 doi:10.20944/preprints202009.0110.v1

Security and Privacy Issues in Wireless Networks and Mitigation Methods

1st Alya Hannah Ahmad Kamal
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
alyahannah@gmail.com

2nd Caryn Chuah Yi Yen
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
carynchuah3@gmail.com

3rd Pang Sze Ling
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
szelingpang46@gmail.com

4th Fatima-tuz-Zahra
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
fatemah.tuz.zahra@gmail.com

Abstract – The rapid growth of network services, Internet of Things devices and online users on the Internet have led to an increase in the amount of data transmitted daily. As more and more information is stored and transmitted on the Internet, cybercriminals are trying to gain access to the information to achieve their goals, whether it is to sell it on the dark web or for other malicious intent. Through thorough literature study relating to the causes and issues that are brought from the security and privacy segment of wireless networks, it is observed that there are various factors that can cause the networks to be an insecure; especially factors that revolve around cybercriminals with their growing expertise and the lack of preparation and efforts to combat them by relevant bodies. The aim of this paper is to showcase major and frequent security as well as privacy issues in wireless networks along with specialized solutions that can assist the related organizations or the public to fathom how great of an impact these challenges can bring if everyone took a step in reducing them. Hence, through this paper it is discovered that there are many ways these challenges can be mitigated, however, the lack of implementation of privacy and security solutions is still largely present due to the absence of practical application of these solutions by responsible parties in real world scenarios.

1 Introduction

In this era of technology, the world has become interconnected and technology has become more powerful. The growth of the Internet has led to the increase of devices such as laptops, smartphones and more. Without any doubt, wireless technology [1] has been very important and a breakthrough in the telecommunication world. An easy installation, low cost and connectivity capability make wireless networks popular in this current century. Meanwhile, the high demand for wireless networks and insecure interconnectivity of IoT devices causes different categories of security threats [2], [3]. It also poses the threats of privacy in sensitive data such as personal information, financial data and medical data. The relationship between security and privacy issues is relevant to each other and many solutions to one or both the issues have been proposed by researchers in the form of authentication schemes, use of artificial intelligence and machine learning techniques to overcome security attacks [4], [5].

Security is a common term that includes the main attributes of confidentiality (C) which refers to encrypting and protecting sensitive information from unauthorized access by other parties. By the way of explanation, the data can be only accessible to the people who have been authorized. The second attribute is integrity (I), assuring the information is secured and not altered by malicious users. It ensures the accuracy and consistency of data over the network. The last attribute is availability (A) which means giving to users the authorization access system freely. The common issue in availability belongs to DoS attacks that disturb access to information and system. In a nutshell, security in the wireless network as well as internet of things is about the preservation of data against unauthorized access by coding or technique [6-9].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

Privacy is a user's right to prevent the exposure of personal information to non-related people or organizations. Privacy breach normally starts with a security breach but not necessary. Applications that need to collect personal information from users will ask for a sign of privacy policy which will acknowledge the users about the privacy issues. This may lead to privacy being compromised. Privacy issues [10] are concerned with how the website and organization handles, processing, storage and how they would use. All in all, privacy is about the preservation of personal data from unwarranted access by organization or individuals.

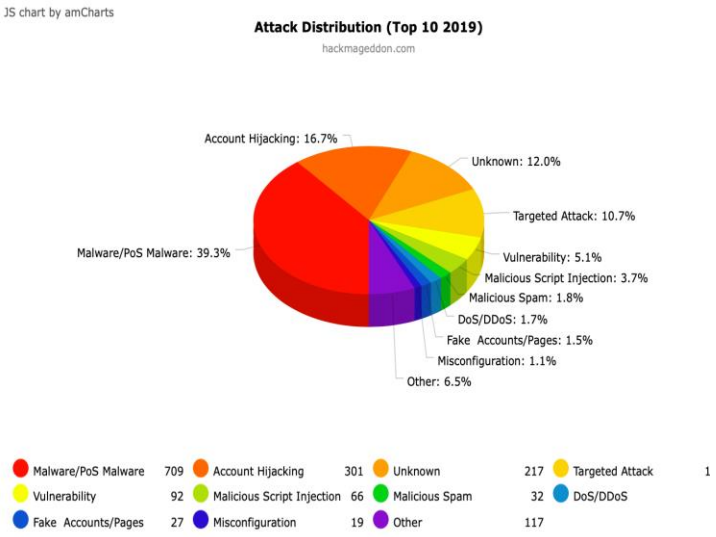

Fig. 1 Statistics of different cyberattacks in 2019 [11]

Figure 1 shows that the top cyberattack belongs to malware which proves that the public is advised not to neglect and ignore these worrying issues.

Throughout this paper, the security and privacy issues in a wireless network are critically discussed. It is hoped that the contents will be able to show the importance of users protecting themselves and at the same time raising awareness among the society. The content and information about this topic have given the public critical thinking as well as giving them to carry out their active role in a wireless network. This paper strives to influence the public by applying quality and reliable resources [12] from various kinds of research databases such as IEEE [13] and ResearchGate [14]. Anyhow, the paper contributes to society as it is presented in an effective way to let users know that the security and privacy issue is not limited to what they think.

In this paper, the main section would be starting with an introduction which covers the topic of security and privacy issues in wireless networks and a figure to show how important this topic is. After the introduction, the literature review section discusses security issues, privacy issues and a table consisting of the breakdown of cyberattacks happening each year. Moving on is the methodology for data collection and discussion on our findings. Moreover, the solution for issues will be analyzed and discussed with specific reference to the issue. The conclusion will summarize the overall significance of the topic and remind the readers about the important point of the research.

2 Literature Review

Security is about keeping unwanted traffic from entering a network whereas privacy is about keeping wanted information from leaving a network. Hence, security issues and privacy issues are two different topics, although they

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

involve some kind of unauthorized access to achieve the attacker's goals. Security issues [15] happen when an attacker gains unauthorized access to a website's or system's written language. On the other hand, privacy issues involve unwarranted access to sensitive and personal information which do not 100% have security breaches involved. In this section, both the issues are discussed with examples of scenarios.

2.1 Security Issues

A. Denial of Service (DoS) and Distributed DoS (DDoS) Attacks

A denial of service attack is an explicit attempt to prevent legitimate users from using the desired resources. An attacker can perform this attack by flooding a network with traffic, hence preventing legitimate network traffic. DoS attacks include disrupting connections between multiple machines, preventing access to a certain service. It can also be disrupting service to a system or to particular individuals. Moreover, a DDoS [16] [17] makes this type of attack even more difficult to prevent. The attack involves 4 elements which are victim(s), attack daemon agents, control master program and lastly the mastermind who is behind the attack. Victim(s) is the one who is chosen by the attacker to receive the brunt of the attack. Attack daemon agents refer to programs that are used to conduct the attack. These daemons affect not only the target computer but also the host computer. Deploying these daemons requires attackers to have access and infiltrate the host computer. Control master program is used to coordinate the attack and it allows the real attacker, who is the mastermind, to stay hidden during the attack.

Steps during a DDoS :

1. The real attacker sends a message to the control master program for execution.
2. The control master program propagates the command to the attack daemons upon receiving the execution message.
3. The attack daemons will then begin the attack on the target victim after receiving the attack command.

B. Spoofing Attacks

Spoofing attacks [18], [19] are when the attackers disguise a piece of information from an unknown source as a trusted source. There are many types of spoofing attacks, such as IP Spoofing and DNS Spoofing.

a) IP Spoofing

IP spoofing **[20]** is when IP packets with forged source IP addresses are created to conceal the identity of the sender or a system. IP is used during data transmission between machines over the Internet and each packet that is sent out has its own IP address which identifies the source of the information. This attack is used to either commit cybercrime online or to breach network security. IP spoofing prevents attackers from getting caught as the source of the messages cannot be determined due to the forged IP address. On the other hand, breaching network security is where attackers use an IP address that is the same as one of the IP addresses that is valid on the network. With this, the attacker does not need a valid username and password to have access to the network.

b) DNS Spoofing

DNS spoofing [21] is the act of creating a DNS entry to point to another IP address instead of the supposed IP address. This will then navigate users to the wrong websites or emails routed to unauthorized mail servers. The attacker who is connected between the DNS server and the victim will be able to see all the DNS traffic and hijack the DNS session. Attackers can mirror any websites and redirect users to the websites for password collection or payment details collection. Users can happen to download fake updates when they download some form of malicious code from the attacker's website.

C. Man in the Middle Attack (MitM)

Man in the Middle [22-24] is an active attack whereby an attacker will intercept in the communication between client and server. The attacker will sit between the connection of both parties to eavesdrop or alter the traffic between them. The aim of MitM attack is to gain access to users' personal information such as financial data, account details and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

more. Normally, the attacker will target an online shopping site, finance site and others that require login. MitM attack [25], [26] might involve phishing as they can make the email act as legitimate in order to trick users to click on the malicious link or file. Techniques of MitM can be distributed to 4 types as below:

a) Sniffing

An attacker will obtain the data by capturing the network using sniffing tools. They are allowed to view the packet such as a packet addressed to hosts by using the specific tools and devices that are able to put them in a monitor mode [27], [28].

b) Packet Injection

A common technique used by attackers to access and alter network traffic. An attacker will insert the malicious code in the packet [29] and then inject the packet into the communication stream. By doing this, attackers are able to disrupt victims to use certain services.

c) Session Hijacking

An attacker will take over a session of the client and network server. The attacker will use the sniffing technique to sniff the traffic in order to replace the clients' IP address to its own address [30-32].

d) SSL Stripping

A legitimate website will have an HTTPS against ARP and DNS spoofing. However, an attacker will use SSL stripping [24] to alter the based address and request the user to use HTTP. By using HTTP, the request to the server will become unencrypted. Thus, important information will be leaked in plain text.

2.2 Privacy Issues

A. Identity Theft

Identity theft [33-35] is where a cybercriminal obtains personal information without authorized access to impersonate another person. There are many types of identity theft, such as medical identity theft, financial identity theft and criminal identity theft. Financial identity theft, in which the cybercriminal gets economic benefits using the identity stolen remains the most common type. Medical identity theft is where the attacker obtains information such as health insurance numbers in order to receive medical services. Next is criminal identity theft. Criminals sometimes give the identity information that he has stolen to the police when he is under arrest. This will then cause the victim to be charged instead of the criminal himself. Identity theft can be done using social engineering techniques such as phishing and dumpster diving.

B. Password Leaks (Data Breach)

Passwords that are leaked might be sold on the dark web or shared on the Internet for everyone to see. Attackers can easily use the leaked login information to attempt to gain access to other accounts as users always use the same password for different services for convenience. Attackers also used brute force attacks [36] to get the passwords. This attack is done by inputting every possible combination in the credentials until the password is guessed correctly. Therefore, the shorter the password, the weaker it is, the quicker it can be cracked by this brute force attack.

C. Spyware

Spyware is a software that is installed on a device to gather information about an organization or an individual without them knowing. The information gathered will then be sent to a third party without user consent. It is estimated that this software is installed on more than 85% of personal computers. Internet Service Provider stated in its survey that there is an average of 28 spywares installed on each computer. Spyware includes adware, keystroke loggers and trojan horses [37]. Adware [38] is a software that monitors the user's activity on the browser and sends advertisements to the target user based on his/her browsing activity. This software is also capable of changing the default settings of the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

browsers and redirects searches to other search systems. Keystroke logger is a user monitoring software used to capture (logging) the keys struck on the keyboard while the user is unaware of their actions being monitored. The data captured include username, passwords, document contents and other potentially sensitive information. Lastly is a trojan horse, software that installs programs on the user's computer that allows the attackers to control the user's computer.

D. Phishing

One would wonder about the difference between phishing and spoofing attacks. To clarify, spoofing is the means of delivering the attack whereas phishing is the method of retrieving sensitive information after successfully spoofing the victim. Phishing [39], [40] contributed the most in terms of data breaches with 34% of incidents happening in the form of phishing attacks. One notable and most negatively impactful phishing attack is the WannaCry ransomware attack. This attack exposed many powerhouses like Nissan, FedEx and NHS which caused them to be vulnerable. The WannaCry attack used the vulnerability of organizations that did not have their Windows updated which in turn gave an opening for the malware to overflow their networks and provided an opportunity for arbitrary code to be inserted. Other than that, there are many types of phishing attacks [41] that can occur including email phishing, whaling and spear phishing [42].

a) Email Phishing

The most common type of phishing attack is email phishing. The attacker obtained email addresses of victims from different sources. An email that looks legitimate will be generated and sent. The victim who is the recipient of the email will be requested to perform some kind of action, it can be opening a malicious attachment, filling up a form or visiting a website. The attacker will then acquire the victim's information.

b) Whaling

Whaling [43], [44] is a type of phishing attack that specifically targets high ranking employees like the CEO or CFO of a company, to steal information that the higher positions hold. Most whaling phishing attacks are to manipulate victims to approve fraudulent wire transfers to the attacker. The attacker can also impersonate the CFO or CEO to convince employees of the organization and order them to carry out the financial transfers. The difference between whaling phishing and spear phishing is that whaling focuses on specific high-profile victims whereas spear phishing focuses on each individual. Both require a lot of time and effort compared to normal phishing attacks.

c) Spear Phishing

This type of phishing attack mainly targets organizations to collect customers' sensitive information such as financial information and credentials. The emails sent out normally use malicious attachments and website links, which is highly customized just for the target group. The email content might mean nothing at all to a recipient outside the organization. The difference between normal phishing and spear phishing is that spear phishing requires a higher level of sophistication of social engineering required by the attacker. Normal phishing emails only need to know the demographics and common financial institutions to help the attacker in customizing the attack. However, for spear phishing, every email must focus on each individual recipient, which eventually requires a much more focused social engineering method for email and attachments customization.

Year	Attacks	Details
2014	Data breach	Yahoo [45] reported 500 million of users' (all users) data are stolen. Stolen data includes account names, phone numbers, email address, hashed passwords and security questions and answers.
2015	Man-in-the-Middle	A British couple lost 340,000 pounds in an email hijacking MITM attack [46].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

	DNS Spoofing	Unknown hackers hacked Malaysia Airlines, blocking access to the website and flight status checks for hours.
2016	Spyware	SmeshApp, a messaging app on Play Store was used to spy on the Indian military personnel by the Pakistans [47].
	Whaling Phishing	A high-ranking employee from Snapchat disclosed employees' payroll information when an attacker pretended to be the CEO of Snapchat and sent him an email.
2017	Identity Theft	Major credit bureau, Equifax confirmed it was attacked by a data breach that exposed over 147 million clients' data. $425 million was spent as a compensation to the users affected.
	Spyware	Viperat spyware was used to target Israeli soldiers, stealing media using social engineering techniques.
2018	DDoS	GitHub experienced an attack that came in at 1.35 Tbps, 129.6 million packets per second. The attack lasted for 8 minutes.
	DDoS Spoofing	At least 500 Humana's clients have their medical records stolen including expenses and details of health claims. *Humana: American health insurance provider
2019	DDoS	Imperva reported one of its clients thwarted the attack which peaked at 580 million packets per second.
	Phishing	Attackers successfully got $100 million from Google and Facebook through phishing emails [48].
2020	DDoS	Amazon Web Services mitigated a 2.3 Tbps UDP attack [49].
	DDoS	A bank in Europe was attacked with 809 million packets per second [50].
	Data Breach	An online B2B, IndiaMART has 40,000 suppliers' data leaked [51].
	Data Breach	230,000 COVID-19 patient records from Indonesia are on sale on the dark web [52].
	Data Breach	900,000 South Koreans' credit card information was leaked and traded on an overseas online black market [53].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

3 Methods Used to Collect Results

Online documents:
Throughout this paper, the method used for analysis is secondary data which is collected through primary sources and made ready to be accessed by others. The first and foremost database used is the Institute of Electrical and Electronics Engineers (IEEE). The reason of using IEEE is that it is the prime academic database in the field of engineering and computing. It is also broadly used for the articles, scholarly references and conference papers publishing. While using their highly professional cited publication around the world, authors were able to inquire about the applicable information about the topic on IEEE databases.

Moreover, authors also used the ResearchGate database to acquire the related information. ResearchGate [54] is popular in discovering scientific knowledge, allowing us to locate useful articles and journals about the topic of privacy and wireless issues. Another research database used is Google Scholar [54]. The reason Google Scholar is used is that it provides vast range of search options across many articles, books and journals from various publishers, universities and websites. Google Scholar is not only fast and convenient to use, but also provides formatted citations for the convenience of users. Last but not least, Internet resources also have been used for additional analysis.

By default, these platforms will search the full text of the research paper. However, by typing the keywords such as “security issue”, “wireless network”, “privacy issue” and “security and privacy threats”, results are easily generated within seconds on these platforms. The platforms will automatically show the results that are related to keywords such as cloud computing, wireless sensor networks and more in order to provide us a wide range of options to choose from. Besides that, to make sure the information is accurate and consistent, the advanced searching is used by setting the year range to ‘from 2015 to 2020’ with the aim to narrow down and retrieve the recent research paper.

Different research papers and case studies with the same topic can be found on these platforms. However, there are different opinions and views coming from different authors hence reading and analyzing their findings allow us to understand more. After doing some in-depth research and comparison between what authors found from the scholarly documents, they were able to have a wider view of the concerned topic.

4 Discussion on Findings

Based on the findings in previous sections, it is concluded that the importance of privacy and security reinforcement and enhancement of wireless networks were not considered enough. As shown in the earlier literature review, be it security or privacy, attacks have been constantly been initiated by these cybercriminals. For an example in terms of the security issue, we will discuss a specific attack to see just how dangerous these privacy issues are to the masses which is the Distributed Denial of Service attack, DDoS. As mentioned earlier in the paper, DDOS attacks are one of the most common types of active attacks that allow the lawbreakers to steal sensitive information by overwhelming the systems to give themselves an opening to strike. To further discuss how this security issue works, we will look into a recent DDoS Attack that was made on a prominent code management service, GitHub, in 2018. The attack was done with the use of a strategy called mem caching where a spoofed packet is sent to a potential victim and then floods the server with aggressive traffic. During this, GitHub was hit with 129.6 million packets of data in its servers. This was considered one of the biggest DDoS attacks recorded. However, this attack only brought the company’s servers down for 20 minutes which was due to GitHub’s usage of a DDoS mitigation software. This shows how a precautionary measure, if taken, can help lessen the damage taken by an organization.

Moving on to privacy challenges, to delve deeper into the findings, phishing has been a more growing concern to the public especially during this unexpected time where the pandemic, COVID-19 **[55]**, is being faced by the whole population. With people staying at home and using wireless networks to stay connected with others, there is a possibility where people are more likely to not only socialize but work outside the normal privacy protections making them vulnerable and more susceptible to phishing attacks. To strengthen the case where privacy and security of one's device in a network are important, we will be discussing a recent attack that was made in relation to the pandemic.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 September 2020 doi:10.20944/preprints202009.0110.v1

This phishing attack targeted public sector employees in Mongolia by taking advantage of people being alert regarding coronavirus information [56]. The attack involved an email and word document disguised as being sent from Mongolia's Ministry of Foreign Affairs. The disguised file when opened will cause the installation of a malicious code that allows the hackers to remotely access and control the victim's device. The hackers can spy on the machine and steal sensitive data moreover direct further attacks. This justifies that being lax and unassuming of the potential privacy issues that could occur due to our negligence can prove devastating outcomes. Attackers have taken advantage of current coronavirus situation to launch cyberattacks and threats have increased during this pandemic [55].

5 Solution for Issues and Challenges

While technology evolves at a fast speed, the privacy issues and security issues in a wireless network [57] also emerge in an endless stream. However, no matter what the issues are, there have been solutions proposed by researchers and they continue to develop them according to the requirements. For example, in [58-60] authors have proposed detection of attacks in communication protocols used in internet of things networks, while in [61], RFID technology has been proposed to be used for secure attendance monitoring. In [62] authors have performed comprehensive analysis of privacy protection issues in cloud computing applications which can be used as a basis for development of secure solutions in the context of mobile cloud computing. Similarly many other studies have also been performed in specialist field contexts which are capable of providing awareness of security and privacy issues in current wireless network technologies, internet of things and communication protocols for these technologies [63], [64].

In client-based systems, firewall is an extremely useful tool to protect data. A firewall can be used as a software or hardware to provide a barrier between the client network and traffic from the Internet. By analyzing the incoming traffic based on the pre-setup rules, firewalls [65] can filter the traffic in order to block malicious traffic like malware and prevent hackers from accessing the entry point. Besides that, antivirus software is also an effective solution to solve the privacy and security issues. Antivirus software can detect and auto remove the virus and malicious software such as trojan horses, worms, spyware and ransomware. By real-time scanning the client network, it is able to safeguard against the potential vulnerabilities to happen. Apart from downloading antivirus and firewall software, keeping the software up to date is also a vital matter. Hackers are now getting smarter to design sophisticated issues, it is critical to update the software in order to combat them.

In server-based systems, Virtual Private Network (VPN) is an efficient tool for online business. It is able to strengthen security by securing and encrypting the data. It also assures private browsing and unrestricted access to content. By applying VPN, the traffic that goes through the Internet Service Protocol(ISP) will be encrypted by VPN protocols. Meanwhile, malicious intruders are unable to view and monitor them. While in a Client-server-based solution, the encryption-based solution will encrypt the information between the web hosts. Pretty Good Privacy (PGP) is an encryption-based protocol that addresses how to encrypt and decrypt the texts, files from emails. PGP uses symmetric and asymmetric keys to encrypt data. Meanwhile, the public key would be given from the receiver to whoever wants to send the message. While the recipients who have the private key can only be allowed to decrypt the message.

Moreover, thinking smart is also much more important as it can prevent identity theft which obtains personal information without acknowledgment of the users. It is necessary to be aware of and not to trust people who are unknown and share the personal information on social media accounts. There is no such thing as a free lunch, think smart and evaluating to the website that claims to offer benefits. In addition, enhance the strength of the access point to avoid security issues of MITM. By using WPA2 encryption alongside with the AES algorithm can prevent brute force attacks.

It is also essential to change the device name and password of the access point as malicious intruders can change the server and sadly even destroy the system.

6 Conclusion

Throughout our research, authors found that the security and privacy issues of wireless networks are constantly in the

increase but being taken lightly as we are continuing towards an age of technology that is ever changing notably during these unpredictable times where privacy and security of devices and networks are more sought after than ever. We believe that actions and efforts must be done and continue to be reinforced as cyber attackers are becoming more persistent and maturing. These cybercriminals are bombarding and injecting worry as well as fear into the unknowing public, becoming more forceful and knowing no fear since the intention of safeguarding privacy and security of wireless networks are not put as a priority enough within the related organizations. In our views, we believe that these issues can be overcome by the public if we take the necessary actions and move our approach to be more secure and also aware of the implications of leaving the challenges as they are without action. Concluding our views, we believe that with the right steps, a more protected system in our network can be attained. It is found that many privacy and security issues are still surfacing in the cyber world and that it is continuing to increase due to organizations' lacking resolve and the population's ignorance towards these current issues are becoming more visible. Furthermore, with the increased sophistication in the cybercriminals abilities prove to be a growing thorn in the cybersecurity efforts in maintaining a robust privacy and security system as well.

References

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

[2]. K. Ramesh Rao, "Wireless Communication Security and Privacy issues and Challenges", Academia.edu, 2017. [Online]. Available: https://www.academia.edu/34148630/Wireless_Communication_Security_and_Privacy_issues_and_Challenges. [Accessed: 04- Jul- 2020].

[3]. Alferidah, D.K. and Jhanjhi, N.Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.4, April 2020.

[4]. M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 481-487, doi: 10.23919/ICACT.2018.8323802.

[5]. 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.

[6]. B. Franklin, "Wireless Networking Security", Cs.bham.ac.uk, 2007. [Online]. Available: https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS7/Wireless%20Networking%20Security.htm. [Accessed: 04- Jul- 2020].

[7]. Y. Zou, J. Zhu, X. Wang, L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", Ieeexplore.ieee.org, 2016. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467419. [Accessed: 04- Jul- 2020].

[8]. A. Kavianpour, "An Overview of Wireless Network Security", Computer.org, 2017. [Online]. Available: https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNynJMDX/pdf. [Accessed: 04- Jul- 2020].

[9]. U. Wadhwa, "Wireless Network Security: Tough Times", Computer.org, 2015. [Online]. Available: https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNBRsVvm/pdf. [Accessed: 04- Jul- 2020].

[10]. L. Zhang, O. Oksuz, L. Nazaryan, B. Wang, A. Bamis, "Encrypting Wireless Network Traces to Protect User Privacy", Computer.org, 2016. [Online]. Available:

https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNzkMlSN/pdf. [Accessed: 04- Jul- 2020].

[11]. [31]. "2019 Cyber Attacks Statistics", HACKMAGEDDON, 2019. [Online]. Available: https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/. [Accessed: 05- Jul- 2020].

[12]. "The best academic search engines [2019] - Paperpile", Paperpile, 2019. [Online]. Available: https://paperpile.com/g/academic-search-engines/. [Accessed: 05- Jul- 2020].

[13]. "IEEE (Institute of Electrical and Electronics Engineers) Definition", Techterms.com, 2015. [Online]. Available: https://techterms.com/definition/ieee. [Accessed: 05- Jul- 2020].

[14]. "What is ResearchGate? Charlesworth Author Services", Cwauthors.com, 2016. [Online]. Available: https://www.cwauthors.com/article/WhatisResearchGate. [Accessed: 05- Jul- 2020].

[15]. G. Ijemaru, I. Adeyanju, K. Olusuyi, "Security Challenges of Wireless Communications Networks: A Survey", ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/324979423_Security_Challenges_of_Wireless_Communications_Networks_A_Survey. [Accessed: 04- Jul- 2020].

[16]. F. Lau, S.H. Rubin, M.H. Smith, "Distributed Denial of Service Attacks", Citeseerx, 2000. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.6999&rep=rep1&type=pdf. [Accessed: 04- Jul- 2020].

[17]. B. Felter, "5 of the Most Famous Recent DDoS Attacks", vXchnge, 2019. [Online]. Available: https://www.vxchnge.com/blog/recent-ddos-attacks-on-companies. [Accessed: 07- Jul- 2020]

[18]. K. Jindal, "Analyzing Spoofing Attacks in Wireless Networks", ResearchGate, 2014. [Online]. Available: https://www.researchgate.net/publication/261960458_Analyzing_Spoofing_Attacks_in_Wireless_Networks. [Accessed: 04- Jul- 2020].

[19]. T. Mores, "What is Spoofing? The Top 5 Examples You Need to Know", SoftwareLab, 2020. [Online]. Available: https://softwarelab.org/what-is-spoofing/#:~:text=Some%20of%20the%20best%2Dknown,three%20local%20banks%20in%20Florida. [Accessed: 04- Jul- 2020].

[20]. S. Behal, R. Arora, "IP Spoofing", ResearchGate, 2010. [Online]. Available: https://www.researchgate.net/publication/285112521_IP_Spoofing/link/565bf09608ae1ef929819af5/download. [Accessed: 04- Jul- 2020].

[21]. N. Tripathi, M. Swarnkar, "DNS Spoofing in Local Networks Made Easy", ResearchGate, 2017. [Online]. Available: https://www.researchgate.net/publication/320558120_DNS_Spoofing_in_Local_Networks_Made_Easy. [Accessed: 04- Jul- 2020].

[22]. A. Ahsan, J. Tsou, A. Mallik, M. Shahadat, "Man-in-the-middle-attack: Understanding in simple words", ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words. [Accessed: 04- Jul- 2020].

[23]. M. Agarwal and S. Nandi, "Advanced Stealth Man in The Middle Attack in WPA2 Encrypted WiFi Network", Citeseerx.ist.psu.edu, 2015. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1030.9452&rep=rep1&type=pdf. [Accessed: 05- Jul- 2020].

[24]. "What is SSL Stripping (MITM) ?", Secret Double Octopus, 2020. [Online]. Available: https://doubleoctopus.com/security-wiki/threats-and-tools/ssl-stripping/. [Accessed: 05- Jul- 2020].

[25]. S. Gangan, "A Review of Man-in-the-Middle Attacks", Arxiv, 2015. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf. [Accessed: 05- Jul- 2020].

[26]. "Man-In-The-Middle", Cs.du.edu, 2009. [Online]. Available: https://www.cs.du.edu/~ramki/downloads/papers/cloakPreprint.pdf. [Accessed: 05- Jul- 2020].

[27]. B. Tawo, "An Enhanced Sniffing Tool for Network Management", ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/332369942_An_enhanced_Sniffing_Tool_for_Network_Management_I_Background. [Accessed: 05- Jul- 2020].

[28]. "What are Sniffing Attacks and their types?", EC-Council Official Blog, 2020. [Online]. Available: https://blog.eccouncil.org/what-are-sniffing-attacks-and-their-types/#:~:text=Sniffing%20is%20the%20process%20of,are%20called%20network%20protocol%20analyzers. [Accessed: 05- Jul- 2020].

[29]. "Packet injection", Wikipedia, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Packet_injection#:~:text=Packet%20injection%20(also%20known%20as,of%20the%20normal%20communication%20stream. [Accessed: 05- Jul- 2020].

[30]. "Session hijacking Attack", OWASP Foundation, 2020. [Online]. Available: https://owasp.org/www-community/attacks/Session_hijacking_attack. [Accessed: 05- Jul- 2020].

[31]. "Session hijacking", Wikipedia, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Session_hijacking. [Accessed: 05- Jul- 2020].

[32]. A. Kumar, "Session Hijacking and Prevention Technique", ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/325117343_Session_Hijacking_and_Prevention_Technique/link/5c1a0e8c458515a4c7e9028f/download. [Accessed: 05- Jul- 2020].

[33]. P. Jougleux, "Identity theft and internet", ResearchGate, 2012. [Online]. Available: https://www.researchgate.net/publication/264437434_Identity_theft_and_internet/link/542eac1b0cf29bbc126f3b7a/download. [Accessed: 04- Jul- 2020].

[34]. K.B. Anderson, E. Durbin, M.A. Salinger, "Identity Theft", ResearchGate, 2008. [Online]. Available: https://www.researchgate.net/publication/4981808_Identity_Theft/link/00b495214d980c8024000000/download. [Accessed: 04- Jul- 2020].

[35]. M. Rouse, "What is Identity Theft and How to Prevent it?", SearchSecurity, 2020. [Online]. Available: https://searchsecurity.techtarget.com/definition/identity-theft#:~:text=Identity%20theft%2C%20also%20known%20as,numbers%2C%20to%20impersonate%20someone%20else. [Accessed: 05- Jul- 2020].

[36]. J. Sres, B. Brumen, "Brute-force and dictionary attack on hashed real-world passwords", ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/326700354_Brute-force_and_dictionary_attack_on_hashed_real-world_passwords/link/5c6b6504a6fdcc404ebadec1/download. [Accessed: 04- Jul- 2020].

[37]. M. Kumar, B. Kumar Mishra and T. Panda, "Predator-Prey Models on Interaction between Computer Worms, Trojan Horse and Antivirus Software Inside a Computer System", Pdfs.semanticscholar.org, 2016. [Online]. Available: https://pdfs.semanticscholar.org/444a/6405a6769e8dd95e7ce33db3ce7a5230b7ef.pdf. [Accessed: 05- Jul- 2020].

[38]. S. Yilmaz, “Adware: A Review”, ResearchGate, 2015. [Online]. Available: https://www.researchgate.net/publication/294709236_Adware_A_Review/link/56c30e8a08aee3dcd4163820/download. [Accessed: 04-Jul.-2020].

[39]. S. Kumar, "Phishing Challenges and Solutions", ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/322823383_Phishing_-_challenges_and_solutions/link/5acde9fa4585154f3f420911/download. [Accessed: 05- Jul- 2020].

[40]. B. Goyal and M. Bansal, "Type of Phishing Attack Detection Using Multi-Layer Neural Network", Pdfs.semanticscholar.org, 2017. [Online]. Available: https://pdfs.semanticscholar.org/6a9e/3cf21fe0c919719c454917dd6ab9c492661d.pdf. [Accessed: 05- Jul- 2020]. [Accessed: 05- Jul- 2020].

[41]. L. Irwin, "The 5 most common types of phishing attack", IT Governance Blog En, 2020. [Online]. Available: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack. [Accessed: 05- Jul- 2020].

[42]. D. T. Merritt, "Spear Phishing Attack Detection", Apps.dtic.mil, 2011. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA540272.pdf. [Accessed: 05- Jul- 2020].

[43]. M. Rouse, "What is whaling attack (whaling phishing)?", SearchSecurity, 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/whaling. [Accessed: 05- Jul- 2020].

[44]. "What is a Whaling Attack?", Kaspersky, 2020. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack. [Accessed: 05- Jul- 2020].

[45]. “Yahoo! data breaches”, Wikipedia, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Yahoo!_data_breaches. [Accessed: 04-Jul.-2020].

[46]. T. Nidecki, “All about Man-in-the-Middle Attacks”, Acunetix, 2019. [Online]. Available: https://www.acunetix.com/blog/articles/man-in-the-middle-attacks/. [Accessed: 04-Jul.-2020].

[47]. "An Invasive Spyware Attack on Military Mobile Devices", Check Point Software, 2020. [Online]. Available: https://blog.checkpoint.com/2018/07/05/an-invasive-spyware-attack-on-military-mobile-devices/. [Accessed: 04- Jul- 2020].

[48]. S. Ikeda, "The Phishing Scam That Took Google and Facebook for $100 Million", CPO Magazine, 2019. [Online]. Available: https://www.cpomagazine.com/cyber-security/the-phishing-scam-that-took-google-and-facebook-for-100-million/. [Accessed: 05- Jul- 2020].

[49]. C. Crane, P. Nohe, "The Largest DDoS Attacks in history", Hashed Out by The SSL Store™, 2020. [Online]. Available: https://www.thesslstore.com/blog/largest-ddos-attack-in-history/. [Accessed: 05- Jul- 2020].

[50]. K. Yedakula, "New Botnet Breaks the Record of the Biggest PPS DDoS Attack | Cyware Hacker News", cyware-social-nuxt, 2020. [Online]. Available: https://cyware.com/news/new-botnet-breaks-the-record-of-the-biggest-pps-ddos-attack-69aaa78d. [Accessed: 05- Jul- 2020].

[51]. J. Haworth, "IndiaMART data breach: 40,000 company records discovered on cybercrime forums", The Daily Swig | Cybersecurity news and views, 2020. [Online]. Available: https://portswigger.net/daily-swig/indiamart-data-breach-40-000-company-records-discovered-on-nbsp-cybercrime-forums?&web_view=true. [Accessed: 05- Jul- 2020].

[52]. P. Paganini, "230k+ Indonesian COVID-19 patients’ records for sale in the Darkweb", Security Affairs, 2020. [Online]. Available: https://securityaffairs.co/wordpress/105043/deep-web/indonesian-covid-19-patients-leak.html?web_view=true. [Accessed: 05- Jul- 2020].

[53]. "Korean credit card data leaked overseas, group reports | Yonhap News Agency", Yonhap News Agency, 2020. [Online]. Available: https://en.yna.co.kr/view/AEN20200608011200325?&web_view=true. [Accessed: 05- Jul- 2020].

[54]. M. Thelwall and K. Kousha, "ResearchGate and Google Scholar", Core.ac.uk, 2017. [Online]. Available: https://core.ac.uk/download/pdf/96707949.pdf. [Accessed: 05- Jul- 2020].

[55]. Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1

[56]. M. Ketchell, "Coronavirus pandemic has unleashed a wave of cyber attacks – here's how to protect yourself", The Conversation, 2020. [Online]. Available: https://theconversation.com/coronavirus-pandemic-has-unleashed-a-wave-of-cyber-attacks-heres-how-to-protect-yourself-135057. [Accessed: 07- Jul- 2020]

[57]. A. Rezgui, A. Bouguettaya and M. Eltoweissy, "Privacy on the Web: Facts, Challenges, and Solutions", Computer.org, 2003. [Online]. Available: https://www.computer.org/csdl/magazine/sp/2003/06/j6040/13rRUwd9CJP. [Accessed: 05- Jul- 2020].

[58]. A. Almusaylim, Z.; Alhumam, A.; Mansoor, W.; Chatterjee, P.; Jhanjhi, N.Z. Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things. *Preprints* 2020, 2020070476 (doi: 10.20944/preprints202007.0476.v1).

[59]. Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z. Jhanjhi (2020). Proposing a Secure RPL based Internet of Things Routing Protocol: A Review. Ad Hoc Networks, Volume 101. https://doi.org/10.1016/j.adhoc.2020.102096.

[60]. Fatima-tuz-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.

[61]. Khan, A., Jhanjhi, N.Z. and Humayun, M. (2020). Secure Smart and Remote Multipurpose Attendance Monitoring System. EAI Endorsed Transactions on Energy Web.

[62]. 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

[63]. Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 45, 3171–3189 (2020). https://doi.org/10.1007/s13369-019-04319-2

[64]. Seungjin, L., Abdullah, A. Jhanjhi, N.Z. (2020). A Review on Honeypot-based Botnet Detection Models for Smart Factory. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 6, 2020.

[65]. K. Salah-ddine, "Overview Of Firewalls", ResearchGate, 2017. [Online]. Available: https://www.researchgate.net/publication/315614367_Overview_Of_Firewalls_Types_And_Policies_Managing_Windows_Embedded_Firewall_Programmatically. [Accessed: 05- Jul- 2020].