 doi:10.20944/preprints202008.0523.v1

Security and Privacy Issues in Wireless Networks

1st Nurul Fatini Azhar
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
nurulfatiniazhar@sd.taylors.edu.my

2nd Ngoo Qi Jie
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
ngooqijie@gmail.com

3rd Kim Tae Hyun
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
kimtaehyun@sd.taylors.edu.my

4th Kohei Dozono
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
koheidozono@sd.taylors.edu.my

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

Abstract—**Communication between devices has transitioned from wired to unwired. Wireless networks have been in use widely around the globe since the advent of smartphones, IoT devices and other technologies that are compatible with wireless mode of communication. At the same time security issues have also increased in such communication methods. The aim of this paper is to propose security and privacy issues of the wireless networks and present them through comprehensive surveys. In context of security issues, there are 2 typical DDoS attacks - HTTP flood and SYN flood. Other than DDoS attacks, there are several other threats to wireless networks. One of the most prevalent include security issues in Internet of Things. In terms of privacy issues in a wireless network, location-based applications, individual data, cellular network and V2G (Vehicle to Grid) network are surveyed. The survey is hosted using questionnaire and responses of 70 participants is recorded. It is observed from the survey results that many groups of people lack the knowledge of security and privacy of wireless technologies and networks despite their increased use, however, students are relatively more aware and have strong knowledge of those issues. It is concluded from the results that an effective solution to these problems can be hosting campaigns for spreading the security and privacy laws to help the groups of people who are lagging behind in this domain of knowledge become more aware. A unique solution is also presented to overcome the security issues which include implementation of detection and mitigation techniques, implementing Blockchain in the IoT devices and implementing fog computing solutions. The unique solutions to overcome the privacy issues are proposed in the form of a privacy approach from the LBS server between pairs of users to increase the implementation of DSPM and blockchain as a solution.**

Keywords— Wireless networks and communication, Security issues, HTTP flood attack, SYN flood attack, Internet of Things, blockchain

I. Introduction

It is remarkable that the first wireless technology was invented in 1800s [1] but this was limited to wireless telephone technology alone. At that time only the conversation over the phone could be held, no transmission or connection to the internet was possible. However, since the advent of the smartphone, wireless networks began to be used widely around the world [2]. Connecting to wireless network has made life more convenient and comfortable. Unlike the day when we had to use fiber cable to access the internet and laptops were not completely portable, now in the modern days it is possible to see how the world goes around on the internet even while walking. Finally laptops and phones have become utterly free from cables. However, on the opposite side of the internet world, hackers are eager to abuse this new technology. They dig and use the security weaknesses in wireless communication which takes place over wireless networks to instigate attacks.

What is networking in computer science? Networking is a group of devices that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes [3][4]. A wireless networking enables users to communicate with other devices without wires, which means that every device which connects to the internet can transmit and receive data like PCs do. This also can be translated as that every device connected to the internet can be exploited since they use the same protocols to communicate. The possibility that the data can be leaked has not only doubled, but tripled and more.

According to statistics, mobile threats such as malware have increased since 2018 and 2019 [5]. Furthermore, 24,000 average number of malicious mobile apps are being blocked each day. Some apps intend to leak the users' sensitive information such as phone numbers and device location. There has been a dramatic increase in attacks against IoT devices which are interconnected for communication hence posing larger threat surface area and possibility of attacks [6-8], which is found to be an overwhelming 600 percent. Additionally, what wireless networks and IoT have made possible is generation and sharing of huge amounts of data. For example, users can share what they like, where they often go, their hobbies, where they have been and so on. Moreover, in the medical field, many IoT devices have already been utilized in various domains, such as smart logistics and transportation [9], in digital governance [10], in smart factories [11], in healthcare domain [12] for patients so as to provide efficient as well as accurate treatment, smart cities [13] and more. Furthermore, 5G technology [14] is developing rapidly and it enables to solve

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

problems such as automated driving and telemedicine, traffic accidents, and medical countermeasures in underpopulated areas [15][16]. In addition, remote monitoring will become possible through the linkage with the IoT, which is expected to improve business efficiency in a wide range of fields [17]. There is no doubt that 5G will allow more devices than ever before to be connected to the wireless network, and will rapidly evolve the systems and services we've seen in the past.

It is observed that aforementioned improvements in technology have made our life convenient. However, they have also led to insecure transmission of huge amounts of sensitive data causing security and privacy issues. It is therefore a security engineer and related stakeholders' job to prepare beforehand and expect humongous range of transactions with privacy data on the wireless network and manage them securely in order to prevent threats from malicious intents. Therefore, in this paper, an in-depth study of the security and privacy issues in terms of wireless networks is performed. In the next section, existing issues are explored in the wireless network domain. This is followed by surveys for collection of relevant data in terms of data security and privacy law awareness in various groups of people. Next, an in-depth discussion on the finding of this study is presented. Moreover, unique solutions for those described issues are presented followed by concluding remarks.

II. Literature Review

A. *Security*

There are uncountable traffics transmitted in the networking world. A giant company such as Google generates a huge number of network traffic. According to research, 228,000,000 searches are done per day. The number of traffic Google generates is expected to be much higher than that [18]. Nevertheless, no one worries about Google's server because it is an acceptable figure for Google and their server can stand with it. However, what will happen if a small scale business receives 228 million traffics per day? Will that be okay? Is that normal? In this case, we consider it a Denial of Service(DoS) attack. A DDoS attack is a malicious attempt to disrupt normal traffic of a targeted server, service or even network by sending an overwhelming number of traffic[19][20]. It can also exploit machines including computers and other networked resources such as IoT devices. But how does a DDoS attack work? As the name said, it is a distributed attack, which means it requires many devices. In order to conduct this attack, the attacker may need to infect other machines with malware, turning each one into a bot [21]. Once the machine is infected, the attacker then has control over the group of bots, which is called a botnet. The DDoS attack is conducted in various ways and we can categorize it by the OSI model. Open Systems Interconnection (OSI) model is a conceptual model created to visualize communication in networking [22]. As it can bee seen in Fig. 1, there are 7 layers in the OSI model [23].

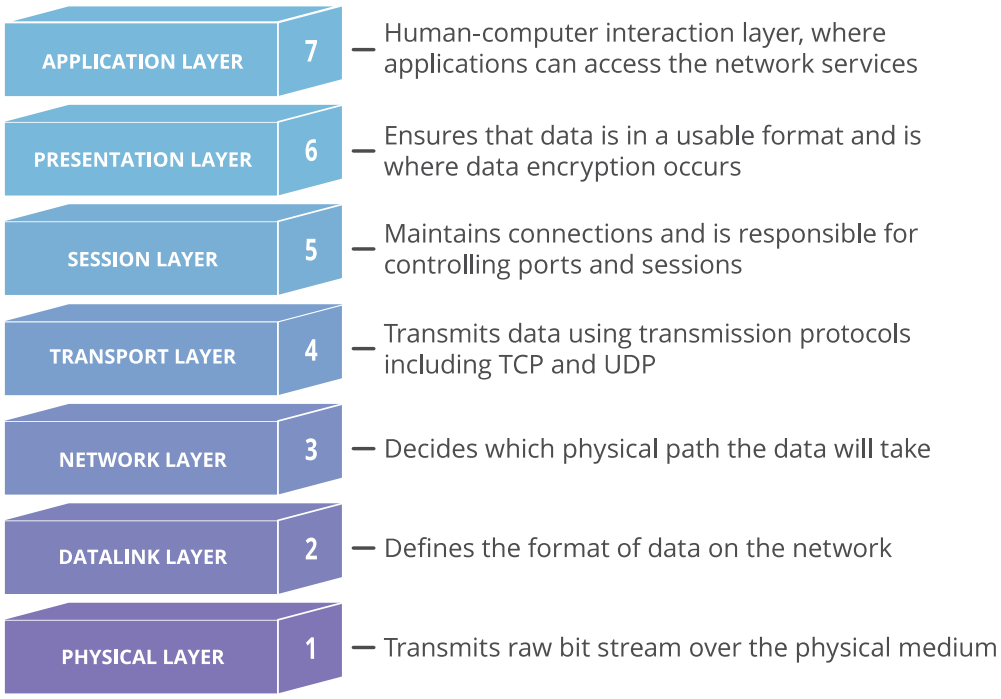

Figure 1: OSI model [23]

There are two typical DDoS attacks – HTTP Flood (Fig. 2) and SYN Flood (Fig. 3). They are conducted in Layer 7 and Layer 4 respectively. When we enter a website, our browser sends a GET request. As the website gets our request, it decides whether it accepts the user or not. In other words, the webserver has to respond to every GET request. This is where hackers aim for. If the infected bots send GET requests more than the webserver could handle, the server will shut down.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

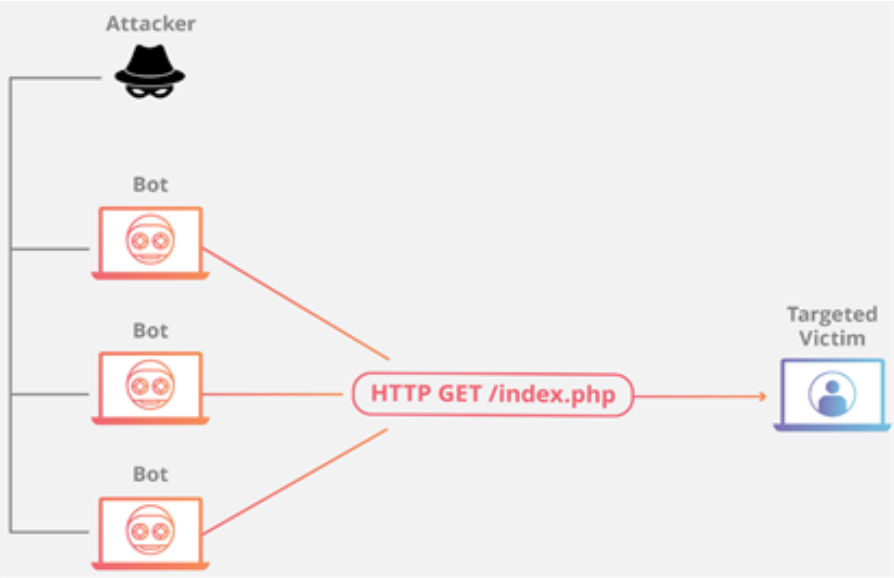

Figure 2: HTTP Flood [23]

SYN Flood is similar to HTTP Flood attack except for the fact that it is conducted in Layer 4. Before client and server communicate, they firstly have a handshake to see whether the opposite side is up or not [24]. This is called 'TCP handshake'. The client sends SYN packet and if the server is up, the server will send SYN/ACK packet then the client will send ACK packet ending up the conversation. This also, similar to the previous one, has a vulnerable point, which is that the webserver responds to every SYN packet it receives. Likewise, if the server gets more SYN packets than it can handle, the server will shut down and be unavailable.

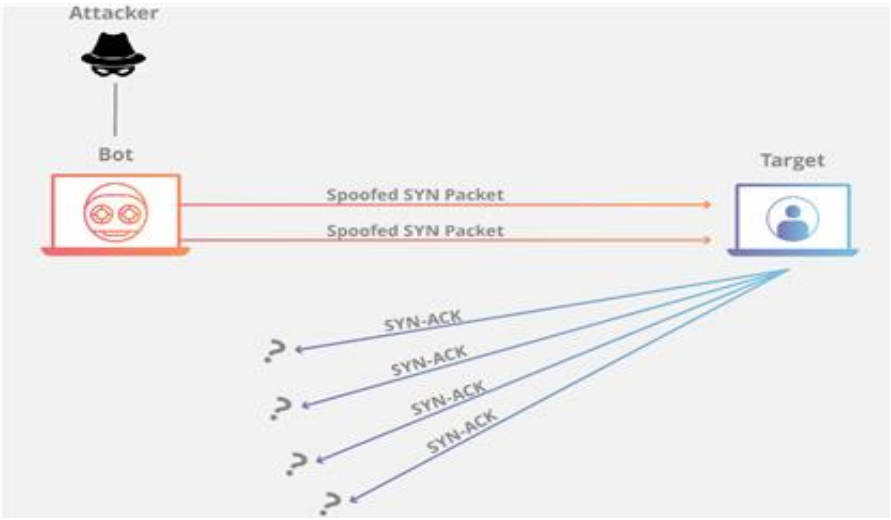

Figure 3: SYN Flood [23]

These days, it is almost impossible to talk about networking without mentioning IoT. IoT is a network of devices and things which are interconnected forming a system that has the ability to communicate with other without human intervention [25]. This technology has made life easier since the machines under the network operate automatically. However, this technology could also throw security challenges. Once one of the machines under the network is exploited, the whole machine could be affected. In the following, we are going to see what major security challenges IoT environments has.

Since wireless network machines are not connected with physical cables, it has a higher possibility for hackers to intercept the data in the middle. This is why authentication plays a more important role in IoT than other networks. However, in the IoT environment, many IoT devices lack memory and CPU power to calculate cryptographic operations [26][27]. Many wireless devices such as our smartphone or laptop use complex cryptographic operations to authenticate protocol so that no one can steal the data. Since lack of memory and CPU power, IoT devices have no other choice but using a relatively simple cryptographic algorithm to authenticate. This is a big problem because some symmetric cryptographic algorithm can be cracked.

This problem can be solved by outsourcing expensive computations to another device which has enough memory and CPU power. The thing is, however, it does not scale well for IoT systems. IoT is implemented not only in a company or factory but also in our daily life. Nowadays electronic companies have released household electrical appliance with IoT technology

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

implemented. These machines are neither equipped with good memory and CPU power nor outsourcing machine. Therefore, it cannot be said that the problem has been totally solved.

Next challenge is 'Rogue Node'. We call devices as nodes in networking. Rogue node is a device which is installed maliciously to access the database or crack the whole system [28]. Fig. 4 shows how devices are connected and retrieve data.

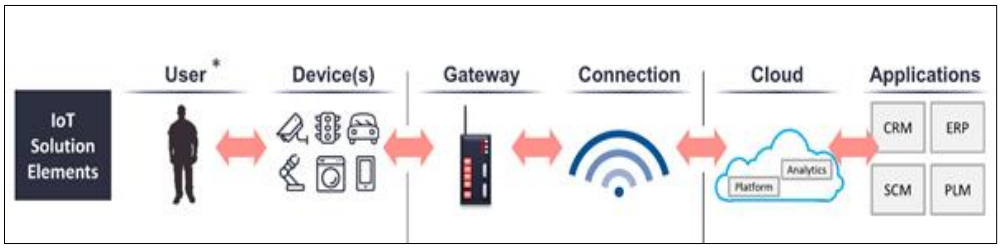

Figure 4: How IoT works [29]

B. Privacy

Nonlinear time-series analysis (NTSA) refers to methods that extract dynamical information, mainly complexity measures, from complex non-linear systems. Because the brain is a complex dynamical system exhibiting chaotic behaviour in which nonlinearity is introduced at neuronal level, NTSA of the EEG is a much better alternative to study different functional activities of the brain and neurological disorders, AD and MCI in the context of this study, and can provide a better insight into abnormal EEG dynamics. Moreover, it is a very relevant in method in complexity analysis of EEG time series.

Location: The authors proposed the privacy issue of location data. Location-based service is to get location information of the mobile and to offer location-based services to the mobile on the wireless network [30]. The well-known dominant mOSNs such as Facebook, YouTube, Twitter have been rising rapidly both in size and popularity due to the growth of Internet technology [31][32]. Users can easily exchange information in these conventional online social networks, and share forums, videos, photos, etc. When mOSNs and location-based services are merged together, mOSNs can provide several location-based services such as the query near friends, "check-in," and simple location sharing [33]. For example, users may use the "check-in" services to get some preferential service. Additionally, users may query their friends and strangers who are close to the current position and obtain information about their location. We draw a significant number of users from startup operations after Facebook merged with location-based services, and the number of users is still increasing rapidly. Location-based service (LBS) is one of the most critical components of mOSNs providing users with services based on the mobile device's geographic location [34]. With mobility and the world's Internet connectivity ever-present, vast numbers of users take advantage of LBS to demand information based on their location. Users can ask the nearest hospitals, stores, bars, and so on in LBS, which offers a lot of comfort for users. As LBSs and mOSNs become increasingly popular, many new services are spawned, such as recommendations on friends and travel routes. However, there are also other issues that need to be overcome. Location knowledge is one of the most valuable user rights and is therefore of great importance. For example, if mOSNs collect a lot of location information from users, they will give it to third parties because of the commercial intent, which would compromise the privacy of the location of users. However, as the more advanced methodology is used, more confidential information may be derived from the position details. For example, attackers may make a guess which school user is studying at. Additionally, the attacker may be able to deduce that if the user searches the nearest bars on the Internet frequently, he/she is a heavy drinker. The privacy of the location includes published location information time, space position, and position service request material. In particular, spatial location is the most concerning problem of privacy of location in mOSNs. Knowledge about the geographical position of users primarily relates to the spatial location, which is one of the main concerns.

Individual Data: The authors in [35] have explained the data privacy issue in terms of individual data with healthcare applications using wireless network technology [35]. Recently, advances in wireless technology and ICT (information and communication technology) systems have allowed the health care sector to quickly and efficiently track and implement a range of solutions and health services. Progressed ICT systems should be able to communicate administration of medicinal services to patients in healing facilities and clinical attention, as well as in their homes and work environments, along these lines providing expense reserve funds and improving individual patient fulfilment. Sensors are used to gather a patient's sensitive and important medical information or can be used in sports as well. WBANs connect with the network and other devices such as ZigBee, WSN, WI-FI, Bluetooth, Wireless Personal Area Network (WPAN) technology. The sensor gathers patient-related data, uses various technologies to move it to the cloud, the doctor uses this data or information, and so on. It can contribute to many risk factors when data is exposed to unauthorized individuals (persons), and an individual's medical information is a very sensitive subject, and can only be accessed by an authorized person. For instance, the effects may range from inadequate treatment of patients to violations that debilitate patients' lives on the off chance that the knowledge is contaminated or confiscated.

Cellular Network: The authors in [36] have raised the privacy issues of cellular networks, especially 5G mobile networks (Fig. 5). Based on recent developments in wireless and networking technologies, such as software-defined networking and virtualization, the next-generation wireless network technology is being developed as shown in the below figure. Compared to 4G technology, 5G is distinguished by much higher bit rates of more than 10 gigabits per second as well as more bandwidth and very low latency, which is a big advantage to the trillions of connected objects in the Internet of Things [37] setting. By creating various new network services such as mobile fog computing, car-to-car communications, smart grid, smart parking, named data

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

networking, blockchain-based services, unmanned aerial vehicle (UAV), etc., 5G will enable a fully mobile and connected society in the IoT era. Telecommunications firms, therefore, agree that 5G will begin commercialization in 2020. In a 5G world, the combination of various wireless technologies and service providers that share an IP-based core network would provide mobile users with the ability to move between networks and technologies to maintain a high level of service quality (QoS) [38]. Fast vertical transfer and general network accessibility make designs susceptible to multiple vulnerabilities such as access control, communication protection, data privacy, availability a well as privacy [39][40]. Furthermore, As mobile devices are connected to the network all the time, they will get a notion of social nodes through the vertical handover. These nodes can be monitored more easily and are more vulnerable in different forms of attacks, such as impersonation, eavesdropping, man-in-the-middle, denial of service, replay attack, and repudiation attack [41].

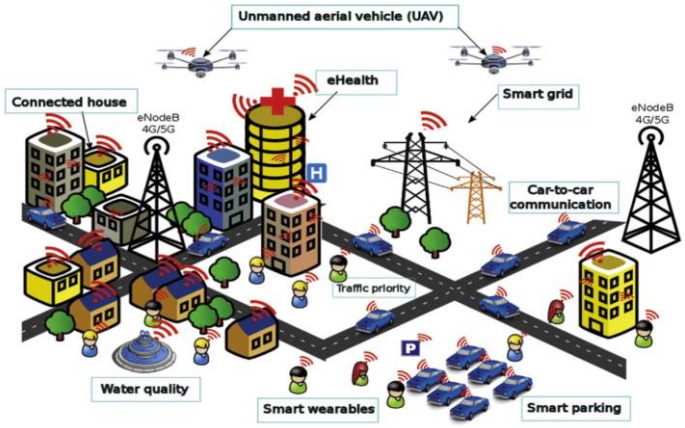

Figure 5: The overview of 5G network [36]

V2G (Vehicle to Grid) Network: The authors in [42] have presented the privacy issues in Vehicle to Grid (V2G) networks Fig. 6 shows the V2G network framework and components. The electric vehicle (EV) uses electricity instead of gasoline in a V2G network, and this protects the atmosphere and helps alleviate the energy crisis. The vehicle will temporarily act as a distributed energy storage device by using its battery capacity to reduce the peak power grid load. Yet the two-way contact and power flow not only facilitate V2G network connectivity but also encourage attackers. Privacy now poses a significant barrier to the growth of V2G networks. Although the two-way communication and energy flow greatly increase the performance, reliability, and versatility of V2G networks, they also pose major security concerns and privacy protection challenges. In conventional power systems, metering data is usually read on a monthly basis, but in smart grid, more granular and accurate data on energy usage are read using smart meters about every 15 min or less. These data could potentially expose a large amount of customer personal information, including energy usage patterns, types of household appliances, the number of people in a household, along with their schedules or activities. Problems with privacy protection are more difficult in V2G networks than in other smart grid networks [43], such as location-fixed HAN. Compromising an appliance in your house is much harder for an adversary than compromising a charging spot or a LAG deployed along the lane. In addition, a vehicle can frequently join or depart a network due to e-mobility, whereas an appliance in your home is always in its network. Thus, if a fake appliance joins the network a detector can easily detect two identifications (IDs) of the same value.

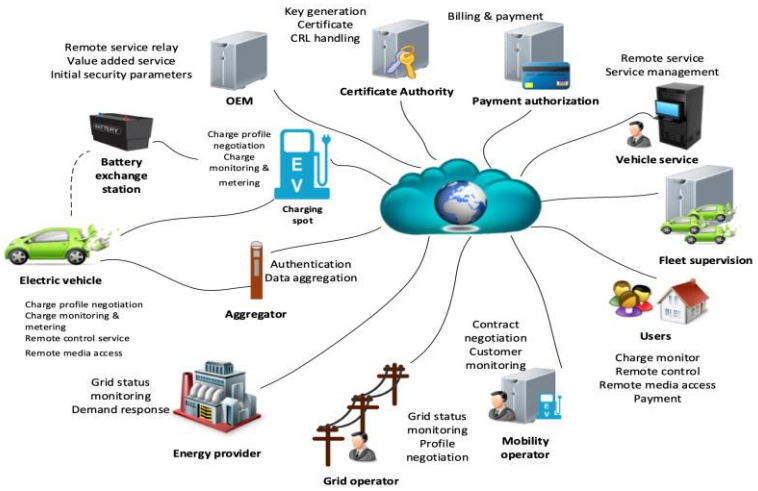

Figure 6: V2G networks framework and components [43]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

III. Survey Methodology

In this survey, there are two ways that are used to collect our information and data. The first method to collect data is online sources which are journals, websites, and other types of reliable sources. The motive of having sources from other authors or websites is to follow up on the trend of investigating different categories. Other than that, the sources are also reliable, especially on the practical aspect.

The second method that is used to collect data is a questionnaire survey is conducted to achieve the goals of unique finding. The questionnaire is to test the participants' knowledge of security and privacy on the wireless network. There will be a total of 70 participants who answer the questionnaire. The questionnaire survey is successfully spread with the help of social media. There will be a total of 4 questions on basic information of the participants and 6 questions to test the knowledge of security and privacy on the wireless network of each participant.

The four questions in Fig. 7 show the basic information of the participants. All the categories are the ones that have a different level of knowledge. For example, teenagers are not concerned about privacy of their data [44][45][46][47][48]. Fig. 8 and Fig. 9 present survey questions on security and privacy issues in wireless networks, respectively.

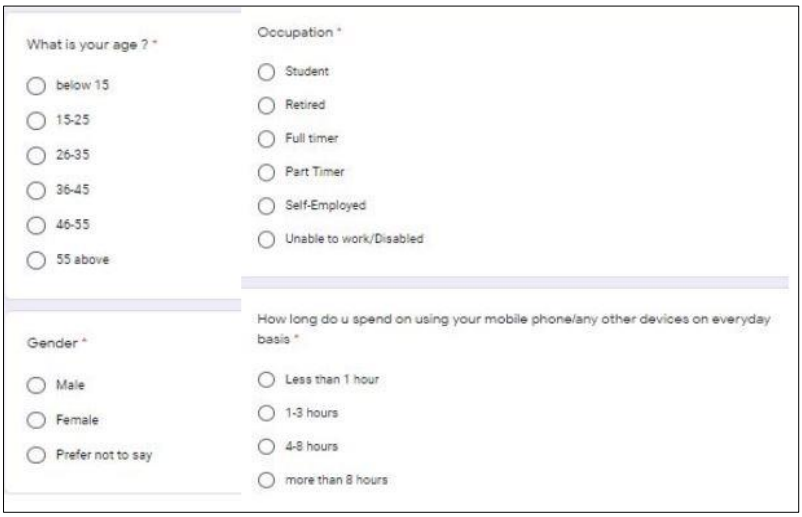

Figure 7: Image of basic info questions

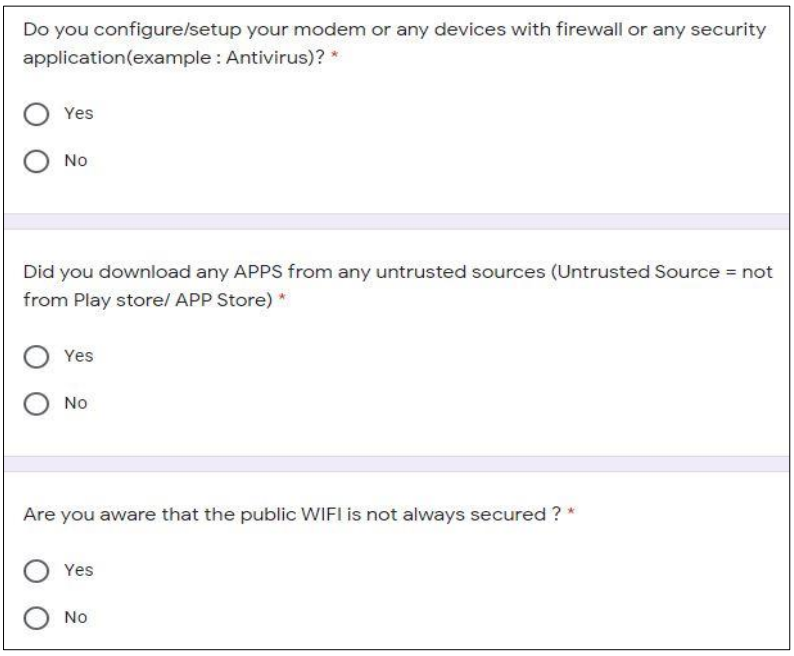

Figure 8: Image of 3 questions regarding security issues in wireless network

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

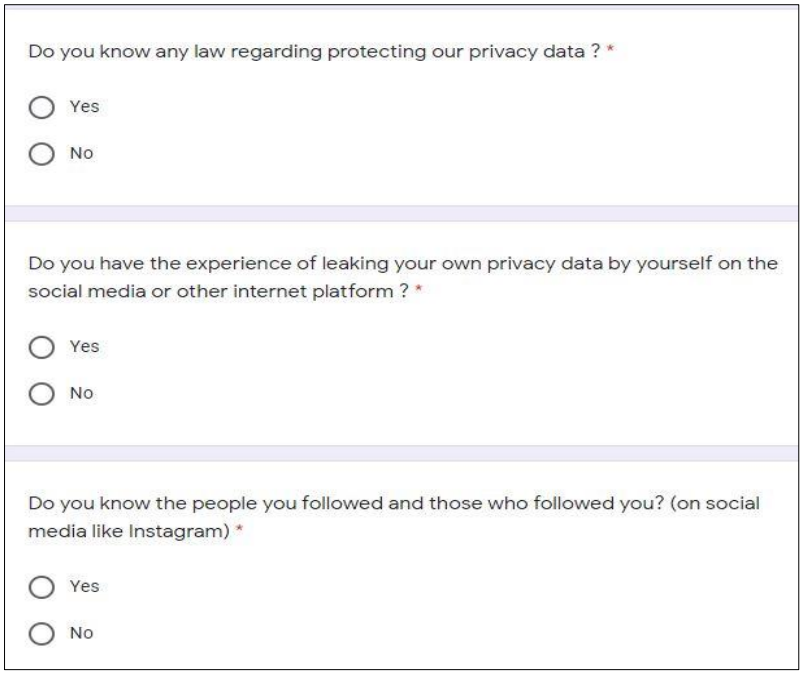

Figure 9: Image of 3 questions regarding privacy issues in wireless network

IV. Discussion of Results

The section is dedicated to test knowledge and awareness of data protection laws and measures to be taken for secure data communication among various groups of people. The 6 questions are divided into 2 parts in which 3 related to security issues and another 3 related to privacy issues. The questions above mostly are the factors of how security or privacy issues are created.

Fig. 10 represents the study between the gender and age variable and the output value of whether the participants have experience of leaking their data on social media. From the image, the information that can be concluded is that females have much less experience of leaking their own private data to social media. But for female, as the age is between 36-45, the amount of having the experience of leaking their own private data have been exceeded. The image also shows that males have a large amount of leaking privacy data experience from age of 15-45. The age of 26-35 for males has the biggest gap between the amount of experience and non-experience.

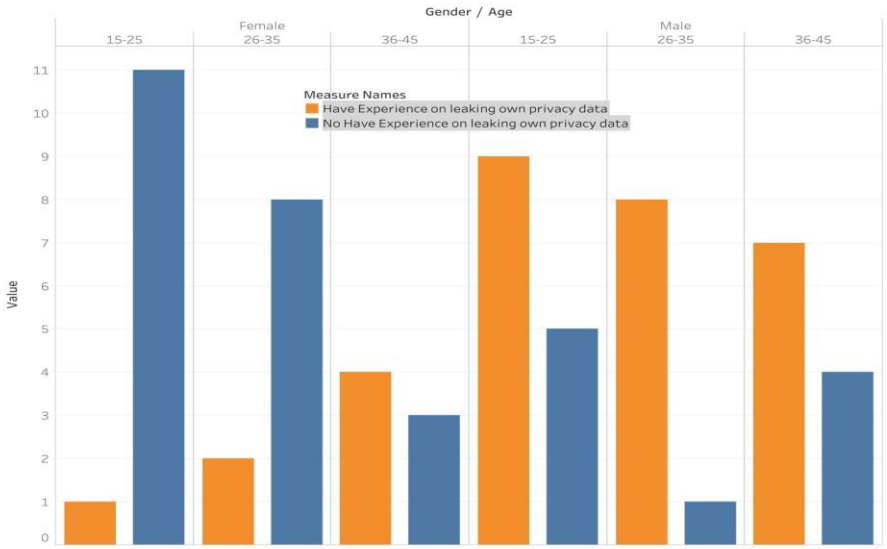

Figure 10: Bar chart representing leaking data

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

Fig. 11 shows the relationship between gender and time spend on the phone and the dependent variable of whether the participants downloaded untrusted software. The participants spend less than one hour on their devices have a larger amount of download software from untrusted sources. The male has the largest amount of download software from trusted sources and untrusted sources with the condition of spending more than 8 hours on their devices.

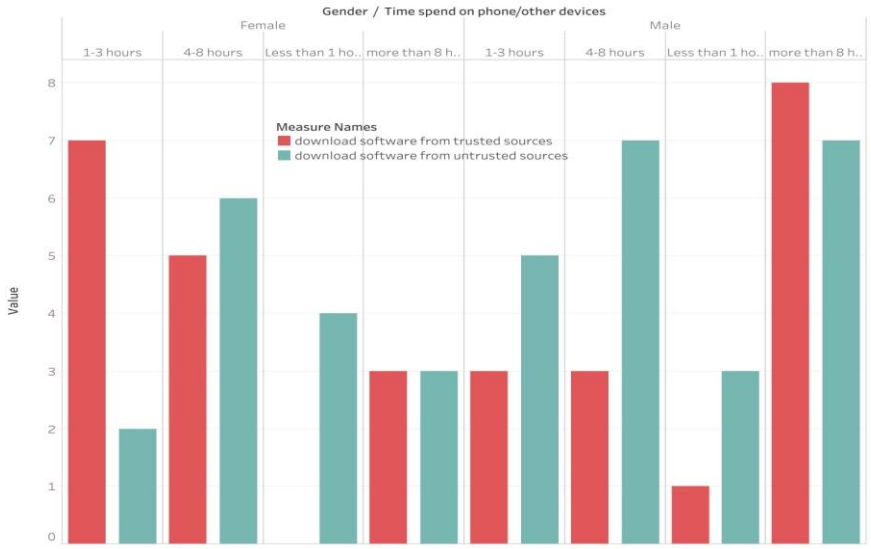

Figure 11: Bar chart representing the downloading of trusted versus untrusted software

Fig. 12 shows the study between gender and occupation and the awareness of participants to the security of public WIFI. The results can conclude that the students and self-employment have a higher amount of awareness compared to other occupations.

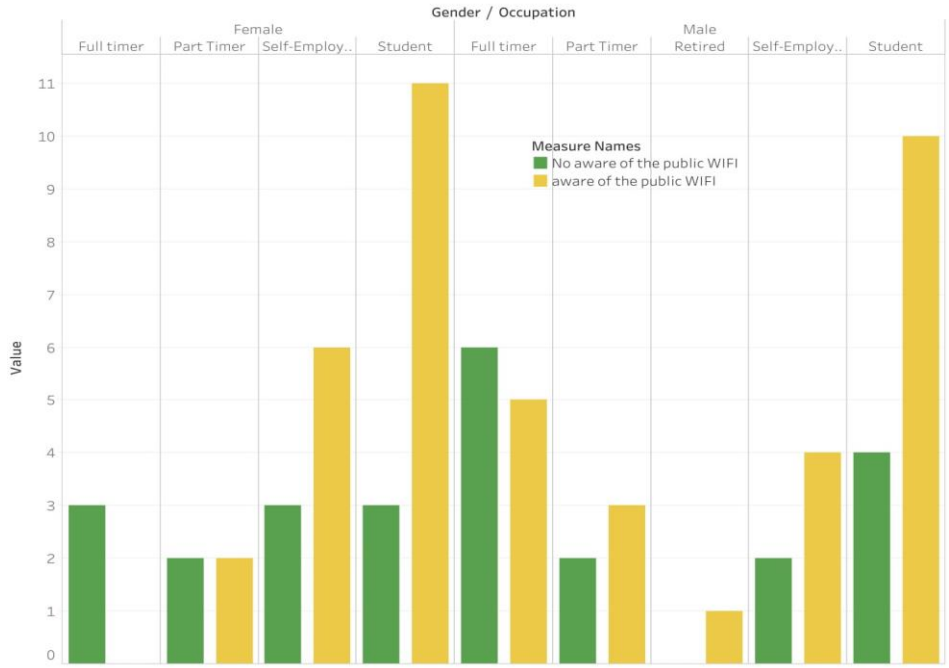

Figure 12: Bar chart illustrating awareness level of the security of public WIFI

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

Fig. 13 shows the relationship between gender and time spend on the phone and the awareness of knowing someone that is following you or you followed on the social media platform. The results can conclude that males have more awareness compared to females. The females have a weaker awareness of social media "friends" as the time spends on their devices is higher.

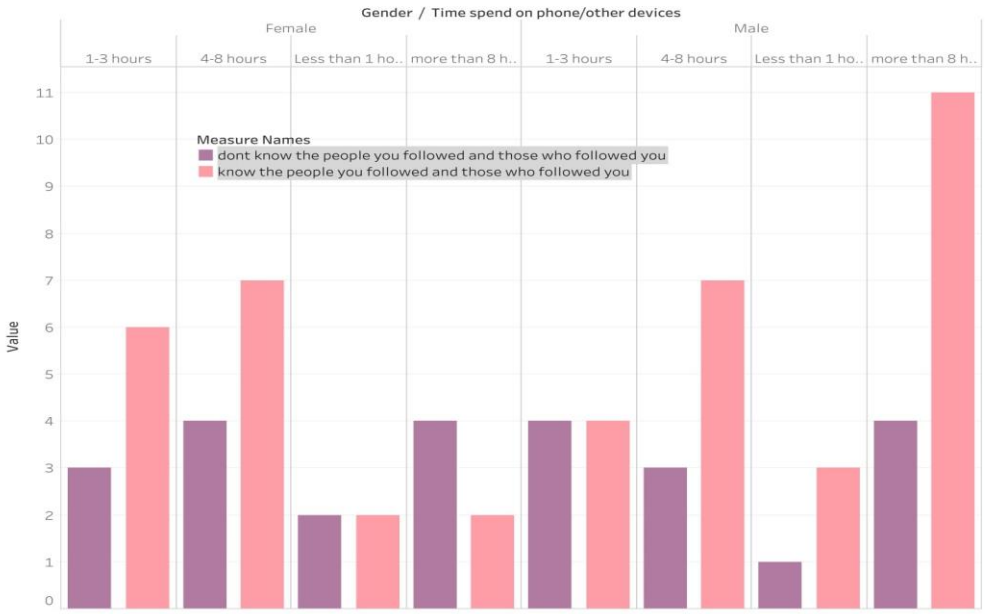

Figure 13: Bar chart represesnting the awareness levels of social media “friends” in males and females

Fig. 14 shows the study of the independent variable of occupations and time spend on devices and the dependent variables of knowing any law regarding protecting private data. The results that can be concluded are full-timer and students have more awareness of the laws on protecting data.

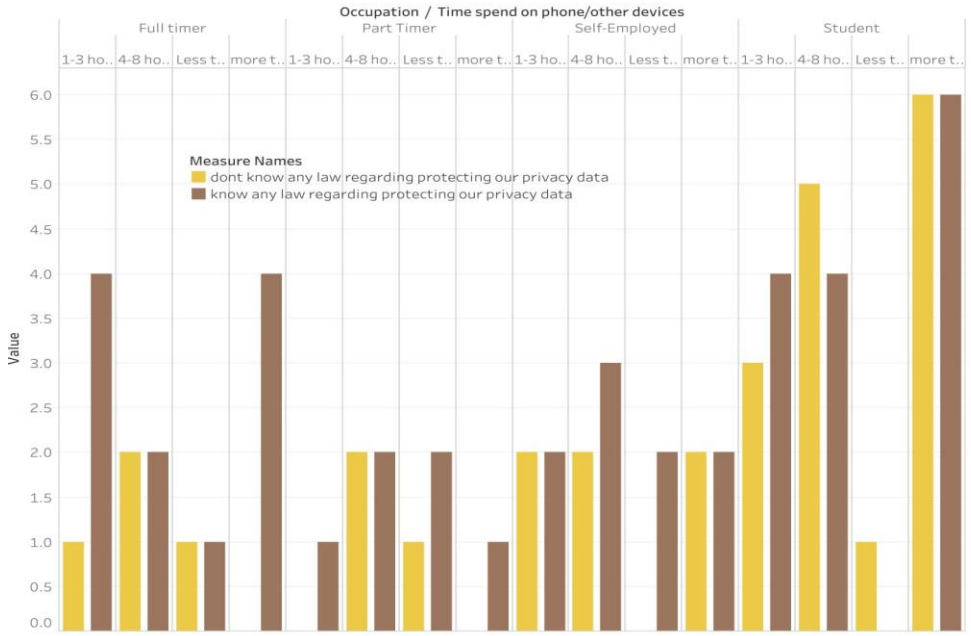

Figure 14: Awareness level in context of data protection laws

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 August 2020 doi:10.20944/preprints202008.0523.v1

Fig. 15 shows the study of the independent variable of occupations and gender and the dependent variables of whether the participants configured any security software on their devices. Most full-timers did not configure any security software on their devices. While students have the awareness to configure security software on their devices

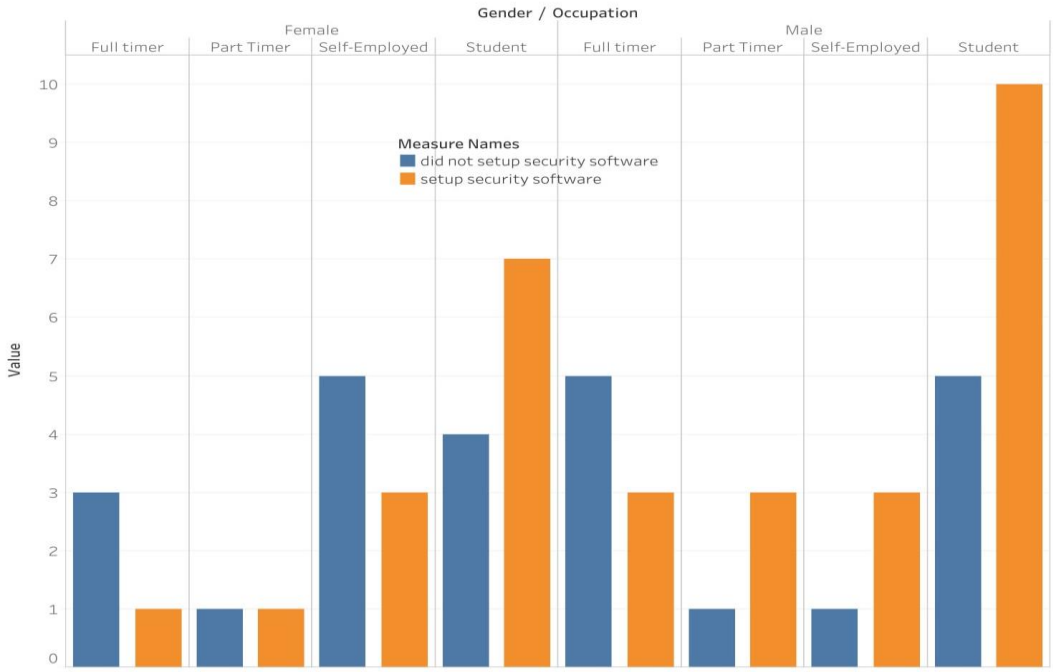

Figure 15: Bar chart illustration of whether the participants configured any security software

V. Unique Solution

The issues about the security and privacy of wireless networks that were discussed in the Literature Review section have given insight to users on what issues can be found in this type of network. The issues in security can be grouped into two categories which are DDoS attack and IoT. The DDoS attack can be prevented by implementing the detection and mitigation techniques to detect insider and attackers [44-46]. It would study the networks and detect the attackers and will blocking or dropping the malicious traffic [44][45]. The security issue in IoT can be solved by implementing Blockchain to the network [47][48]. Blockchain will prevent unauthorized access via communicating through encrypted public and private keys. Thus, it will prevent attackers from attacking the IoT devices [47][48]. The fog computing could be implemented to the IoT devices to avoid rogue node and node capture attack store the data in locally [47].

The privacy issues in wireless networks can be grouped into four categories which are location, individual data, cellular network and V2G network. Yamin et. al. proposed a privacy approach from LBS server between a pair of users to increase the privacy [49]. which led the LBS to be unable to collect accurate information about these users. Next, individual data could be prevented by implementing DSPM which is a system that allows personal data exchange while enhancing individual control and data discovery [50]. The privacy issue for cellular networks can be increased by implementing blockchain schemes to the cellular network [51]. V2G network privacy issues can also be solved by implementing blockchain to preserve the payment mechanism [52].

The results from the unique finding on the survey are :

- Females have lesser experience of leaking their own privacy data.
- For female, the higher the time spend on devices, the lower awareness on social media "followers/ following"
- Males spend more than 8 hours on their devices and have a big chance to download software from untrusted sources.
- Most self employees and students have an awareness of the security of public WIFI.
- Most Full-timers and students are more aware of any law regarding protecting privacy data.
- Most full-timers did not configure any security software on their devices, most students have configured security software on their devices.

Firstly, the focus group will be on the female that spends plenty of time on their phone especially on social media. This group will lack knowledge on the privacy issues on the wireless network. Then, Males and full-timers are the other groups to focus as well. Full-timers and Males that spend plenty of time on their devices have a larger chance to have a lack of knowledge on the security issues on the wireless network. Basically, the solution to these problems is to have a campaign focus on these groups on gaining knowledge of privacy and security issues

VI. Conclusion

In conclusion, it is observed that wireless networks play an important role in the lives of people around the world in context of ease of communication that it provides. However, it also poses security threats which can violate privacy at individual and organizational level. The criminal activity has increased since the advent of wireless communication medium and technology which supports such communication. This has also led to manipulation of data generated by devices which run on wireless networks such as IoT which are originally implemented in their insecure form, leading to increase in cybercrimes. The security and privacy issues of wireless networks should be the addressed along with the awareness among people of all age groups who use these technologies. People and organizations should be aware of the solutions and precautions that they can take to increase the security and privacy of their devices which are running on wireless networks such as implementing the blockchain to the IoT devices and other detection and mitigation techniques. From the findings through the surveys carried out, the effective solution to solve the problem is to focus on the people who have a higher spending time on devices or social media. Another group of people to be focused on is full-time workers who use these technologies. It is essential to create campaigns, whether online or onsite, to help them gain technical knowledge on the issues in wireless network from security perspective. It is also observed that the students have a better understanding and relatively good knowledge of security issues which can lead to data manipulation by attackers and therefore, they tend to be more careful when using their devices. However, there is a need of increase in awareness strategies and training to educate other groups of people so they can use their devices securely.

References

[1]. “History of Wireless Communications", Microwavejournal.com, 2020. [Online]. Available: https://www.microwavejournal.com/articles/24759-history-of-wireless-communications. [Accessed: 08- Jul- 2020].

[2]. A brief history of the smartphone", Science Node, 2020. [Online]. Available: https://sciencenode.org/feature/How%20did%20smartphones%20evolve.php. [Accessed: 08- Jul- 2020].

[3]. C. DNA, "What Is Computer Networking?", Cisco, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html. [Accessed: 08- Jul- 2020].

[4]. What is a Computer Network?", Fieldengineer.com, 2020. [Online]. Available: https://www.fieldengineer.com/blogs/what-is-a-computer-network. [Accessed: 08- Jul- 2020].

[5]. Phishingbox.com, 2020. [Online]. Available: https://www.phishingbox.com/assets/files/images/Symantec-Internet-Security-Threat-Report-2018.pdf. [Accessed: 07- Jul- 2020].

[6]. Humayun, M., Jhanjhi, N.Z., Alsayat, A. and Ponnusamy, V. (2020). “Internet of things and ransomware: Evolution, mitigation and prevention”, Egyptian Informatics Journal, 2020, https://doi.org/10.1016/j.eij.2020.05.003.

[7]. 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.

[8]. Almusaylim, Z.A., Zaman, N. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless Netw 25, 3193–3204 (2019). https://doi.org/10.1007/s11276-018-1712-5

[9]. M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, "Emerging Smart Logistics and Transportation Using IoT and Blockchain," in *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 58-62, June 2020, doi: 10.1109/IOTM.0001.1900097.

[10]. Khan A., Jhanjhi N.Z., Humayun, M. and Ahmad M. (2020).”The Role of IoT in Digital Governance”, in Employing Recent Technologies for Improved Digital Governance DOI: 10.4018/978-1-7998-1851-9.ch007

[11]. Seungjin L., Azween, A. and Jhanjhi, N.Z. (2020). “A Review on Honeypot-based Botnet Detection Models for Smart Factory”, International Journal of Advanced Computer Science and Applications. 11. 10.14569/IJACSA.2020.0110654.

[12]. S. Jacob, M. Alagirisamy, V.G. Menon , B.M. Kumar , and N.Z. Jhanjhi (2020). "An Adaptive and Flexible Brain Energized Full Body Exoskeleton With IoT Edge for Assisting the Paralyzed Patients," in *IEEE Access*, vol. 8, pp. 100721-100731, 2020, doi: 10.1109/ACCESS.2020.2997727.

[13]. Humayun M., Jhanjhi, N.Z., Alamri, M.Z. and Khan, A. (2020). “Smart Cities and Digital Governance”, in Employing Recent Technologies for Improved Digital Governance, DOI: 10.4018/978-1-7998-1851-9.ch005.

[14]. Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment," *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, 2018, pp. 1-5, doi: 10.1109/ICCOINS.2018.8510588.

[15]. X. Cheng, C. Chen, W. Zhang and Y. Yang, "5G-Enabled Cooperative Intelligent Vehicular (5GenCIV) Framework: When Benz Meets Marconi," in IEEE Intelligent Systems, vol. 32, no. 3, pp. 53-59, May-June 2017, doi: 10.1109/MIS.2017.53.

[16]. H. Magsi, A. H. Sodhro, F. A. Chachar, S. A. K. Abro, G. H. Sodhro and S. Pirbhulal, "Evolution of 5G in Internet of medical things," 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, 2018, pp. 1-7, doi: 10.1109/ICOMET.2018.8346428.

[17]. Ahokangas, P., Moqaddamerad, S., Matinmikko, M., Abouzeid, A., Atkova, I., Gomes, J. F., & Iivari, M. (2016). Future micro operators business models in 5G. The Business and Management Review, 7(5), 143–149. http://www.abrmr.com/myfile/conference_proceedings/Con_Pro_20588/conference_46507.pdf

[18]. 63 Fascinating Google Search Statistics (Updated 2019)", seotribunal.com, 2020. [Online]. Available: https://seotribunal.com/blog/google-stats-and-facts/. [Accessed: 06- Jul- 2020].

[19]. What is a DDoS Attack?", www.cloudflare.com, 2019. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Accessed: 06- Jul- 2020].

[20]. DDoS in the IoT: Mirai and Other Botnets - IEEE Journals & Magazine", Ieeexplore.ieee.org, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7971869. [Accessed: 07- Jul- 2020].

[21]. M. Antonakakis et al., "Understanding the Mirai Botnet", Usenix.org, 2020. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis. [Accessed: 07- Jul- 2020].

[22]. "What Is The OSI Model?", www.cloudflare.com, 2020. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/. [Accessed: 06- Jul- 2020].

[23]. Clouflare (n.d.). "What is a DDoS Attack?", [image]. Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[24]. m. process, "US9742732B2 - Distributed TCP SYN flood protection - Google Patents", *Patents.google.com*, 2020. [Online]. Available: https://patents.google.com/patent/US9742732B2/en. [Accessed: 07- Jul- 2020].

[25]. Fatima-tuz-Zahra, Jhanjhi, N., Brohi, S. N. and Malik, N.A. (2019). '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.

[26]. Yang, Yuchen & Wu, Longfei & Yin, Guisheng & Li, Lijie & Zhao, Hongbin. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2017.2694844.

[27]. Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," 15-May-2016. [Online]. Available: https://www.jstage.jst.go.jp/article/ipsjjip/24/3/24_522/_article/-char/ja/. [Accessed: 07-Jul-2020].

[28]. Alrawais, Arwa & Alhothaily, Abdulrahman & Hu, Chunqiang & Cheng, Xiuzhen. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing. 21. 34-42. 10.1109/MIC.2017.37.

[29]. "Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers - IoT Analytics", Iot-analytics.com, 2020. [Online]. Available: https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/. [Accessed: 06- Jul- 2020].

[30]. Sun, G., Xie, Y., Liao, D., Yu, H., & Chang, V. (2017). User-defined privacy location-sharing system in mobile online social networks. Journal of Network and Computer Applications, 86(November 2016), 34–45. https://doi.org/10.1016/j.jnca.2016.11.024

[31]. L. Zhonghua and Z. Wei, "Pricing Strategies of MOSNS Platform Based on the Theory of Two-Sided Markets," 2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA), Nanchang, 2015, pp. 659-662, doi: 10.1109/ICICTA.2015.167.

[32]. J. Li, H. Yan, Z. Liu, X. Chen, X. Huang and D. S. Wong, "Location-Sharing Systems With Enhanced Privacy in Mobile Online Social Networks," in IEEE Systems Journal, vol. 11, no. 2, pp. 439-448, June 2017, doi: 10.1109/JSYST.2015.2415835.

[33]. Xiao, X., Chen, C., Liu, X., Hu, G., & Jiang, Y. (2017). Privacy-Preserving Location Sharing System with Client / Server Architecture in Mobile Online Social Network. 11(2), 200–206.

[34]. Sun, Y., Chen, M., Hu, L., Qian, Y., & Hassan, M. M. (2017). ASA: Against statistical attacks for privacy-aware users in Location Based Service. Future Generation Computer Systems, 70, 48–58. https://doi.org/10.1016/j.future.2016.06.017

[35]. Arshad Malik, M. S., Ahmed, M., Abdullah, T., Kousar, N., Shumaila, M. N., & Awais, M. (2018). Wireless body area network security and privacy issue in E-healthcare. International Journal of Advanced Computer Science and Applications, 9(4), 209–215. https://doi.org/10.14569/IJACSA.2018.090433

[36]. Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 101(August 2017), 55–82. https://doi.org/10.1016/j.jnca.2017.10.017

[37]. C. Lee and A. Fumagalli, "Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 24-28, doi: 10.1109/WF-IoT.2019.8767227.

[38]. J. Kim and Y. H. Song, "Dynamic Transaction Management for System Level Quality-of-Service in Mobile APs," in IEEE Transactions on Consumer Electronics, vol. 64, no. 2, pp. 204-212, May 2018, doi: 10.1109/TCE.2018.2843287.

[39]. Z. Zhang, K. Long, A. V. Vasilakos and L. Hanzo, "Full-Duplex Wireless Communications: Challenges, Solutions, and Future Research Directions," in Proceedings of the IEEE, vol. 104, no. 7, pp. 1369-1409, July 2016, doi: 10.1109/JPROC.2015.2497203.

[40]. A. Zhang, J. Chen, R. Q. Hu and Y. Qian, "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2659-2672, April 2016, doi: 10.1109/TVT.2015.2416002.

[41]. Ferrag, M. A., Maglaras, L., & Ahmim, A. (2017). Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey. IEEE Communications Surveys and Tutorials, 19(4), 3015–3045. https://doi.org/10.1109/COMST.2017.2718178

[43]. K. Gai, Y. Wu, L. Zhu, L. Xu and Y. Zhang, "Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7992-8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303.

[44]. Q. Dan and J. Dudeck, "Certainty factor theory: Its probabilistic interpretations and problems", Artificial Intelligence in Medicine, vol. 4, no. 1, pp. 21-34, 1992. Available: 10.1016/0933-3657(92)90035-n.

[45]. M. Imran, M. Durad, F. Khan and A. Derhab, "Toward an optimal solution against Denial of Service attacks in Software Defined Networks", Future Generation Computer Systems, vol. 92, pp. 444-453, 2019. Available: 10.1016/j.future.2018.09.022.

[46]. T. Pascoal, I. Fonseca and V. Nigam, "Slow denial-of-service attacks on software defined networks", Computer Networks, vol. 173, p. 107223, 2020. Available: 10.1016/j.comnet.2020.107223.

[47].]V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", IEEE Access, vol. 7, pp. 82721-82743, 2019. Available: 10.1109/access.2019.2924045 [Accessed 8 July 2020].

[48]. S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017.

[49]. M. Yamin and A. Sen, "Improving Privacy and Security of User Data in Location Based Services", International Journal of Ambient Computing and Intelligence, vol. 9, no. 1, pp. 19-42, 2018. Available: 10.4018/ijaci.2018010102 [Accessed 8 July 2020].

[50]. X. Dong, B. Guo, X. Duan, Y. Shen, H. Zhang and Y. Shen, "DSPM: A Platform for Personal Data Share and Privacy Protect Based on Metadata", 2016 13th International Conference on Embedded Software and Systems (ICESS), 2016. Available: 10.1109/icess.2016.10 [Accessed 8 July 2020].

[51]. K. Fan, Y. Ren, Y. Wang, H. Li and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G", IET Communications, vol. 12, no. 5, pp. 527-532, 2018. Available: 10.1049/iet-com.2017.0619 [Accessed 8 July 2020].

[52]. F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan and K. Ren, "A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks", IEEE Network, vol. 32, no. 6, pp. 184-192, 2018. Available: 10.1109/mnet.2018.1700269 [Accessed 8 July 2020].