IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, January 2022
Impact Factor: 6.252

The Dangers of Connecting Your Smartphone to A Public WiFi Network

Rinku Pal[1] and Farraz Shaikh[2]
Assistant Professor, BSC CS, Suman Education Society's LN College, Borivali East, Mumbai, India[1]
Student, BSC CS, Suman Education Society's LN College, Borivali East, Mumbai, India[2]

Abstract: *A wireless network is used to connect various wired structural structures and provide property inside the company for workers to move freely by bypassing the obstacle of a physical network. Because WLANs are directly tied to the core organization's network, maintaining area unit network |WLAN| wireless fidelity| Wi Fi| local area network |LAN| security is critical to a firm. The increased availability of public wireless access points (hotspots), as well as the emergence of wireless computing devices such as tabletop mobiles, have made it simpler for people to access data on the internet. The first goal of this paper is to examine the users' awareness of privacy run publicly hotspots from activities such as internet browsing, computer programme querying, and use Social Networking. The second goal of this paper is to assist university decision-makers in considering the interests of public Wi-Fi users to open or close those frequently searched sites within the university's domain and to form the best use of university resources.*

Keywords: Public Wi-Fi ·Privacy ·Websites ·Leakage ·Network.

I. INTRODUCTION

Nowadays, the internet has become a fundamental need of human life and is used for employment rather than entertainment purposes; however, it aids in routine activities such as fund transfer, bill payment, price ticket reservations, instructional analysis, learning perspectives, business trade, media coverage, and so on. If we have a propensity to, we have a tendency to the net in an incredibly single sentence then it needs to be, "net-work of networks termed internet". If we merely quote a network, what exactly is it? Where did it come from? As a result, the answer is two or more nodes (also known as system or PC).

Public Wi-Fi hotspots are becoming increasingly common across the world. Most users connect to hotspots since they are free of charge (in comparison to mobile cellular connections) and ubiquitous. The number of public Wi-Fi APs (Access Points) spread globally has reached 94 million and is expected to increase to 549 million by 2022. Over the previous ten years, mobile gadgets such as smartphones and tablets have become implausibly common. Over three.3 billion smartphones and 230 million tablets were used in the previous several years, according to the New Zoo Research Organization. Wi-Fi may be a vital component of mobile devices that allows them to connect to the internet.

In computer networks, nodes or hosts are computers, mobile phones, and servers, each with their own unique code known as raincoat address. Initially, variety emerges when network suppliers sell products such as switches, routers, and alternative products to the market. To prevent wires into a structure, a strategy by which house, business, and communications networks establish property was required; one is that the expensive and lengthy approach, which is why to consider as lengthy method. It enables the development of various wireless connections such as wire-less native space networks (WLAN), mobile phone networks, wireless sensing element networks, satellite communication networks, and microwave networks.

II. RELATED WORK

Wireless networks provide a handy way for customers to connect to the internet, and many companies find it beneficial to provide free Wi-Fi. In 2016, there were almost 269,000 free Wi-Fi hotspots in the United Kingdom [16], and over 200 London subway stations still provide free Wi-Fi, allowing individuals to find other transport options in Disconnection. However, there are square measure security risks associated with the use of public Wi-Fi. The release of privacy in conventional online social networks (OSN) has been widely explored, as this literature focuses mostly on privacy issues in social networks backed by known user knowledge, such as the study of user relationships and hence

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, January 2022
Impact Factor: 6.252

the characterisation of user behaviours. It is possible to aggregate the privacy information received from several websites and characterise the linkable property to the profile of specific users on third-party servers. To address this issue, many solutions for protecting the privacy of third-party aggregators square measure being investigated.

Several prior investigations have demonstrated the possibility of eavesdropping on Wi-Fi data to detect personal information at public hotspots. According to the report, users have inadequate knowledge of the hazards associated with Wi-Fi use and have a false feeling of security. Online pursuit, a popular web development, is used for a variety of purposes, including targeted advertising, identity verification, web analytics, and customization. Net chase tactics are often classified as homeless or homeless.

III. METHODOLOGY

To investigate the privacy run publicly Wi-Fi, we tend to planned a three-phase experiment, the first of which was discovered a public Wi-Fi, the second of which was collecting users' traffic, and the final of which was evaluating the gathered data. Figure 1 depicts the flowchart of the proposed experiment.

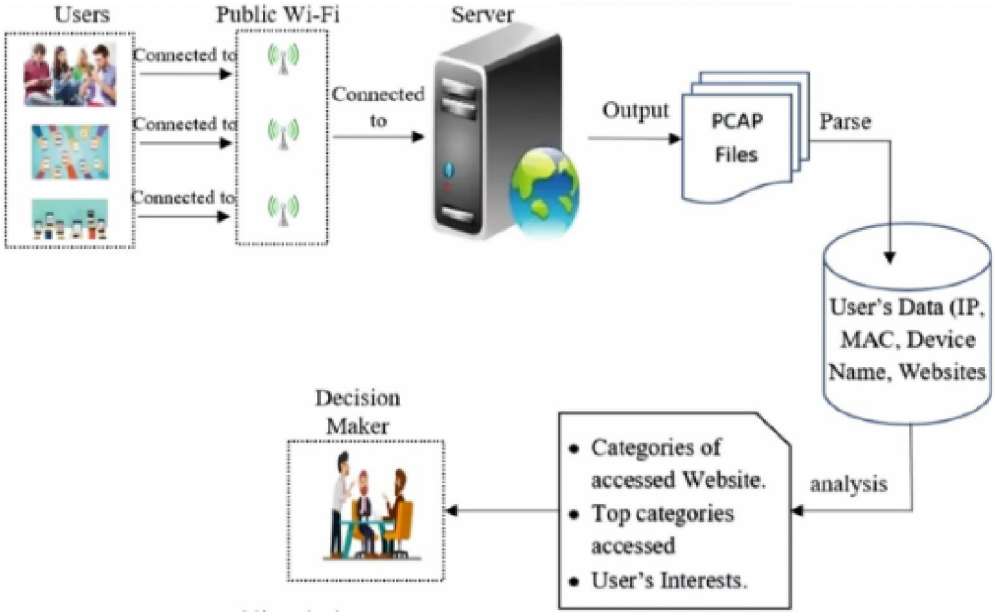

Fig. 1. Stages of the followed methodology

3.1 Configuring Public Wi-Fi

We collaborated with Minia University's knowledge technology center, which provides large-scale Wi-Fi service for students, employees, and teaching staff. The administrator of the center assigned three hotspots for our experiment, made them public, and supplied them with web service via a specific server. To monitor and observe users who use the web via these hotspots, we installed Wireshark (version three.0.6, 64 bit), on the Windows server, as shown in fig 2.

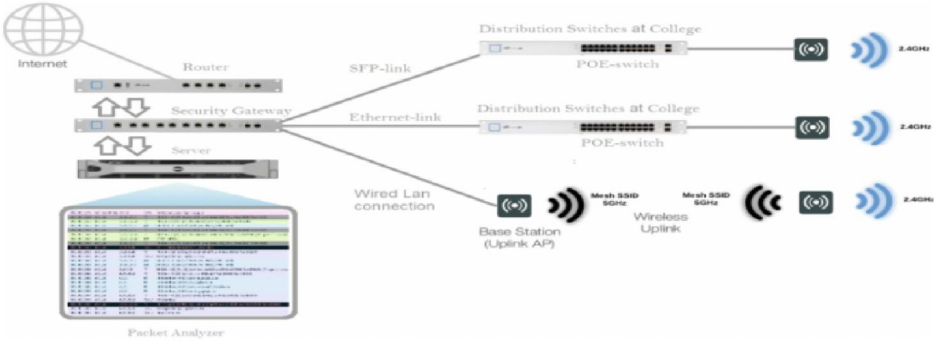

Fig. 2. Stages of setting up public Wi-Fi network

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, January 2022
Impact Factor: 6.252

3.2 Obtaining User Traffic

We discovered our experimental open free public Wi-Fi network (3 hotspots) in Minia University in various locations and times. When participants connected to the internet via our public Wi-Fi, Wireshark captured traffic routing from the participants' devices to the internet via our experimental Wi-Fi network, and the collected information was saved as PCAP files on the permanent memory of the Server at each interval of your time (twice per day), and picked up and picked up 3 days. The data was gathered in a single month, from the Gregorian calendar month through December 2020, with 7295 users.

3.3 Data Collection Analysis

In this section, we developed a model using the Python programming language to research the collected data. This model analyses the data in two steps. The first step is to dissect PCAP files to extract the information and header of HTTP, DNS, ICMP, SMTP, and POP3 for traffic routing from the participants' devices to the web, then save this information in CSV files (separated file for each protocol) as records.

If a device connects to our experimental Wi-Fi network more than once, it is considered the same user. In the second stage, we examine the data within the to extract the visited websites and any user's privacy leak.

IV. ARCHITECTURE OF WIRELESS NETWORKS

Wireless access points collaborate effectively with a radio transceiver to establish a connection that allows both radio signal transmission and reception. These signals are received by consumer devices that determine the signals, and once one of the communication channels is established, it gives greater network access. Wireless access points use the IEEE 802.11 protocol, which is the industry standard for wireless communication. The most prevalent use of this standard is Wi-Fi, sometimes known as WIFI.

Wireless access points collaborate effectively with a radio transceiver to establish a connection that allows for the transmission and receipt of radio signals. These signals square measure received by consumer devices that establish the signals, and it grants additional access to the network one of communication channels is established. The IEEE 802.11 protocol is used by wireless access points as the final standard of wireless communication. The most prevalent use of this standard is Wi-Fi, often known as WLAN.

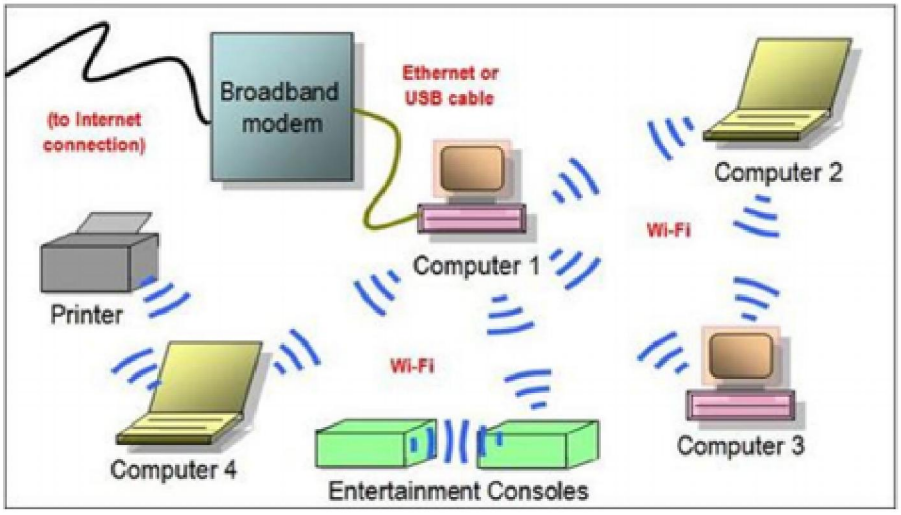

Fig 3. Ad hoc mod

V. PROTOCOLS AND STANDARDS FOR WIRELESS

The word wireless refers to data transfer by magnetic attraction waves rather than wires. The earliest wireless transmitters were used in the first twentieth century by using Morse radiotelegraphy. Technology is always changing and is becoming an increasingly important element of many people's lives. It has prompted many people to grow reliant on technology for practically every type of job.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, January 2022
Impact Factor: 6.252

Wireless access technologies are classified as follows:

1. Wireless Personal Area Network (WPAN): These square measurements are designed for a wide range of applications. IrDA and Bluetooth are two examples. Additional square measurement technologies are also on the rise for this approach. 802.15.4a—Zigbee and 802.15.3c—UWB are the square measurements.
2. Wireless local area Network (WLAN): this approach has a range of 100m and a speed of up to 200 Mbps. Wi-Fi (802.11a/b/g) is one of the most commonly utilized wireless local area network technologies.
3. Wireless Metropolitan Area Network (WMAN): This technology can offer up to 75 Mbps. Many 802.16 versions are together referred to as WiMAX.

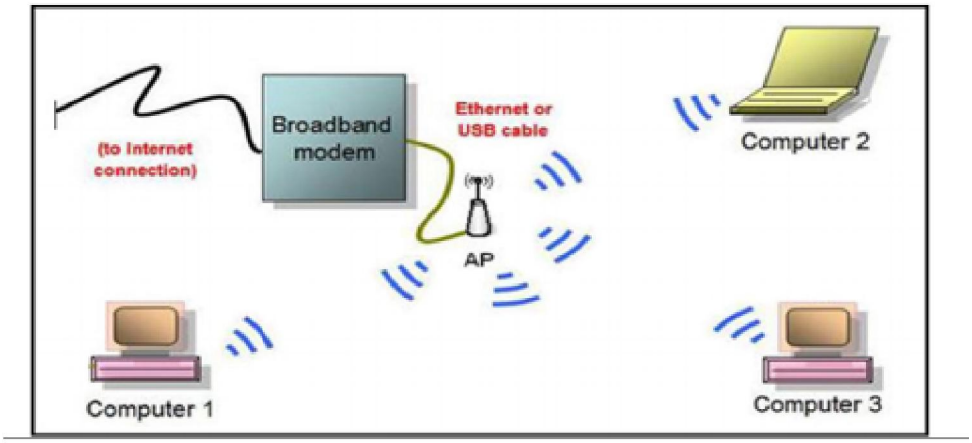

Fig. 4 Infrastructure mod

VI. USING PUBLIC WI-FI POSES SECURITY AND PRIVACY RISKS.

To discover possible security and privacy risks from exploiting public Wi-Fi networks, we examined net packets collected by Wireshark as they passed through our experimental Wi-Fi network. We specifically look for packets containing sensitive data such as passwords, cookies, and packets moving across port 80, a common port for unencrypted communications protocol traffic. We also evaluated packets that go over well-known email protocols, such as net Message Access Protocol, Post Office Protocol, and simple Mail Transfer Protocol, because they can betray the content of emails if not correctly arranged.

VII. INVESTIGATE THE PRIVACY BREACH

We assigned a unique variety to every device connected to our experimental Wi-Fi networks exploitation the MAC address and therefore the device name, making it simple for America to track a specific user like sites he visited frequently, and his information is under privacy leakage, we took ten random users and tested the sites they visited frequently.

Table 1. Sample details of the collected data from users

N0.	Device name	MAC address	Most category used
1.	HUAWEIY_9a-7346697ffa	C6:fe:49:**:**	Instant messaging
2.	OPPO-Reno2-*	6a:3a:b6:f3:**:**	Social networking
3.	HUAWEI_ Mate	C4:fe:5b:f:**:**	Streaming media and download
4.	Oppo-F9	44:46:87:4c:**:**	Sports
5.	Realme-6-pro	44:46:87:fc:**:**	Education
6.	Oppo-F11	00:0c:29:9d:**:**	Information technology
7.	Galaxy-Grand-prime-pro	F0:67:28:9d:**:**	Business and finance

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, January 2022
Impact Factor: 6.252

8.	Oppo-A31	F0:67:28:93:**:**	Search engines and storage
9.	Galaxy-17-2016	4c:02:20:e9:**:**	File sharing and portals
10.	HUAWEIY_9a-prime-2019	00:be:3b:f1:**:**	Web analytics

Table 2. Some data explaining the leakage of users' privacy

No.	Device name	Mac address	Privacy leakage
1.	Oppo-Alk	00:87:01:64:**:**	Email Mobile no. user id User name
2.	Redmi8A-Redmi	24:79:f3:0d:**:**	√ √ × √
3.	Realme-6-pro	48:83:b4:4b:**:**	√ √ × √
4.	Oppo-Reno3	86:11:df:57:**:**	× √ × ×
5.	Ebtsams-iphone	44:ae:ab:6d:**:**	× √ × ×
6.	Alnjm-alsat-59	18:d7:17:75:**:**	× × × √
7.	Galaxy-A20-alkhas-b-hesham	7e:76:68:46:**:**	× × × √
8.	Galaxy-A20-alkhas-b-reda	7e:89:56:a4:**:**	× × × √
9.	Galaxy-A20-alkhas-b-shaimaa	A6:2e:d2:f5:**:**	× × × √
10.	M2004JI9c-kerobebawy	B8:c9:b5:bc:**:**	× × × √

VIII. WIRELESS NETWORK CONNECTION CONSTRAINTS

Although wireless networks have made our life more mobile, quicker, accessible, handy, and linked, they are not without restrictions. These restrictions are inherent in their styles, ranges, or other weaknesses they may have. Continue reading this text till the end to learn more about the limitations of a Wireless Network.

The following are some of the constraints of a wireless network:

- The wired or cabled network allows for far quicker file sharing than the wireless network. Wireless networks can only transport data at a specific capacity due to physical and technological constraints. When compared to a cabled connection, the speed of wireless devices reduces as the user moves away from the router or Wi-Fi source. The signal strength deteriorates as well, and at some points, even within a structure, the router's signal may be inaccessible. This may cause data and file transfer disruptions, as well as slower rates away from the router.
- The signal of wireless systems can be obstructed by household goods and interiors such as the refrigerator, window panes, walls, and ceilings. These factors might divert or weaken the signals. Wireless systems may suffer as a result of this.
- Setting up a wireless network might be difficult at times. It may be especially true for those who are unsure or unfamiliar with the use of wireless gadgets.

IX. CONCLUSION

To summarise Wireless networking offers several chances to increase productivity and reduce costs. It also changes a company's overall laptop security risk profile. Though it is not feasible to completely remove all hazards associated with wireless networking, it is possible to achieve an inexpensive degree of overall security by using a scientific approach to risk assessment and management. This study discussed the dangers and vulnerabilities associated with each of the three fundamental technical components of wireless networks (clients, access points, and the transmission medium), as well as several commonly available solutions that may be used to reduce such risks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, January 2022
Impact Factor: 6.252

It also emphasised the significance of training and educating users on safe wireless networking methods. Public Wi-Fi can be beneficial in a variety of ways, but it comes with its own set of concerns. VPNs and encrypted connections are your greatest alternatives for staying secure when utilising public networks. Wireless communication has the potential to improve communication in general. However, there are a few technological issues that must be solved.

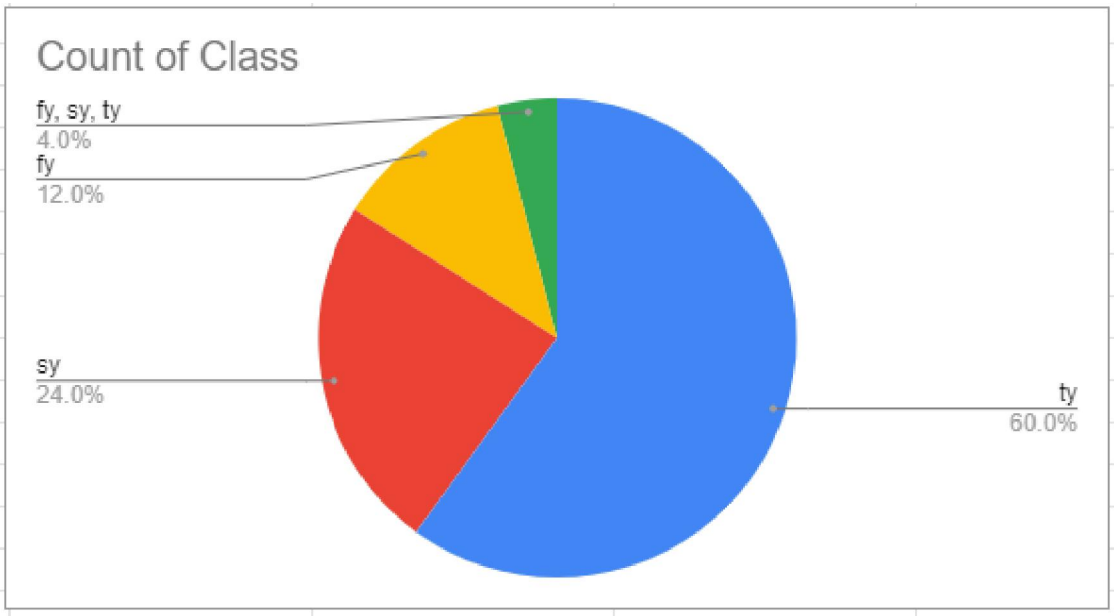

Fig: A pie chart of the percentage of the research paper question-answer based

A single pie chart question is often simple and easy to categories the information; we simply need to look at each part and find out how much of a percentage each segment makes up. This is really basic, and you will observe that there is one section that is the largest and one that is the smallest. According to the poll results, ty students are the most interested in public wife networks, while fee students are the least interested.

REFERENCES

[1]. Ali, S., Osman, T., Mannan, M., Youssef, A. :On privacy risks of public WIFI captive portals. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 80-98 (2019).

[2]. (PDF) Privacy Issues of Public Wi-Fi Networks (researchgate.net)

[3]. Cisco, V.: Cisco visual networking index: Forecast and trends, 2017–2022 White Paper, vol. 1 ,p. 1 (2018)

[4]. Fang, Z., Fu, B., Qin, Z., Zhang, F., Zhang, D.: Private Bus: privacy deification and protection in large-scale bus Wi-Fi___33 system in: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 4 , pp. 1–23 (2020)

[5]. Cheng, N., Wang, O., Cheng, M., Prasant, S., Aruna, : Characterizing privacy leakage of public win networks for users on travel. In: 2013 Proceedings IEEE INFOCOM, pp. 2769–2777 (2013)

[6]. Sumatran, N., Kad Obayashi, Y., Sasse, M., Baddeley, M., Miyamoto, D.: The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1–11 (2018).

[7]. Klarna, P., Consalvi, S., Jung, J., Greenstein, M., Le Grand, L., Powledge, P., Wetherall, D.: When I am on Wi-Fi, I am fearless privacy concerns & practices in everyday Wi-Fi use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1993–2002 (2009)