Security and Privacy Concerns in Wireless Networks: A Survey

1st Yong Weixiong
School of Computer Science & Engineering Taylor's University
Selangor, Malaysia
yongweixiong000321@gmail.com

2nd Robin Lee
School of Computer Science & Engineering Taylor's University
Selangor, Malaysia
leerobin22@gmail.com

3rd Alvin Kon Soon Seng
School of Computer Science & Engineering Taylor's University
Selangor, Malaysia
ahkonkon@gmail.com

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

***Abstract*—The paper aims to raise awareness of security and privacy concerns in network communication that takes place among machines. Knowing that there are lots of possibilities that an attacker or hacker may get a slight chance of causing exploits from network vulnerabilities leads to threats at personal and organizational level. In this paper, research has been carried out using survey methodology to gather user viewpoints on general awareness and importance of network security and privacy. The results will be used to support the overall significance of how a network should behave and work on behalf of the users. The main goal as developers and engineers is to prioritize and improve user satisfaction and data protection standard. Therefore, this paper will also discuss the methodologies and possible ways to offer the best strategies for protection against security and privacy attacks.**

Keywords—communication security, network security, machine-to-machine communication, user privacy concerns, user awareness and behavior

I. INTRODUCTION

Computer Networking is the heart of the entire computer system in the world today, almost every industry requires a good and secure network topology/set up in order to provide an outstanding service to the clients. Many people may think that computer networking just involves internet connection, as well as 2 peers communicating and exchanging information with each other, but it takes more than that, networking is a kind of crucial technology that helps computers to break through their limits, enables remote access, smart devices, applications like Facebook, Google and so on. Despite the web applications, in this topic, we will be focusing on the wireless mediums between Machine-to-Machine and Machine to Web Application connection, which may fall into different types of computer networks in terms of both scalability and usability. For instance, Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), and Home Area Network (HAN) [1].

Each of them is used in different places and for different significant purposes. Commonly used or normally known by most people type of networks are PAN, LAN, and WAN. PAN networks are a great example of the Bluetooth networks, which is a small network in size and involves many Internet of Things (IoT) devices that work in master-slave network control. A LAN network is widely used in almost every corner of the world, it is necessary for every file-sharing network to have LAN cable-linked between machines, especially the server and the client. LAN can be both wired or wireless connection, a closed network that uses private IP addresses that determine each device's identity in the network allows data exchange as well as sharing. Wired LAN provides a stable connection between machines along with faster speed compared to a wireless connection, in which wireless connections provide mobility with a reasonable data speed rate. Similarly, a MAN network that interconnects all of the network's resources in a larger geographical area compared to a LAN network, but considerably smaller than a WAN network. Usually used for a campus network rather than enterprise usage, since LAN networks are much more effective for enterprise use [2]. Moreover, WANs are a much larger network that could possibly cover the entire state or country. WANs serve a similar purpose as the LANs but on a larger scale, connecting with either phone lines, fiber optic cables, or satellites [1]. Mainly used for interconnection between countries or for mobile phone services such as 4G LTE cellular. Lastly, a HAN network, a type of LAN network that contains devices such as phones, IoT devices, Smart TV, or any smart electrical appliances that are connected to a central router with wired or wireless connection [3].

Almost everyone on Earth is using the Internet or has access to any network connection, which may involve very important information that is transferred in between. Information that could be beneficial to someone, or creates threats to someone who may concern, a single information leakage may also cause dreadful consequences. For example, a simple threat to a business like a Distributed Denial-of-Service (DDoS) Attack may cause millions of cost or loss to a company. If it happened, the users may lose their trust in the company's product security, which is a long-term consequence for the company. This is where security in networking takes place and also takes in a major part to prevent as well as avoid the possible wireless network attacks from the unauthorized. Avoid unnecessary attacks that could cause harm to both clients and the hosts. The threats are unnecessary for just aiming for desktops and servers, it also creates problems on mobile devices, as well as causing more threats towards it. Compared to desktops, mobile devices are more vulnerable to wireless network attacks, since mobile devices are mainly accessible with wireless connections. Protecting wireless network security is much tougher than a wired network, while data are traveling in an unprotected environment which in this case it will be referring to the air interface communication between machines, including RFID, Bluetooth, Wi-Fi and many more [4]. Skilled personnel, can

easily create exploits and attacks towards users, stealing, eavesdropping, or even tracking every piece of information, which had made mobile phones or any IoT devices one of the greatest threats to everyone that's involved. This shall be the major challenge that developers and network security engineers would have to face in order to protect themselves as well as the clients involved.

II. Literature Review

A. *Cryptography*

Cryptography is an algorithm which uses for encrypted or decrypted the message. Nowadays, there are two main types of cryptography which are symmetric and asymmetric cryptography. Other than that, there is also special cryptography calls hybrid cryptography which is the combination of symmetric and asymmetric.

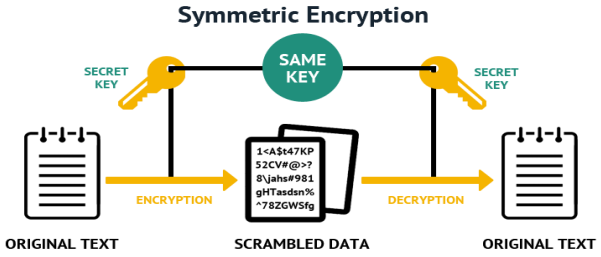

Figure 1: Symmetric Encryption [5]

Symmetric is simple cryptography. It only has one secret key to use for encrypted and decrypted data. Once the data was encrypted, the content of data will show as ciphertext. The ciphertext is 'unreadable' text until it has been converted or decrypted into plain text. Because symmetric cryptography has only one key to encrypt and decrypt, so the speed is faster. But, it is easy to be attacked by brute-forced, linear and differential cryptanalysis attack because of the weak key usage.

There are two well-known symmetric encryption algorithms which are block algorithm and stream algorithm [6]. A block algorithm uses a specific secret key to encrypt a set of lengths of bits in blocks of data. The system will hold the encrypted data in its memory as it waits for complete blocks. Stream algorithms will encrypt the data while it streams but retained in the system's memory. There are few famous symmetric encryptions such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish.

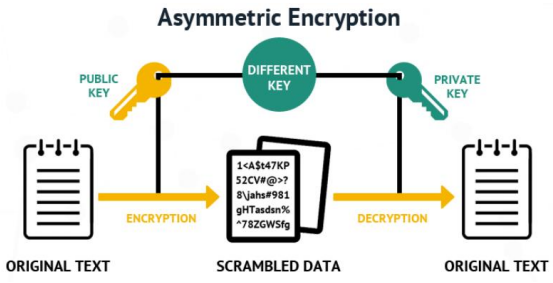

Figure 2: Asymmetric Encryption [5]

Asymmetric cryptography, also known as public-key cryptography. The main difference between symmetric and asymmetric is that asymmetric encryption has two different keys, one is a public key used for encrypted data and one is the private key used for decrypted data. Because there are two keys that are implemented so the speed of encryption and decryption will slower than symmetric encryption instead it has a higher level of security.

The public key and private key used by asymmetric are mathematically-related key pair. Private Key is always kept with the user or computer that generates the key pair. But the public key is able to distribute to anyone who wants to send encrypted data to the holder of the private key. That means the security services it provides are including confidentiality, integrity, authenticity and also non-reputability. The popular asymmetric encryption is included Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA) and so on. Other than that, the protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on asymmetric cryptography for encryption and digital signature function. Bitcoin and other cryptocurrencies are using asymmetric algorithms as well.

B. *HTTP and HTTPS*

HTTP stands for Hypertext Transfer Protocol, which was initiated by Tim Berners-Lee in 1989 during the innovation of World Wide Web (WWW). HTTP is a protocol where the application layer and used for distributed, collaborative, hypermedia information systems, in layman terms, HTTP is used for transporting data packets from a client to the host or transversely [7]. The latest version of HTTP was published in 2018 which is HTTP version 3.0.

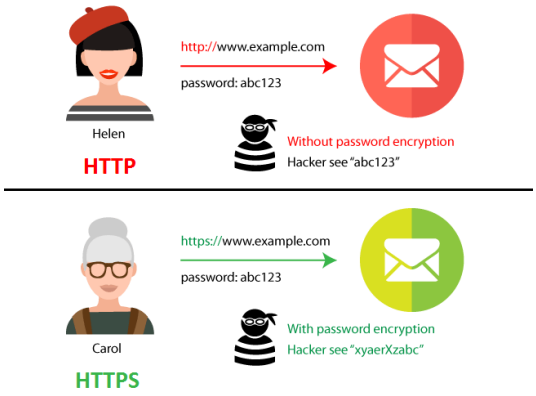

Figure 3: HTTP and HTTPS [8]

HTTP provides a request-response protocol in the client-server computing model. First, a client sends a request to the web. Once the webserver received the request, it will process the request, Then, the server returns a response to the client so that the client able to browse. However, since the internet had gained its popularity today, internet users are increasing significantly. Since more data are involved in the web, as well as most companies uses internet to communicate and exchange information for business purposes. Therefore, security will be much concerned compared to the past, secure function of HTTP are outdated and it may vulnerable to the internet user. So this is where, Secure Hypertext Protocol (HTTPS) have been released.

HTTPS has almost the same concept as HTTP, it uses separate protocols which are Transport Layer Security (TLS) and Secure Socket Layer (SSL). TLS is a protocol that mainly focus to prevent Man-in-the-Middle or eavesdropping attacks, it has the confidentiality that helps to prevent information

getting leaked in the transmission process by using specialized handshake techniques between the client and the host. SSL is a protocol that will encrypt all the sensitive data including credit card numbers, personal information that is being sent and ensures the data are transmitted through a safe tunnel to its destination [9]. It uses port 443 by default as well.

These are the advantages of implementing HTTPS:

- Trust

HTTPS provides the website a certificate which means it had proof that the website is secure. So, the visitor's data or information are under protection.

- Verification

HTTPS provides the website a secure certificate which means that the website is verified. You may see if it is an HTTPS website, there is a padlock in the address bar. You can click on it to see the certificate.

- Integrity of Data

If without SSL, it is possible to intercept data or even change it from the webserver. HTTPS provides SSL to encrypt the data, so the data transfer between the network will be secure.

HTTPS is widely used nowadays. It is good at preventing man-in-the-middle attacks or known as spoofing attacks. The data shows the website that used HTTPS had over 1 billion in 2018. We believe that it will totally replace HTTP in the future, where Google right now has been stepping forward to force everyone must have the appropriate SSL Certificates and HTTPS service on the browser.

C. Importance of Wireless Network Security

Wireless network security is to ensure a wireless connection is secure by implementing multiple security protocols or standards that will help prevent attacks to the network. A wireless network or wireless connections are more vulnerable to eavesdropping and easily being manipulated compared to wired networks or connections. This is because a wired network uses a shielded copper wire or fiber optic cables as their medium to transmit and receive data which will be more difficult for an unauthorized user to perform eavesdrop and steal or manipulate information/data that are being transmitted, while a wireless network uses radio frequency to transmit data and this radiofrequency are traveling in the air, this allows unauthorized people to intercept the radio frequency and steal the information easily if the connection is not properly secured.

There are multiple types of attacks that can be used by an attacker to gain data that are being transmitted in the network for illegal used. As wireless networking is playing an important role in ubiquitous computing where more devices are continuously being connected to the internet connection and this causes more data or information to be transmitted wirelessly [10]. If all these data are not encrypted or secured than many unauthorized people may manipulate this data or steal the data, this is where a secure wireless network is required. The importance of a secure wireless network is to achieve the primary objectives. The primary objectives are to maintain the confidentiality of data, the integrity of data, and the availability of data.

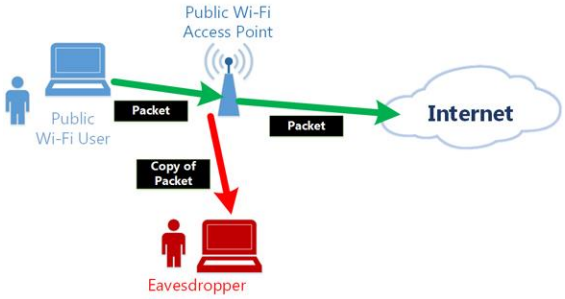

Figure 4: Eavesdropping [11]

Confidentiality of data/information is to make sure that the information being transmitted through the wireless network are being received by the authorized or intended receiver. Since information is valuable and should be disclosed to unauthorized personnel to prevent misuse of critical information by them and causing harm [12]. Sniffing attack is a very common type of attack where the attacker intercepts the data by capturing and monitoring the network traffic [13]. A way to prevent the attacker to sniff the data is by using encryption, the data will be sent through an encrypted connection and there are multiple different types of encryption protocols such as SSL/TLS. By encrypting the connection it will protect the confidentiality of the data/information.

The integrity of data/information is to make sure that the information has not been altered or manipulated by unauthorized personnel. Accuracy of the data transferred should be high because the data will be valuable only if the data is valid or correct. Man-in-the-middle attack or MITM attack is when an attacker is intercepting data in a network connection and may or may not manipulate the data that is being intercepted and then sending it to its original destination, this violates the integrity of data being sent. To keep the integrity of data/information an encryption protocol such as SSH/TLS can be implemented to have a secure connection in the network and when data is manipulated it can be easily detected [14].

The availability of data/information is to make sure that the information is accessible by authorized personnel when required. Information needs to be accessed and available when it is needed and it should be accurate so the information or data can be used as it is intended to do. A denial-of-service attack is a common attack where it stops or prevents authorized users to access the available information or resources by disrupting the traffic flow [12]. These attacks should be prevented by having a secure wireless network infrastructure, regularly monitor for unusual activity, and perform regular backups on the data [15].

Figure 5: Network Security CIA [16]

Wireless network security is an important part of nowadays ubiquitous technology since almost the majority of data are being transmitted through wireless connections. With a secure wireless network, common attacks can be mitigated or prevented to keep and protect the data and making sure of the confidentiality, integrity, and availability of data are maintained.

Researchers are actively working in the area of data privacy in various domains. For example, [17] have offered a comprehensive review on privacy protection in mobile cloud computing focusing on user privacy protection who use location-aware service. Similarly [18] have performed a systematic study on cyber security threats and vulnerabilities. Another example of highlighting the cybersecurity issues is [19] in which the focus is on security challenges in smart cities. [20] have proposed a data privacy-aware protocol to secure video reporting services used for roadside accident monitoring. Other solutions include authentication schemes [21]-[24], evaluation of available authentication techniques such as those proposed for healthcare domain which are highly sensitive [25], proposing secure routing protocols for wireless sensor network such as [26], energy efficient protocols which may play crucial role in energy security [27]-[29], highlighting the challenges of protocols for secure communication to address them [30], attack detection techniques [31], link prediction in criminal networks using techniques like deep reinforcement learning [32], phishing detection techniques [33]. Despite many efforts, networks are still prone to attacks, both internally and externally. Threats caused by wireless networks to data security are further discussed in forthcoming sections.

III. WEP VS WPA VS WPA2

The wireless network is causing a threat to data security since it is widely used as the main data communication link between two points, to overcome this threat, wireless security protocols or encryption methodologies are implemented [34]. To obtain a secure wireless network, encryption is used to encrypt the information that is being transmitted, these encryption methodologies are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access version 2 (WPA2).

A. Wired Equivalent Privacy (WEP)

WEP is a part of the IEEE 802.11 wireless security standard. WEP uses the Cyclic Redundancy Code (CRC-32) to provide data integrity and security and the RC4 algorithm to provide data confidentiality [35]. The WEP standard supports a 40-bit key length and a 24-bit Initialization Vector (IV) to act as encryption and decryption key.

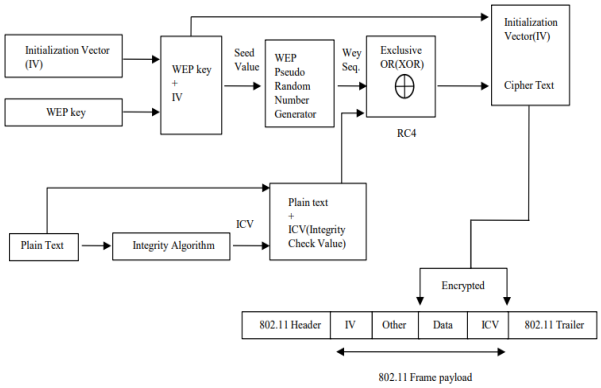

Figure 6: Encryption of WEP [35]

The encryption process of WEP standard shown in figure 6 starts by initializing the 40-bit WEP key and 24-bit IV, then an integrity algorithm is performed to the plain text to generate an Integrity Check Value (ICV), and finally, RC4 algorithm is used to generate the ciphertext and also for the key sequence.

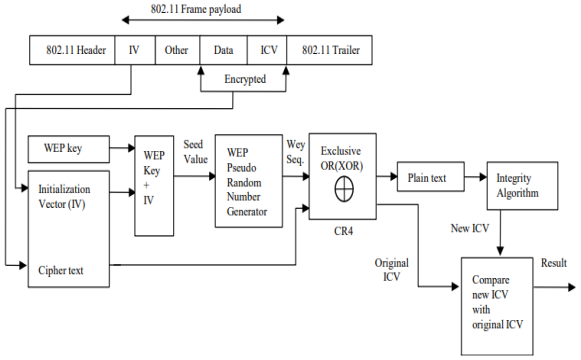

Figure 7: Decryption of WEP [35]

The decryption process of the WEP standard shown in figure 7 by using the CR4 algorithm to the ciphertext and key sequence. Then a new ICV is generated and is compared with the original ICV to make sure the integrity of the data.

WEP security standard does have some vulnerabilities and weaknesses which makes WEP a less secure option such as WEP have weak cryptography, small key size, reusing of Initialization Vector, Authentication issues, and more.

B. Wired Equivalent Privacy (WEP)

In late 2002, the Wi-Fi alliance introduces a new standard to overcome the limitations and vulnerabilities of the WEP standard, which is called Wi-Fi Protected Access (WPA). WPA provides better security features such as Temporal Key Integrity Protocol (TKIP) that generates a random 128-bit key for data encryption, together with Michael algorithm to provide protection against replay, and Message Integrity Code (MIC) for data integrity as shown in figure 8 [35]. WPA has 2 authentication mechanisms which are WPA-PSK or WPA-Personal and WPA-Enterprise. WPA-PSK or WPA-Personal uses a pre-shared key that is static to authenticate users and usually used in small offices or home networks, while WPA-Enterprise is designed for enterprise networks which are larger and uses EAP for authentication.

WPA security standard still has some weaknesses and vulnerabilities even though it is more secure compared to the WEP standard, WPA still uses the RC4 cryptography

algorithm, complicated configuration process, and vulnerable to brute force attacks, DOS attacks and more.

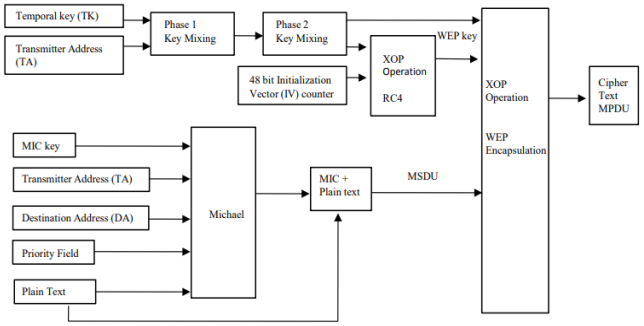

Figure 8: Encryption of WPA [35]

C. *Wired Equivalent Privacy (WEP)*

WPA2 standard is an improvement made over the WPA standard, the improvement focuses on the data encryption algorithm. A cipher block chaining Message Authentication Code Protocol (CCMP) and utilizing Advanced Encryption Standard (AES) for encryption of data [34]. WPA2 standard also uses WPA2-Personal and WPA2-Enterprise for authentication and validation message integrity is by using Cipher Block Chaining message validation. WPA2-Personal uses a pre-shared key for authentication in smaller networks such as home networks or office networks while WPA2-Enterprise uses EAP for authentication in larger networks or enterprises.

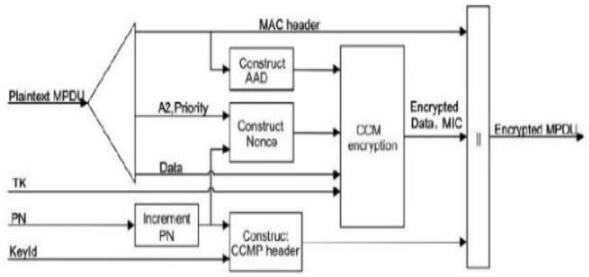

Figure 9: CCMP Encryption [34]

Figure 9 and 10 show the encryption and decryption process respectively that occurs in WPA2 standard, using CCMP and AES to have a high level of data security in wireless network transmission.

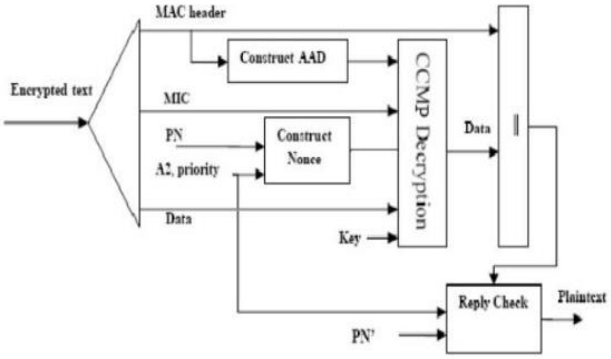

Figure 10: CCMP Decryption [34]

WPA2 standard is recommended to be implemented in a wireless network to have more security, with AES and CCMP in WPA2 it increases the level of security to a higher level than compared with WPA or WEP standard. To see a comparison between WEP, WPA, and WPA2 standard is shown in the table below.

	WEP	WPA	WPA2
The main Purpose	Security is provided in contrast to wired networks	Implementation of major IEEE802.11i standards with WEP without requiring new hardware	Complete IEEE 802.11i standards are implemented with new enhancements of WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Authentication is provided through chipper blocks with CCMP and AES.
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Data integrity is provided through Message Integrity Code.	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Key management is not provided	The 4 way handshaking mechanism is used to provide for key management	The 4 way handshaking mechanism is used to provide for key management
Compatibility in terms of Hardware	Possible to deploy on current hardware infrastructure	Possible to deploy on both current and previous hardware	Older Network Interface Cards are not supported. Only the 2006 and newer.
Vulnerability	Vulnerable against Chopchop, Bittau's fragmentation and DoS attacks including variety of DoS attacks.	Vulnerable against Chopchop, Ohigashi-Morii, WPA-PSK, and Dos attacks.	Vulnerable against DoS attacks due to unprotected control frames and MAC spoofing
Deployment in terms of complexity	Easy to deploy and configure		WPA-2 requires complicated setup with WPA enterprise.
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	Implementation of 48-bit datagram/packet number protects against replay attack

Figure 11: Comparison of WEP, WPA, WPA2 [35]

IV. Data Collection

Researching is part of the data collection techniques [36], which is considered as part of the secondary data collection [37]. Looking through existing information and data that was already published online or physically, in this case, we have been searching for academic papers that are written by professional contributors and researchers.

Table 1: User awareness survey form

Question	Answering Method
Are you aware of the possibilities of Wireless Network Attacks?	Yes, No, Maybe
Are you aware that a WiFi Password can be cracked?	Yes, No, Maybe
Are you aware of the danger while an attacker/hacker is connected to your network?	Yes, No, Maybe

However, using secondary data are not specific enough to be a part of the research, therefore the team decided to conduct a survey/questionnaire with specialized questions that are specifically aimed for this topic of research. The questions are divided into 4 different sections, "User Awareness", "User Behaviour", "Policies and Procedures", and "General Security & Privacy Concerns"; which are given in Tables 1, 2, 3 and 4.

Table 2: User behaviour survey form

User behaviour	
Question	Answering Method
You will use Random/Public Wi-Fi often.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
You will browse online banking websites using public Wi-Fi.	Rating (Strongly Disagree 1 - 5 Strongly Agree)

You will use a Virtual Private Network (VPN) while connecting a public Wi-Fi.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
You will set a strong Wi-Fi password for your personal Wi-Fi.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
You will change your Wi-Fi password/SSID (Wi-Fi Name) once a month/year.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
You will check who is connecting to your network.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
You will check the website's security before filling-in details (HTTPS).	Rating (Strongly Disagree 1 - 5 Strongly Agree)
You will save your account passwords (e.g. Facebook, Gmail) in a browser.	Rating (Strongly Disagree 1 - 5 Strongly Agree)

Table 3: Policies and procedures survey form

Question	Answering Method
Are you aware of the standard policies and procedures to browse the internet safely?	Yes, No, Maybe
Do you surf any random/unknown/possibly malicious websites?	Yes, No, Maybe
Do you think that companies/organizations should have strict policies and procedures for surfing the Internet?	Yes, No, Maybe
Do you think that a company network should have limited access (blocking certain websites)?	Yes, No, Maybe

Table 4: General security & privacy concerns survey form

Question	Answering Method
Wireless Connections should be encrypted.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
Wireless networks should authenticate users that want to connect to the network.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
The latest encryption standards (such as WPA/WPA2) should be implemented to all wireless networks except Open Public Networks.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
A router/access point should be well-configured.	Rating (Strongly Disagree 1 - 5 Strongly Agree)
Do you want other people to know what website are you browsing?	Yes, No, Maybe
Do you want other people to know the information about you?	Yes, No, Maybe
Do you want other people to track your browsing habits?	Yes, No, Maybe

The main purpose of the questions are been set into 4 different sections is because each section aims to discuss different aspects of a broad idea of network security. For the "User Awareness" section, it is intended to investigate whether users are aware of the general danger and risks that could occur within their network. As part of the questions shown above, the survey participants needed to answer the questions with "Yes, No or Maybe" answers for the 3 specific questions. Then, to the "User Behaviour" section, which is mainly aimed to find out how do the majority of network users behave while browsing through the Internet or connecting to a network. Besides, it also involves the possible ways on how would the users will protect themselves from being harmed or attacked. Meanwhile, in the third section, the "Policies and Procedures" section is focusing on the policies factor and also on how would the user feel about the importance of the appropriate policies. Finally, there will be the final section, "General Security & Privacy Concerns", the main objective of this section will be collecting users' views towards the idea and concept on how should network actually work and what it should do. For instance, end-to-end encryption, and the encryption techniques used by a network such as Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access 2 (WPA2).

V. Discussion

Our very own survey that we have created with Google Forms (link provided under Appendix) has gathered a total of 37 responses by published and shared through public social media by our team members. Even though, we believe that all of the survey participants that took part in our very own survey are answered unbiasedly. Apart from the sections as discussed above, we have also included the demographical questions in order to find who and do they have experience in IT work or studies.

A. Demography

Here we will be collecting Names, Age and a question that aims to know if the respondents have any general knowledge and experience on IT. Since names would not be required for our project analysis, therefore will not include it into part of the discussion findings analysis.

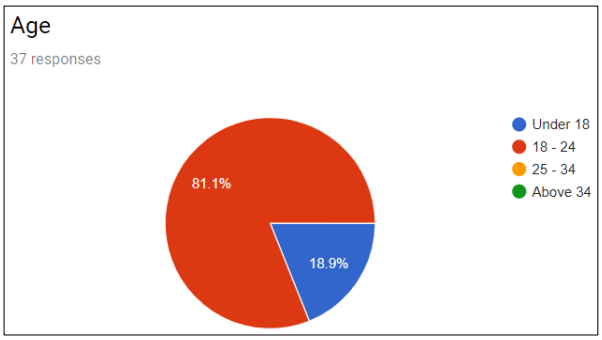

Figure 12: Demography (Age)

Here as we can see, out of the 37 respondents, **81.8%** are at the age of 18-24 and the rest are under 18, which are all considerably young. Also, the majority of **56.8%** of them are having occupation/studies related to IT, still there are possibilities that IT students or employees are not aware of the network security even though a majority of them do have a general knowledge of IT.

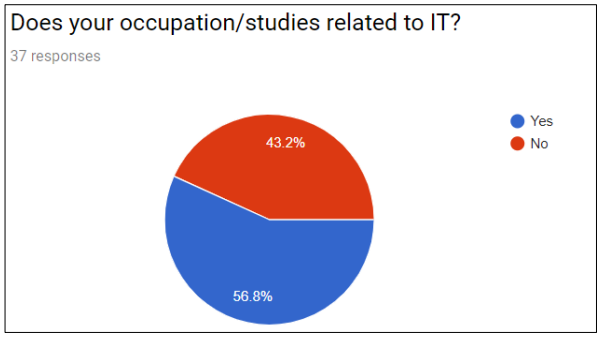

Figure 13: Demography (IT)

B. *User Awareness*

The second section of the survey, collecting information about the general user's awareness of networks in general. The statistics summary will be given in Table 5.

As we can see from the data above, most of the survey participants are aware of the network attacks and also the danger of the hackers while connecting to the same network overall. Firstly, **83.8%** of the respondents are aware of there are many possibilities of different types of wireless network attacks, which would make the network a very dangerous place. Next, Wi-Fi password cracking is one of the ways that hackers could breach through the network, and the result shows that **91.9%** are aware that Wi-Fi can be easily cracked with hacking tools, such as Aircrack-ng or any other tools. In the meantime, **81.1%** of the respondents also aware of the danger while the hacker has control or access to the user's network. In conclusion, most of the respondents are well-aware of the danger and risks when it comes to wireless networks.

Table 5: User awareness survey results

Question	Rating (Yes, No, Maybe) Percentage (%)			Summary
	Yes	**No**	**Maybe**	
Wireless Network Attacks Awareness	83.8	5.4	10.8	Yes
Cracking Wi-Fi Passwords Awareness	91.9	5.4	2.7	Yes
The danger of Hacker in the same network	81.1	5.4	13.5	Yes

C. *User Behaviour*

The third section of the survey, collecting information about a user's behavior on networks or connecting to any network. The statistics summary will be given in Table 6.

First and foremost, this section has 3 different categories of questions, Public Wi-Fi Concerns, Personal Wi-Fi Concerns, and Browsing Habits. Starting from the Public Wi-Fi Concerns, a total of **45.9% (highest)** agreed on they will use a random or Public Wi-Fi, which is very risky due to the fact that public network is large and uncontrolled, as well as the random network may be a rogue network. There may be potential attackers connected to the same public network that could steal or track the user's information that's in the same network. Nonetheless, **75.6%** of participants also disagree on browsing online banking websites while connecting to a public Wi-Fi, but there might be a risk for the rest of 24.4%, where banking accounts may be exposed to hackers which may cause serious consequences. If the user has to use it for an urgent matter, utilizing Virtual Private Network (VPN) will be a great choice to prevent information leakage. It is proven that VPN does help in preventing and hiding client's information in the network and untraceable. It seems like **45.9%** of the respondents do not use VPNs while connecting to a public network. This shows that VPNs software should be well advertised and spread among the world, in order to keep the clients themselves safe from the wireless network attacks.

Towards the next category, the configuration, and maintainability of a personal or local network. A great number **(86.5%)** of respondents claimed that will set a strong Wi-Fi password for their very own network, and the rest (13.5%) were neutral, no one disagreed. However, what determines a "strong" password, a perfect strong password should contain 16 characters along with alphanumeric, several symbols, a mix of capital and small letters, which should take ages for a hacker to crack through. 16 characters long passwords may be inconvenient for some people, but a considerably strong password should contain at least 8 characters and above with digits, capital letters, and a symbol will be recommended. As for the next question, **64.8% (highest)** of the respondents does not change the Wi-Fi password and SSID once a month or a year, and remain unchanged, with only **10.8%** would change their Wi-Fi passwords and SSID. This may be a crucial factor because anonymous or unknown devices may connect to the network without realizing it. Resetting the SSID and password will prompt the devices to key in the password once again. If it is a nuisance to change the password so frequently, users can keep track of the connected device inside the same network by checking the default gateway of the router or access point. **51.3%** of the respondents also agreed they would check the devices that are connected to the network.

Table 6: User behaviour survey results

Question	Rating (1-5) Percentage (%)					Summary
	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	
Using a Random/Public	12.5	24.3	16.2	32.4	13.5	Positive
Browse banking websites using Public Wi-Fi	48.6	27	16.2	5.4	2.7	Negative
Use VPN on Public Wi-Fi	16.2	29.7	27	8.1	18.9	Negative
Set strong Wi-Fi password for Personal Wi-Fi	-	-	13.5	27	59.5	Positive

Changing Wi-Fi Password/SSID once a month/year	35.1	29.7	24.3	2.7	8.1	Negative
Checking who is connecting to the same network	5.4	24.3	18.9	13.5	37.8	Positive
Check website's security	10.8	13.5	37.8	8.1	29.7	Neutrally Positive
Saving account passwords in browser	18.9	18.9	24.3	18.9	18.9	Neutral

The final category would be the general browser habits of the user. It is shown that the summary for checking the website's security before filling-in details are neutrally positive, which means that the highest rate was neutral **(37.8%)**, along with 37.8% of positive ratings. Website security such as HTTPS is an upgraded version of HTTP that offers a much secure connection between the client and the host. Websites without HTTPS may be very dangerous since the connection medium was not encrypted, filling-in sensitive information may be unimaginable dangerous. Also, some people prefer convenience over security, therefore it will save their passwords for either Facebook or Google accounts. The survey results show that the readings are neutral, which means **24.3%** (highest) of respondents are neutral towards this question, and the rest are evenly distributed among negative and positive symmetrically. Saving passwords in a browser will be utilizing the cookies feature in the browser. Ultimately, cookies do have the risks that are possible to be stolen as well as the information within. Theoretically saying, saving passwords would not be recommended.

D. Policies and Procedures

The fourth section of the survey, collecting information about the general policies and procedures, also the views by the user on networks or connecting to any network. The statistics summary will be given in Table 7.

Table 7: Policies and procedures survey results

Question	Rating (Yes, No, Maybe) Percentage (%)			Summary
	Yes	**No**	**Maybe**	
Standard Policies and Procedures for browsing Awareness	43.2	32.4	24.3	Yes
Surfing any random / unknown / possibly malicious websites	24.3	43.2	32.4	No
Strict Policies and Procedures for surfing Internet in Companies	78.4	5.4	16.2	Yes
Limit Browsing Access in Companies	43.2	18.9	37.8	Yes

There are many tips or known methods to browse securely in the network, however, most of the methods only work personally but not for companies. As shown in the table above, **43.2%** of the survey participants, which is the majority are aware of the policies and procedures to browse securely in the network. On none special occasions in a personal network, users are not necessary to browse "securely" in the network unless it is financially important. However, surfing through random websites or possibly malicious websites are dangerous because there might be viruses harvested inside the websites, which could be malware or other forms of malware. **43.2% (majority)** do not browse through the malicious websites, 32.4% uncertainty and 24.3% would. Compared to a company's network, it should have a strict policy and procedure that makes sure the company's network is not harmed by the outsiders, **78.4%** of the respondents also agreed to it. It is an important factor that helps to keep away all of the possible attacks externally. The policies and procedures should also include limiting the browsing access towards certain websites, **43.2%** of the respondents also do think that it should be limited.

E. General Security and Privacy Concerns

The final section of the survey, collecting information about user's ideas on general security & privacy on networks or connecting to any network. The questions in this section will be divided into 2 categories by different types of answering methods. The statistics summary will be given in Table 8.

Table 8: General security and privacy concerns survey results (a)

Question	Rating (1-5) Percentage (%)					Summary
	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	
Encrypted Wireless Connections	-	2.7	10.8	27	59.5	Positive
Authenticating Users	-	-	10.8	29.7	59.5	Positive
Implement latest standards	2.7	-	24.3	27	45.9	Positive
Well-configured router/access points	-	2.7	8.1	21.6	67.6	Positive

A standard wireless network in this world today, must have several requirements in order to protect user's data and privacy. The first would be encryption, regardless of the encryption techniques, all of the wireless networks should have end-to-end encryption that prevents a third-party to access. Since wireless networks are prone to many different kinds of attack especially Man-in-Middle Attack, therefore

symmetric or asymmetric encryption is very important. **86.5%** of the respondents also agreed that wireless networks should be encrypted. Then, **89.2%** of the respondents think that the wireless network should authenticate users when it wants to connect to the network. Part of the authentication would be using the WPA-PSK (Pre-Shared Key) or the WPA2-PSK network system, the one with the valid key will be able to connect into the network. As for WPA and WPA2 are part of the current standards for local or personal networks, **72.9%** of the respondents also had the same thoughts on the latest encryption standards should be implemented, except for Open System Networks. Besides, the home or company routers should be well-configured with no loophole that allows exploits by the attackers, which **89.2%** also agrees on it.

As for the second category, will be questions about privacy concerns that might invade users' privacy. Passive Attacks such as Network Traffic Sniffing is one of the greatest privacy threats to both clients and hosts. Where many users are unconsciously tracked by the hackers with the passive attacks, since it is a passive attack, it cannot be stopped easily or detected, so precautions may be needed especially when using a public Wi-Fi. As the data are shown above, **89.2%** of the respondents would not want others to know or be able to trace what the user is browsing. Moreover, precisely **100%** of the respondents also do not allow others to know every information and their browsing habits about them. Legally speaking, network traffic sniffing or network tracking is an illegal action if any person's privacy was invaded or financially affected, but if it is used for security analysis or others with legal permissions then there will not be a penalty.

F. Unique Solution

There is no definite solution for securing the wireless network, there are many possible ways to solve and face the attacks. Besides, there are also many types of attacks that can have different purposes and source, therefore by dealing with different types of attacks will require different types of solutions. Compared with a software system, wireless networks are much harder and complex to protect from harm, as network consists of more external connections which mean there are more possibilities for hackers to exploit through the system.

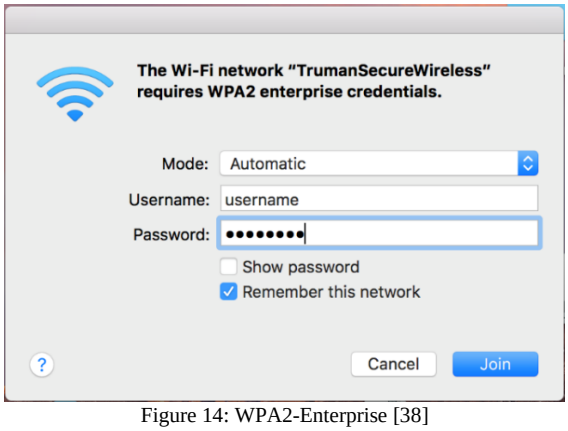

Figure 14: WPA2-Enterprise [38]

As developers and network engineers, securing the company's network will be our duty and responsibility. Understanding the network topology and make use of powerful tools will be very important, network management software such as SolarWinds Network Performance Monitor will be an ultimate tool for network engineers. Not only that it provides sub-tools to manage network and tracking, but also with tools like finding misconfigured access points, rogue access points, unknown clients, etc. Apart from managing the network, strong authentication would also be very important for a company. Techniques such as WPA2-PSK (Personal) and WPA2-Enterprise, would also help to strengthen the security of the network to avoid intruders. WPA2-Enterprise will be a recommended technique for a company, which *is a technique that allows the administrator to create users for the clients with their own specialized account, which means each of the clients can log in to the network with their password to their account. It is also easier for the network engineers to add, edit or remove the accounts if any one of them goes rogue or stolen.

Additionally, updating network devices firmware is also a very important factor that helps to secure a network. There are many networks that were prone to be hacked because most of the firmware is outdated with the least standards. Therefore, network engineers should keep track of the firmware version of all access points, servers, SSL, and TLS, as well as encryption techniques. In the meantime, companies should have proper policies and procedures to support the employees by strictly comply with safety policies and procedures. This was to make sure that the attacks are not internally harvested and also to minimize the risk of being attacked.

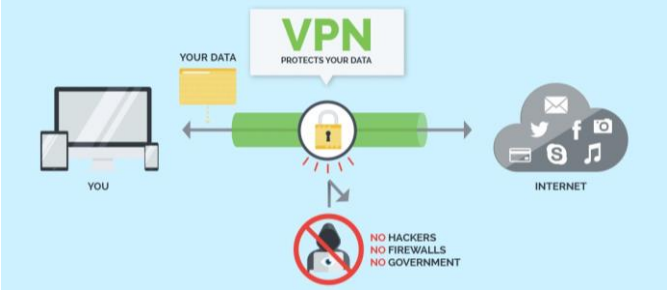

Figure 15: VPN [39]

As the clients of the network, there are also times that we need to protect ourselves from the attackers especially when connecting to other networks that do not belong to you. Using a Virtual Private Network (VPN) tool would be the best solution of all, as previously mentioned, VPNs allows the client to create a virtual network environment that allows the client to browse freely in the network. Everyone except for the client will not be able to see what the client is browsing and accessing. However, VPNs [40] are not cheap and usually subscription-based, but there are still other methods such as avoiding Public Networks and make sure that every website that you have browsed into has HTTPS certificates protection.

Password properties

Property	Value	Comment
Password length:	16	OK
Numbers:	4	USED
Letters:	9	USED
Uppercase Letters:	2	USED
Lowercase Letters:	7	USED
Symbols	3	USED
Charset size	94	HIGH (a-z, 0-9, A-Z, symbols)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 143 quadrillion years
Fast Desktop PC	About 36 quadrillion years
GPU	About 14 quadrillion years
Fast GPU	About 7 quadrillion years
Parallel GPUs	About 717 trillion years
Medium size botnet	About 143 billion years

Figure 16: Password Brute-Force Check [41]

For a home network, it is a good practice that the owner uses a strong password for their WPA2-PSK network. A strong password would consist of at least 16 characters that are mixed with alphanumeric, symbols, capital letters and small letters, which should look something like **"j8bnEth4?/,xZx76"**. Even strong passwords like that may get brute-forced coincidentally, but it average will take quadrillion years to crack the password. If the hacker managed to break in with a powerful tool, the owner can check and keep track of the clients that are connected in the network by using the default gateway interface from the router or access points, can easily disconnect them if any unknown or unauthorized device is in the network. The default gateway interface is a powerful built-in tool, it has all of the detailed configurations that can be used and enhance the network. There are also sections that allow administrators to select an encryption type, which defaults will be AES technique. As the owner of the network, it is a crucial factor to make sure that the network is encrypted with AES techniques or the others, and also confirm that the firmware version of the router is up to today's version as well as the latest standards.

VI. Conclusion

The wireless network may be a promising domain in the field of communications, however, it brings along with both convenience and dangers, knowing that there are many different types of attacks and can easily be easily instigated using various tools. Some of the attacks are uncontrollable and hard to prevent, such as cyber-attacks, which caused billions of dollars in a short period of time. Although there is no 100% guaranteed protection network, we can make it as safe as possible by taking security measures. A network with high domain security, will lead to hight time consumption on the attacker side, in addition to cost and effort. To maximize the security, procedures and network security techniques should be implemented for protection. As it is concluded in this survey of various strategies for security and privacy provision, it is evident that network security is crucial both at individual as well as organizational level, whoever uses the internet and Wi-Fi, should be conscious and be careful while surfing the internet. This is also supported by surveying user behaviour in terms of their attitude towards security measures, privacy concerns and awareness of network communication attack vulnerability.

References

[1] Steele, C., "Why is Computer Networking Important?," 2019. Available: http://www.digitaldividecouncil.com/why-is-computer-networking-important/ [Accessed: 13-Nov-2019].

[2] Rouse, M. et al., "What is metropolitan area network (MAN)?," 2005. Available: https://searchnetworking.techtarget.com/definition/metropolitan-area-network-MAN [Accessed: 13-Nov-2019].

[3] Tiwari, A., "What Is The Difference Between LAN, WAN, MAN, CAN, VPN, BAN, NAN, SAN?," 2017. Available: https://fossbytes.com/difference-lan-wan-man-can-vpn-ban-nan-san/ [Accessed: 13-Nov-2019].

[4] Gilani, S., "Mobile Phone Security: All You Need to Know," 2018. Available: https://www.technewsworld.com/story/85661.html [Accessed: 13-Nov-2019].

[5] "Symmetric vs Asymmetric Encryption - Which One is More Secure?," Cheap SSL Shop. Available: https://www.cheapsslshop.com/blog/symmetric-vs-asymmetric-encryption-whats-the-difference/. [Accessed: 13-Nov-2019].

[6] P. Smirnoff and D. M. Turner, "Symmetric Key Encryption - why, where and how its used in banking," Cryptomathic. Available: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking. [Accessed: 13-Nov-2019].

[7] M. Kranch and J. Bonneau, "Upgrading HTTPS in mid-air: An Empirical Study of Strict Transport Security and Key Pinning," Proceedings 2015 Network and Distributed System Security Symposium, 2015.

[8] J. Teh, "HTTP vs HTTPS: The Difference And Everything You Need To Know," SEOPressor WordPress SEO Plugin HTTP vs HTTPS The Difference And Everything You Need To Know Comments, 2019. Available: https://seopressor.com/blog/http-vs-https/. [Accessed: 13-Nov-2019].

[9] Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Bailey, J. A. Halderman, and V. Paxson, "The Security Impact of HTTPS Interception," Proceedings 2017 Network and Distributed System Security Symposium, 2017.

[10] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," International Journal of Ad Hoc and Ubiquitous Computing, vol. 17, no. 4, p. 197, 2014.

[11] EvilSin225, "Безопасность при подключении к общественным Wi-Fi-сетям," Компьютерные технологии, 2017. Available: https://computerinfo.ru/bezopasnost-pri-podklyuchenii-k-wi-fi/. [Accessed: 13-Nov-2019].

[12] Doavi, Abdollah, Hossein Parvan, A. A. Salama, Mohamed Eisa, S.A.El-Hafeez, Mai M. Lotfy and AbdolNabi Ansari-Asl. "Security in Wireless Sensor Networks," International journal of Computer Science & Network Solutions, vol. 3, no. 1 2015.

[13] Passi, H., "What Is A Sniffing Attack And How Can You Defend It," 2018. Available: https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it [Accessed: 13-Nov-2019].

[14] Swinhoe, D., "What is a man-in-the-middle attack?," How MitM attacks work and how to prevent them, 2019. Available: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html [Accessed: 13-Nov-2019].

[15] Dobran, B., "7 Proven Tactics To Prevent DDoS Attacks: Make a Security Plan Today!," PhoenixNAP Global IT Services, 2018. Available: https://phoenixnap.com/blog/prevent-ddos-attacks [Accessed: 13-Nov-2019].

[16] Comtact, "What is the CIA triad?," What is the CIA triad?. Available: https://www.comtact.co.uk/blog/what-is-the-cia-triad. [Accessed: 13-Nov-2019].

[17] Reddy, B.I., & Srikanth, V., "Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2019.

[18] A. Almusaylim, Z., Jhanjhi, N. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Pers Commun (2019). https://doi.org/10.1007/s11277-019-06872-3

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

[20] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-7.

[21] 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

[22] 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), 481-487.

[23] M. Almulhim, N. Islam and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications", International Journal of Computer Science and Network Security 19 (1), 107-120.

[24] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020.

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

[26] Noor Zaman, and Mnueer Ahmed, "Towards the Evaluation of Authentication Protocols for Mobile Command and Control Unit in Healthcare," Journal of Medical Imaging and Health Informatics, Vol 7, no 3, pp 739-742, 2017

[27] Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z. Jhanjhi, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review, Ad Hoc Networks, Volume 101, 2020, 102096, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102096

[28] Vasaki Ponnusamy, Thinaharan Ramachandran, Low Tang Jung and Noor Zaman, "Bio-Inspired Energy Scavenging in Wireless Ad Hoc Network", in IEEE Innovations in Electrical Engineering and Computational Technologies (ICIEET), April 2017 Karachi Pakistan

[29] Fatimah Abdualaziz Almusalli, Noor Zaman and Raihan Rasool "Energy Efficient Middleware: Design and Development for Mobile Applications", in 19th IEEE International Conference on Advance Communication Technology ICACT 2017, February 2017 Korea.

[30] Noor Zaman, Tung Jang Low, Alghamdi, "Energy efficient routing protocol for wireless sensor network", in 16th IEEE International Conference on Advance Communication Technology ICACT 2014,. February 2014, pp. 808-814 Korea

[31] N. A. Khan, NZ. Jhanjhi, S. N. Brohi, A. Nayyar, "Emerging use of UAV's: secure communication protocol issues and challenges," in Drones in Smart-cities: Security and Performance 1st Edition Security and Performance, ISBN: 9780128199725, Elsevier 2020

[32] K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", International Conference on Computer and Information Sciences (ICCIS), 1-4, 2019.

[33] M. Lim, A. Abdullah, N. Jhanjhi, M. Khurram Khan and M. Supramaniam, "Link Prediction in Time-Evolving Criminal Network With Deep Reinforcement Learning Technique," in IEEE Access, vol. 7, pp. 184797-184807, 2019. doi: 10.1109/ACCESS.2019.2958873

[34] Alyssa Anne Ubing, Syukrina Kamilia Binti Jasmi, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam, "Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning" International Journal of Advanced Computer Science and Applications(IJACSA), 10(1), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100133.

[35] A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA," International Journal of Communications, Network and System Sciences, vol. 08, no. 12, pp. 483–491, 2015.

[36] Ainsworth, Q., "Data Collection Methods," 2019. Available: https://www.jotform.com/data-collection-methods/ [Accessed: 13-Nov-2019].

[37] "Connecting to the Secure Wireless Network in Mac OS X 10.9, 10.10, 10.11, or macOS 10.12, or 10.13," Information Technology Services. Available: https://its.truman.edu/docs/connecting-to-the-secure-wireless-network-in-mac-os/. [Accessed: 13-Nov-2019].

[38] A. L. N. HasanahPercayalah, "Apa Saja Perbedaan PROXY dan VPN? Selengkapnya Cek Disini!," Nesabamedia, 2019. [Online]. Available: https://www.nesabamedia.com/perbedaan-proxy-dan-vpn/. [Accessed: 13-Nov-2019].

[39] Online Domain Tools, (n.d.). 'Password Checker Online'. [image]. Available at: http://password-checker.online-domain-tools.com/

[40] TheBest VPN, "5 Basic Network Security Tips for Small Businesses," IT Infrastructure Advice, Discussion, Community - Network Computing, 2017. Available: https://www.networkcomputing.com/network-security/5-basic-network-security-tips-small-businesses [Accessed: 13-Nov-2019].

[41] Rouse, M. et al., "What is Asymmetric Cryptography?," 2019. Available: https://searchsecurity.techtarget.com/definition/asymmetric-cryptography [Accessed: 13-Nov-2019].

[42] Rubens, P., "How to secure your Wi-Fi at home and in your business," 2018. Available: https://www.techradar.com/sg/news/networking/wi-fi/five-tips-for-a-secure-wireless-network-1161225 [Accessed: 13-Nov-2019].

[43] Gray, J., "Wireless Network and Wi-Fi Security Issues to Look Out For in 2019," AT&T Cybersecurity, 2019. Available: https://www.alienvault.com/blogs/security-essentials/security-issues-of-wifi-how-it-works [Accessed: 13-Nov-2019].

[44] Irei, A., "Differences among WEP, WPA and WPA2 wireless security protocols," 2019. Available: https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2 [Accessed: 13-Nov-2019].

[45] Dosal, E., "How to Secure a Business Network: 10 Easy Steps," Compuquip Cybersecurity, 2018. Available: https://www.compuquip.com/blog/how-to-secure-a-business-network-10-easy-steps [Accessed: 13-Nov-2019].

[46] Chia, T., "Confidentiality, Integrity, Availability: The three components of the CIA Triad," Stack Exchange Security Blog, 2012. Available: https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/ [Accessed: 13-Nov-2019].