Active and Passive Security Attacks in Wireless Networks and Prevention Techniques

Active and Passive Security Attacks in Wireless Networks and Prevention Techniques

1st Ee Sun Jun
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
sunjun.ee@gmail.com

2nd Jeshua Woon Tien Ming
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
jeshuawoon@gmail.com

3rd Yap Jia Suan
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
jiasuanya@gmail.com

4th Scott Lee Chuen Yuen
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
leechuenyuen@gmail.com

5th Fatima-tuz-Zahra
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
fatemah.tuz.zahra@gmail.com

Abstract – In this modern day and age, wireless networks are everywhere. It is not a far stretch to say that it is downright crucial due to its ability to keep people connected and updated everywhere from universities and workplaces down to our personal homes. Though the benefits of wireless networks are undeniable, it also brings a new host of security concerns due to the amount of sensitive data being transmitted through these networks. A simple attack such as packet sniffing is enough to "sniff" out just enough data to cripple even giant corporate bodies if left unchecked. The aim of this research paper is to dissect and discuss the security and privacy issues of wireless networks that surround us. An interesting finding would be that wireless networks are heavily susceptible to both malicious attacks such as denial of service attacks and passive attacks like eavesdropping. It was also noted that information is more easily obtainable through wireless networks as compared to wired networks due to the ability to gleam information from long distances without having to be physically present on site. A literature review and a survey were conducted to learn about the opinions of casual users of wireless networks. The information gathered suggests that while there are many who care about privacy, they still lack the necessary knowledge to protect said privacy. These users carelessly connect to public wireless networks wherever it is available without proper precaution and care. Appropriate relevant solutions are presented based on literature study to overcome insecure wireless network usage practices in order to avoid active and passive attacks.

Keywords: wireless networks, active attacks, passive attacks, privacy issues

1 Introduction

Technology has come a long way. New inventions and breakthroughs are being unveiled daily with no signs of slowing down. Being on the cutting edge of technology is certainly an exciting feeling, though some of the key inventions of the past still holds a prominent place in this era, albeit with major improvements and all its kinks ironed out. One of these revolutionary technologies is none other than the Internet. This piece of technology helped create a more connected and faster paced world, bridging the physical gaps between people. Today, the ability to easily and instantaneously connect with others, from friends to family to even workplace colleagues, is an integral part of our lifestyle.

Sadly, there is no such thing as a free lunch. Although the Internet has undeniably been a godsend to humanity, its invention and implementation also sparked a new host of issues and problems. Malicious individuals looking to inflict damage and steal information from organizations and individuals began utilizing this same technology to do so, exploiting loopholes and vulnerabilities for their personal selfish gains. These are not small isolated cases either as by 2021, cybercrime damages are estimated to have impact the global economy by upwards of US$6 trillion each year [1].

Originally, the internet was created by having multiple devices interconnected with each other, making a network. It was developed in the 1980s and could only be used with existing devices with physical connections via wires. The original purpose of this technology was to exchange military related information efficiently between devices [2]. Due to the wired-only nature of the Internet at the time, it was considerably harder to gain access to the network as a malicious individual would have to have physical access to the devices in order to do anything with it.

Fast forward to the 1990s and Wireless Fidelity networks, or as it is now commonly referred to as Wi-Fi networks, surfaced. Wi-Fi made it possible for devices to be interconnected with each other minus the direct physical medium requirement of the past. This gave birth to wireless networks and made way for people to get connected to the Internet without having to be physically connected through wires. While it was a massive breakthrough leading to one of if not the most prominent and iconic technologies of today, it also sparked a new wave of security and privacy concerns.

Since the Internet no longer requires a physical connection for access, vulnerabilities and loopholes cropped up by the dozens, with new ones being discovered and potentially exploited daily. This became a massive cause of concern as more and more companies move to the Internet as a platform to power business and connect with customers, as well as when more of the general public begin to use the Internet for various purposes such as social media and entertainment. The Internet turned into a goldmine for hackers and cybercriminals alike as personal and sensitive information being shared through this medium became easily accessible from quite literally anywhere on the planet due to the wireless nature of the networks of today. With the digitization of money, cryptocurrencies and all sorts of e-banking technologies becoming more prominent nowadays to make the lives of users more comfortable, unauthorized extraction and exploitation of sensitive data have become more lucrative, sparking more interest and effort from among those with malicious intent. The vulnerability to security attacks has increased exponentially due to increased interconnectivity. Systems are now connected with each other which has made it easier for attackers to target their victims. One type of attacks can lead to another attack type, for example, SYN flood attacks can lead to denial of service attacks [3]. Moreover, where deployment of IoT devices offers convenience, it also increases the attack vulnerability due to insecure implementation [4] and sensitive data transmission over its insecure network.

Despite the many security measures in place to combat hackers and cybercriminals being developed each day, there can never be a fully secure and impenetrable solution. Both software and hardware play a role in making Wi-Fi networks a reality, and neither are completely immune to vulnerabilities and loopholes. While security patches can be deployed to patch the holes being exploited by hackers to extract sensitive information, it is only a matter of time before a new vulnerability is discovered and subsequently exploited in a never-ending cycle.

Nowadays, the vulnerability may not even lie in the hardware nor software, but rather in the users themselves being ignorant and careless with their sensitive information. This opens a new avenue for hackers to attack from, one that no security patch or update can repair. Be it a social engineering attack or just the lack of attention from the end user in updating their devices to follow the most current security standards and protocols, the fault in wireless technology vulnerabilities lie in the mindset of users just as much as it does in the loopholes in software and hardware.

2 Literature Review

2.1 Security

In this era of modernization, technological advancement is not a surprise, the phase of technology improving has been progressing tremendously fast [5], be it from smart phones, computer systems or even wireless networks. Thus, not forgetting for those that are misusing this opportunity to do harm on others, whereby viruses and hackers are also advancing at the same time with new features and technological tools to aid in terms of their hacking objectives [6]. Hence, it is clear that not only big corporate companies but small business have to step up in order to prevent themselves from falling into being a victim of these cyberattacks. With that, it is crucial that organizations must be crystal clear on the tools that can help in terms of cyberattacks prevention. Thus, with that, it is clear that when the complexity of networks grows, the concern of wireless security also increases accordingly [7].

Firstly, the main reason of organizations or even small businesses to fall victim in cyberattacks is mainly because of the lack of knowledge in the field of wireless security as well as weak implementation of security tools [7]. Thus, one should focus on implementing few security tools in order to upgrade security of wireless networks [8][9]. Therefore, intrusion detection system (IPS), firewalls as well as antivirus software must be look into because without further upgrading the available security tools that can bring huge benefits in protection sensitive and valuable data, hackers can easily gain access into the organizations systems through its wireless access points without leaving any sign of alerts [10], thus this is no surprise if any sensitive information that can be potentially leaked out. Therefore, this will not only jeopardise the organizations reputation but also losses valuable resources alongside with facing issues at the same time, such as slow processes or even failure of systems[11-13].

On the other hand, the basic infrastructure of using wireless networks to transfer data has become a must-have in order for one to communicate to one another [14][15], with that this will then involve two different devices in order to carry out communication via wireless networks, which includes a transmitter and a receiver [16][17]. Thus, radio waves will be used whereby data will be transferred in the form of radio signal that has been translated by a wireless adapter (transmitter), on the other side, a router (receiver) will then decodes signal into information [17][18], hence this have clearly shown a loophole through which a hacker can conduct an malicious act by manipulating or altering information before the transmitter has send the data out, thus the receiver will then receive the copy of the forged information without knowing its true source [17-20].

Therefore, there are two types of major attacks from wireless network that users and organizations should be aware of, which are passive attacks (Fig. 2) and active attacks (Fig. 1). Hackers that only have the intention to steal valuable information [21] such as emails identification or passwords, but does not have the intention to take advantage on any digital resources are considered as an passive attack [22][23], besides, passive attacks do not usually leaves obvious tracks behind, hence it is much more detrimental towards the users, as the they might not realize from the very beginning, whereas for active attacks, hackers are more aggressive whereby the victim are instantly aware of the attack being carried out and hackers that fall under the category of active attacks usually have the intention to search and destroy targeted system directly [24]. With that being said, the wireless network that are owned by users and organizations are generally vulnerable for both types of attacks, be it passive or active [19][23].

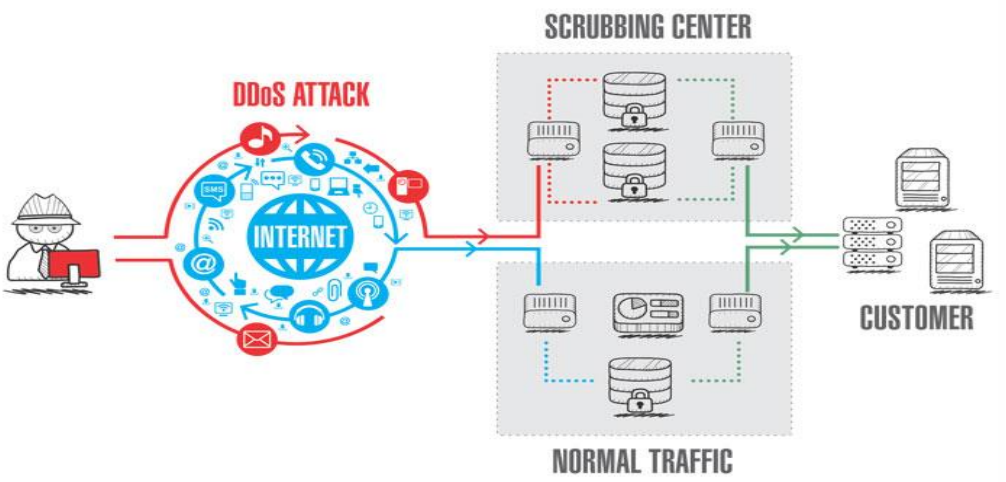

Fig. 1. Active attack prevention example [25]

In order to defend these types of attacks, users have to be always on standby with strategies and backup plan whenever attack occur, thus this can only effectively prevent users from being one of the victim of these attack [26]. With that being said, by using intrusion prevention system (IPS) alongside encryption [27] and pre-encryption methods [28] such as Secure Sockets Layer (SSL) often prevent active attacks [26][29]. To prevent active attacks such as DDoS attack, users must be clear that, firewalls does not have the capability in preventing DDoS attacks. According to [30] Reo, using a firewall as a defence method for the prevention of DDoS attack is pretty much useless. The saying of using firewalls to prevent DDoS attack is still a myth until this day, this is because DDoS attacks can find loopholes in a firewall, whereby it will bypass a firewall like a legitimate user [30].

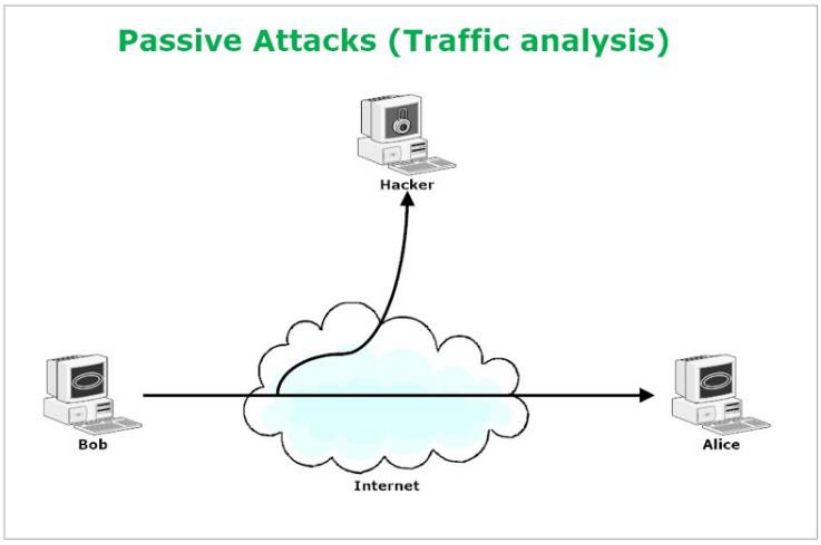

Fig. 2. Passive attack example [31]

2.2 Privacy

Another major concerning issue in wireless network is about privacy [32]. According to a survey done by Minch (2004), privacy has been the ranked as the top concern by internet users [33]. Ensuring the privacy of sensitive data is essential as nowadays many situations are now using wireless networks such as banking data, social networks, e-commerce [34], health and medical data [35][36]. Researchers have been finding efficient techniques such as social network [37], cloud services, smart grid [38], secure systems using smart technologies [39], secure communication and routing protocols [40][41], and enhanced authentication techniques to preserve privacy as the Internet has made a huge amount of private information including data, location and usage available [42]. Companies and organisations also collect user's private information in order to find out what user needs and to produce a product that is needed by a user. This shows that users are being monitored by companies and they can be tracked by companies easily. However, there are also some advantages with all these 'public' data. For example, corrupt politicians and people can be easily traced and found by using these data gathered by the companies.

A. Data Privacy

Firstly, one of the leakages of privacy information in wireless network is data of users. Privacy-preserving algorithms in the fog network can run between the fog and the cloud [43]. Those algorithms are normally resource-prohibited at the end services. Several techniques can be used in this including homomorphic encryption that is able to allow privacy-preserving aggregation at the local gateway without decryption [44]. Another technique is differential privacy, and this technique is used in case of statistical queries. This is to ensure that there are no disclosures of a single, arbitrary entry in the dataset.

B. Location Privacy

Furthermore, location privacy is another important problem that contributes to privacy issues in wireless network. Often, wireless networks are used for the purpose of monitoring in an application such as high value assets, the military, and healthcare monitoring. Thus, it is vital to ensure that transmission of data through wireless network is always safe and data such as location information being monitored is always kept private [45]. Without proper protection of the information, attackers can eavesdrop the information and use it for blackmail, stalking, and other privacy violations [46] [47]. Several threats including tracking threats, identification of threats, and profiling threats may arise if location information of users are disclosed. In tracking threats, attackers are able to receive updates of user location in real time continuously. This information is then used to predict and identify user's location routes. Next, identification threat is where attackers are able to receive user location updates thereby use it to identify locations that the user frequently visited. The disclosure of the user frequently visited locations may then cause the user's identity to be disclosed [48]. While in profiling threats, attackers use locations information to profile user instead of identifying users [49]. This means that an attacker gathers location information of a user such as which hospital or shopping mall the user often visits to obtain clues about a user's private information including user lifestyle and purpose of visiting different location without the user revealing their identity.

C. Usage Privacy

Homes are becoming increasingly "smart" with increasing deployments of internet-connected devices in the house as shown in figure above [50]. When using internet-connected devices such as lighting systems, smoke alarms, health or fitness data systems to both manage and monitor a home environment remotely, consumer's data will be sent directly from home to the cloud for further analysis. Thus, this results in the increase of risks and privacy issues as eavesdroppers can illegally pry into family activities and even a device manufacturer may also gather data of consumers without their consent [51].

One of the most significant attacks example in internet-connected building systems was the attack on Target. In this attack, attackers compromise the heating, ventilation and air-conditioning company that provide supply for Target. By compromising these systems, the company will then need to access to the Target network to perform checking and

maintenance. As a results, attacker utilise this entry point and access to the system which then causes almost 40 million of customer records to be exposed [49].

3 Data Collection and Methodology

The literature review in the previous section is used as a reference to conduct the rest of the research using two methodologies which are survey analysis and systematic review of literature.

3.1 Systematic Review

Systematic review of past literature by means of analyzing and comparing the findings from these papers allow the research to accurately pinpoint the most prevalent issues regarding wireless privacy and security as well the ways to mitigate such issues as suggested by previous researchers. Numerous studies have done an extensive research on the topic in order to raise awareness about the seriousness of the issue, and hence by referencing from these studies boost the credibility of this research. The systematic review is done based on articles and journals obtained from credible repositories such as IEEE and ACM as well as information from reputable companies and organizations such as Microsoft and Cisco.

To ensure that the results obtained from systematic review are genuine, accurate and consistent, about 40 different articles from different authors are collected of which comparative analysis is performed in order to filter out any inconsistencies and/or discrepancies resulted from research bias and systematic errors in the methodology. Systematic review also allows the rest of the research to be conducted in an efficient manner with minimal errors.

3.2 Survey Analysis

A survey in the form of a web-based questionnaire is conducted to gain insight on public awareness regarding safe practices for using wireless network or Wi-Fi. The questionnaire is composed using Google Form which consists of 10 multiple-choice questions that test respondents' habits and knowledge on how to stay safe on a wireless network. Since the target population for this survey are people who use wireless network on a daily basis, the survey is shared and distributed to social media users via websites such as Facebook, WhatsApp, Instagram and Twitter because it is easier and faster to spread the information out through social media, and that almost every social media user uses Wi-Fi to access the Internet The target population is limited to only those residing in Malaysia.

The survey is conducted in a 2-week period from 22nd June 2020 to 6th July 2020 with a targeted minimum of 60 respondents to prevent any bias resulting from sample size that is too small. Fortunately, at the end of the 2 week-period, a total of 125 responses are received. The responses collected are analyzed and presented in the following section.

4 Discussion of Results

The first question serves as an introductory to see if respondents value their online privacy when using wireless networks. Respondents are given the "Yes" or "No" options to answer this question.

Out of all the 125 responses collected, 96% of respondents think that it is important for their data and activity online to be kept private and confidential while the remaining 4% think otherwise. This finding is consistent with Cisco Consumer Privacy Survey 2019 whereby the majority of respondents (84%) indicated that they value their own privacy very much and want to have more influence on how their personal information is used and whom their information is disclosed to. [52] The result is not surprising as people nowadays do not want their personal data from being disclosed to irrelevant personnel, which can lead to severe consequences such stalking and data theft. [53]

The remaining 4% who do not value their privacy as much could be due to the lack of cybersecurity awareness, or

that they simply do not mind having their information seen by everyone. Nevertheless, online privacy must not be neglected, and one of the ways to preserve privacy is by following safe practices when using wireless network.

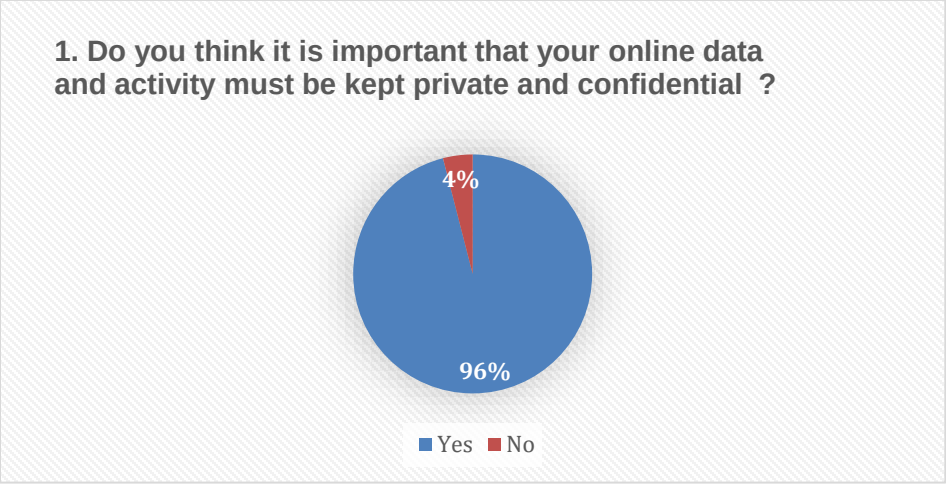

Fig. 3. Survey question 1

Public Wi-Fi is often the breeding ground for cyber attackers and this question serves to see how frequently respondents connect to a free public Wi-Fi in order to test their awareness on the dangers of using a public wireless network. Respondents are given the options to answer “Everytime”, “Sometime”, or “Never”. A majority of respondents admitted to having connected to a public Wi-Fi sometimes at 52%, which is followed by respondents who connect to a public Wi-Fi every time at 36% and lastly respondents who never connect to public Wi-Fi at 12%.

The finding indicates that most respondents are not aware of the dangers of using a public Wi-Fi, as people who are aware of such dangers would avoid using it unless necessary. The 36% of the respondents who connect to public Wi-Fi every time clearly do not possess such knowledge to protect their online presence. Public Wi-Fi is dangerous because it is easy for attackers to gain access into the network and launch a MITM or Evil Twin Attack to steal user information with. [54] Attacker can also propagate malware through the public network, if file sharing is enabled on the victim’s computer. [54] Hence, it would be best to avoid using a public Wi-Fi unless necessary.

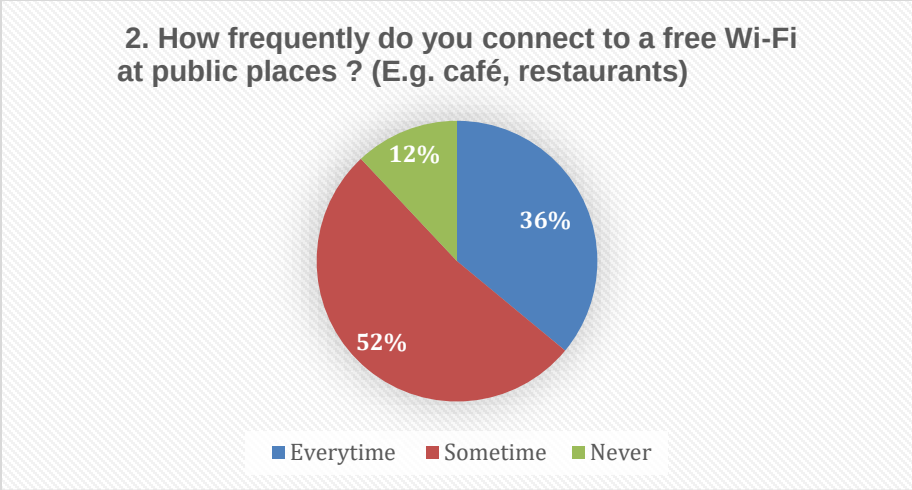

Fig. 4. Survey question 2

A Virtual Private Network or VPN is used to encrypt the communication between two end points by creating a private network from public network resources. The encryption is done at the network layer using a technology known as IPSec. [8] VPN is also one of the most effective methods for ensuring privacy and confidentiality when using a public wireless network. [55]

From the chart, it can be seen that only half of the respondents use a VPN when connecting to a public Wi-Fi, with every time at 23% and sometime at 27%. The remaining half either do not use a VPN at 31%, or that they do not know what a VPN is at 19%. The finding shows that again, there is still quite a lot of Internet users who either lack the knowledge to protect their online presence, or they refuse to follow the safety procedures when using a public network. Without VPN, a user is susceptible to all kind of wireless attack which could compromise their privacy and data confidentiality.

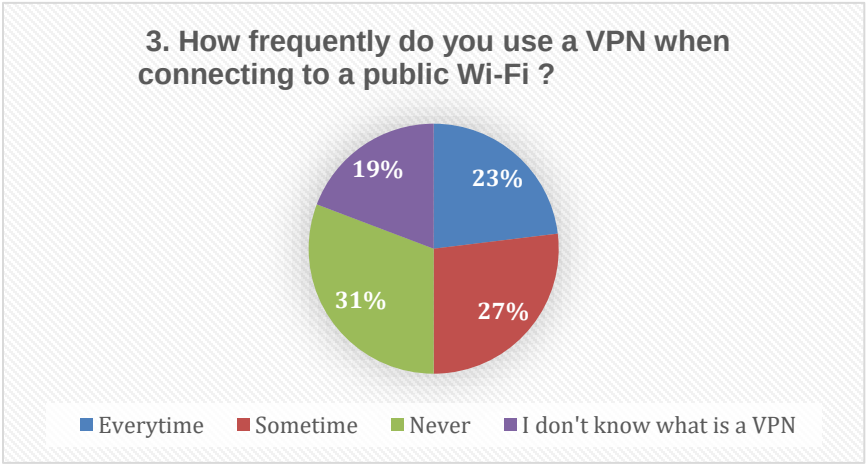

Fig. 5. Survey question 3

This question again tests if respondents know the safety precautions when using a wireless network, because antivirus

software is useful in detecting and disabling malware that makes user machine vulnerable to wireless attack, such as malware that disables the firewall and/ or enables public file-sharing that allows attacker to plant script that steals user information. It is pleasant to discover that 64% of the respondents use antivirus software to ensure the security of their mobile devices while there is still a minority of users who do not use an antivirus software, at 36%.

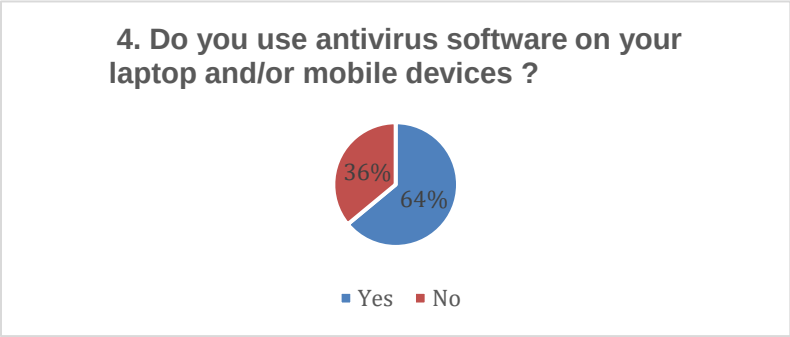

Fig. 6. Survey question 4

Most of the time when an attacker is able to steal sensitive information from a user's device is because that information is present in the device itself. Although there are many solutions that claim to secure user information, the safest option is not to store any sensitive information on any mobile devices as they are prone to data theft when roaming from one network to another. From the survey, 62% of respondents store such information on their mobile devices while 38% do not. It is not correct to assume that storing sensitive information on mobile devices is completely vulnerable but there definitely is a risk. Encryption must be used if users wish to save such information.

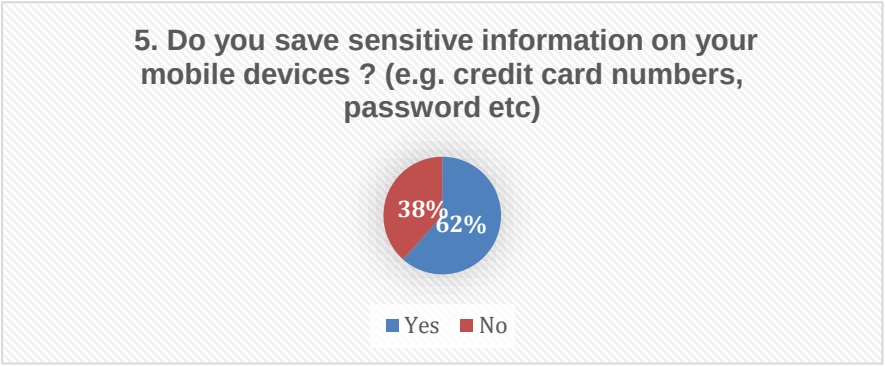

Fig. 7. Survey question 5

From question 6 onwards, respondents are asked if they know the several practices to keep their home wireless network secure. The finding of this question is very worrying, because majority of the respondents uses easy-to-guess password for their home Wi-Fi which can be easily cracked by attackers through a brute-force or dictionary attack. The password can also be guessed easily by unauthorized guests if they know the network owner well enough to do an inference attack based on the owner's information. As such, it is advisable to use a more complex password to prevent unwanted guests from connecting to the home WiFi.

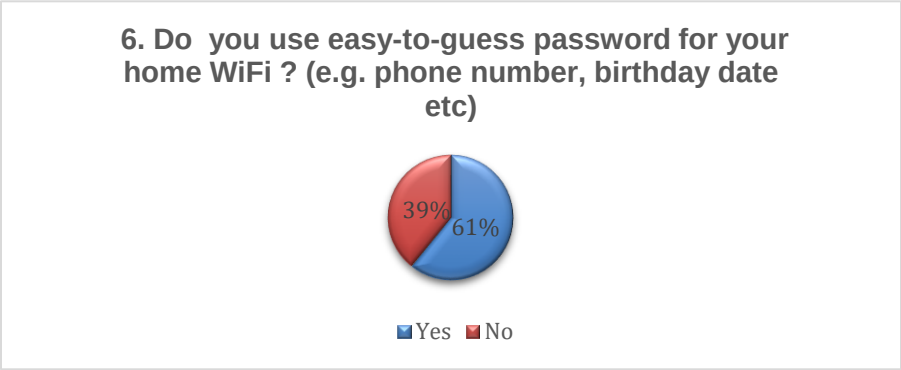

Fig. 8. Survey question 6

Changing password frequently is required to ensure that no one has cracked the password and to prevent unwanted guests from piggybacking on the home Wi-Fi. Additionally, the current password could also have been stolen and uploaded to an online repository to allow people to steal the Wi-Fi when they are in the same proximity. [56] Unfortunately, most respondents at 69% do not have the habits to changes their Wi-Fi password frequently, which can be prone to all kinds of wireless attack. Hence, the lack of awareness and/or the technical knowledge to change Wi-Fi password could be the main cause here.

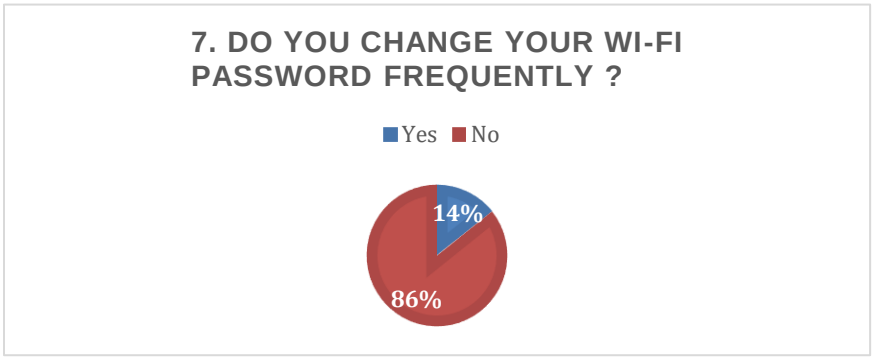

Fig. 9. Survey question 7

The worst thing about a wireless attack is that the attacker has already broken into the wireless network but the network owner is not aware of such event. If immediate action is not taken, the attacker would achieve their malicious goals and leave harm to the owner. From the survey, 42% of respondents know how to check devices that are currently connected to their home Wi-Fi while 58% do not. This functionality can usually be accessed from the router web interface, and is one of the easiest methods to check for unrecognized leechers. 58% of respondents who do not know how to perform this check could have been taken advantage by malicious users for as long as their Wi-Fi password remains unchanged.

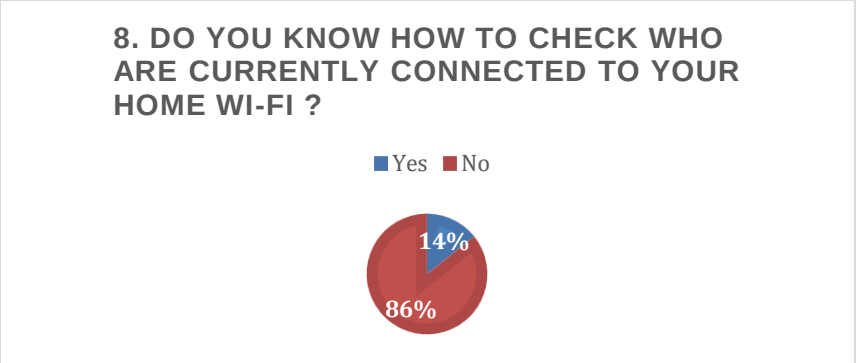

Fig. 10. Survey question 8

Leaving a router's configuration to its default can be very dangerous: if the SSID is unchanged, attackers can derive the router model from its default SSID and target exploit specifically on that model of router; if the default administrator password is not changed, attackers and guests can access the router gateway interface and change a whole bunch of settings and/or lock the network owner out. From the survey, 72% of respondents do not leave the router settings to its default while 28% does. Hence, it is good that most respondents are aware of the vulnerability that the default settings introduce.

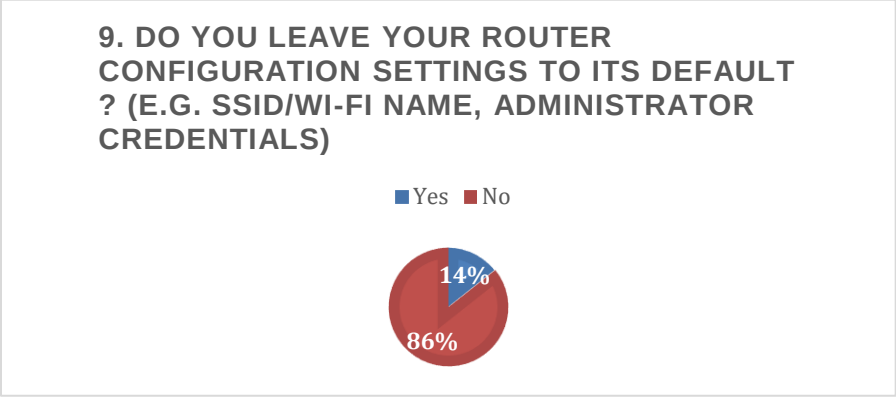

Fig. 11. Survey question 9

The is this the most interesting finding from the survey: only 4% of respondents update their router's firmware frequently while the rest of the respondents either do not update or they do not know how to update. The result is not unexpected as most people are not informed by their ISPs that their routers need to be updated, let alone teaching them how to update the router's firmware. Besides, most routers nowadays are equipped with auto-update feature. Nevertheless, it is better if users could monitor the update of their router's firmware to ensure that it is always the latest, as outdated firmware may contain vulnerabilities or security loopholes that attackers can exploit. Additionally, there are still people who are using old routers with no auto-update feature and/or is no longer supported by their manufacturers. Hence, these users should know how to update their routers manually, or they should replace their routers with the newer models.

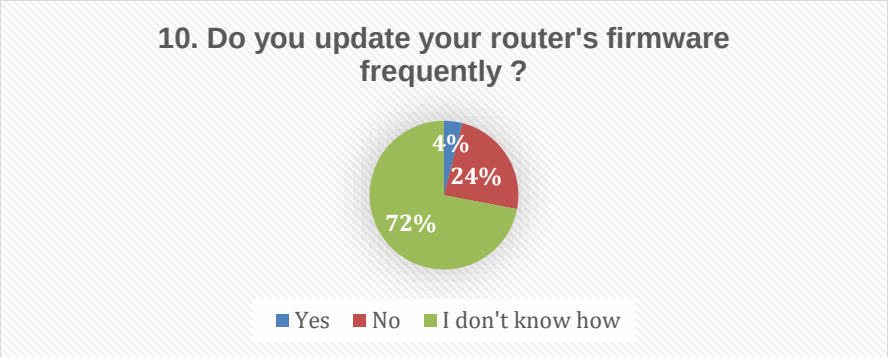

Fig. 12. Survey question 10

5 Unique Solution to Prevent Active and Passive Attacks

In order to effectively prevent active attacks, it is important for users to have an as strong as possible defence architecture to minimise the risk of getting attacked by malicious hackers [57][58]. Firstly, to effectively prevent active attacks, users have to split and diverse the paths to servers, hence by diverting servers and resources into different geographical areas, hackers will not be able to gain access into the entire system during an attack [58]. Besides, users and organizations can also monitor different environments, which include both physical and cloud-based environment, in order to identify any potential DDoS attacks [15]. Hence, another method of early prevention is to keep an eye on the volumetric flood by using network monitoring, whereby a sudden spike in the volume implies an early attack [59].

On the other hand, the main method to eliminate and prevent passive attacks is by implementing network encryption [16]. Encrypting the network traffic makes it difficult, if not impossible, for attackers to derive any useful information from the packets even if they have successfully intercepted the traffic. Meanwhile there's also the elevation of privilege attack whereby the attackers scan for loopholes in the system in order to intercept any sort of data that can grant them access to better privileges [60]. Organizations can then fully utilise the benefits of cryptography and encryption techniques in order to further enhance its defence system against attackers, such as by using Secure Socket Layer (SSL) encryption. With this, valuable information that are meant to be kept confidential will be safe as SSL will scramble the wordings into an unreadable form of text for recipient that does not have the privilege to view it. Therefore, it is clear that, even though any sort of information that have been spoofed or stolen by malicious attackers, they won't be able to read the file [61]. Another solution which is currently an active area of research as well is machine learning. Developing security solutions using machine learning techniques [62] is a promising field for development of security techniques to prevent active and passive security attacks.

One solution to privacy issues in wireless network is the implementation of Personal Data Protection Act (PDPA). The PDPA is an act that grants strict requirements on anyone or organizations who collects or processes personal data and enforces individual rights to 'data subject' [63]. The purpose of the PDPA is to protect individual's data from being used arbitrarily by getting user's consent when collecting data as it is vital for user to know about their rights on data privacy in order to prevent negative issues that might happened on them in the future [64].

Next, another solution to mitigate location privacy issue is to use a method called mix zones. Researchers Beresford and Stajano proposed a solution whereby anonymity services are used based on an infrastructure that delays and reorders messages from subscribers. Within a mix zone area where a user is untraceable, all the users' identities in the same zone will be mixed. This results in an indiscernible identity [65]. Lastly, to effectively mitigate wireless security and privacy issues, awareness on cybersecurity must be instilled into the public so that every wireless network user knows how to protect themselves from wireless attack. From the survey conducted, it is clear that many users do not possess such knowledge whereby most of them are willing to sacrifice their data privacy in exchange for free Wi-Fi.

Hence, a sophisticated security technology does not matter if the user is not capable of following the safe practices themselves when using a wireless network.

6 Conclusion

Wireless network security is more important than ever in todays fast paced information-driven world. Security issues always crop up whenever three main factors come into play: confidentiality, integrity and availability. All three of said factors and more are always present in wireless networks. Unfortunately, despite technology evolving at such a rapid pace, there is no perfect solution to all these issues; loopholes and vulnerabilities will always be present in wireless network technologies for hackers and cybercriminals to exploit. New ways to circumvent attacks will be developed each day, and new ways to exploit new and previously undetected vulnerabilities will inevitably be created too in a never-ending cycle. While it is true that perfection is a myth in developing security measures for wireless networks, it is still possible and recommended to err on the side of caution and deploy measures to be as secure as possible when interacting with wireless networks. Solutions such as encryption, packet filtering and access control should be in place to stop most of the threats that have been discovered so far. Casual users of the Internet and other wireless networks should also take the time to educate themselves on how to stay safe on public networks as well as how to react and what to do when under an attack. Privacy issues that have become more prominent recently can also be avoided to an extent by educating users to be more careful about what data is being shared and what permissions are given to other third parties on said data. Data legislations that are in place to protect a user's data should also be understood and made aware of to help increase awareness on how and what data should be collected and processed. Knowing one's rights to privacy online can help keep oneself safe from abusers of personal data.

References

[1] "The 2020 Official Annual Cybercrime Report - Herjavec Group", Herjavec Group, 2020. [Online]. Available: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/. [Accessed: 01- July- 2020].

[2] J. Naughton, "The evolution of the Internet: from military experiment to General Purpose Technology", Journal of Cyber Policy, vol. 1, no. 1, pp. 5-28, 2016. Available: 10.1080/23738871.2016.1157619 [Accessed 01-July-2020].

[3]. K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.

[4]. Dhuha Khalid Alferidah, NZ Jhanjhi, A Review on Security and Privacy Issues and Challenges in Internet of Things, in International Journal of Computer Science and Network Security IJCSNS, 2020, vol 20, issue 4, pp.263-286

[5] N. WINARSKY, "Exponential tech advances will change the world faster than we think | VentureBeat," 2019. [Online]. Available: https://venturebeat.com/2019/11/17/exponential-tech-advances-will-change-the-world-faster-than-we-think/. [Accessed: 08-Jul-2020].

[6] J. CRISALLI, "Cybersecurity: As technology advances, so do potential threats to privacy and security – Orange County Register," 2019. [Online]. Available: https://www.ocregister.com/2019/03/28/cybersecurity-as-technology-advances-so-do-potential-threats-to-privacy-and-security/. [Accessed: 08-Jul-2020].

[7] CISA, "Securing Enterprise Wireless Networks | CISA," 2018. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST18-247. [Accessed: 07-Jul-2020].

[8] B. Carle, "Risks of Aging Technology and Benefits of Upgrading -- Campus Security & Life Safety," 2019. [Online]. Available: https://campuslifesecurity.com/Articles/2019/04/01/Risks-of-Aging-Technology-and-Benefits-of-Upgrading.aspx. [Accessed: 08-Jul-2020].

[9] K. Lindros, “Upgrade Your Business Technology for Greater Productivity - Business News Daily,” 2017. [Online]. Available: https://www.businessnewsdaily.com/10167-upgrade-technology-for-productivity.html. [Accessed: 08-Jul-2020].

[10] S. K.S., “Importance of configuring firewall Importance of configuring firewall,” 2018. [Online]. Available: https://malware.expert/firewall/importance-of-configuring-firewall/. [Accessed: 08-Jul-2020].

[11] M. Gluck, “Understanding the Cost of a Data Security Hack | Sanity Solutions INC,” 2018. [Online]. Available: https://www.sanitysolutions.com/understanding-the-cost-of-a-data-security-hack/. [Accessed: 08-Jul-2020].

[12] L. BELL, “Hacking- This Is what your company could be held responsible for - Live Consulting,” 2017. [Online]. Available: https://www.liveconsulting.com/news/hacking-this-is-what-your-company-could-be-held-responsible-for/. [Accessed: 08-Jul-2020].

[13] C. Schueler, “What Happens When Your Small Business Is Hacked,” 2017. [Online]. Available: https://www.entrepreneur.com/article/295105. [Accessed: 08-Jul-2020].

[14] J. Walrand and P. Varaiya, “Wireless Networks - an overview | ScienceDirect Topics,” 2000. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/wireless-networks. [Accessed: 08-Jul-2020].

[15] G. Manganaro and D. Leenaerts, “Wireless Infrastructure - an overview | ScienceDirect Topics,” 2013. [Online]. Available: https://www.sciencedirect.com/topics/engineering/wireless-infrastructure. [Accessed: 08-Jul-2020].

[16] J. Donovan, “How Do Wireless Networks Transmit Data? - Commscope Training,” 2017. [Online]. Available: https://blog.commscopetraining.com/how-do-wireless-networks-transmit-data/. [Accessed: 08-Jul-2020].

[17] C. Press, “WiFi Networking: Radio Wave Basics | Network Computing,” 2017. [Online]. Available: https://www.networkcomputing.com/wireless-infrastructure/wifi-networking-radio-wave-basics. [Accessed: 08-Jul-2020].

[18] M. BRAIN, T. V. WILSON, and B. JOHNSON, “What Is WiFi? | HowStuffWorks,” 2020. [Online]. Available: https://computer.howstuffworks.com/wireless-network1.htm. [Accessed: 08-Jul-2020].

[19] G. Meyer, D. An, Sarge, D. Banttari, and S. Casco, “Hack Proofing ColdFusion - Syngress - Google Books,” Syngress, 2002. [Online]. Available: https://books.google.com.my/books?id=mu1U7IdYO_4C&pg=PA29&lpg=PA29&dq=hackers+decode+information+in+the+router&source=bl&ots=oK13OlQi2D&sig=ACfU3U1OXtK-oFskUHoVW_AL6x-gndJnEw&hl=en&sa=X&ved=2ahUKEwis7qCbxrzqAhWU4HMBHUmqC6cQ6AEwC3oECAkQAQ#v=onepage&q=hacke. [Accessed: 08-Jul-2020].

[20] Akamai, “What are Network Security Attacks? | Akamai,” 2020. [Online]. Available: https://www.akamai.com/uk/en/resources/network-attacks.jsp. [Accessed: 08-Jul-2020].

[21] TechDifferences, “Difference Between Active and Passive Attacks (with Comparison Chart) - Tech Differences,” 2018. [Online]. Available: https://techdifferences.com/difference-between-active-and-passive-attacks.html. [Accessed: 08-Jul-2020].

[22] M. Rouse, “What is passive attack? - Definition from WhatIs.com,” 2014. [Online]. Available: https://whatis.techtarget.com/definition/passive-attack. [Accessed: 08-Jul-2020].

[23] K. Thakur and A.-S. K. Pathan, “Cybersecurity Fundamentals: A Real-World Perspective - Kutub Thakur, Al-Sakib Khan Pathan - Google Books,” CRC Press, 2020. [Online]. Available: https://books.google.com.my/books?id=pL_gDwAAQBAJ&pg=PA204&lpg=PA204&dq=loophole+in+wireless+ne

twork+for+hackers&source=bl&ots=DQwpdYcqh0&sig=ACfU3U0J2edw8IwpRPPnpdrteiw_03UTtA&hl=en&sa=X&ved=2ahUKEwi6iub1yLzqAhV6yzgGHQRmAv4Q6AEwD3oECAoQAQ#v=onepage&q=loo. [Accessed: 08-Jul-2020].

[24] J. DiGiacomo, "Active vs Passive Cyber Attacks Explained | Revision Legal," 2017. [Online]. Available: https://revisionlegal.com/internet-law/cyber-security/active-passive-cyber-attacks-explained/. [Accessed: 08-Jul-2020].

[25]. https://investorsking.com/wp-content/uploads/2018/05/DDoS-Mitigation.jpg

[26] J. Herbst, "Threat Response: How to Deal with Active Network Attacks - Summit Information Resources," 2017. [Online]. Available: https://www.summitir.com/2017/03/28/threat-response-how-to-deal-with-active-network-attacks/. [Accessed: 08-Jul-2020].

[27]. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, http://dx.doi.org/10.1109/ACCESS.2020.2983117 .

[28]. Kok, S.H.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M. Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm. Computers 2019, 8, 79.

[29] J. R. Vacca, "Computer and Information Security Handbook - John R. Vacca - Google Books," 2017. [Online]. Available: https://books.google.com.my/books?id=05HUDQAAQBAJ&pg=PA401&lpg=PA401&dq=With+that+being+said,+by+using+firewalls+and+intrusion+prevention+system+(IPS)+can+often+prevent+active+attacks&source=bl&ots=KCNtf36ebg&sig=ACfU3U29zU51lwfm8MTyr5pL1SAN-1Zl9g&hl=en&s. [Accessed: 08-Jul-2020].

[30] J. Reo, "Massive Botnet Attack Proves That Firewalls Offer No DDoS Protection - Corero | Corero," 2020. [Online]. Available: https://www.corero.com/blog/massive-botnet-attack-proves-that-firewalls-offer-no-ddos-protection/. [Accessed: 08-Jul-2020].

[31]. https://www.venafi.com/sites/default/files/content/body/1_2.png

[32] Sangaiah, A., Karuppiah, M. and Li, X., 2017. Wireless and Mobile Networks: Security and Privacy Issues. Journal of Electrical and Computer Engineering, 2017, pp.1-2.

[33] Robert P, M., 2004. Privacy Issues In Location-Aware Mobile Devices. [online] Citeseerx.ist.psu.edu. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.441.9513&rep=rep1&type=pdf> [Accessed 5 July 2020].

[34] K.Ramesh, R., S.N.Tirumala, R. and P.Chenna, R., 2017. Wireless Communication Security and Privacy issues and Challenges. International Journal of Computer Science and Information Security (IJCSIS), vol. 15(7), pp.202-209.

[35] Al Ameen, M., Liu, J. & Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. J Med Syst 36, 93–101 (2012).

[36]. Hussain, S.J., Irfan, M., Jhanjhi, N.Z. et al. Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07702-7

[37] Beach, A., Gartrell, M. and HAn, R., n.d. Solutions To Security And Privacy Issues In Mobile Social Networking. [online] Cs.colorado.edu. Available at: <https://www.cs.colorado.edu/~rhan/Papers/SMW09_Secure_Mosonets.pdf> [Accessed 5 July 2020].

[38] Ma, D., 2010. Security and Privacy in Emerging Wireless Networks. [online] Sprout.ics.uci.edu. Available at: <http://sprout.ics.uci.edu/pubs/05601953.pdf> [Accessed 5 July 2020].

[39]. Azeem Khan, NZ Jhanjhi, Mamoona Humayun, Year: 2020, Secure Smart and Remote Multipurpose Attendance Monitoring System, EW, EAI, https://doi.org/10.4108/eai.13-7-2018.164583

[40]. A. Almusaylim Z, Alhumam A, Mansoor W, Chatterjee P, Jhanjhi NZ. Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things. Preprints.org; 2020. DOI: 10.20944/preprints202007.0476.v1.

[41]. Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z. Jhanjhi, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review, Ad Hoc Networks, Volume 101, 2020, 102096, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102096.
(http://www.sciencedirect.com/science/article/pii/S1570870519308388)

[42] Javadi S.S., Razzaque M.A. (2013) Security and Privacy in Wireless Body Area Networks for Health Care Applications. In: Khan S., Khan Pathan AS. (eds) Wireless Networks and Security. Signals and Communication Technology. Springer, Berlin, Heidelberg

[43] Gruteser M., 2011 Location Privacy in Wireless Networks. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA

[44] Shanhe, Y., Zhengrui, Q. and Qun, L., 2015. Security And Privacy Issues Of Fog Computing: A Survey. [online] Cs.wm.edu. Available at: <http://www.cs.wm.edu/~zhengrui/papers/wasa15-fog.pdf> [Accessed 5 July 2020].

[45] Mutalemwa, L. and Shin, S., 2019. Achieving Source Location Privacy Protection in Monitoring Wireless Sensor Networks through Proxy Node Routing. Sensors, 19(5), p.1037.

[46] Benjamin, F., 2020. Wireless Networking Security. [online] Cs.bham.ac.uk. Available at:<https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS7/Wireless%20Networking%20Security.htm> [Accessed 5 July 2020].

[47]. A. Almusaylim, Z., Jhanjhi, N. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Pers Commun 111, 541–564 (2020). https://doi.org/10.1007/s11277-019-06872-3

[48] Cremonini, M., Braghin, C. and Claudio Agostino, A., 2013. Computer And Information Security Handbook (Second Edition). 2nd ed. pp.739-753.

[49] Fredrik, E., Martin, B. and Henric, J., 2016. [online] Available at: <https://www.researchgate.net/publication/259231159_Privacy_Threats_Related_to_User_Profiling_in_Online_Social_Networks> [Accessed 5 July 2020].

[50] Carsten, M., 2017. Security and privacy in the internet of things. Journal of Cyber Policy, 2(2: The Internet of things), pp.155-184.

[51] Shanthi, K., 2019. The Privacy, Data Protection And Cybersecurity Law Review. 6th ed.

[52] "100 Data Privacy and Data Security statistics for 2020 – Data Privacy Manager", Data Privacy Manager, 2020. [Online]. Available: https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/. [Accessed: 27- Jun- 2020].

[53] "Why Your Online Privacy Matters", Norton, 2020. [Online]. Available: https://us.norton.com/internetsecurity-privacy-why-your-online-privacy-matters.html. [Accessed: 27- Jun- 2020].

[54] "How to Avoid Public WiFi Security Risks", Kapersky, 2020. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks. [Accessed: 27- Jun- 2020].

[55] "What is a VPN?", Norton, 2020. [Online]. Available: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html. [Accessed: 27- Jun- 2020].

[56] "How Often Should You Change Your Home WiFi Password?", Detroit.cbslocal.com, 2016. [Online]. Available: https://detroit.cbslocal.com/2016/05/16/how-often-should-you-change-your-home-wifi password/#:~:text=A%20safe%20interval%20between %20sensitive%20technological%20devices) [Accessed: 27- Jun- 2020].

[57] N. Lord, "Social Engineering Attacks: Common Techniques & How to Prevent an Attack | Digital Guardian," 2019. [Online]. Available: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack. [Accessed: 08-Jul-2020].

[58] R. Kartch, "Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response," 2016. [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html. [Accessed: 08-Jul-2020].

[59] Cisco, "A Cisco Guide to Defending Against Distributed Denial of Service Attacks," 2020. [Online]. Available: https://tools.cisco.com/security/center/resources/guide_ddos_defense. [Accessed: 08-Jul-2020].

[60] N. Hassan, "Active & Passive Attacks [Definition & Differences] | Venafi," 2020. [Online]. Available: https://www.venafi.com/blog/what-active-attack-vs-passive-attack-using-encryption. [Accessed: 08-Jul-2020].

[61] J. Davies, "Implementing SSL / TLS Using Cryptography and PKI - Joshua Davies - Google Books," 2011. [Online]. Available: https://books.google.com.my/books?id=LfsC03f8oGsC&pg=PA29&lpg=PA29&dq=ssl+scramble+messages&source=bl&ots=JXlWES4suF&sig=ACfU3U2NJQR9rW391-7SykBFhBqxp6jqNQ&hl=en&sa=X&ved=2ahUKEwidp_ezq73qAhUzzjgGHUI9BdoQ6AEwAHoECAYQAQ#v=onepage&q=ssl scramble messages&f=. [Accessed: 08-Jul-2020].

[62]. F. Zahra, N. Jhanjhi, S. N. Brohi and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-9, doi: 10.1109/MACS48846.2019.9024821.

[63] Data Security is Not Data Privacy, Here's Why It Matters [updated for 2020]", Managed Solution, 2020. [Online]. Available: https://www.managedsolution.com/data-security-vs-data-privacy-why-it-matters/. [Accessed: 5 July 2020].

[64] A. C. Uzialko, "How and Why Businesses Collect Consumer Data", Business News Daily, 2018. [Online]. Available: https://www.businessnewsdaily.com/10625-businesses-collecting-data.html. [Accessed: 5 July 2020].

[65] Evans, J., Wang, W. and Ewy, B., 2006. Wireless networking security: open issues in trust, management, interoperation and measurement. International Journal of Security and Networks, 1(1/2), p.84.