DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

Study of Cyber Security Effects on Wireless Sensors Networks

Shaymaa Mahmood Naser[1], Yossra Hussain Ali[2]
[1,2]Department of Computer Science, University of Technology, Baghdad, Iraq
[1]cs.19.29@grad.uotechnology.edu.iq, [2]yossra.h.ali@uotechnology.edu.iq

Abstract- *In recent two years, information systems have been adopted in most fields of life due to the health state around the world. At the same time, the risk factor of security attacks is increased sharply as well. These attacks consider different actions toward damaging the data of systems or even making down their work. In this paper, a study of cyber-threats (attacks) on Wireless Sensor Network (WSN) is presented. This study illustrates the effects of the cyber-threats on the WSN according to the network layers, as well as their privacy concerns. The outcome of this study is the classification of these attacks that can lead to produce cyber-security systems which can prevent them from damaging the involved information systems.*

Index Terms— *Cyber-Security, Wireless Sensor Network, Internet of Things.*

I.INTRODUCTION

Sensors in a Wireless Sensor Network (WSN) operate together to monitor the physical surroundings. Sensor nodes use their wireless radios to connect each with other and with the Base Station (BS) as well for storing, processing and exchanging the data. The resource constrained nature of WSNs prevents the usage of standard protocols. Because of comprising of a different type of sensor nodes that are connected through wireless channels and capable of giving digital interfaces to real-world objects, WSN is a main part of the Internet of Things (IoT) [1], [2]. The IoT is defined as a network of scattered devices that are linked together by software, servers, sensors, and other devices. The parts of IoT can be involved in the cyber world as devices that can improve their usability and serviceability [3], [4].

At the other hand, the WSN and IoT environments are attacked by different types including the cyber ones. Therefore, there is a need to analyze these attacks in different directions for producing solutions, presented as cyber-security systems. The threats or attacks can be analyzed according to the effect of them on the information systems, such as data damage, layer constructing, and system operation.

II. CLASSIFICATION OF THREATS IN WSN-CYBER-SECURITY SYSTEMS

Banking, hospitals, education, emergency services, and military have all become increasingly reliant on cyber-space that can affect the level of complexity. Cyber assaults (attacks/threats) are used to disseminate false information, disable tactical services, get access to sensitive information, conduct espionage, steal data, and cause financial damage. Over time, the nature, complexity, and severity of these attacks are developed in which their complexity is increased as well. Many organizations and countries can be attacked because of the weakness of security system in understanding the work mechanism of these attacks. Developing effective security measures necessitates a full understanding of such assaults and their classification, which is established on the following criteria: Purpose Legal Classification, severity of Involvement, Scope and on

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

Network Types (Wireless Sensor Network (WSN), Mobile Ad Hoc Network (MANT)) [5]. In addition, systems with WSN are more vulnerable to various security assaults since sensor nodes are deployed unattended.

In this section, the well-known attacks are classified according to their effects on the layers of WSN [6]-[8]. *Fig.* 1 explains the attacks (threats) classification according on their effect of WSN layers.

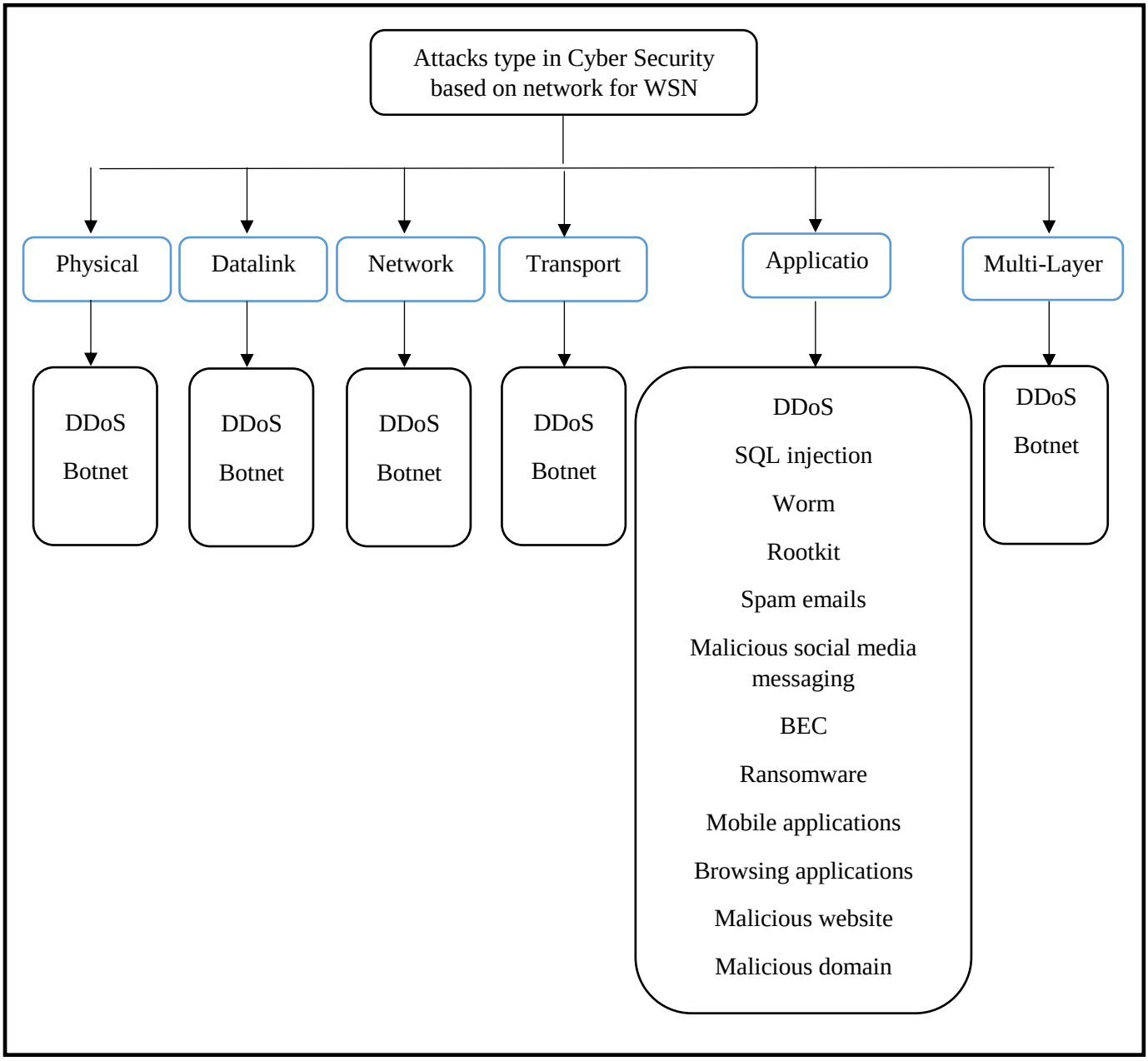

FIG. 1. CYBER-ATTACK ON WSN LAYERS

From *Fig.1*, it is well shown that the attacks (threats) in cyber based WSN work in different layer, but most of them in application layer. The Distributed Denial of Service (DdoS) type is a multi-layer attack that can affect the working flow of these layers in efficient way to produce noted

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

problems. In order to know more information regarding each threat (attack), some of them are explained below.

A. DDoS Attack

DDoS (Distributed Denial of Service) is a well-known network attack that disrupts and blocks legitimate user requests by flooding the host server with a large number of requests via geographically distributed internet connections employing a collection of zombie computers. DDoS degrades service by causing network congestion and preventing network components from performing their regular activities, which is significantly more disruptive for IoT [9]. The difference between DoS and DDoS is that DDoS uses more than just connecting to the internet to attack the victim, making it difficult to detect and execute through botnets or devices under the attacker's control. Whereas DoS is carried out using a script or a DoS tool [10]. DDoS has an impact on all layers of the Open Systems Interconnection (OSI) model, including Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol (FTP), Secure Sockets Layer (SSL), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Code-division multiple access (CDMA), coding, modulation, and transmission medium [5], [11], and [12]. The WSN Dataset (WSN-DS) is usually used in WS for DoS attack detection and classification. WSN-DS allows numerous intelligence and data mining methodologies to be used for better detection and classification of DoS assaults [13].

B. Malicious domain

Malicious domains are considered as the most important resources that adversaries need to carry out operations on the Internet. The Domain Name System (DNS) protocol is a critical component of the Internet. It converts difficult-to-remember Internet Protocol (IP) addresses into simple domain names. When it is compared to other methods, detecting malicious domains through DNS data analysis has a number of advantages. For starters, DNS data makes up a modest portion of overall network traffic, making it appropriate for studying large or small networks that cover different areas. Moreover, it normally helps in reduction of the amount of data to be evaluated, in which the researchers are allowed to investigate DNS traffic to Top Level Domains (TLD). Furthermore, there are useful characteristics in the DNS traffic for specific threat behavior like domain owner, and Autonomous System (AS) number, for this reason traffic if DNS became important to testing the artificial intelligent algorithms to detect the disaster before happening [14].

C. Malware

Malware is just malicious code that disguises itself as a helpful piece of software/message/document/data and exploits any and all system weaknesses. Some dangerous programs, such as Trojan horses, spyware, viruses, and rootkits, require the usage of a host application to mask their tracks, whilst others, such as Worms, Automated Viruses, and Zombies (Botnets), live and spread independently. A common malware package now includes a Trojan, Rootkit, Virus, Worm, and Botnet, all packaged together for survival and dissemination, as well as command and control [8], [12]. According to [15] and [16] malware is classified as shown in *Fig. 2.*

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

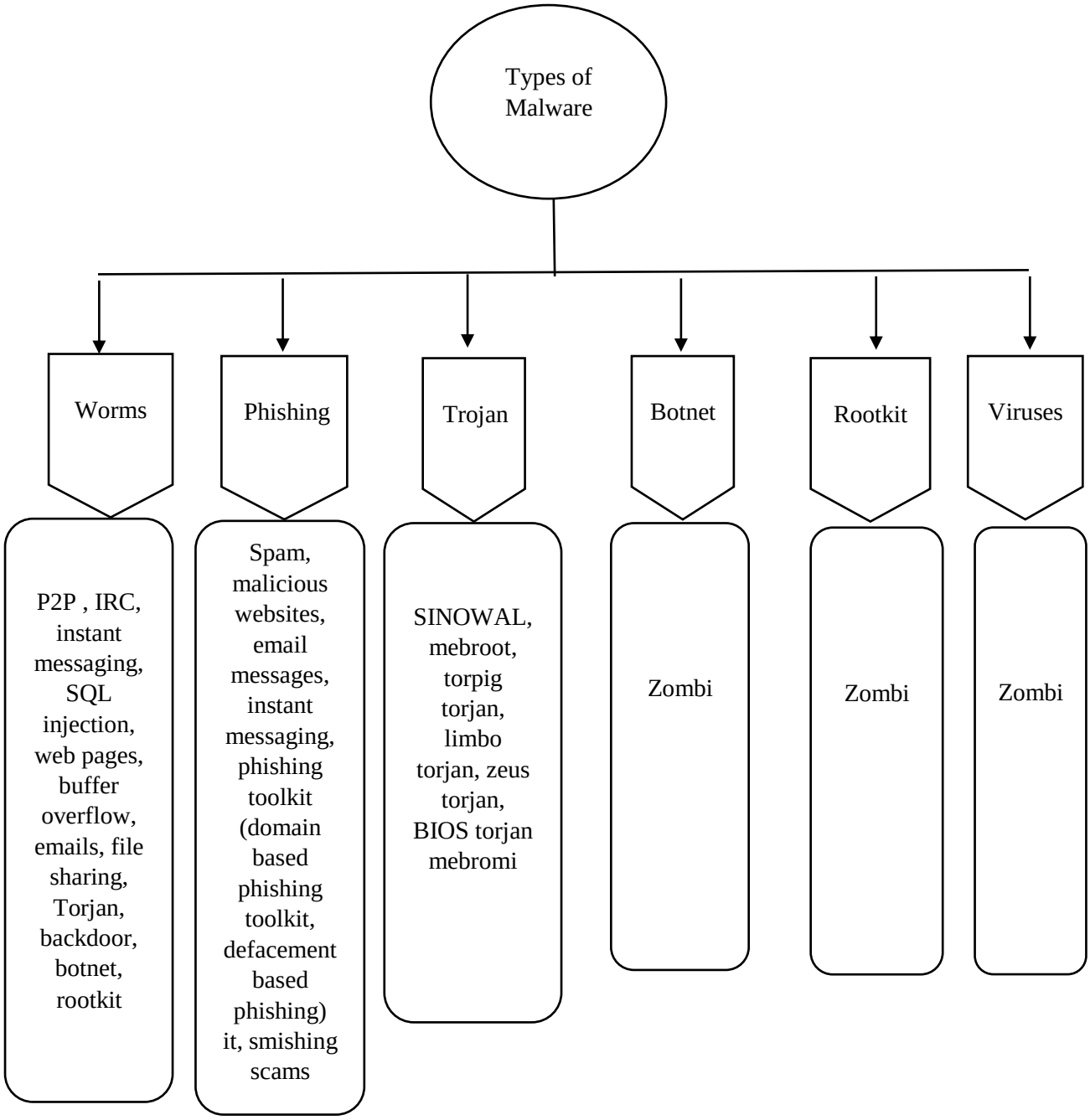

FIG. 2. MALWARE CLASSIFICATION [15], [16]

D. Spam Email

It is usually used in different applications including scammers and hackers in order to obtain their aims of destroying the data in a way that cannot be retrieved. The received spam message can record the whole system in WSN to confuse the operating system and the applied application in the application layer [14] and [16].

E. Malicious Social Media Messaging

People can use social media to connect, share life events, photos, and videos. However, excessive sharing or a failure to spot impostors can result in the compromise of both company and

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

personal accounts. During the reconnaissance phase of a social engineering or phishing operation, attackers frequently use social media accounts. In application layer assaults, social media can provide attackers with a platform to impersonate trusted people and brands, as well as the knowledge they need to carry out subsequent assaults, such as social engineering and phishing [16].

In on-line application, particularly in social media applications, the Phishing attack works on getting the user identity. It also provides the attacked users with fake instructions that can speed up the time of getting the user name and password in efficient way. This attack works in two steps algorithm that starts with sending a friend request and after accepting it, the attack performs its ability in getting the identity [17]-[18].

F. Business Email Compromise (BEC)

When conducting an email-only attack, the attacker must appear as unobtrusive and credible as feasible. This can be accomplished in a variety of ways, but one of the most effective one is to structure an email to appear as if it were a routine part of the organization's business transactions.

Business email compromise (BEC) is one most costly of cyber- security risk that takes several forms that personified to transfer money to attacker by recipient some emails from victim or follows fishing links then impersonates the leaders for oriented the transfer. This type is targeted the organizations that have money or global providers. For example, the attacker hacks the network of wireless sensors for storing the Covid-19 vaccine and transfers a number of doses to a special center, or destroys the existing doses by changing the temperature of the containers and requesting new ones. There are five different types of BEC scams [19]-[20]:

- **Bogus Invoice Scheme**: it works on the email exchanging between the users or providers and the suppliers. The providing companies are available to be attaches by BEC, whilst they use emails for exchanging the information.
- **CEO Fraud:** the attacker sends official emails to the bosses of the companies for transferring money to accounts under the control of attackers in specific banks. This is done through urgent communication links that cannot be followed.
- **Account Compromise**: the aim of this attack is the employers to inform them to transfer money to specific bank accounts in official emails from trusted institute.
- **Attorney Impersonation**: attackers take fake identity, such as lawyers for achieving more secure position to send email for persons requiring information including the phone number and so on.
- **Data Theft**: this type is targeting the employees or leaders in human resources for getting personal or tax information for such person.

G. Ransomware

Ransomware attacks are primarily spread through email phishing and spam sent for administrators of the adopted WSNs. The majority of ransomware assaults are sent via email and many staff is not sufficiently educated to spot a malicious email attachment. While training personnel to be more alert to assaults can be time-consuming and costly, it is one of the most effective ways for a company to defend itself against ransomware. By establishing an indirect contact link between users and connected devices, the IoT has entered to our life with a wide area left for attackers to do their job in a bad way. An application layer ransomware attack is one of the scariest attacks that face IoT network [21]-[22].

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

H. Mobile Applications

Currently, it has become possible to connect a network of wireless sensors based IoTs to a mobile phone for monitoring and controlling purposes. These applications use the structure of client server. The operating systems, such as Android and iOS, increased the safe factors to users. The applications are downloaded to the phone devices using the available platforms that are being always under the development. These types of programs are downloaded to the smartphone from application. At the other hand, the server, hosted by the developer, plays a big role in providing the right operation to such devices. It includes all the web applications that manage the data exchanging with the clients. This is done by using the communications links that are considered in the mobile network. As a result, the server is considered to be the most critical component as it contains the data and information. The security systems are available for mobile and web applications to prevent the devices from attacks [23]-[24].

I. Browsing Application Attacks

Browser attacks are widely distributed and affected the information system that has not considered this type of attacks, particularly in systems that adopt WSN. Most of the well-known browser is protected now against this attack, by applying security system. Unfortunately, the most widely used operating systems only have a rudimentary implementation of capability-based security, which rarely extends beyond permission sharing between apps. In most cases, additional layers of security in the form of programs or plug-ins are required to neutralize the assaults we outlined [25]-[28].

J. Malicious Website

A harmful website can be used in cheated malware installation on WSN and the IoTs. After installation it, the information from the attacked device is downloaded including images, movies and so on. In the event of a drive-by download, however, this usually necessitates some activity on your part. The website tries to install software on your computer without previously obtaining your consent.

At the other hand, rogue websites frequently appear to be trustworthy websites. They may prompt you to install software that your computer appears to require on occasion. A video website, for example, may urge you to install a codec, which is a little bit of data that a video player needs to work on a website. You may be accustomed to install safe codecs, but they are risky installation to jeopardize your device, as well as the important data. Similarly, the website may ask for permission to install one program but actually install another one that you do not want on your computer. Google's Safe Browsing reports are one source that can assist us to determine the prevalence of harmful websites. According to Google statistics, phishing websites are becoming more widespread, whereas malware sites are becoming less popular among cybercriminals [29].

In order to push the browser to connect to the targeted malicious website, the attacker can use server-side or client-side redirection. Different frameworks are used in targeted assaults to disturb the performance of such website. This framework follows two tasks in case of infection:

- **Redirect**: In order to recruit users to specific malicious domain, the attacker installed the attacking program in the target website. The attackers try to enter the website, if they are failed, the redirection process is adopted. The same trying is repeated many times to enter the desired website.
- **Exploit**: On the malicious domain, the attacker uses an automated exploit framework like BEP. An exploit can be loaded straight from the BEP by a malicious iframe [30]-[32].

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

III. DISCUSSION

As explained previously, cyber-attacks are performed in different behaviors and can affect the focused target in numerous ways, such as workflow, structure, datasets, and so on. In addition, these attacks work on specific layer of network OSI structure to disturb the performance of such network to produce a fault results.

The classification of the most popular attack types is shown in *Fig*. 1, which explains the real effect of such attacks on the whole layer including the adopted protocols. Most of them are acting on the application layer as it is related to data processing and information and provides the users with the final results. The DDoS attacks are different as they are working cross different layers, in which they are nominated to be the most danger cyber-attacks.

When the explanation of these attacks is read, a clear idea on each attack behavior is obtained. This leads to build a strong cyber-security system that can detect and predict the attacks in early stages. In addition, numerous solutions can be provided to overcome the losses in the data and information, particularly the real-time systems that have a critical data.

IV. CONCLUSIONS

An efficient classification to cyber-attacks was presented. This classification was performed based on the effects of attacks on layers and related protocols. This study opened the research door for producing active cyber-security systems that can solve the risky problems of such attacks on the information systems. In addition, detailed information for the most popular attacks was included to give a wide vision for researchers to understand the work steps of them, thoroughly. At the other hand, a discussion was provided to look out on the main points of the included cyber-attacks.

REFERENCES

[1] W. Dargie, C. Poellabauer, Fundamentals Of Wireless Sensor Networks: Theory and Practice, WILY, 2010.

[2] 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

[3] F. Yavuz, " Deep Learning in Cyber Security for Internet of Things",M.Sc. Thesis, Istanbul shehir University, 2018.

[4] J. Graham, R. Howard, R. Olson, Cyber Security Essentials, Taylor and Francis Group, 2011.

[5] 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.

[6] U. Jain, M. Hussain, " Wireless Sensor Networks: Attacks and Countermeasures", 3rd International Conference on Advances in Internet of Things and Connected Technologies, 2018.

[7] D. Reed, " Applying the OSI Seven Layer Network Model To Information Security", SANS Institute Information Security Reading Room, November 21, 2003.

[8] 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.

[9] C. Zhang, R. Green, " Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack Over IoT Network", SpringSim, January 2015.

[10] 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.

[11] 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.

[12] 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.

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.21.4.7

[13] 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.

[14] 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.

[15] C. Hwa, J. David Irwin, Introduction to Computer Networks and Cybersecurity, Taylor & Francis Group, 2013.

[16] J. Deogirikar, A. Vidhate, "Security Attacks in IoT: A Survey", IEEE, International conference on I-SMAC, October 2017, p.p 32-37.

[17] 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.

[18] H. Parker; S. Flowerday, " Contributing factors to increased susceptibility to social media phishing attacks", South African Journal of Information Management, 2020.

[19] L. Remorin, R. Flores, B. Matsukawa, " Tracking Trends in Business Email Compromise (BEC) Schemes", Trend Micro Forward-Looking Threat Research (FTR) Team, eBook, 2018.

[20] N. Al-Musib, F. Al-Serhani, M. Humayun, N.Z.Jhanjhi, "Business email compromise (BEC) attacks", International Virtual Conference on Sustainable Materials, Elsevier, 2021.

[21] 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.

[22] F. Malecki, S.Craft, "Best practices for preventing and recovering from a ransomware attack", Computer Fraud & Security, March 2019.

[23] PTsecurity Company, "Vulnerabilities and threats in mobile applications ", Report, 2019, https://www.ptsecurity.com/ww-en/, 12-2-2021, 8:pm.

[24] 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.

[25] B. Akhgar, H. Arabnia, " Emerging Trends in ICT Security", Elsevier, Chapter 3 - Authorization and Access Control, 2014.

[26] B. Akhgar, H. Arabnia, " Emerging Trends in ICT Security", Elsevier, Chapter 28 - Man-in-the-Browser Attacks in Modern Web Browsers, 2014.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

Received 13/6/2021; Accepted 1l9l2021

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*