Examining the Impact of Cyber security on Wireless Sensor Networks

Mohanad Hameed Rashid[1*]

* 1 Department of Total Quality Computer Science and Information Systems, Ministry of Education, Directorate of Anbar Education, Ramadi, Iraq
E-mail: [1*] rashid_mohanad@yahoo.com

ABSTRACT

Information systems have been used in most spheres of life in the last two years. Simultaneously, the risk of security threats has increased dramatically. These attacks take a variety of forms aimed at destroying system data or even shutting down their operations. A study of cyber-threats (attacks) on Wireless Sensor Networks (WSNs) is described in this publication. The consequences of cyber-threats on the WSN according to network tiers, as well as privacy concerns, are depicted in this paper. The study's findings include a classification of these attacks that can lead to the development of cyber-security solutions that can prevent them from causing damage to the information systems concerned.

Keywords: Cyber security , Wireless sensor networks , attacks

1. Introduction

A Wireless Sensor Network (WSN) is a collection of sensors that work together to monitor the physical environment. Sensor nodes use their wireless radios to communicate with one another as well as with the base station (BS) for data storage, processing, and exchange. WSNs are resource constrained, so normal protocols aren't an option. WSN consists of various kinds of sensor nodes that are linked through wireless channels and are able to provide digital interfaces to physical things. It is a crucial part of the Internet of Things (IoT) [1]. The Internet of Things (IoT) is a network of various things that are joined together through servers, sensors, software, and other hardware. IoT components can be used as devices in the cyber world to improve their usability and serviceability. WSN and IoT environments, on the other hand, are targeted by a variety of threats, including cyber ones. As a result, it is necessary to investigate these attacks from many angles in order to develop remedies, which will be provided as cyber-security systems. Threats and attacks can be classified based on their impact on information systems, such as data loss, layer construction, and system operation.

2. Materials and Methods

Classification of threats in WSN - Cyber - Security Systems

Banking, healthcare, education, emergency services, and the military have all become more reliant on cyberspace, which has the potential to increase the level of complexity. Inaccurate information is disseminated, tactical services are hindered, sensitive data is accessed, espionage is carried out, data is stolen, and financial loss is caused by cyber-attacks (threats).Over time, the nature, complexity, and severity of these attacks have developed in such a way that their complexity has grown as

well. Because security systems are weak in comprehending how these attacks work, many companies and governments are vulnerable to attack. Developing efficient security measures involves a thorough understanding of such assaults and their classification, which is based on the following criteria: purpose, legal classification, involvement severity, scope, and so on [2].

Furthermore, because sensor nodes are placed unattended, WSN systems are more vulnerable to various security attacks. The well-known attacks are grouped in this section based on their effects on the WSN layers [3]–[5]. Figure (1) depicts the classification of assaults (threats) based on their impact on WSN layers .The attacks (threats) in cyber-based WSNs work in several layers, but the majority of them work on the application layer, as shown in Fig (1). The Distributed Denial of Service (DDoS) assault is a multi-layer attack that can efficiently disrupt the working flow of various layers to achieve noticeable results. issues. Some of them are discussed here so that you can learn more about each threat (attack).

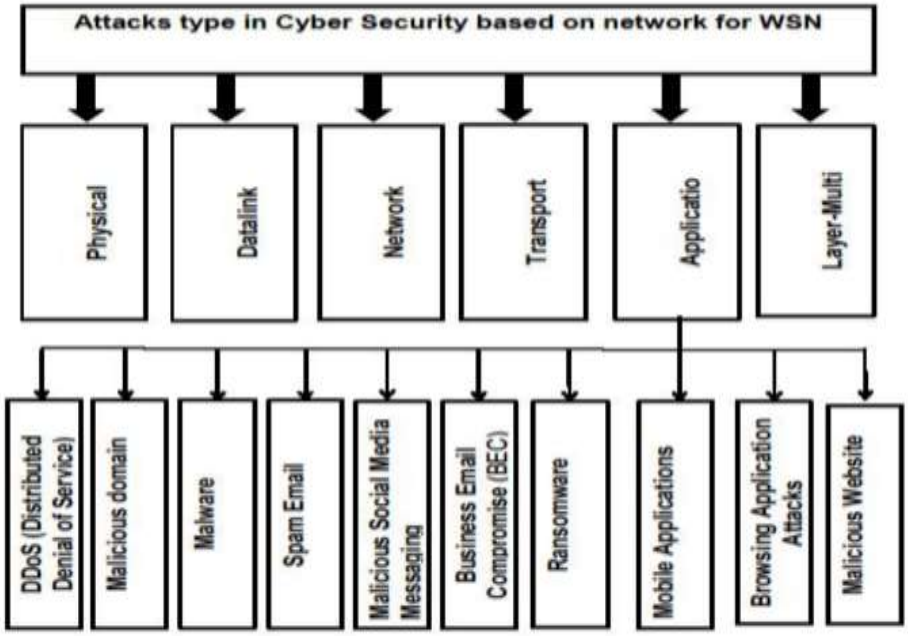

Figure 1. Cyber-Attack on WSN layers

2.1. DDos(Distributed Denial of Service)

It is a well-known network attack that uses a collection of zombie computers to flood the host server with a huge number of requests via geographically spread internet connections, disrupting and blocking genuine user requests. DDoS impairs service by generating network congestion and preventing network components from carrying out their normal functions, which is much more disruptive for IoT [6]. The distinction between DoS and DDoS is that DDoS attacks the target by doing more than just connecting to the internet, making it harder to detect and execute through botnets or machines controlled by the attacker. DoS is carried out with the use of a script or a DoS tool [7].

DDoS affects all layers of the Open Systems Interconnection (OSI) model, Secure Sockets Layer (SSL), User Datagram Protocol (UDP), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol (FTP), and Internet Control Message Protocol (ICMP) are among the protocols used. Code-division Multiple Access

(CDMA), coding, modulation, and transmission media [8] , [9]. The WSN Dataset (WSN-DS) is commonly used in WS to identify and classify DoS attacks. WSN-DS enables the use of a variety of intelligence and data mining approaches to improve the detection and categorization of DoS attacks [10],DDoS is classified as shown in Fig (2).

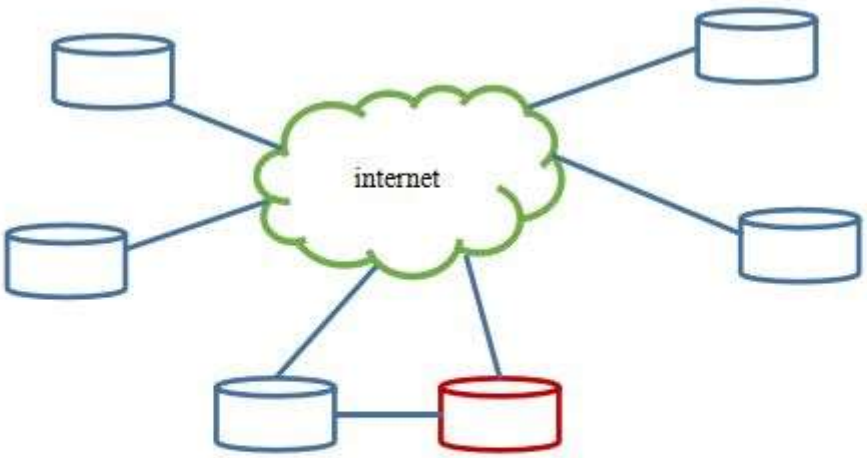

Figure 2.DDos attacks

2.2. Malicious domain

Malicious domains are regarded as the most critical resources that adversaries require in order to conduct operations on the Internet. The DNS (Domain Name System) protocol is an important part of the Internet. It simplifies Internet Protocol (IP) addresses that are tough to remember into easy-to-remember domain names. When compared to other methods, DNS data analysis for detecting rogue domains provides a number of advantages. For starters, DNS data only accounts for a small part of overall network traffic, making it ideal for analyzing large or small networks that cover a wide range of topics. Furthermore, it typically aids in the reduction of the amount of data to be analyzed, allowing researchers to explore DNS traffic to Top Level Domains (TLD). Furthermore, useful characteristics in DNS traffic for specific danger behavior, such as domain owner and autonomous system (AS) number, have made DNS traffic important for testing artificial intelligence algorithms to detect disasters before they occur [11]. Malicious domains are classified as shown in Fig. (3).

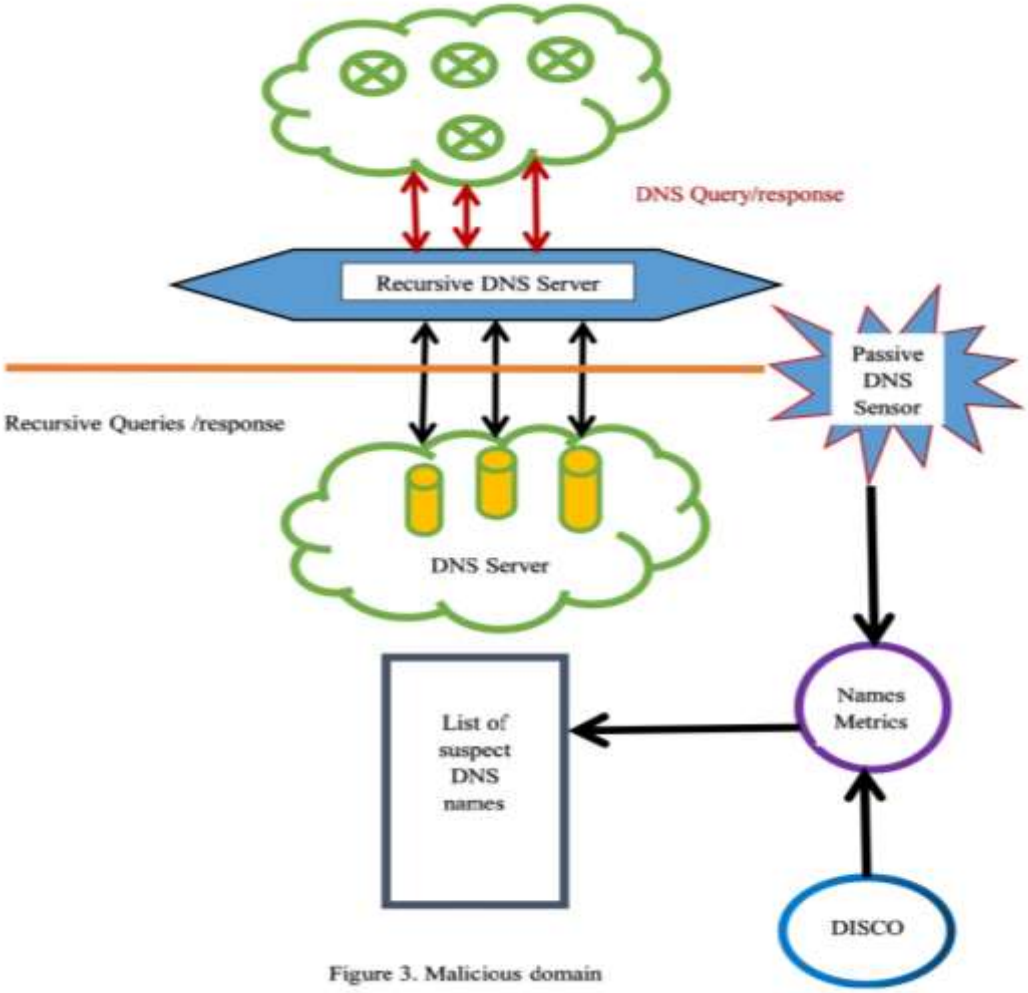

Figure 3. Malicious domain

2.3. Malware

Malware is just malicious code that poses as a helpful piece of software, message, document, or data and exploits all system weaknesses. Some dangerous programs, including Trojan horses, spyware, viruses, and rootkits, require the use of a host application to mask their tracks, while others, like worms, automated viruses, and botnets, can live and spread on their own. A Trojan, rootkit, virus, worm, and botnet are all types of malware that are packaged together for survival, transmission, and command and control . According to [12], malware is classified as shown in Fig (4).

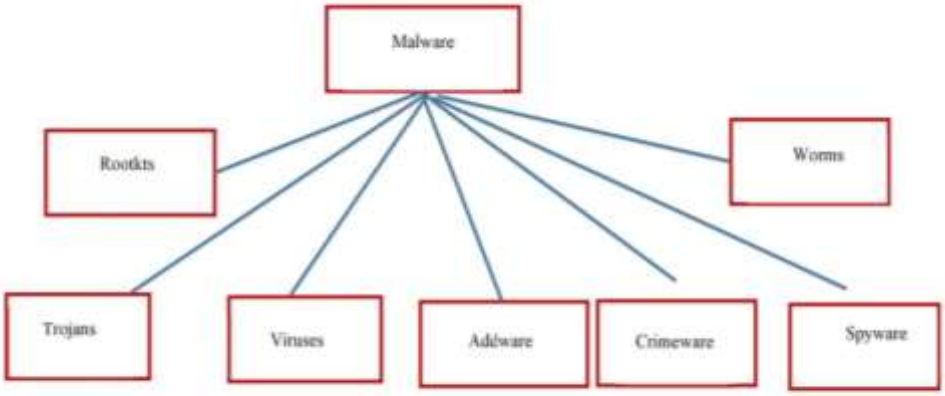

Figure 4. types of malware

2.4. Spam Email

It is commonly used by a variety of applications, including fraudsters and hackers, to achieve their goals of destroying data in an unrecoverable manner. In the application layer, the received spam message can record the entire system in WSN, confusing the operating system and the applied application. Spam email is classified as shown in Fig. (5).

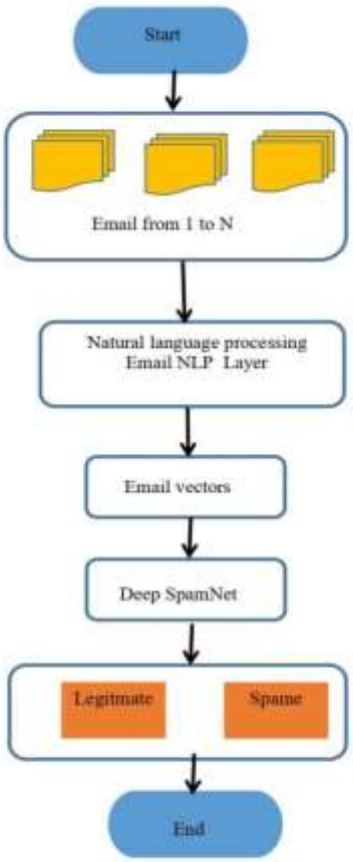

Figure 5. Spam Email

2.5. Malicious Social Media Messaging

Social media allows people to interact and share life events, images, and videos. Excessive sharing or a failure to recognize impostors, on the other hand, might put the organization and its employees at risk. distinct accounts Typically, social media accounts are used by attackers during the reconnaissance stage of a social engineering or phishing campaign. Social media may provide attackers a platform to impersonate reliable individuals and businesses and the information they need to launch further assaults like social engineering and phishing [13]. Phishing is a type of online attack that focuses on obtaining the user's identity, notably on social networking platforms. It also gives the infected people fictitious instructions that can help them gain their user name and password more quickly. This attack uses a two-step technique that begins with sending a friend request and continues with the attack's ability to obtain the identity after it is accepted [14]–[15].

2.6. Business Email Compromise (BEC)

The attacker must appear as unobtrusive and credible as possible when performing an email-only attack. This can be done in a number of ways, but one of the most effective is to format an email such that it appears to be a typical part of the company's business dealings. BEC (business email compromise) is one of the most expensive cyber-security risks. It takes numerous forms, including transferring money to the attacker by receiving some emails from the victim or by following fishing links and impersonating the leaders to direct the transfer. This category is aimed towards money-making companies or global providers. BEC is classified as shown in Fig (6).

For example, the attacker breaks into a network of wireless sensors used to store the COVID-19 vaccine and sends a large number of doses to a secure location or kills current doses by changing the temperature of the containers and demanding fresh ones. BEC scams are classified into six types [16]-[17]:

- Bogus Invoice Scheme : It relies on consumers, providers, and suppliers exchanging emails with one another. While they exchange information via email, the supplying firms are available for BEC to connect with.
- CEO Fraud : For the purpose of moving funds to accounts controlled by the attackers in certain banks, the attacker writes official emails to the executives of the firms. This is accomplished using unfollowable urgent communication links.
- Account Compromise : The aim of this attack is to inform employers to transfer money to specific bank accounts in official emails from trusted institutes.
- Attorney Impersonation : Attackers use fictitious identities, such as those of lawyers, to send emails to people who require information such as phone numbers and other details in a more secure way. These assaults often target lower-level workers because they lack the expertise to evaluate the legitimacy of the request .
- False Invoice Scheme : This method, where attackers pose as suppliers and seek money transfers for payments to an account held by fraudsters, is often used to target businesses with international suppliers.
- Data Theft : In order to get personal or tax information for such a person, this kind targets human resources leaders or workers.

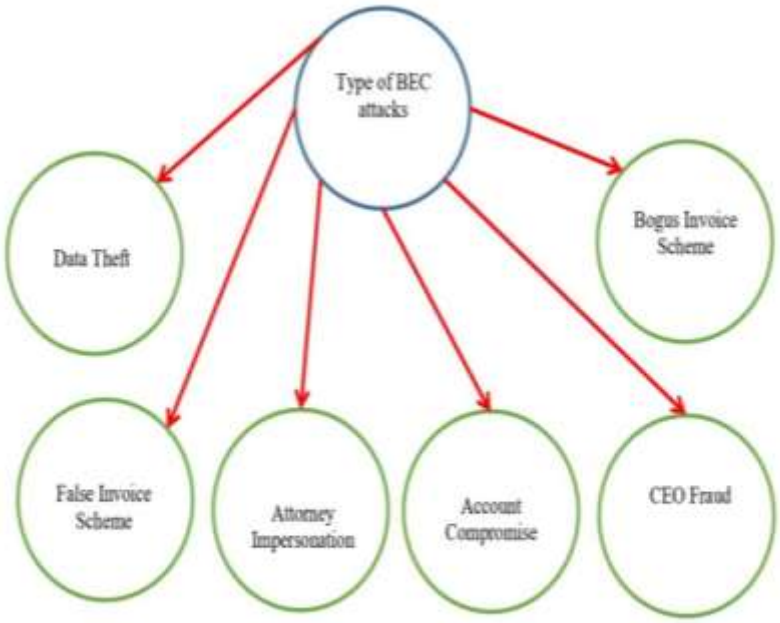

Figure 6. Business Email Compromise (BEC)

2.7. Ransomware

Email phishing and spam addressed to administrators of adopted WSNs are the most common ways for ransomware to proliferate. The majority of ransomware assaults are email-based, and staff members aren't taught how to spot a malicious email attachment. One of the best ways for a business to protect itself against ransomware is to teach personnel to be more alert to assaults, even if this requires time and money. The IoT has infiltrated our lives by establishing an indirect contact link between people and linked gadgets, leaving a large area for attackers to execute their job in a bad way. One of the scariest assaults that IoT networks face is an application layer ransomware attack. [18]-[19]

2.8. Mobile Applications

It is now possible to monitor and control a network of wireless sensor-based IoT devices using a mobile phone. These applications employ a client-server architecture. Operating systems such as Android and iOS have improved user safety. The programs are downloaded to mobile devices utilizing various platforms, which are constantly being updated. Apps are used to download these types of programs to the smartphone. In contrast, the developer's server is critical in ensuring that such devices work properly. It encompasses all web applications that deal with data exchange with clients. This is accomplished by utilizing the mobile network's communications links. As a result, the server is regarded as the most important component because it houses all of the data and information. To protect devices from attacks, security measures are available for mobile and web applications [20] – [21]. Mobile applications are classified as shown in Fig. (7).

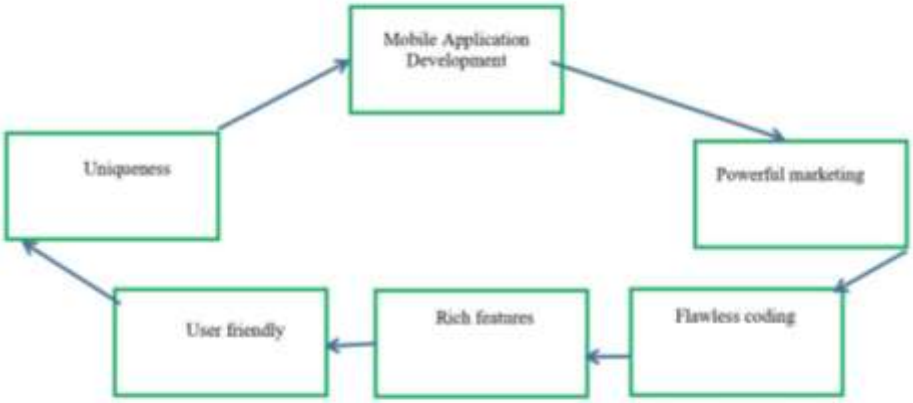

Figure 7. Mobile Application Development(MAD)

2.9. Browsing Application Attacks

Browser assaults are frequent and have damaged unprepared information systems, especially those that employ WSN. The majority of well-known browsers have security mechanisms in place to defend them against this attack. Unfortunately, capability-based security is only poorly implemented in the most widely used OS systems, seldom going beyond application permission sharing. To defend against the attacks mentioned, additional security measures in the form of software or plug-ins are often needed [22–25].

2.10. Malicious Website

On the WSN and IoT, a malicious website can be used to install malware without permission. After installation, it downloads information from the infected device, including photographs, movies, and other files. A drive-by download, on the other hand, usually necessitates some effort on your part. Without your permission, the website attempts to install software on your machine. Rogue websites, on the other hand, frequently appear to be legitimate. They may occasionally prompt you to install software that your computer appears to need. For example, a video website may prompt you to download a codec, which is a little piece of data that a video player needs to function on the site. You may be used to installing secure codecs, but they are a risky installation that could put your device and vital data at risk. Similarly, a website may ask for permission to install one program but then install another on your computer that you do not want.

Google's Safe Browsing data is one source that can help us figure out how common hazardous websites are. Phishing websites are getting more common, but malware sites are becoming less popular among hackers, according to Google statistics [26]. The attacker can utilize server-side or client-side redirection to force the browser to connect to the infected website. Various frameworks are used in targeted attacks to disrupt the website's performance. In the event of an infection, this structure has two tasks:

Redirect :The attacker placed the assaulting program on the target website in order to recruit users to a certain malicious domain. If the attackers are unable to get access to the website, the redirection process is used. The same attempt to access the specified website is made several times.

-Exploit : The attacker utilizes an automated exploit framework like BEP on the infected domain. An exploit can be loaded directly from the BEP by a malicious iframe [27-29].

3. Discussion

As previously said, cyber-attacks take several forms and can harm the targeted target in a variety of ways, including workflow, structure, datasets, and so on. In order to impair the functioning of the network and cause a malfunction, these attacks also target a

particular layer of the OSI structure of the network. The most common attack types are classified in Fig. (1), which demonstrates the real impact of such attacks on the entire layer, including the protocols used. The majority of them operate on the application layer, which deals with data processing and information as well as user interaction. with the final outcomes. DDoS attacks are distinct in that they operate across multiple tiers, and they are considered the most dangerous cyber-attacks. When reading the explanations for these attacks, a clear picture of each attack's behavior emerges. As a result, a powerful cyber-security system capable of detecting and predicting attacks in their early phases is being developed. Furthermore, a variety of solutions can be provided to overcome data and information loss, particularly in real-time systems with crucial data.

4. Conclusion

Effective classification is used for cyber-attacks. This categorization was determined using the effects of attacks on layers and associated procedures. The results of this study pave the way for the creation of proactive cyber-security tools that may lessen the risks associated with such assaults on information systems. To provide researchers a comprehensive understanding of the labor steps involved, precise information about the most frequent assaults was also provided. However, a discussion was convened to concentrate on the key aspects of the cyber-attacks that were raised.

5. Acknowledgments

The authors thank the Ministry of Education/Directorate of Education Department of Total Quality in Anbar, and its facilities, which helped improve the quality of this work.

References

1. A. Johana, S. Johan, M.T. Portocarrero, "Contrasting Internet of Things and Wireless Sensor Network from a conceptual overview", IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), December 2016, p.p 252-257
2. M. Uma, G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification", International Journal of Network Security, Vol.15, No.5,September 2013, PP.390-396.
3. U. Jain, M. Hussain, " Wireless Sensor Networks: Attacks and Countermeasures", 3rd International Conference on Advances in Internet of Things and Connected Technologies, 2018.
4. D. Reed, " Applying the OSI Seven Layer Network Model To Information Security", SANS Institute Information Security Reading Room, November 21, 2003.
5. M. Ahemd, M. Shah, Abdul Wahid, " IoT Security: A Layered Approach for Attacks & Defenses", International Conference on Communication Technologies, April 2017, p.p 104 - 110.
6. 6. C. Zhang, R. Green, " Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack Over IoT Network", SpringSim, January 2015.
7. R. Rizal, I. Riadi, Y. Prayudi, " Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) ", International Journal of Cyber-Security and Digital Forensics, September 2018, p.p 382 – 390.
8. 8. H. Obaid, E. Abeed, " DoS and DDoS Attacks at OSI Layers", International Journal of Multidisciplinary Research and Publications, Volume 2, Issue 8, 2020, pp. 1-9.
9. 9. P. Sinha, A. Rai, V. K. Jha, B. Bhushan, " Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A

Survey", International Conference on Signal Processing and Communication, July 2017, p.p 288 – 293.
10. 10. T.Huong Le, T. Park, D. Cho, H. Kim, "An Effective Classification for DoS Attacks in Wireless Sensor Networks", IEEE, Tenth International Conference on Ubiquitous and Future Networks (ICUFN), August 2018, p.p 689 – 692.
11. 11. Y. Zhauniarovich, I. Khail, T. Yu, "A Survey on Malicious Domains Detection through DNS Data Analysis", Qatar Computing Research Institute, Vol. 51, No. 4, Article 67. July 2018.
12. 12. C. Hwa, J. David Irwin, Introduction to Computer Networks and Cyber security, Taylor & Francis Group, 2013.
13. 13. J. Deogirikar, A. Vidhate, "Security Attacks in IoT: A Survey", IEEE, International conference on I-SMAC, October 2017, p.p 32-37.
14. 14. M. Al-Kasassbeh, M. Almseidin, K. Alrfou, S. Kovacs, " Detection of IOT-botnet attacks using fuzzy rule interpolation", Journal of Intelligent & Fuzzy Systems xx, July 2020.
15. 15. H. Parker; S. Flower day, " Contributing factors to increased susceptibility to social media phishing attacks", South African Journal of Information Management, 2020.
16. 16. L. Remorin, R. Flores, B. Matsukawa, " Tracking Trends in Business Email Compromise (BEC) Schemes", Trend Micro Forward-Looking Threat Research (FTR) Team, eBook, 2018.
17. 17. N. Al-Musib, F. Al-Serhani, M. Humayun, N.Z.Jhanjhi, "Business email compromise (BEC) attacks", International Virtual Conference on Sustainable Materials, Elsevier, 2021.
18. 18. M. Humayun, NZ Jhanjhi, A. Alsayat, V. Ponnusamy," Internet of things and ransomware: Evolution, mitigation and prevention", Egyptian Informatics Journal, Elsevier, 2020, p.p 105-117.
19. 19. F. Malecki, S.Craft, "Best practices for preventing and recovering from a ransomware attack", Computer Fraud & Security, March 2019.
20. 20. PTsecurity Company, "Vulnerabilities and threats in mobile applications ", Report, 2019, https://www.ptsecurity.com/ww-en/, 12-2-2021, 8:pm.
21. 21. N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli, " EyeSim: A Mobile Application for Visual-Assisted Wormhole Attack Detection in IoT-enabled WSNs", 9th IFIP Wireless and Mobile Networking Conference, August 2016.
22. 22. B. Akhgar, H. Arabnia, " Emerging Trends in ICT Security", Elsevier, Chapter 3 - Authorization and Access Control, 2014.
23. 23. B. Akhgar, H. Arabnia, " Emerging Trends in ICT Security", Elsevier, Chapter 28 - Man-in-the-Browser Attacks in Modern Web Browsers, 2014.
24. 24. S. Yu, G. Zhao, S. Guo, Y. Xiang, A. Vasilakos, " Browsing Behavior Mimicking Attacks on Popular Web Sites for Large Botnets", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), June 2011, p.p 947-951.
25. 25. X. Luo, X. Di1, X. Liu1, H. Qi1, J. Li1, L. Cong, H. Yang, “Anomaly Detection for Application Layer User Browsing Behavior Based on Attributes and Features", IOP Conf,, June 2018.
26. 26. X. Li, B. Azad, A. Rahmati, N. Nikiforakis, " Good Bot, Bad Bot: Characterizing Automated Browsing Activity", IEEE Symposium on Security and Privacy (SP) , August 2021.
27. 27. A. Sood, R. Enbody, " Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware", 1st

Edition, Kindle Edition, Chapter 4 - System Exploitation, Pages 37-75, 2014.

28. 28. A. AL-Hamami, S. Hashem, " A proposed Firewall Security Method against Different Types of Attacks", Iraqi Journal of Computers, Communications, Control and System Engineering, 2005, Vol. 5, Issue 1, p.p 65-74.
29. 29. S. Hashim, M. Jawad, B. Wheedd, "Study of Energy Management in wireless Visual Sensor Networks", Iraqi Journal of Computers, Communications, Control and System Engineering, 2020, Vol. 20, Issue 1, p.p 68-75