An investigation of the different risks associated with: The public Wi-Fi and Hotspots

التحقيق في المخاطر المختلفة المرتبطة بـ:

شبكة ال WiFi العامة و النقاط الساخنة

by

ASMA JAMAL ALMARRI

Dissertation submitted in fulfilment

of the requirements for the degree of

MSc PROJECT MANAGEMENT

at

The British University in Dubai

May 2019

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Signature:

COPYRIGHT AND INFORMATION TO USERS

Acknowledgements

Special thanks go to Asma Al Amiri who spent time and effort to help me write this dissertation. Her pieces were the bricks on which this work could continue.

My dear sister may your soul rest in peace.

Thanks to Mahmoud Elsayed for his contribution to this project. Thanks for the inspiration and all of the guidance you have provided during this journey.

Abstract

The use of Wi-Fi and public hotspots has increased during the past years. A statistical study done by Cisco declared that there were roughly 279 million hotspots in 2018, which further demonstrates the importance of a review of the risks associated with these networks.

This research paper investigates some of the risks associated with the usage of public hotspots from different aspects and discusses some of the ways to mitigate these risks. Discussions and findings in this paper not only emphasize on UAE as the case point of the study but also look into it from different countries, different opinions through a survey for 150 participants.

While in this research paper we will touch on risks of using public Wi-Fi hotspots and its impact on personal safety when it comes to personal data, privacy as well as national security, this research paper will narrow down the research to a more specific point which represents the gap in the study and which clearly represents same limitations in different countries while dealing with various challenges related to public hotspots. This point and research gap are simply about the government role in protecting public Wi-Fi hotspot users. Even in countries like India and UK as referenced before in previous chapters where the government took actions in protecting end-user smart devices, unfortunately, all experiments were done inside government workplaces itself.

Looking at the entire picture and how quickly technology advances we expect more initiatives to be done by governments in different countries to handle this huge risk of unprotected or not regulated public Wi-Fi users. Following that we expect more research paper to surface that covers the results of these initiatives and put it into the discussion from different aspects.

نبذة مختصرة

ازداد استخدام ال Wi-Fi والنقاط الساخنة العامة خلال السنوات الماضية. أعلنت دراسة إحصائية أجرتها شركةCisco أنه كان هناك ما يقرب من 279 مليون نقطة ساخنة في عام 2018 ، مما يدل كذلك على أهمية مراجعة المخاطر المرتبطة بهذه الشبكات.

تبحث هذه الورقة البحثية في بعض المخاطر المرتبطة باستخدام النقاط الساخنة العامة من جوانب مختلفة وتناقش بعض الطرق للتخفيف من هذه المخاطر. لا تركز المناقشات والنتائج في هذه الورقة على دولة الإمارات العربية المتحدة فقط باعتبارها نقطة دراسة في هذه الدراسة ولكن أيضًا تنظرإلى دول مختلفة ، و إلى وجهات نظر مختلفة من خلال استطلاع ل 150 مشاركًا.

بينما في ورقة البحث هذه ، سنتطرق إلى مخاطر استخدام النقاط الساخنة لشبكة Wi-Fi العامة وتأثيرها على السلامة الشخصية عندما يتعلق الأمر بالبيانات الشخصية والخصوصية والأمن القومي ، هذه الورقة البحثية سوف تضيق البحث إلى نقطة أكثر تحديدا والتي تمثل الفجوة في الدراسة والتي تمثل بوضوح نفس القيود في مختلف البلدان أثناء التعامل مع مختلف التحديات المتعلقة بالنقاط الساخنة العامة. تتعلق هذه النقطة والفجوة البحثية ببساطة بالدور الحكومي في حماية مستخدمي نقاط اتصال Wi-Fi العامة. حتى في بلدان مثل الهند والمملكة المتحدة على النحو المشار إليه في الفصول السابقة حيث اتخذت الحكومة إجراءات لحماية الأجهزة الذكية للمستخدم النهائي لسوء الحظ ، أجْرِيَت جميع التجارب داخل أماكن العمل الحكومية نفسها.

عند النظر إلى الصورة بأكملها ومدى تقدم التكنولوجيا ، نتوقع أن تقوم الحكومات في مختلف البلدان بمبادرات إضافية للتعامل مع هذا الخطر الكبير المتمثل في مستخدمي Wi-Fi العامين غير المحميين أو غير الخاضعين للتنظيم. بعد ذلك نتوقع ظهور المزيد من الأوراق البحثية التي تغطي نتائج هذه المبادرات ووضعها في المناقشة من جوانب مختلفة.

Table of Contents

Chapter 1 Introduction

1.1 Introduction

Electronic devices like smartphones and tablets connect to the Internet using Wi-Fi technology through radio waves. (Tufts University) Hotspots or open Wi-Fi are physical areas that offer Internet get to utilizing WLAN and Wi-Fi innovation by utilizing switches that are connected to Internet Service Providers (ISP). These days, hotspots are effectively found in numerous spots, for example, air terminal, coffeehouses, inn hall, and eateries that offer sans charge and secret key free access to their Wi-Fi. The majority of the populace currently is fit for associating with the Internet through these open hotspots due to the convenience and depending on the shrewd gadgets itself that gives a so common configurable setting reasonable for all age ranges.

As indicated by the examination done at Tufts University in spite of the fact that people get to the Internet in open spots like at a bistro or a shopping center in a manner that is by all accounts a free administration, there could be a gigantic effect on end client's protection and their own data. In view of the decoded idea of traffic sent and got over Wi-Fi systems, end clients are liable to numerous kinds of security and protection dangers. One of the essential and fundamental dangers related with open hotspots is the loss of individual information. Wafers can sniff on system traffic and concentrate private data from other individuals on the hotspot. For whatever length of time that the information is decoded, the programmer can for right away get fundamental information in plaintext (Visa number, for instance) about the people in question and adventure this spilled information for their very own advantages. Notwithstanding sniffing, programmers can likewise execute a sort of ridiculing identified with a convention called

Address Resolution Protocol (ARP), this caricaturing diverts the traffic to the programmers and changes the parcels sent to the people in question; additionally session seizing should be possible by means of the unbound system to such an extent that the programmers can use against unfortunate casualties' site sessions to exchange cash or take development; moreover, Man-in-the-Middle sort of assault can likewise be deceptively utilized by the programmers to listen stealthily on the Internet traffic and take login accreditations for such a significant number of every single unlawful reason and deeds. Experimentation technique for assault where it continues endeavoring to interface with the system or target

1.2 Research Background

Web get to have turned out to be fundamental to numerous individuals today, because of the measure of work and correspondence done through online administrations. The predominance of Wi-Fi get to has enormously encouraged specialists by giving advantageous, quick and free access to the Internet as the administration notwithstanding when individuals are voyaging abroad. In the meantime, as digital life and life on the Internet turns out to be progressively predominant, numerous individuals will in general invest a greater amount of their energy perusing the Internet, talking with companions on their cell phones, shopping on the web, or by means of free Wi-Fi. With the expanding reception of Wi-Fi as innovation and everybody's pressing requirement for availability, the quantity of WIFI hotspots in our reality is relied upon to achieve 7 million by 2020, making it a 400% expansion from 2015. Notwithstanding, what supplements the developing presence of hotspot is the expanding seriousness of security dangers. (Tufts University).

The numerous sorts of known digital assaults referenced in the past passage could be perniciously exploited to encroach on hotspot clients' security and budgetary well creatures. As Wi-Fi basically utilizes radio wave for system correspondence, PCs furnished with sniffers and associated with the equivalent unbound hotspot can get practically any information sent through the radio waves. Login qualifications sent through unbound site sessions can be effectively sniffed in plaintext by the programmers; regardless of whether data, for example, quantities of charge card and security code is scrambled, the programmers may conceivably utilize secret word saltines, for example, numerous product accessible today in the market to split the data. Because of the inconvenience of retaining a few well-planned passwords, numerous individuals like to utilize clear passwords or utilize similar passwords for huge numbers of their records. This conduct adds to their potential misfortune brought about by programmers, since the effective split of one client record may promptly be utilized with the assistance of social building technique to break a similar six clients other, possibly increasingly basic records. Basic data, for example, wellbeing records, business inner, and individual correspondence could be stolen, causing high hazard or even high harm and misfortune to influenced individuals (numerous individuals could be influenced by only one spillage).

(security risks of using Wi-Fi hotspot - Tufts University.) Additionally, programmers may utilize split money related records for illicit monetary profits or cause different harms. With respect to the dangers as referenced before, this exploration paper means to raise individuals' attention to the numerous worries raised by the way that having a free web access in open spots could be an immense advance toward taking individual data which numerous people don't understand it. In the meantime, in this exploration paper, we will investigate and assess a potential technique to

improve the security of Internet access at open WIFI areas, making suggestions on the most proficient method to limit or diminish the related dangers. While the specialized subtleties referenced in this exploration paper plans to animate exchanges among innovation clever individuals, different pieces of the article are custom fitted towards the overall population use who once in a while for much of the time utilize open Wi-Fi to work together or as a way of life. (security risks of using Wi-Fi hotspot - Tufts University.)

Additionally, the Internet of Things (IoT), alludes to the systems of which different gadgets of numerous fields are associated with the Internet and transmit information forward and backward. The IoT is additionally utilized in human services where it is expanded into the Internet of Bodies (IoB) or Medical Internet of Things (MIoT). The past has a system called the Body Area Network (BAN), which alludes to a system of gadgets associated with bodies just as the Internet. IoT gadgets can likewise be associated with open systems or hotspots, which acts like an extreme security danger if an aggressor accesses the BAN or any of the IoB/MIoT gadgets because of its network to people and thusly the hazard is on human life just as imperative information, delicate client information, or wellbeing information.

Taking a gander at the procedures by which Iot works and how it identifies with Wi-Fi for sending and accepting information raises another basic concern from a security point of view as well as from prescient and information investigation viewpoint. All of innovation huge players like Microsoft, Google and, for example, are so sharp now like never before on gathering client information and sparing it in what is called information lakes so as to apply some preparing

calculations on it and consequently get more understanding on human conduct, foreseeing anticipated conduct thus numerous other certifiable applications.

1.3 Research Problem

In this research paper, we will be discussing a research problem represented as the point of research. We are going to discuss and try to touch the perspective by which the individuals or end user think about their own data, think about their own piracy and think about the various services offered and is accessed over the Internet. We will narrow down the research problem or research gab to the role of the government of protecting public end users while using public hotspots and Wi-Fi access points in public. The government could take several steps in order to protect its own national security with the threads curve that is going high in recent years. These steps could be through a new set of regulations or privacy acts that when put in place would improve how end users feel about their own privacy and data protection as well as will improve the national security posture towards new security and privacy challenges.

1.4 Aims and objectives

This research aims to investigate and list some of the different risks associated with public wireless networks, whether it is Wi-Fi or hotspots, both in theory and in practice in order to determine the standard mitigation plans.

This research paper aims to start by some critical definitions from the technical perspective and then present some of the risks associated with Wi-Fi technologies and its impact on individuals, society as well as national security.

Then we will focus on the primary research gab and discuss the role of the government in protecting end users while using a public access point to access different Internet services. Finally, we will back up the research paper with a survey conducted to different categories of participants from different disciplines to analyze the findings and be able to build some conclusions on the collected results.

1.5Study structure

This research study is split into different chapters to serve the academic purpose of the dissertation. Each chapter handles an area that when combined together with all chapters will construct the entire dissertation in its final form.

The dissertation chapters are as follows:

Chapter 1: The first chapter of the dissertation acts as a general introduction and provides a research background along with an analysis of the purpose of the study.

Chapter 2: The Second chapter focuses on the literature review of Wi-Fi as a technology and how technically it forms the base of all public hotspots being accessed today everywhere like in coffee shops, airports shopping malls. This chapter continues to present and discusses the objectives of this dissertation and focuses on the research gap to take it forward for analysis and consequently a solid conclusion.

Chapter 3: The Third chapter is based on a methodology that the researcher has applied for approaching the right process in order to conduct the research work effectively.

Chapter 4: The Fourth chapter of the dissertation starts with presenting how the survey was conducted and how participants were chosen and were categorized in order to serve the purpose of the research paper. It also provides analysis of the data collected and findings from the research study then finally it puts the conclusion and opens it up for discussion and more research to follow on this particular area

Chapter 2 Literature Review

2.1 Introduction

Hotspots are areas or destinations that give Internet administration utilizing remote LANs and utilizing Wi-Fi innovation using switches that are connected to (ISP) Internet Service Providers. today, hotspots are effectively found in present day social orders. a few places, for example, airplane terminals, coffeehouses, lodgings, and cafés offer without charge and secret word free access to their Wi-Fi.

In this chapter we are starting our research by putting a base or a foundation of some key definitions from technical point of view related to Wi-Fi technology and hotspots then we will move slowly to discuss the research objectives like attack vectors and different risks associated with using public Wi-Fi and hotspots in order to meet the expected aims and focus on the research gab. The research analysis and summary are provided in another chapter where we will present the final conclusion.

2.2 Key Definitions:

- IEEE Wi-Fi Standards

In this research paper I have taken the technical definitions from one of the leading networking manufacturers which is Cisco as mentioned in one of the market leading networking entry certification exam guides CCNA Wireless 200 355 Official Cert Guide Ignoring information the remote connection as the vehicle of correspondence requires sticking to a

specific standard. Remote systems began at its beginning periods as basic as one transmitter and one recipient which around then needed to agree to the general media transmission specialized gauges, later on, the extension was augmented to serve the need of the business. Starting there on remote systems needed to fill precisely the same need as ordinary LANs and here the need emerges to have a specific standard. Remote LAN gauges are kept up by The Institute of Electric and Electronic Engineers (IEEE) that are utilized for remote systems, with numerous others.

The IEEE is an expert association that comprises of designers from around the globe. It is composed into gatherings or social orders that are concentrating on explicit regions of designing. For instance, the IEEE Computer gathering (or network) creates and keeps up measures on an assortment of subjects identified with registering frameworks, that incorporate Ethernet and remote systems. The gauges of the IEEE 802 all arrangement with neighborhood or LANs and metropolitan-zone systems or MANs. The benchmarks chiefly manage layers one and two or the physical and information interface layers of the OSI model and with transporting various sizes of bundles of information over a specific medium.

As you will investigate the part of the 802 norms that are devoted to remote LANs, you will find that they are for the most part about getting to the mutual radio recurrence medium (which is the physical layer or Layer 1 in OSI model) and on sending and accepting information outlines (information connects layer or Layer 2 in OSI model). (CCNA Wireless 200 355 Official Cert Guide).

To develop the network standards and protocols, the IEEE is organized internally and divided into working groups; these groups have open membership for all. Also, each working group is

being assigned an index number that is appended to the 802 standards family number. For instance, 802.1 refers to the first working group, which known to have developed standards for bridging networks. Table 2-1 shows a few familiar groups of 802. Note that the eleventh working group, 802.11, is the one responsible for the wireless LAN ptg16412603 46 CCNA Wireless 200-355 Official Cert Guide standards that are used by Cisco, many other wireless vendors, and users like us. For the remainder of this section, the focus will be on 802.11. (CCNA Wireless 200 355 Official Cert Guide)

Name	Description
802.1	Network bridging (includes Spanning Tree Protocol)
802.2	Link-layer control
802.3	Ethernet
802.4	Token Bus
802.5	Token Ring MAC layer
802.11	Wireless LANs
802.15	Wireless PANs (personal – area networks such as Bluetooth, ZigBee and so on)

Table 2-1: IEEE 802 workgroups

As another improvement is required or with the development advances and needs, an examination group investigates the point to see whether a review on the 802.11 models is required or if there are any things to be included that ought to be considered. Each time

something else as added to the corrections list and is indispensable, another task pack is molded to manage it together and make it to a semi-create state. Errand packs are dispensed a letter as an expansion in alphabetic solicitation. For instance, as rectifications were being displayed, their individual titles become 802.11a, 802.11b, 802.11c, and so on. If there are adequate changes to accomplish letter z, any subsequent adjustments are given a two-letter postfix, which begins with the letter a wrapped up by letters a z. At the period of this organization, the 802.11 working get-together had designated adjustments 802.11aa through 802.11ay. At the point when a draft adjustment is done, it must be casted a vote on and authorized. By at that point, creators would then have the option to begin to manufacture things that function according to all or a bit of the standard. For example, when the 802.11n amendment was settled and circulated, the new features of 802.11n were then added to various remote LAN devices. All over a change takes the time that is long to move beyond the improvement organize, last support shapes, such colossal quantities of creators will push forward and realize the draft modification into their things early. As a rule, a maker needs to decide in any case if the draft update is sufficiently consistent to complete into contraption hardware or is most likely going to get uncommon changes before it is embraced. This circumstance occurred with the 802.11n amendment. Various creators offered early executions as "Draft N-reliable" things, which could be immaculate with near devices by various makers.

The 802.11 principles as a rule have the year they were approved added to their names. For example, taking a gander at the first 802.11 standard arrangement of conventions, it was discharged in 1997, so it is currently being known as 802.11-1997. Correspondingly, the name 802.11a-1999 implies that the 802.11a amendment was confirmed in 1999. ptg16412603 2

Chapter 2: RF Standards 47 often, the IEEE 802 gathering overhauled the 802.11 norms set all in all. At the point when this occurs, each change that has been confirmed since the last 802.11 amendment is "moved up" and consumed into the recently refreshed standard. The thing is to keep up one report that characterizes the whole measures, starting at a particular date or time, so remote architects and designers can recover the majority of the specialized subtleties from one area. Despite the fact that the changes become some portion of the more critical standard set, their names are still ordinarily used to reference the particular capacities they presented. Since the presentation in 1997, the 802.11 norms have been modified in 1999, 2007, and 2012. The current 802.11-2012 standard is about in excess of 2700 pages, and the 2016 update is anticipated to be at any rate 3700 pages!

2.2.2 IEEE 802.11 Standards

The 802.11 standard spotlights on the frameworks that are used by contraptions to confer over remote with each other. As described in 802.11 standard radio repeat signals, balance, coding, channels, gatherings, and data rates all got together to give strong correspondence media. Since the first IEEE 802.11 standard was circulated in 1997, there have been various corrections added to it.

The modifications are fundamentally covering basically every conceivable piece of remote LAN correspondence that consolidates things like nature of organization (QoS), security, estimations of radio repeat, remote LAN the administrators, logically beneficial adaptability,

and reliably growing throughput. At this point, the majority of the corrections and upgrades have

been folded up into the in general 802.11 models and no longer as an independent. All things considered, the corrections may forge ahead and be perceived in the entire business and be alluded to by their unique undertaking bunch names. For instance, as the alteration of 802.11b was endorsed in 1999, and was folded up into 802.11 in the time of 2007, yet is as yet being perceived by its name till now. When anyone endeavors and shop for remote LAN devices, you will find that the 802.11a, b, g, and n changes recorded in the specs of the remote LAN device itself may be as a blemish on the contraption itself. The going with regions talk about the headway of 802.11 redresses that have empowered remote frameworks to augment constantly in execution after some time. The primary amendment names are used to perceive each one. In the wake of examining this part and the accompanying portions, you will get settled with these amendments. As you read through the remainder of this part, perceive how the transmission types, modification types, and data rates brought before into the 802.11 measures.

2.2.3Wi-Fi Alliance

Any remote LAN gadget must hold fast to the IEEE 802.11 arrangement of gauges to be good and have the option to speak with each other. Despite the fact that the 802.11 principles set are far reaching and long, it is as yet feasible for a maker to assemble a gadget dependent on one elucidation of one of the standard components, while another producer works with an alternate translation.

This is naturally evident when items are created while an 802.11 amendment is still in draft structure. Notwithstanding that, there is no commitment on producers to actualize each capacity depicted in a standard; they may pick and pick just a few pieces of the standard or simply apply the whole standard, and some of the time they may even include some exclusive highlights. The Wi-Fi Alliance (http://wi-fi.org) is a philanthropic relationship of building industry that is comprised of remote producers from around the globe, all dedicated to extending remote LAN utilization. To address the issue of inconsistent remote items, the Wi-Fi Alliance presented the Wi-Fi CERTIFIED program in 2000. Remote LAN gadgets are tried in approved testing labs against stringent criteria that speak to the right execution of a standard. In the event that a gadget breezes through the tests, at that point it is confirmed and gets a Wi-Fi CERTIFIED blessing, utilizing the logo appeared in Figure 2-11.

The Wi-Fi Alliance has numerous accreditation programs that are based around standard arrangements of highlights—not simply explicit 802.11 changes. The outcome is a push to make Wi-Fi better by guaranteeing a superior client experience. The accompanying rundown depicts some precedent projects: Wi-Fi Certified n—Products using 802.11n correctly implement features like multiple spatial streams, channel aggregation, block acknowledgment, and dual-band operation.

- Wi-Fi Certified ac—Products using 802.11ac correctly implement all of its features, including each of the two 802.11ac waves.
- Wi-Fi Direct—Products can interoperate without the use of an AP for printing, display, and content sharing.

- WPA2—Products correctly implement premium personal and enterprise wireless security features.
- Protected Management Frames—Extends premium security to protect Wi-Fi management frames between AP and wireless devices.
- Wi-Fi Protected Setup (WPS)—Products offer an easy-to-use initial configuration of wireless security features.
- Wi-Fi Multimedia (WMM)—Wi-Fi products interoperate to prioritize and handle various types of traffic with quality-of-service (QoS) mechanisms.
- Voice-Personal—Tests the performance of Wi-Fi devices to make sure they can deliver excellent voice quality wirelessly.
- Voice-Enterprise—Tests the ability of Wi-Fi devices to deliver excellent voice quality, efficient roaming, and robust management while voice-capable devices are mobile.

2.2.4Wireless LAN Topologies

Wireless network communication usually involves a data that is being exchanged between two devices a sender and a transmitter. A wireless LAN goes even further; many devices can participate in sharing the medium for data exchanges. This section explains the topologies that can be used to control access to the wireless medium and provide data exchange between devices

2.2.5 Types of Wireless Networks

The term wireless network is used quite freely in this research paper. After all, it is the central keyword of the Wireless discussion everywhere, but also it is the only one type of wireless

network that you might come across. Wireless LANs can be categorized into four main types according to the geographic scope where a signal and service is available. Figure 2-1 gives a general idea of the network types and their scopes.

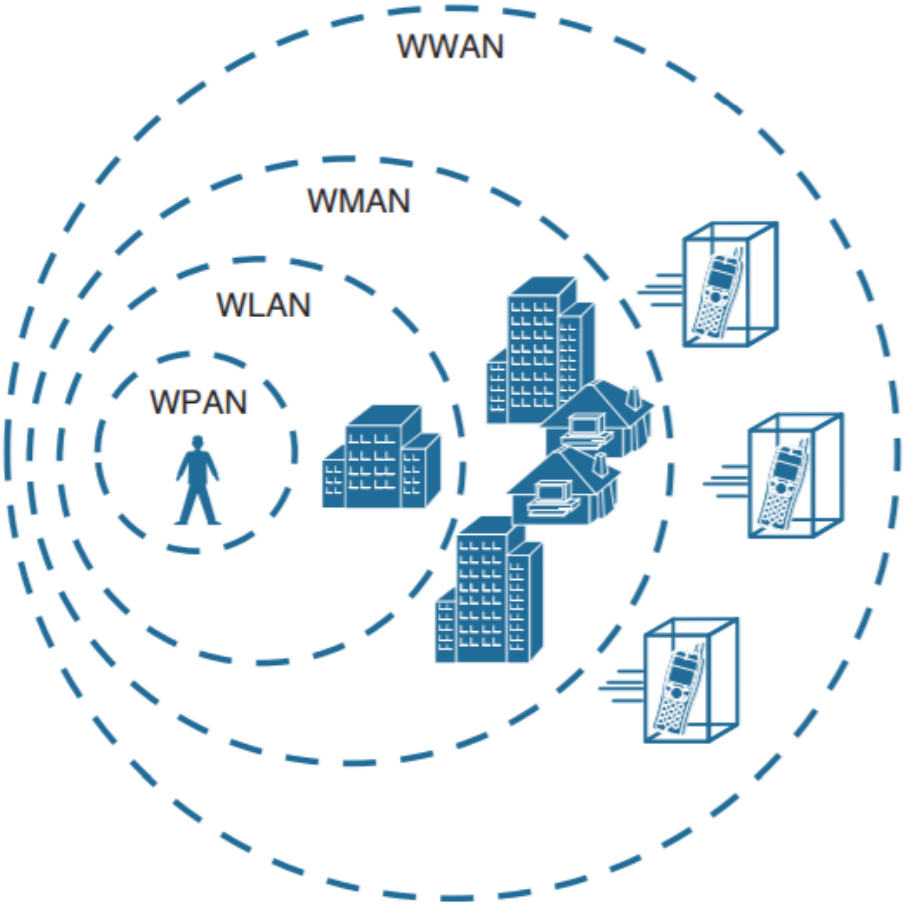


Figure 2-1: wireless network types and scopes

- Wireless individual zone arranges (WPAN)— As its name infers, a WPAN utilizes low fueled transmitters to make a system with a short inclusion, for the most part 20 to 30 feet (7 to 10 meters). WPANs depend on the standard of IEEE 802.15 and incorporate advancements like Bluetooth, despite the fact that ZigBee can have a more

prominent range. Unlicensed ISM frequencies are utilized, including the 2.4-GHz band.

- Wireless neighborhood (WLAN)— Unlicensed frequencies in the 2.4-and 5-GHz band are utilized. A remote availability administration that interfaces different gadgets utilizing the IEEE 802.11 standard over a medium-sized range, more often than not up to 300 feet (100 meters).

- Wireless metropolitan-territory organize (WMAN)— A remote administration over an enormous geographic region, for example, all or a part of a city. One run of the mill precedent, WiMAX, depends on the IEEE 802.16 standard. Authorized frequencies are generally utilized.

- Wireless wide-territory arrange (WWAN)— A remote information administration for cell phones that are offered over an exceptionally huge geographic region (local, national, and even worldwide) by media communications transporters. Authorized frequencies are utilized.

The remainder of coming definitions focuses on WLANs and how they are constructed.16

2.2.6 Extended Service Set

In normal situations, one access point cannot cover the entire area where clients might be in need of service. As an example, the reader might need wireless coverage throughout a whole floor of a business, hotel, hospital, or other large building. To cover a broader area than a single access point cell's coverage, you simply need to add more access points and spread them out geographically in the entire location or building. When access points are placed at different geographic locations, they can all be interconnected by means of switched infrastructure. The 802.11 standard calls this an extended service set (ESS), as shown in Figure 2-2.

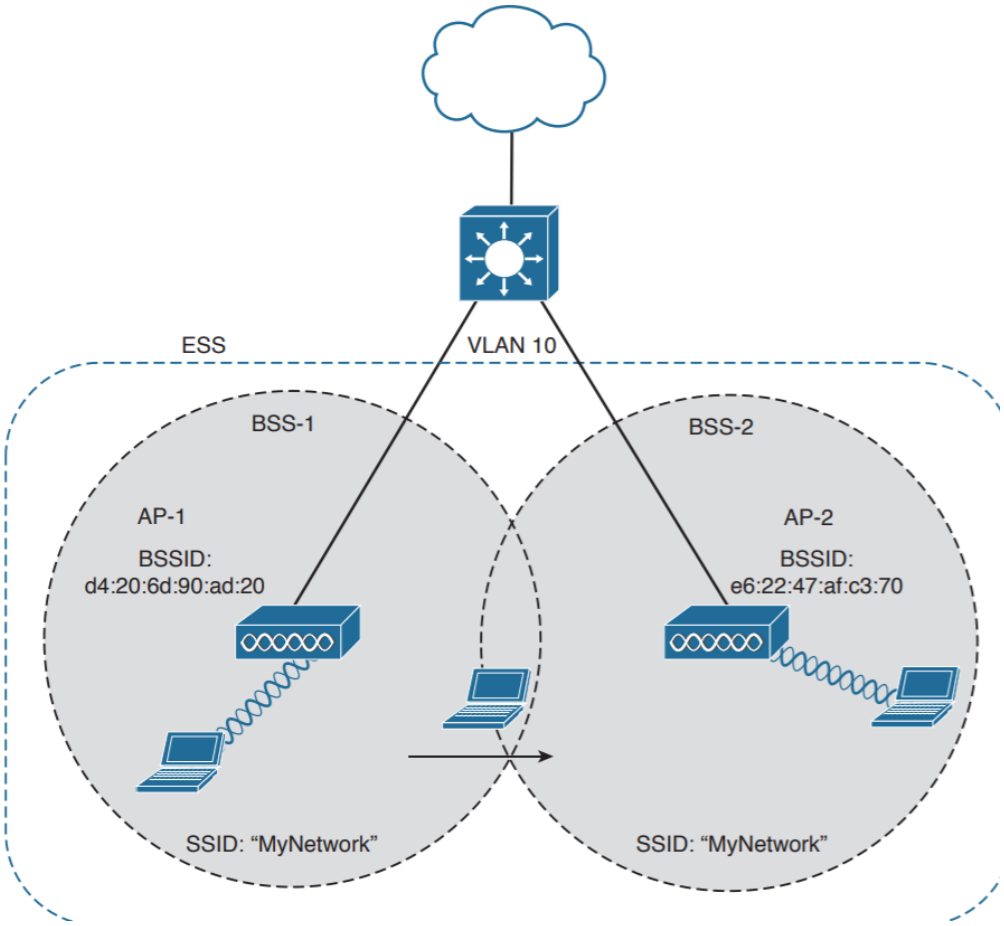


figure 2-2 Scaling Wireless Coverage with an 802.11 Extended Service Set

The thought is to make numerous passageways cooperate as a solitary unit with the goal that the association administration is steady and consistent from the customer's perspective. In a perfect world, all SSIDs that are characterized on one passageway ought to be characterized on all the passageways in an ESS; else, it would be extremely awkward and badly arranged for the end client to be reconfigured each time it moves into an alternate passage's cell. Notice that every cell in Figure 2-2 has a one of a kind BSSID, yet the two cells share one regular SSID. Notwithstanding a client gadget's area inside the ESS, the SSID will continue as before, yet the customer can generally recognize one passageway from the other. In an ESS, a remote end-client gadget can connect with one passage while it is physically situated close to that passageway. On the off chance that the customer later moves to an alternate area, it can connect with an alternate adjacent passage naturally. Going starting with one passage then onto the next is called wandering, and it won't be talked about in this exploration paper.

2.2.7A Client Scans for APs

For the wireless capable device to join a BSS, a wireless device first has to do scanning to get a list of available access points that are, and that might offer network services. Moreover, the device might need to build a list of SSIDs that are available. A device ideally does the scanning process for the wireless horizon in two different ways:

- Passive scan—The device simply listens for any beacon frames broadcast from nearby access points. Passive scan has two disadvantages: a device has to wait until beacon frames are broadcast at the next cycle, which might not be soon enough in a time critical situation; and beacons don't always contain specific SSID names, so a device cannot always depend on learning that the desired SSID exists on an access point.

- In Figure 2-3, Host#1 is able to receive beacon frames from AP#1 and AP#2. The beacon frames specify the BSSIDs and SSIDs that are being offered, as well as other information about their BSSs and supported data rates.

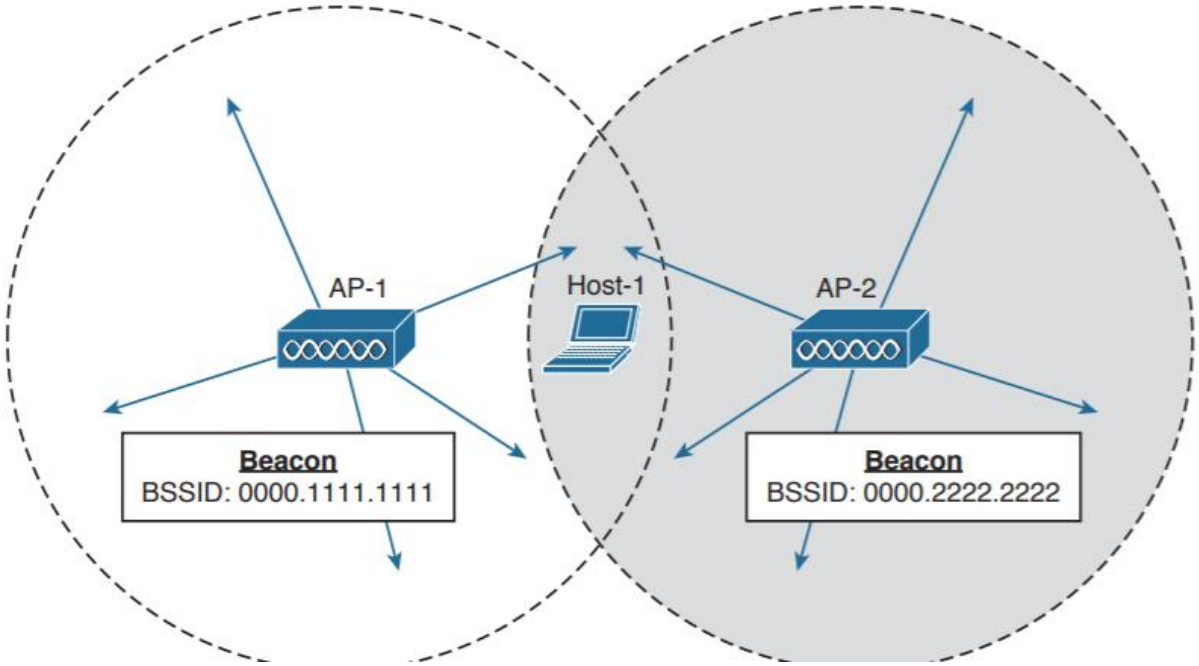


figure 2-3 Using a Passive Scan to Discover BSSs

• Active output - The remote gadget must play a functioning job and communicate a test demand casing to ask any passageway inside range to recognize themselves. The remote gadget can incorporate a particular SSID name in the solicitation. Any passages that get the test demand must send a unicast test reaction outline back to the gadget. In Figure 2-4, a gadget communicates a test solicitation to search for any passageways that can offer the "visitor" SSID. Both AP-1 and AP-2 get the solicitation and send test reactions containing their BSSIDs and other data about the BSS and SSID.

2.2.7 A Client Joins a BSS

Assume there is a remote gadget that isn't as of now joined to any remote system. The gadget comes quite close to two diverse passages that structure a solitary ESS and offer a typical SSID. The remote gadget plays out a functioning output and finds the two APs. Through some calculation, it chooses that AP#1 is best than AP#2. Figure 2-4 demonstrates the means that the gadget takes to join the system offered by AP#1. (CCNA Wireless 200 355 Official Cert Guide)

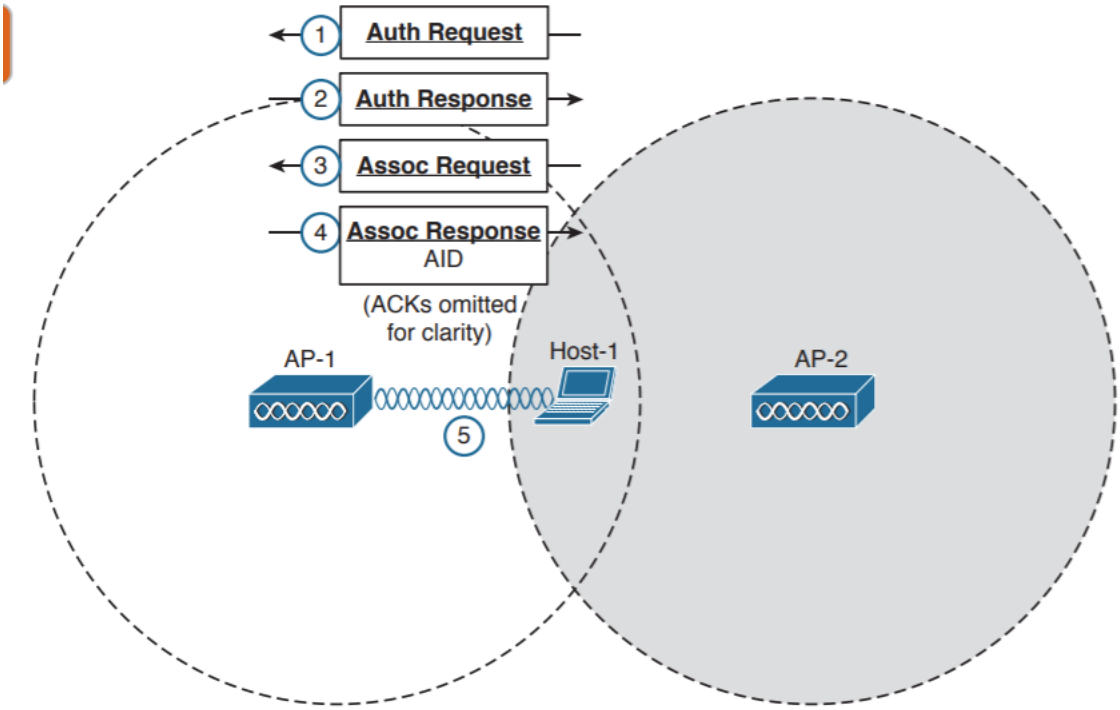


figure 2-4 Wireless Client Joining a BSS

Stage 1. Host#1 sends a verification demand edge to AP#1's BSSID address.

Stage 2. On the off chance that AP#1 is happy with the host's character, it sends a confirmation reaction outline back to Host#1.

Stage 3. Presently that Host#1 is known to the AP, it must request BSS enrollment by sending an affiliation demand casing to AP#1. Host#1 incorporates a rundown of the 802.11 abilities, the SSID it intends to join, a rundown of channels it supports and information rates, and any parameters that are expected to tie down the remote connect to the passage.

Stage 4. On the off chance that the passage is happy with the solicitation, it sends an affiliation reaction outline back to Host#1.

Stage 5. The reaction also contains the AID that particularly distinguishes Host#1 as a related customer.

2.2.9 A Client Moves Between BSSs

To proceed on utilizing same Cisco CCNA remote book When a remote empowered gadget is inside scope of a few passageways, it must connect with just a solitary one of them. A remote gadget can join one and only BSS at one time. In the event that the customer changes its very own physical area, it may remain inside its unique BSS station, or it may escape limit extend and into the cell of a neighboring BSS. wandering flawlessly starting with one BSS then onto the next is called meandering. The vital meandering ability process isn't so very different contrasted with finding and connecting with a BSS, then again, actually the customer does this while it is effectively associated with another BSS and consequently there will be no administration interferences. To switch between two BSSs easily, the customer must perceive

that it is moving toward the phone limit extend and that it needs to discover other potential cells to move into before totally losing the sign.

Figure 6-13 shows the fundamental strides of the meandering procedure. The remote customer begins with a functioning relationship with AP#1 utilizing SSID "visitor":

Stage 1. Client#1 sees that the sign from AP#1 is debasing. In light of various conditions like the got sign quality marker (RSSI) and SNR, the customer will conclude that it needs to wander.

Stage 2. Client#1 begins to search for another BSS to move inside. It communicates a sign solicitation casing to search for adjacent APs that can offer the equivalent "visitor" SSID.

Stage 3. AP#2 gets the test solicitation and returns a test reaction, promoting its BSSID and the "visitor" named SSID. Different passageways may likewise hear the solicitation and send test reactions of their own.

Stage 4. Client#1 must choose which passageway is the best applicant out of all test answers that have been gotten. It at that point transmits a re-affiliation demand casing to the new passageways, requesting to exchange its ESS enrollment from AP#1's BSS to AP#2.

Stage 5. AP#2 speaks with AP#1 over the wired DS system to start the customer handoff. Customer 1's affiliation will be moved from AP#1 to AP#2. Any edges with goal to the customer amid the handoff will be supported on AP#1, at that point transferred to AP#2 and transmitted to the customer.

Stage 6. On the off chance that the re-affiliation is acknowledged, AP#2 will educate the customer with a re-affiliation reaction outline.

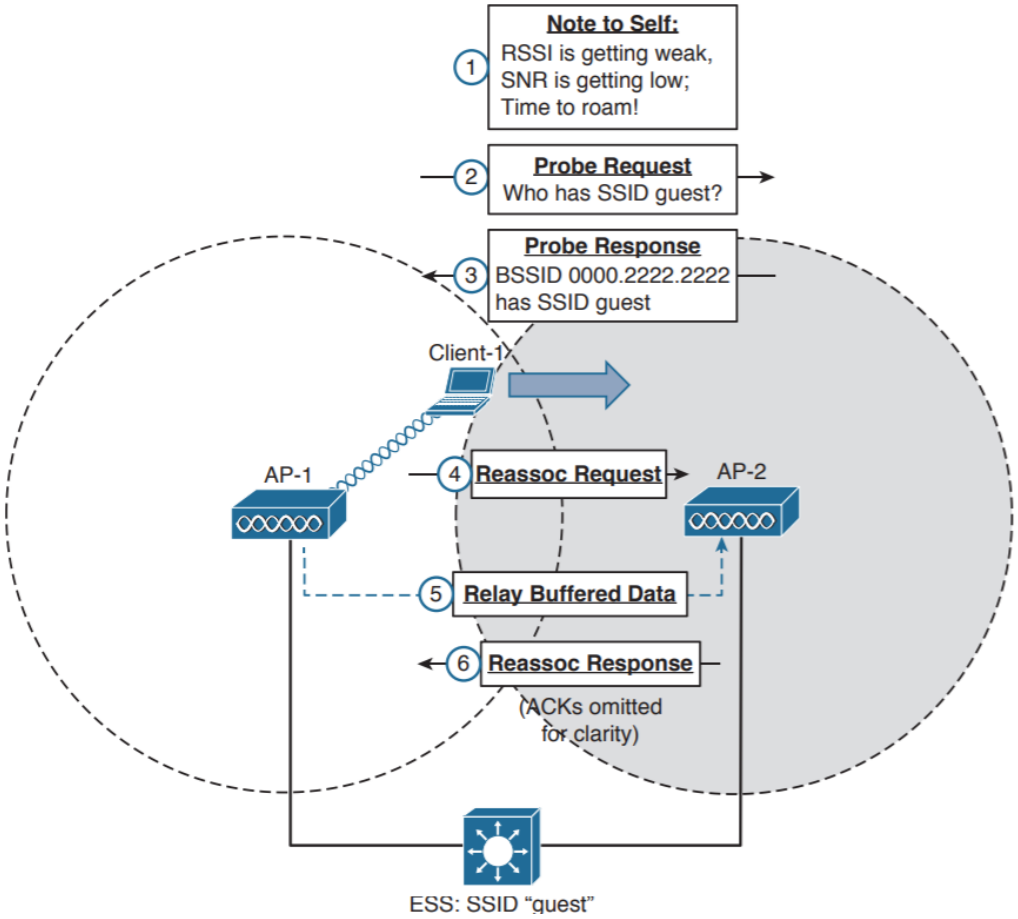


figure 2-5 Roaming Between Two BSS

2.3 Defining public Wi-Fi

In light of its broad use in homes, Wi-Fi innovation is surely known. More than four out of five UAE family units that are associated with the web at home work a Wi-Fi switch, empowering remote web network. Be that as it may, characterizing open Wi-Fi can be shockingly mind boggling. In this exploration paper, we will investigate that open Wi-Fi comprises Wi-Fi systems accessible unreservedly (without direct expense) in open spaces and freely available spaces, regardless of whether given by the administration, business, or network associations. This spreads Wi-Fi gave in strip malls, bistros, open libraries, municipal spaces, etc.

We incorporate openly available Wi-Fi that might be unreservedly accessible after buy of products, for example, hotspots in Starbucks.

2.4 What risks are associated with public Wi-Fi hotspots?

So, is using public Wi-Fi represents a risk? Looking at ideally how Wi-Fi works then we can quickly understand the risks associated with using the same Wi-Fi technique but in public. Given the nature of how data travels within the medium which in this case it is the air surrounding the access points with coverage range dictated by the access point's specifications we realize that since the transmission medium is shared between all users and access points than the need to have a study and evaluation of different risks associated with this trend arises. In this research paper, we are going to classify risks associated with public Wi-Fi into two main categories. Those will be:

Risks that affect the confidentiality of end users directly

Risks that affect the privacy of end users indirectly

Risks that affect service provided by public Wi-Fi

Incoming sections, we are going to start with exploring the above mentioned two risk categories and get into depth in each one of them while at the same time focusing on the research gap.

2.4.1 Risks that affect the confidentiality of end users directly

Confidentiality means everything that is owned by the end user and private to the end user at the same time.

So, given the fact that the transmission medium that public Wi-Fi hotspots rely on is simply the air then possibly any data transmitted or received will be subject to a risk to be intercepted or read by an external party who doesn't belong to either sender end or receiver end.

Alluding to another paper by same college Public Wi-Fi: Friend or Foe? - Tufts University we come to following fundamental point: So how could this occur? This area of the paper depicts a few assault techniques that can be utilized on open Wi-Fi systems. As a rule, it is very difficult if certainly feasible, to distinguish that an assault is occurring. This is because of the open default nature of Public-Wi-Fi and hotspot network. Two primary properties of open hotspot or open Wi-Fi furnish aggressors with moderately simple access to another clients' information:

(1) unencrypted default nature of public wireless networks; and

(2) not having a physical barrier to receiving all packets on the network.

With neither of these security assurances set up, an assailant can join the system namelessly, sniff bundles proposed for different clients, divert traffic to the aggressor's PC framework, or generally disturb organize administration. Besides, these assaults are for all intents and purposes untraceable, and much of the time very difficult to recognize, making open Wi-Fi hotspots a considerably increasingly appealing focus to lawbreakers. The remainder of this area records the most broadly utilized assaults on open Wi-Fi organizes yet absolutely does exclude every conceivable helplessness. (Public Wi-Fi: Friend or Foe? - Tufts University)

2.4.1.1 Sniffing and Scanning

Sniffing is considered to be the easiest and stealthiest method of intercepting other users' data is known as" packet sniffing." On an open, unstitched network such as most public Wi-Fi hotspots, data packets intended for a specific user are actually sent unencrypted to all other users connected to the network. By nature, since the common medium by which data is traveling is simply the surrounding air it means anyone with access to the same medium can have a copy or a version at any given point of time of same data traveling at that point of time. Several popular tools can perform packet Sniffing with the click of a button, like Wireshark, tcpdump, and Cain and Abel. Once sniffed, packets can be analyzed to find username/password pairs, files, instant messages, or any other unencrypted data sent over the network. Simply examining HTTP traffic can allow an attacker to infer patterns in another user's web browsing, which may facilitate other, more complicated attacks. Packets transmitted may also provide so many information on identities of the users, for instance from the names sent from iPhones. Protection is very little against packet sniffing especially on an open network; the reason is that it is a completely passive operation. The recipient does not need to change network flow in any way but simply has to listen. This also makes it impossible for a sniffer to be identified by technological means.

2.4.1.2 Scanning

Filtering is a route used to decide different has on the system. So examining can fill many real needs, an assailant can check the system for exploitable shortcomings. Outputs are by and large difficult to recognize, and most open hotspots don't have the assets to screen such action. There are a few diff erent sorts of checking strategies, however each pursues the fundamental guideline of sending particular kinds of parcels to all conceivable IP addresses on the nearby system and block these answers from those answers, the assailant might distinguish, or unique mark", explicit data about frameworks, for example, working framework or even open ports. Having this information, an assailant might probably send over a malware, utilize another host in an assault like forswearing of-administration, or additionally play out some other type of unlawful conduct.

2.4.1.3 Man-In-The-Middle

As referenced in one of the papers distributed at Tufts University; an article titled "Open Wi-Fi: Friend or Foe?" A man-in-the-center assault (MITM) is somewhat more muddled type of security assault, however it can take into consideration more. To portray this sort of assault, it is ideal to begin with a situation. Think about Molly, who has associated with the open system at her neighborhood Starbucks and is scanning for mutts on site pets.com. She doesn't realize that Sole, an assailant, is sniffing her bundles being transmitted and setting up a man-in-the-center assault by utilizing her frameworks' IP address. In the first place, Sole discloses to Molly that he is the switch, and after that says the switch that he is Sally. At the point when Sally endeavors to associate with pets.com, Molly is really sending the solicitation to Sole, who at that point peruses Molly's solicitation and later advances it on to the pets.com server.

At the point when the information returns, Sole replaces it with just felines and sends it on to Molly, who supposes it is a unique reaction. This sort of assault depends on Sole's aptitudes to exploit the location goals convention (ARP), which connects the IP delivers to MAC addresses. Frameworks on the system impart utilizing ARP convention and keep a table with the MAC locations of every other host on same subnet. The weakness happens in light of the fact that any host can declare or communicate that it is related with any IP address, which implies any host can claim to be another host on same subnet. This technique is known as ARP satirizing, and there are various apparatuses that can help actualize it. An increasingly serious MITM assault can even bypass measures intended to keep information private, for example, sending information over the Secure Socket Layer (SSL) convention. Going about as a passage from the endpoint to endpoint, SSL gives a layer of encryption to HTTP traffic. In any case, an assailant can trap this framework by persuading another host that it is the planned beneficiary of the first information. In the model above, Sole would take part in Domain Name System (DNS) caricaturing too. At the point when Molly makes her underlying solicitation, she approaches a DNS server for pet's IP address. Since Sole sees that traffic first, Sole by then responds to Molly with his very own IP. By and by Molly begins a sheltered relationship with Sole, who can disentangle the data. He then re-scrambles that data and sends it again to the authentic site. To the different sides, this takes after a sheltered affiliation. There are assurances to these ambushes, yet all things considered these shields are deficient. Numerous SSL servers will utilize a CA (declaration expert) to check the character of the SSL association burrow. In any case, much of the time, the client is just given an elusive message about endorsements,

which is numerous clients will accidentally acknowledge (Public Wi-Fi: Friend or Foe? - Tufts University.)

2.4.1.4 Rogue Access Points

In this sort of assault, an assailant professes to be a passage (AP) which is intended to resemble a run of the mill AP in the equivalent physical spot. A client may then interface with this passageway which thusly gives the assailant complete access to all system associations from that client (Brody, Gonzales, and Oldham, 2013). Maverick passages produce from the recently settled availability worldview: people expect a web access rapidly and wherever they are and with no expense by any means. In light of this interest, demonstrating the legitimacy of a passage is a difficult battle, as it can hamper a client's capacity to interface with a passageway rapidly and straightforwardly in any setting. Dondyk and Zou (2013) point out another assault through a maverick passage, which they call" forswearing of accommodation." The assault comes from the comfort offered to cell phone people, who profit by web associations at pubic areas. In this assault, an individual would endeavor to utilize the false passageway, yet no solicitations for information would go through. Since most cell phones will debilitate broadband network for a Wi-Fi association, this renders the telephone unequipped for getting information. This is only one of numerous assaults that can be performed inside the ever-prominent domain of versatile availability. (Open Wi-Fi: Friend or Foe? - Tufts University.)

2.4.2 Risks that affect the confidentiality of end users indirectly

2.4.2.1 Internet of things

In recent years and with the advancement of technology a new concept is introduced which is the IOT or the Internet of things.

Internet of things is an idea that simply means everything around us can be connected to the internet and hence can mean that individuals can control things remotely and from any smart device. Internet of things came up associated with smart homes where you can simply control your home appliances from your smart device like smartphone or tablet so that you can send commands to your fridge, TV, AC and locking or unlocking doors even. The concept got expanded to not only control your home remotely, but for example, you can also manage your car. Also, some governments started many initiatives to help the public by for instance applying some data analytics and remote sensing to control or avoid traffic jams in streets during rush hours by simply being able to predict the number of cars traveling over single point or street junction.

So from this point another question arises that directly relates to our topic of discussion in this research paper, which is that having this capability and ease of use of technology made it so easy for attackers to not be interested about stealing your passwords or credit card information only but also to simply be interested in collecting as much information as you can. So, for example, they can know about your life behavior patterns by simply tracking your presence on public hotspots. Suppose for example that every Friday after finishing work an individual goes to the same coffee shop and surf the web for an hour then goes to do a grocery shop and stay there for another hour. This constant habit makes it easy for those interested in knowing what

you do and when to simply be able to predict what are you going to do in the next day or even during next month. This data could be taken and analyzed by organizations that are interested in extracting valuable predictions about this specific region or even entire country usage behaviors.

So, this data presents a risk not in a form in insecurity but in the way of "knowing" and predicting behavior about individuals.

2.4.3 Risks that affect service provided by public Wi-Fi

2.4.3.1 Denial of Service

Forswearing of Service is another sort of assault that is like the disavowal of accommodation assault portrayed in the past segment, a refusal of administration (DoS's) assault will likely reason interruption to the web access to a client's (or numerous clients') gadget or framework. A DoS assault can either utilize the satirizing and MITM strategies depicted before, or by methods for system flooding. Utilizing ridiculing, an assailant traps different clients or frameworks on a similar system to send solicitations to the aggressor. To execute the refusal of administration, the assailant need just not pass the solicitation parcels through to the planned beneficiary. In an open Wi-Fi hotspot, a client would never again approach the switch, and all system traffic would appear to stop. One downside of open Wi-Fi is the restricted data transfer capacity it as a matter of course forces on clients, particularly at occupied occasions (Noor, 2013). For this situation, an assailant could flood the system with parcels, chiefly gobbling up the majority of the passable data transfer capacity. Clients would see either extremely moderate or nonexistent system traffic entering and leaving their frameworks. It might appear that the

assailant in this circumstance could be effectively recognizable. Be that as it may, the aggressor can parody the sender address on the awful parcels.

The aggressor could likewise execute an assault wherein another client's machine is fooled into actualizing the assault another client. This sort of redirection makes it very difficult to pinpoint the real culprit and demonstrate blame. (Public Wi-Fi: Friend or Foe? - Tufts University.)

2.5 Mitigation against public risks

Looking at the risks explored in previous sections it becomes apparent that there is a critical need to protect or mitigate against these risks of using public Wi-Fi and hotspots. In order to better discuss the mitigation techniques, we will first start by categorizing the areas of risks associated with public Wi-Fi usage in order to better protect against it.

The risks associated with using public Wi-Fi can be mitigated by considering three factors:

(1) access point security

(2) access point traffic security and encryption

(3) consumer device setup.

2.5.1 Access point security

For what reason are open hotspot systems helpless to hacking or block attempt? The appropriate response lies in a critical position that is struck among openness and security in system plan.

The mass-marketization of Wi-Fi innovation was set apart by the dispatch of Wi-Fi™ as a buyer brand personality for the IEEE802.11 remote systems administration specialized standard in 1999 and the practically synchronous discharge by Apple of a purchaser Wi-Fi AP, the AirPort Base Station, and related Airport Wi-Fi arrange interface card (NIC), for use with its PCs. This was before long pursued by the approach of war plunging and comparable practices went for finding and getting to open, decoded systems.

2.5.2 WEP vs. WPA Encryption protocols

The encryption convention at first discharged with the Wi-Fi standard, Wired Equivalent Privacy (WEP), was found to have noteworthy imperfections. Wi-Fi Protected Access (WPA) was presented by the IEEE in 2003 to connect the WEP security holes before the formal selection of WPA2 in the IEEE802.11i standard in 200418. Self-detailed purchaser information gathered by wiggle.net uncovers that it required investment for WEP ensured arrange gadgets to be supplanted by WPA and WPA2 gadgets regardless of security concerns.

Open Wi-Fi acquaints open doors for APs with be undermined, for the traffic stream between Wi-Fi empowered gadgets to the APs to be caught, seen or decoded if WEP encryption is utilized, and for the Wi-Fi empowered gadgets to be assaulted if the gadget is erroneously setup. A key hazard is a probability that open Wi-Fi APs may have been undermined because of an immediate assault or by means of an assault on some other system gadget or framework that approaches rights to the AP. By expansion, there is the likelihood that the AP may have been inaccurately setup or endured a design breakdown amid startup.

It isn't unordinary for open Wi-Fi APs to be inaccurately designed, the same number of organizations and associations giving systems need fitting specialized skill. As the wiggle.net graph appears, 8% of APs with a known security status are unbound, and 12% have substandard WEP security. Basically, one out of five systems aren’t designed to utilize the best accessible security conventions.

The expansion of Wi-Fi systems has prompted the adjustment of Wi-Fi specialized guidelines for cell phones to encourage meandering, limiting the requirement for re-verifying at each system passageway after the underlying login. This is a component of the 802.11u standard, discharged in 2011 and consolidated in programming, for example, Passpoint and Hotspot 2.0. Notwithstanding the comfort of programmed handover, the standard energizes the utilization of a protected sign in through a pre-confirmation process utilizing the WPA-2 convention.

While Passpoint works out of sight, some cell phone makers are consolidating programming that subtleties the status of Wi-Fi systems, alarming clients that interface with a decoded system might be shaky. Also, a few outsider applications imply to demonstrate whether there is obstruction with web traffic over open Wi-Fi systems. In any case, some all-around recorded 'parodies' or trials, point by point beneath, recommend the requirement for extra client shields and instruction.

The most widely recognized danger at an open Wi-Fi area is the 'man-in-the-center' assault where a digital criminal joins an open Wi-Fi system to assault exploited people's gadgets over the built-up association with the open Wi-Fi passageway, to divert traffic through the digital criminal's gadget or server some place on the web.

In the event that the passageway has been undermined or has not been designed effectively in any case, the traffic leaving the passage to travel further into the system can be diverted to a remote server or caught locally. While the traffic from the shopper gadget to the passageway might be safely scrambled if the passage itself has been undermined, the traffic voyaging further into the system from the passage may not be encoded and is in this manner insecure.31

For clients of an open Wi-Fi passage, regardless of whether the passageway has been set up accurately or has been undermined isn't something that is noticeable to the purchaser's gadget. In the event that the open Wi-Fi passage offers WPA-2 encryption security, traffic between Wi-Fi empowered

Gadgets and the passageway are generally secure, yet this has small bearing on the security of the open Wi-Fi passageway itself. It is basic in this manner to consider just using open Wi-Fi offered by an open or private association or business that would be relied upon to accurately setup and check open Wi-Fi passageways normally.

To moderate the danger of traffic being caught by a man-in-the-center assault or through a traded off passageway, various huge companies have as of late presented a HTTPS-just policy32 and have found a way to lessen the utilization of the unreliable HTTP convention. So while traffic from a customer gadget to a passage might be scrambled, the HTTP traffic leaving the passageway and voyaging further into the system may not be encoded.

2.5.3 Wi-Fi CERTIFIED 6™ coming in 2019

As referenced authoritatively by the Wi-Fi Alliance that with industry energy now a days mounting around Wi-Fi 6, Wi-Fi Alliance® acquaints Wi-Fi CERTIFIED 6™ with guarantee gadgets dependent on IEEE 802.11ax innovation fulfill industry concurred guidelines for interoperability and security. The Wi-Fi Alliance confirmation program, coming in the second from last quarter of 2019, will give limit, inclusion, and execution required by clients to encounter cutting edge Wi-Fi® use cases, from spilling ultra-superior quality (Ultra HD) films to mission-basic business applications. (. (Wi-Fi CERTIFIED 6™ coming in 2019 | Wi-Fi Alliance. https://wi-fi.org/news-events/newsroom/wi-fi-certified-6-coming-in-2019)

Propelled highlights bolstered by Wi-Fi CERTIFIED 6 convey development for Wi-Fi to progress even in assorted Wi-Fi conditions with numerous gadgets. Key advantages incorporate higher information rates, expanded system data transmission, improved execution in clogged conditions, and upgraded control effectiveness. (Wi-Fi CERTIFIED 6™ coming in 2019 | Wi-Fi Alliance. https://wi-fi.org/news-occasions/newsroom/wi-fi-ensured 6-coming-in-2019) These capacities include:

- **Downlink and Uplink symmetrical recurrence division numerous entrance (OFDMA):** builds organize effectiveness and brings down inactivity for extreme interest conditions
- **Multi-client numerous information different yields (MU-MIMO):** enables more information to be exchanged without a moment's delay and empowers a passageway to transmit to an increasingly noteworthy number of simultaneous customers on the double
- **Transmit beamforming:** empowers higher information rates at a given range bringing about more prominent system limit

- **1024 quadrature abundancy adjustment mode (1024-QAM):** expands throughput in Wi-Fi gadgets by encoding more information in a similar measure of range
- **Target wake time (TWT):** altogether improves battery life in Wi-Fi gadgets, for example, the Internet of Things (IoT) gadgets

2.6 Access point traffic security and encryption

2.6.1 HTTP and HTTPS

Hypertext Transfer Protocol (HTTP) is a protocol that operates at OSI Application layer using which hypertext is transferred over the Web. Because of its simplicity, HTTP protocol has been the most widely used protocol for data transfer over the Web but the data (i.e., hypertext) exchanged using HTTP isn't as secure as we would like it to be because the default implementation of HTTP protocol doesn't include any form of encryption or transmitted data protection. In reality, hyper-text exchanged using HTTP goes as plain text, i.e. anyone between the browser and server can read it relatively easy if one intercepts this exchange of data.

So why do we need this kind of security and transmitted data protection over the Web? Think of something like ‘Online shopping' at Amazon or Flipkart.

We all might have already noticed that as soon as we click on the Check-out on these online shopping portals, the address bar gets changed to use https. This is done so that the data transfer (i.e., financial transaction, etc.) is made secure as well as protected from interception. And that's why https was introduced so that a secure tunnel session is setup first between the Server system and Browser of the client system. actually, cryptographic protocols such as SSL and/or TLS turn HTTP into https or in another words https equals HTTP plus cryptographic protocols. Also,

to achieve this security in https protocol, Public Key Infrastructure (PKI) is used because several Web Browsers can use public keys while private key can be used by the Web Server of that particular website. PKI is the system that manages to generate certificates as well as revoking certificates. The distribution and handling of these public keys is done via Certificates which are saved and used by the client Browser running on the client system. Anyone can check these public certificates in the browser settings. We'll detail out this set up a secure session procedure in another post.

Also, another main difference between HTTP and HTTPS protocols is that HTTP uses the default TCP port 80 while https uses the default port 443. But it should be noted very well that this security in https is achieved at the cost of processing time because Web Server and Web Browser needs to exchange cipher keys used for encryption and that is done using public Certificates before the actual data can be transferred between sender and receiver. Basically, setting up a secure session is done before the actual hypertext exchange between server and browser. (What's the difference between HTTP:// and https .... https://www.geeksforgeeks.org/whats-difference-http-https/)

For a consumer, it is essential to only access websites or online locations that are accessible using HTTPS. Currently web browsers do not provide a capability to block access to sites or online locations that utilize HTTP, although the most recent Google Chrome release is now displaying a "Not Secure" identifier next to HTTP URLs in the browser still the decision to continue and browse the not secure website is entirely the decision of the end user.

2.6.2 Using VPN along with HTTP

If accessing websites or online locations that utilize HTTP is unavoidable then currently the only effective way to mitigate the risk associated with public Wi-Fi traffic being compromised at the access point is to use a Virtual Private Network connection either to a VPN provider or to a home Internet gateway that is configured to act as a VPN endpoint.

The VPN connection between a consumer device and a VPN endpoint provides an encrypted tunnel over which traffic can travel to a secure location before the traffic is delivered into the internet. However, it should be remembered that accessing websites or online locations with HTTP is not secure even when a VPN is used because the unencrypted HTTP traffic will leave the secure VPN before it gets to the target website or online location.

Access points may be set up with or without encryption for the traffic between consumer devices and the access point. It is important that consumer devices only connect to access points utilizing WPA2 or more recent security encryption. To ensure that only WPA2 or more recent security encryption is used consumers should check their devices to setup WPA2 and to disable earlier security encryption options.

By far the most important action that a consumer can take to enhance their security when using public Wi-Fi is to ensure that their device is correctly configured and has anti-virus, antimalware, anti-exploit and anti-ransomware software installed. Notebooks, tablets, and smartphones are often configured for use at home or in an office environment where it is necessary to connect to other systems and utilize network devices, such as printers. The standard configuration is not secure when the device is used to connect to public Wi-Fi.

2.7 Consumer device setup.

Gadgets that are to be utilized to interface with open Wi-Fi ought to have the product fixed and at the most recent discharge adaptation, to guarantee that any recognized security openings have been shut. Programming patches ought to be connected to the gadget in a recognizable domain, e.g., at home or in the workplace, and not at an open Wi-Fi area.

Numerous online frameworks today, including banks, Google Mail, and Facebook offer two-factor authentication34. It is significant that while getting to the web at an open Wi-Fi area, two-factor confirmation is utilized wherever conceivable in light of the fact that a traded off secret word does not give access to a site or online area without the code gave during that time layer of insurance. Using two-factor verification for all sites and online areas that offer it is prescribed consistently, independent of how the site or online area is being gotten to.

It is the purchaser's duty to be steady in the utilization of HTTPS wherever conceivable and, to help with decreasing the trouble of distinguishing if HTTPS is being utilized, search out an internet browser that gives a visual cautioning if HTTP is being utilized or gives a square on HTTP.

While moving between home or office systems and open Wi-Fi turn off system perusing, record and printer sharing, and open organizer sharing. All things considered, the gadget will be undermined on the off chance that it gives an opening that can be misused by another person at the open Wi-Fi area or by a malignant application looking for shaky gadgets over the web.

The gadget firewall ought to be turned on and checked consistently to guarantee that it is working accurately and applications have not opened ports through the firewall that ought not be open when associated with open Wi-Fi.

Regularly, gadgets accompany deficient security programming introduced and it is prudent to buy and introduce security programming before a gadget is associated with open Wi-Fi. Choosing fitting security programming and guaranteeing that it is stayed up with the latest is a standout amongst the most significant normal upkeep exercises that customers should complete for all system associated gadgets.

An impressive number of sellers offer programming bundles that give hostile to infection, antimalware, against adventure and hostile to ransomware security, and it is conceivable to discover merchants that offer family or home licenses that grant the product to be introduced on different gadgets, including home PCs, note pads, tablets, and cell phones.

As announced starting at now in this year 2019, Wi-Fi Alliance has introduced another client well-arranged naming demonstrate that gives end customers a clear naming designs for both the Wi-Fi development supported in their contraption and the Wi-Fi advancement open for the relationship with a framework wherever they interface with a Wi-Fi orchestrate. Continuous looking over data by Wakefield Research to help Wi-Fi Alliance shows that about bit of the customers need the latest development in their devices, yet nearly around 75% of audit respondents swear off buying new contraptions when it is too difficult to even consider evening think about understanding particular imprints and depictions. New generational expressing will

help end customers even more viably recognize contraptions with the latest Wi-Fi advancement and better appreciate if devices will pass on the ordinary Wi-Fi experience. (Wi-Fi CERTIFIED 6™ coming in 2019 | Wi-Fi Alliance. https://wi-fi.org/news-occasions/newsroom/wi-fi-affirmed 6-coming-in-2019)

2.8 How safe is surfing on 4G vs. Wi-Fi?

Taking a reference to an article written by Norton When comparing 4G to Wi-Fi technologies and give it a pure technical thought, it is pretty clear that using 4G networks provided by telecommunication providers presents a safer option than using only the mobile device Wi-Fi capability.

The main reason for that 4G networks are locked with certain technical specifications, and all telecommunication providers have to adhere to the country's regulations and data transfer laws related to security and privacy.

In an article published by the US firm "Norton" the famous for its security products and R&D; discussed how secure 4G networks compared to Wi-Fi. In the section of: Can, 4G Be Hacked? We quoted the following:

At the danger of seeming like a messed up record, nothing associated with the Internet is 100% invulnerable to cybercriminals constantly. Notwithstanding, with regards to 4G, hacking appears to even now be in the verification of-idea organize. Verifications of-idea happen when white cap programmers (the heroes, who are normally specialists) search for ways they can bargain a framework. There have been a couple of fruitful instances of individuals hacking into 4G by means of man-in-the-center assaults (MITM). (Norton, 2017)

A MITM assault resembles spying where assailants can put themselves either between the client and the application, two clueless unfortunate casualties, or even between two machines, and "tune in" on the transmissions being sent forward and backward.

As per Norton Along these lines, for the time being, we can infer that the appropriate response is truly, 4G can be undermined. In any case, it is considerably harder to hack than open Wi-Fi, which assailants for the most part have their sights set on.

Since there are a couple of courses in the alternatives an individual may interface with the Internet by means of the shrewd gadget, there is trust. With regards to open hotspots, there are numerous odds for programmers can exploit vulnerabilities by means of your association over Wi-Fi than over 4G. To the extent the security of these associations, here's the way they rank from most secure to least secure:(How Safe Is Surfing on 4G versus Wi-Fi? - Norton.)

1- Using a VPN over a cellular network or using a VPN over Wi-Fi
2- Cellular only
3- Wi-Fi only

2.9 What do we know about risk and behaviors?

Till now we have investigated from a specialized perspective the various dangers related with open Wi-Fi and a portion of the approaches to moderate these dangers. Now and approaching areas, we will attempt survey the general information or person's mindfulness degrees about these dangers, and this will be the section point to the examination hole in this exploration paper.

There has been no precise examination concerning UAE's attention to various dangers related with the utilization of open Wi-Fi, and there is restricted universal writing regarding this matter. The accompanying outlines a portion of the exploration that has been attempted in this field. Klasnja et al.19 attempted an exploratory examination on open comprehension of Wi-Fi and related.

Protection and security concerns, inferring that members had restricted familiarity with the communicated idea of Wi-Fi, while in the meantime receiving danger limiting practices that advanced a misguided feeling that all is well and good. When the dangers were unmistakably comprehended, the examination discovered, members communicated a readiness to change rehearses. This investigation demonstrated that clients - maybe naturally - had restricted specialized learning of encryption forms. Of more concern however, was the finding that a few members "basically believed that budgetary and business organizations made superbly secure Web destinations." Many demonstrated an abnormal state of trust in system names as lawful portrayals, while some trusted that a firewall or against infection programming on workstations verified Wi-Fi exchanges. The investigation by Klasnja et al. bolsters work directed by Kowitz and Cranor20, which reasoned that creation action on remote systems all the more clearly noticeable to clients modifies their basic leadership, and there was a craving among clients for advanced devices that could do as such.

The potential dangers of open Wi-Fi use have been shown by 'satirizing' works out, where specialists set up systems with apparently real names and allure clients to give individual data or consent to sham terms and conditions. Kindberg et al. (2008) conveyed ridiculed organizes

in two UK bistros and requested that potential clients give a remarkable system get to PIN, to be sent to their cell phones for validation. Just about 33% of 361 individuals trying to utilize the system gave their versatile numbers to this reason.

2.10 ‘Herod clause’ experiment

In 2014, the UK Cyber Security Research Institute, backed by the European law enforcement agency Europol, conducted a spectacular spoof to highlight the lack of attention given by users to the terms and conditions (T&C) governing network use. The researchers set up Wi-Fi hotspots in two London locations where users encountered a T&C containing a so-called ‘Herod' clause, promising free Wi-Fi if "the recipients agreed to give away their first born child to us for the duration of eternity." Six people already signed up.

App developers have responded to security concerns by designing a range of Wi-Fi security tools, including in SSID, Easy Wi-Fi, and Authenticate My Wi-Fi. These tools provide ways of identifying, analyzing and securing public networks, with varying levels of sophistication. Mobile phone manufacturers have also responded with proprietary tools to enhance visibility and awareness of Wi-Fi networks.

Network T&Cs are a key consumer contact point which ostensibly provides an opportunity to guide decisions about access and use of public Wi-Fi networks. However, as the ‘Herod' experiment cited above illustrates, the type of ‘click-wrap' T&Cs commonly deployed for public Wi-Fi and other digital products and services may lack effectiveness as a communication

tool22. What do public Wi-Fi T&Cs say about network security, and how is this information presented on screen to the user? The following section discusses these issues.

2.11 A look at the Terms and conditions of Public hotspots

Access to public Wi-Fi in UAE and elsewhere is almost universally governed by a contract between the provider and the user that takes the form of non-negotiable terms and conditions to which the user agrees electronically (generally by 'clicking' an 'agree' button). These click-wrap contracts are generally displayed, or accessible through, the network's 'splash' or first web page.

We analyzed a convenience sample of 26 UAE public Wi-Fi networks T&Cs provided by commercial, government and community institutions, to assess whether and how the contracts disclosed network security status and promoted informed use. We also compared this selection with a selection of nine T&Cs used by public Wi-Fi providers in the USA and UK. Appendix 3 details the selection. The analysis highlighted two issues:

1.T&Cs varied considerably in length, readability, and accessibility, particularly on mobile wireless devices. Several – notably those of community organizations and public libraries – are a few hundred words long and written in plain English. The longest text in the selection is around 6,800 words – half the length of this report. Some books are so long and complicated that they require considerable persistence and perhaps legal training to read and comprehend, yet their "boilerplate" character offers users no option other than to accept entirely in order to gain network access.

2. 18 of the 26 UAEs T&Cs clearly advise users that communications on public Wi-Fi networks may be insecure. However, some network providers prioritize their risk and liability issues over

consumer advice. The typical placement of warnings about network and communications security is towards the end of sometimes-lengthy documents.

This went by and raised many questions about the extent to which users are effectively and fully informed of security risks. Conditions of access that seek to minimize provider risk may also be ineffective, impractical or even punitive. Young people are a particular target here. Several T&Cs specify that people under 18 years of age may only access the network under adult supervision, and one specifies that only persons aged over 18 years may access the network.

A comparison of the T&Cs used by Australian public Wi-Fi providers with T&Cs used by a selection of providers in the USA and UK shows strong international correspondence. Several factors influence this uniformity: the online availability of generic T&Cs, the presence in Australia of multinational public Wi-Fi providers, and the global trend to use click-wrap contracts.

Excerpts from four T&Cs (see right) contrast documents that are oriented towards consumer information (the first two), and those seeking to minimize network provider risk and liability (the second two).

The "name" Wireless system is a non-verified system. data sent to and from your remote gadget might be caught by any other individual with a remote gadget. If it's not too much trouble remember this while getting to individual or business data.

We prescribe that you don't utilize the administration, whenever, to embrace individual banking or unveil any close to home data, (for example, account subtleties, passwords, charge card subtleties and ledger subtleties)

We don't warrant that any data , programming or other materail available through the point of arrival, terms of administration , is free of infections , works , trojan steeds, or other hurtful segments. While we take all due consideration in encuring the privecy and respectability of the data you give, the likelihood exists that this data could be unlawfully seen by outsider while in travel over the web or while put away on our frameworks.

2.12 Government's Role in Protecting against public Wi-Fi

Coronet one of a security detailing site composed a decent article on government job expressing that: here has been significant arrangement dialog and activity in UAE on digital wellbeing issues concentrating on access to unseemly substance and online practices. In any case, there has been considerably less thoughtfulness regarding cybersecurity at a client level.

In September 2018 the UAE Telecommunication Regulation Authority (TRA) released a public warning on Wednesday, to advise all residents in UAE to use public Wi-Fi only with caution.

"When using your devices in public areas, do not leave your data visible to those around you," the TRA said on Twitter. "While you are in public areas, beware of your personal information." (UAE residents warned about using public Wi-Fi - gulfnews.com.)

The UAE government has taken further steps in order to help protect national security. Wi-Fi UAE is a country-wide initiative to provide Wi-Fi access to the public, in line with UAE Vision 2021. With Wi-Fi UAE initiative anyone can have high-speed access to all UAE government services. Wi-Fi UAE is available to all end users with a Wi-Fi-enabled device, including smartphones, laptops, and tablets. Wi-Fi UAE service is being offered in two flavors, a free service, and a premium service. (Wi-Fi UAE. http://www.wifiuae.ae/en/)

As per coronet in the year of 2016, the Government of India issued new regulations and countrywide instructions to its employees across all ministries instructing the use of smartphones in emergency situations only. Officials were requested only to conduct an in-person meeting. Moreover, government employees were no longer allowed to use their devices by connecting or syncing their smartphones through office computers – not even to charge them. But who can define a real emergency? Perhaps emergency was a code word for business as usual, in which case the entire policy was only a stunt for the press. (Coronet)

Over the last year, another move was made in the US where the United States Government has traded the BlackBerry in favor of Android-based phones like Samsung Galaxy in a huge step. The FBI itself has recently ‘adopted' over 40,000 Samsung Galaxy phones, and the Military is devising secured Android devices for its personnel as well. Simultaneously, we see both a 60% rise in Android market share and, more importantly, a 50% rise in the number of mobile malware attacks aimed at Android phones.

However, as previously discussed, a determined hacker will have no more trouble breaking into an Android device than an iPhone or vice versa. The reality is that no phone in its off-the-shelf configuration can be considered sufficiently secure for confidential data or voice communication. Before the Air Force Materiel Command gave their pilots iPads, they had carried an additional 90 pounds' worth of navigational maps with them. The switch, of course, saved on paper and fuel costs and made navigation easier, but at what cost?

The United Kingdom has rolled out a plan to provide the public sector with cloud-based Wi-Fi. A wireless network that serves all public sector employees. The idea was to run a centralized government-controlled Wi-Fi that offers both staff and guests with a secure and seamless Wi-Fi connection as they roam from a place to place. The safety premise was that each user would be provided with encryption keys, each building would ensure that protocol WPA2 enterprise encryption and everyone would be sure that his device was configured to automatically check network certificates to ensure they were on a real network. Furthermore, the system would randomly create new credentials that only work with certain systems.

2.13 Summary

In this chapter, we have listed the most common risks associated with Wi-Fi when end users are using public hotspots in public places to access different online services. We have discussed the impact of these risks on both the individual as well as the national security.

More importantly, we have discussed the differences between 4G and Wi-Fi and how Wi-Fi Alliance is working to enhance their Wi-Fi certification service by introducing Wi-Fi six during this year 2019. Also, we have discussed the role of the government in protecting Wi-Fi and how other countries were responding to different challenges related to public Wi-Fi and related to losing personal data and imposing a threat to the national security.

We have seen an essential point that not only all concerns and risks that are associated with using public Wi-Fi and hotspots are related to security or "stealing," but also, it's related to data analytics and behavior predictions which is going a trend I recent years.

We have discussed the role of the government and tried to present some real-world scenarios from the UAE and other countries as well. We have seen how some countries did some experiments to try and see what steps could be done to protect end users or any individual who is using public hotspots to connect to the Internet.

Incoming chapter, we will present the research methodology and how this research paper was written and based on what methods of the research. We will then go to the final part and present the survey results of the participants who participated in the survey.

Chapter 3 Research Methodology

3.1 Introduction

Research methodology provides analysis of the research methods and processes used by researcher in order to conduct the research work in a successful manner. It develops an understanding of the approaches, tools, and techniques that can help researcher to select the exact process for successful completion of the research work. Moreover, analysis of the research methodology helps in achieving effective solutions to the issues. Research methodology process involves quantitative and qualitative data collection method. Quantitative research methodology deals with statistical, analytical or calculation based data. On the other hand, qualitative data collection process or methodology focuses on quality of the data used for data collection process. However, methodology for research work is applied for helping researcher in constructing an authentic research work. In this context, this chapter deals with analysis of the research philosophy, design, and approaches used for data collection method

3.2 Research Onion:

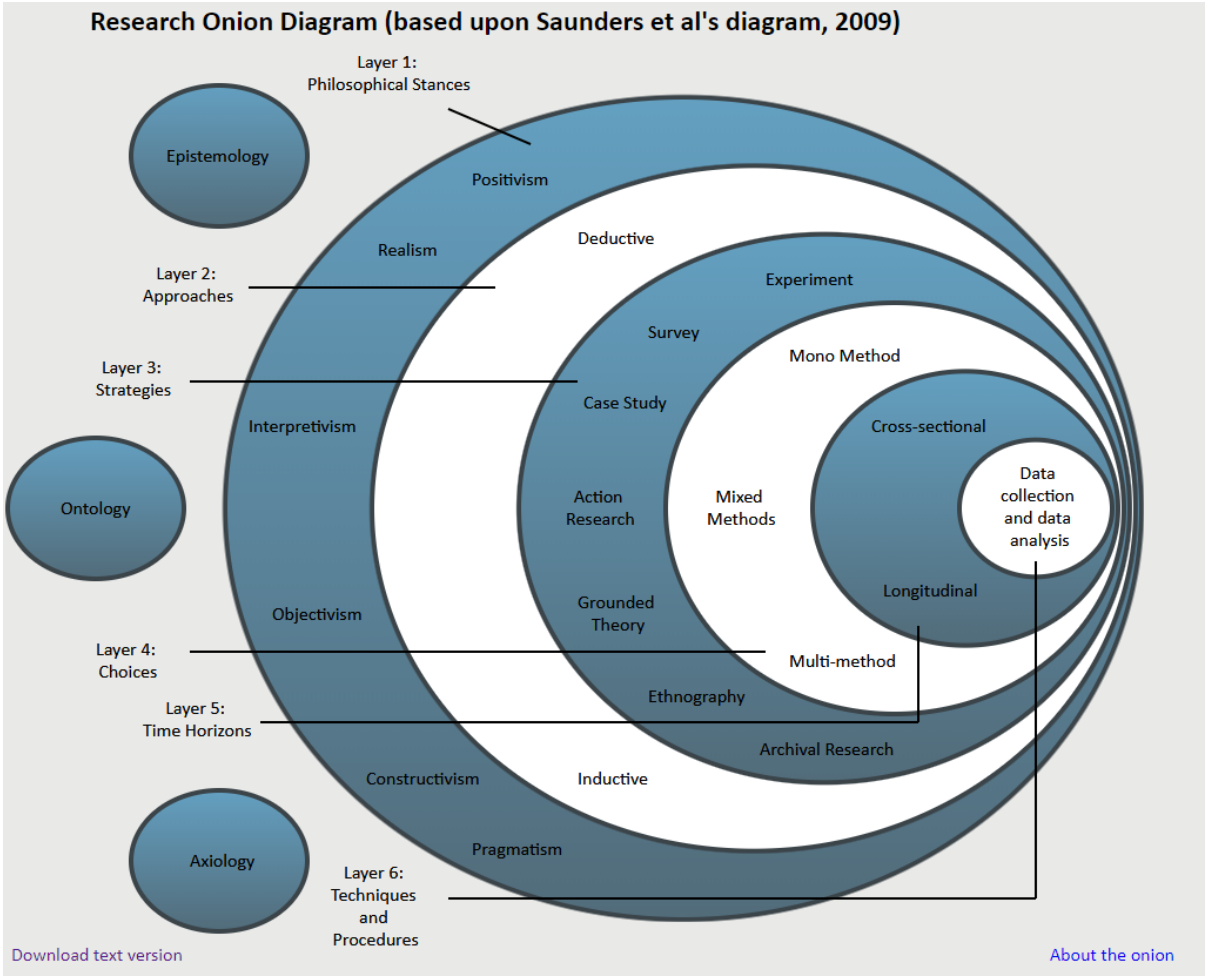
The research onion was developed by Saunders et al. (2007). It illustrates the stages that must be covered when developing a research

strategy. When viewed from the outside, each layer of the onion describes a more detailed stage of the research process (Saunders et al., 2007).

The research onion provides an effective progression through which a research methodology can be designed. Its usefulness lies in its adaptability for almost any type of research

methodology and can be used in a variety of contexts (Bryman, 2012). This essay will examine and describe the different stages

of the research onion and explain the concepts at each stage.



3.3 Methodology:

In this paper, we will utilize quantitative and qualitative techniques for study. Quantitative information is less soliciting to examine for the followers since it portrays the data as figures and numbers that are immediate. Qualitative data is ordinarily used to clear up suppositions through gatherings and reviews.

3.4 Qualitative Research

We can investigate a comprehensive exhibit of measurements through qualitative research of the social world, including the surface and weave of ordinary daily existence. The understandings, encounters, and imaginings of our exploration members, the ways that conventional procedures, organizations, talks or connections work, and the centrality of the implications that they create. Qualitative research will be utilized to concentrate on the graphic piece of the examination to pick up a comprehension of hidden reasons, assessments, and inspirations. Qualitative information accumulation strategies incorporate concentration gatherings and individual meetings.

3.5 Quantitative Research

We can explore an extensive display of estimations through quantitative research by making a questionnaire for a group of people.

3.6 Method of Collecting Information

For this research paper, we are utilizing secondary research. The secondary data will be collected from journals, academic papers, and online research over the internet. The information on past deals likewise has been gathered.

3.7 Primary Data Collection Approach

Primary data will be information assembled by a professional, specifically for this research purpose. Primary data will be information compiled because nobody has collected and distributed the data in a discussion open to people in general. Primary data is the information gathered for particular research objective (Hox and Boeije, n.d.). Different methods collected the primary data, for example, a survey will be conducted in which a questionnaire was distributed amongst the people. We've utilized survey strategy as it'll enable us to gather the information

required for running tests fitting to our exploration. The questionnaire was developed in a way that concentrated on withdrawing data about the respondent's range of work and their supposition

3.8 Secondary Data Collection Approach

Secondary data are the information compiled by a group not identified with the exploration think about but instead collected this data for some other purpose and at different time before. If the researchers utilize this information, then these end up noticeably secondary information for the contemporary patrons. These may be available in created, composed or in

electronic structures. Subsidiary data is gathered for the other reason and reused in various studies (Hox and Boeije, n.d.).

Secondary information proposes second-hand information which is assembled and recorded by any individual other than the customer for a reason, not relating to the ebb into the issue. It is the instantly open kind of data accumulated from various sources like censuses, government creations, inside records of the affiliation, reports, books, journal articles, destinations and so forth (Surbhi, 2016). The secondary information offers a couple of points of interest as it is effectively open, saves time and cash of the authority. For secondary research for this paper, information will be gathered from information available on the internet, journals, academic papers, and daily paper articles on the components influencing the economy.

3.9 Sampling

Sampling is a procedure of picking an agent test from an intended interest group that is under thought in the investigation. Sampling should be possible in different courses, concerning our examination we will utilize non-likelihood inspecting. Non-likelihood testing is an examining method where the specimens are accumulated in a procedure that does not give every one of the people in the populace square with odds of being chosen. Non-likelihood examining should be possible in various courses, for example, portion, comfort, and judgmental inspecting. To assemble information for our exploration, we've utilized convenience examining as that was the most financially stable, efficient and pertinent strategy we could've used.

3.10 Justification for selecting sampling technique

Researcher has focused on collecting data by conducting an in-depth interview with the R&D department of DEWA and IBM Company. In addition, 2 employees from IBM Risk Analytics,

2 employees from research department of DEWA and 2 employees from Enterprise Risk management are selected as samples.

Hence, samples were purposively selected in order to get authentic data along with maintaining the validity of the data. Moreover, analysis of the samples provided understanding of the target audience that can help in getting proper and accurate data for the study. Since, authentic and valid data can be collected by interviewing IT company's members; hence, purposive sampling has been done for this process. Therefore, purposive probability sampling technique is being selected by the researcher for gathering of data.

3.11 Research Limitations

No research work is successfully completed without facing certain limitations (Sadgrove, 2016). In this context, the current research also faced certain limitations while carrying out the research study. At the time of conducting the research study, researcher faced various difficulties while collecting authentic data. Lack of sufficient time hindered the process of data collection to some extent. In addition, it became quite difficult for the researcher to go into validity of information or data gathered. However, finance was another limitation that affected the process of data collection for the required research topic. Language was another factor that restricted researcher to stick only to one language for data collection process. Only English language was given priority for collecting data over other languages.

3.12 Nature and Method of Study

Research configuration is an important rule to make the stream of investigating procedure to be efficient. Hardly any angles that include in this exploration configuration are information gathering, handling, what's more, written work of the report. It is done from the examination issues, and research means to see on education and economic growth and financial development.

3.13 Research Analysis Technique

The method used for analysis of data utilized as a part of this exploration is a quantitative strategy through the survey frames which are disseminated to the 100 chose respondents. It is to pick up data from the respondents about the connection amongst education and economic growth in adding to financial development. The survey shape is the instrument utilized by the analyst to gather information on few segments and components that suits the motivation behind this exploration. The elements in the survey shapes are finished by alluding to the poll from past specialists and adjusted by the reasonableness of flow consider targets.

3.14 Method used to Analyze Data

Information is examined by utilizing measurable examination given the react from polls. The product used for the information investigation is Statistical Package for the Social Sciences (SPSS) adaptation 22. This product helps during the time spent elucidation of the gathered information with a specific end goal to test the centrality of the dependent variable and

independent factor precisely. There are two sorts of test that will be completed in this examination to be specific regression test and Pearson correlation test.

3.15 Regression Test

Regression test examines the extent of the connection between one dependent variable and more than one independent factor. The area between the dependent variable and independent elements depends on the estimation of R2. R2 or the deciding coefficient is the proportion of progress of the reliant variable, economy development (B) which is clarified together by the independent factors, education level (A1) and income (A2).

3.16 Pearson Correlation Test

Pearson's correlation coefficient is the examination insights that measures the actual relationship, or relationship, between two nonstop factors. It is known as the best strategy for measuring the relationship between elements of intrigue since it depends on the technique for covariance. It gives data about the size of the affiliation, or connection, and besides the heading of the relationship. Correlation assesses the extent/quality of at least two factors. The relationship investigation does not consider which variable that impacts it. The quality of association depends on the estimation of r. The higher correlation coefficient, r demonstrates a stable positive relationship as the esteem approaches +1.

3.17 Summary

This chapter provided analysis of different research approaches, methodological tools used for conducting research study. Understanding of the methodologies and data collection techniques helps in identification of the issues related to research study. In addition, it provides researchers to distinguish between right and wrong decisions.

This chapter dealt with understanding of sampling techniques and processes that helps researcher to identify target audience for data collection process. Moreover, this chapter provided analysis of ethical considerations that helped researcher to maintain the rules and regulations along with ethical principles while conducting the research work.

Chapter 4: Findings and Results

4.1 Introduction:

Till this point of the research paper, we went through the research gab from different aspects after putting all technical and non-technical terms in perspective. We started by referring to the foundations first then moved to the research gab discussions and elements. Following that, we have focused on the role of the government when it comes to securing and protecting the public and every individual when using public hotspots.

To back up the research data with realistic statistics from the field, a survey was done as well as an interview to collect opinions of some of the individuals and somehow measure their each and everyone own perspective on how they see the risk and how much they know already.

In this chapter, we are going to present how the survey was done and what questions were asked based on the interest that serves the research paper. The survey consists of 5 questions written in a survey form, which the respondents used and filled it as well as an interview of two questions that were asked to the same respondents.

Respondents to the survey were a total of 150 participants divided into three categories. Respondents to the survey and the interview are employees of three organizations:

Organization name: the general directorate in residency and Foreigners Affairs - Dubai

Organization name: HPE

Organization name: Emaratech

The first category is those who work in an IT technical role in the three organizations we targeted. The reason for that was to get an opinion from some of the subject matter experts and gets to touch their own perspective on their own privacy and personal data.

While the second category were employees who work in non-technical roles like HR, finance and management and the reason for that was to get a second opinion from a type of roles of people who do not necessary belong to a technical role but represent normal employee whether he is a manager of some sort or a junior HR employee for instance.

The third category of respondents were those who are non-technical, and in the same time, over 45 of age and reason for that was to get the perspective from this category of people who most likely give the subject of this research paper a less care compared to the other two categories.

To summarize, the following are the respondent's categories:

Category 1: 50 persons who work in IT roles

Category 2: 50 persons who work in non-IT roles like HR or finance

Category 3: 50 persons who are non-technical roles and over the age of 45 as well

4.2 Survey questions:

The survey questions used were as follows:

How many Wi-Fi enabled device you own?

Have you ever read T&C of Wi-Fi hotspot out of curiosity?

Do you prefer mobile data for public Wi-Fi?

Have you heard about ransomware?

Following the survey questions, an oral interview was conducted to a mix of selected 30 persons out of a total of 90 respondents.

Respondents to the survey and the interview are employees of three organizations:

Organization name: the general directorate in residency and Foreigners Affairs - Dubai

Organization name: HPE

Organization name: Emaratech

4.3 Survey output

Now having the 90 survey forms and notes taken while doing the 30 interviews of mixed persons from the respondents, in following section we are going to present key survey outputs and then we are going to summarize it before giving a conclusion and putting extra items for general discussion.

- How many Wi-Fi enabled device you own?

When asked about how many Wi-Fi enabled device you own, four out of five are already owning and actively using two Wi-Fi enabled devices regardless if they prefer Wi-Fi or mobile data.

- Have you ever read T&C of Wi-Fi hotspot out of curiosity? If yes, did you find it lengthy?

A second and third category of respondents reported that they have never read the T&C of any Wi-Fi hotspot before. Only 8 out of the first category who clicked to read the T&C previously and they reported that it was too lengthy.

- Do you do financial transactions over Wi-Fi in public places?

All respondents with no exception reported that they all do banking online using public Wi-Fi.

- Do you prefer mobile data on public Wi-Fi?

Only half of the first category reported that they do prefer using mobile data assuming it's more secure while the other half and rest of the whole second and third category simply didn't care.

- Are you aware that your location could be tracked while on public Wi-Fi?

The only the entire first category of respondents was aware that technical wise it's possible to track device location and movement while connected to either public Wi-Fi or Bluetooth. 12 out of 20 of the second category were aware of technical possibilities to track Wi-Fi end devices without having many details while the entire third category didn't have any idea what is being discussed.

- Have you heard about ransomware?

When it came to discuss the awareness of the famous attack of ransomware, the first category entirely was aware and have an extension of knowledge about what this malware can represent as a risk to their own data and what losing this data means if they simply decided not to pay the ransom. For the second and third category combined, it was surprising that only 5% read about ransomware but have no awareness about why or how it might affect their Wi-Fi-enabled devices while on public hotspots.

Interview Questions:

For the interviews, only two questions were selected, and the reason was to make the interview as attractive to the respondents as possible and at the same time to serve the purpose of the research paper.

The questions asked in the interview were:

1- Do you think the government should take more steps toward protecting public Wi-Fi users?

2- When was last time you attended or read about security awareness while using public hotspots?

Those two questions were asked to the same three categories of respondents, and in the following section, we will describe their views on each of the two questions.

For the question of the government role in protecting public Wi-Fi users all of the respondents agree on one thing which is that the government holds the bigger responsibility part of protecting the end users while on public Wi-Fi hotspots. 52% of all 60 respondents were specific in describing their view on what actions should the government take in order to protect the public Wi-Fi users. They mentioned that authorities should conduct a kind of inspection and verification on public hotspot places or to enforce certain regulations or policies.

Regarding the other question of attending or reading a general security advisory or awareness only 8 out of the entire 60 respondents reported that they have at least read security awareness articles or advisories related to protecting personal information.

4.4 Summary**:**

Following is a summarize results of the survey as well as the interview:

- 4 out of 5 survey respondents own 2 Wi-Fi-enabled devices like a smartphone or tablet
- 4 out of 5 survey respondents actively use 2 Wi-Fi-enabled derive like smartphone or tablet
- 40% of technical respondents have read Terms and conditions before
- Zero percent of non-technical respondents have ever read terms and conditions before
- Zero percent of the 45+ age group have ever read terms and conditions before
- 50% of technical respondents think that mobile data is more secure than Wi-Fi
- Zero percent of other categories know the difference between Wi-Fi and cellular data
- All of the respondents confirmed that they do banking transactions while on public hotspots

- 100% of technical respondents are aware of possibly tracking movement through public Wi-Fi
- 40% of non-technical respondents were not aware of tracking possibility
- Zero percent of 45+ age group respondents are aware of monitoring possibility

4 out of 5 own and actively use 2 wifi enabled device like: (mobile phone or tablets)

40% of technical respondents read T&C before

0% of non-technical respondents and 45+ of age read T&C before

50% of technical respondents think that mobile data is more secure than wifi

While 0% of other categories care about it

100% of technical respondents are aware of possibility of tracking movement of wifi user

40% of non-technical respondents were not aware of tracking possibility
0% of respondents over 45 of age are aware of tracking possibilities

4.5 Discussion

While in this research paper we have touched on risks of using public Wi-Fi hotspots and its impact on personal safety when it comes to personal data, privacy as well as national security, in this chapter we are have narrowed down the research to a more specific point which represented the gap in research and which clearly represents same limitation in different countries. This point is simply about a government role in protecting public Wi-Fi hotspot users. Even in countries like India and UK as referenced before in previous chapters where the government took actions in protecting end-user smart devices, unfortunately, all experiments were done inside government workplaces itself.

Looking at the entire picture and how quickly technology advances we expect more initiatives to be done by governments in different countries to handle this huge risk of unprotected or not regulated public Wi-Fi users. Following that we expect more research paper to surface that covers the results of these initiatives and put it into the discussion from different aspects.

. Chapter 5: References and Appendix

5.1 References:

Public Wi-Fi: Friend or Foe? n.d. - Tufts University. Viewed 12/5/2019
http://www.cs.tufts.edu/comp/116/archive/fall2013/dmancinelli.pdf

Security risks of using Wi-Fi hotspot - n.d. - Tufts University. Viewed 12/5/2019
http://www.cs.tufts.edu/comp/116/archive/fall2013/hwan.pdf

UAE residents warned about using public Wi-Fi. 2018 by Cleofe Maceda, Senior Web Reporter
https://gulfnews.com/technology/uae-residents-warned-about-using-public-wifi-1.2280524

CCNA-Wireless-200-355-Official-Cert-Guide, Cisco

How safe is surfing on 4G vs. Wi-Fi? – Norton n.d. Viewed 12/5/2019
https://us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html

What's Government's Role In Protecting Wireless Networks?, 2017 – viewed 12/5/2019
https://www.coro.net/whats-governments-role-protecting-wireless-networks/

Practicing safe public Wi-Fi Assessing and managing data-security risks, December 2016. Ian McShane, Mark A Gregory & Chris K Wilson

Elliot, A. K. Users perception about security of the public wireless network. International Journal of Societal Applications of Computer Science,

(2013). Providing Security for Wireless Community Networks. In LCD-Net13, September 30, 2013, Miami, Florida, USA

5.2 Appendix 1: Sample of survey form

Master's Dissertation Questionnaire Research:
Different risks associated with:
The public Wi-Fi and Hotspots

My name is Asma Al Marri and I am currently studying for a master's in project management at the British University in Dubai. I am conducting research into the different risks associated with the public Wi-Fi and Hotspots.

The questionnaire consists of 4 questions and will take no longer than 10 minutes to complete. All responses will be kept anonymous and no one will be identifiable in the research.

Please tick the box provided to show your consent to be part of the research ☐

1. **How many Wi-Fi enabled device you own?**

☐ One ☐ Two ☐ More than two

2. **Have you ever read T&C of Wi-Fi hotspot out of curiosity?**

☐ Yes ☐ No

3. **Do you prefer mobile data of public Wi-Fi?**

☐ Yes ☐ No

4. **Have you heard about ransomware**?

☐ Yes ☐ No

Thank you for taking part in my research.
If you wish your response to be withdrawn from the research contact me via this e-mail address: 20170468@buid.ac.ae