may be stored insecurely. This means that if an attacker was to hack a Bluetooth connection they are able to change the link keys so they could read something completely different or just be able to read personal information because the information isn’t stored securely be read or modified by an attack if they are not stored securely. An easy way to make it harder for hackers to be able to get information from you is to install mobile security software that is able to find any harmful apps, so then it is able to tell you if there has been any type of unknown access, with may have encrypted your mobile data. [2]

WLANS

Wireless local area networks send and retrieve data using radio waves rather than wires. Due to this the physical barrier is virtually nonexistent which makes WLANs vulnerable to unlawful interception, eavesdropping, hacking and a range of other cyber security issues.

WLAN security issues and threats

In the WLAN network there are common attacks that occur these are denial of service attacks, spoofing and eavesdropping. A DOS attack is where the hacker sends hacked messages which make your network slow and restricts how fast your network resources rum. Spoofing is a technique where the attacker pretends to be the victim and accesses the network and gains access to all the victims data .Lastly Eavesdropping is where a third party steals or changes data that is being sent over the secure network without the knowledge of the victim.[4]

The easiest way to keep your WLAN safe from any attack is to keep software and router or wireless access point firmware up-to-date so this makes it much more difficult for hackers to exploit weaknesses due to the software being constantly updated and the hacker may not know the new version so it’s harder to be hacked. [5]

CONCLUSION

This report has identified the pros and cons of wireless networks, as well as what they are and how they can be used in a business to help improve their sales. The wireless network that I would recommend is the WLAN due to it being easy to set up and has a wide range of internet connection which will allow all employees to be able to access online information and documents.

REFERENCES

1. “Contact Details,” TeamIT RSS. [Online]. Available: http://www.team-it.com.au/blog/pros-cons-wireless-networks/. [Accessed: 28-Aug-2019]. [1]
2. “How Bluetooth can work for your business,” ComputerWeekly.com. [Online]. Available: https://www.computerweekly.com/feature/How-Bluetooth-can-work-for-your-business. [Accessed: 28-Aug-2019]. [2]
3. B. Mitchell, “Wireless Local Area Networking (WLAN) Explained,” Lifewire, 24-Jun-2019. [Online]. Available: https://www.lifewire.com/wlan-816565. [Accessed: 28-Aug-2019]. [3]
4. Migrator, “Early WLAN security issues,” nibusinessinfo.co.uk, 15-Jan-2019. [Online]. Available: https://www.nibusinessinfo.co.uk/content/early-wlan-security-issues. [Accessed: 28-Aug-2019]. [4]
5. Migrator, “10 tips for better WLAN security,” nibusinessinfo.co.uk, 15-Jan-2019. [Online]. Available: https://www.nibusinessinfo.co.uk/content/10-tips-better-wlan-security. [Accessed: 28-Aug-2019]. [5]