AVOIDITALS: Enhanced Cyber-attack Taxonomy in Securing Information Technology Infrastructure

Melwin Syafrizal [1], Siti Rahayu Selamat[2†] and Nurul Azma Zakaria[3]
melwin@amikom.ac.id[1], sitirahayu@utem.edu.my[2], azma@utem.edu.my[3]
[1]Faculty of Computer Science, Universitas AMIKOM Yogyakarta, Indonesia
Jl. Ringroad Utara Condong Catur, Depok, Sleman, 55283, DIY, Indonesia
[1,2,3]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

Summary
An operation of an organization is currently using a digital environment which opens to potential cyber-attacks. These phenomena become worst as the cyberattack landscape is changing rapidly. The impact of cyber-attacks varies depending on the scope of the organization and the value of assets that need to be protected. It is difficult to assess the damage to an organization from cyberattacks due to a lack of understanding of tools, metrics, and knowledge on the type of attacks and their impacts. Hence, this paper aims to identify domains and sub-domains of cyber-attack taxonomy to facilitate the understanding of cyber-attacks. Four phases are carried in this research: identify existing cyber-attack taxonomy, determine and classify domains and sub-domains of cyber-attack, and construct the enhanced cyber-attack taxonomy. The existing cyber-attack taxonomies are analyzed, domains and sub-domains are selected based on the focus and objectives of the research, and the proposed taxonomy named AVOIDITALS Cyber-attack Taxonomy is constructed. AVOIDITALS consists of 8 domains, 105 sub-domains, 142 sub-sub-domains, and 90 other sub-sub-domains that act as a guideline to assist administrators in determining cyber-attacks through cyber-attacks pattern identification that commonly occurred on digital infrastructure and provide the best prevention method to minimize impact. This research can be further developed in line with the emergence of new types and categories of current cyberattacks and the future.

Key words:
Cyber-attack taxonomy, AVOIDITALS, Cyber-attack domain.

1. Introduction

Knowledge of cyber-attack is essential for cybersecurity analysts or Information Technology (IT) infrastructure administrators. The earlier someone can recognize cyber threats or attacks, the faster we will respond to threats and increase awareness when carrying out activities in cyberspace. A cyber-attack is an action by a threat actor to carry out illegal actions by entering or disrupting other people's systems with various purposes and objectives.

Hacker and cybersecurity communities share information frequently and rapidly about security developments, hacking techniques, or reports of emerging attacks. However, due to the broad scope of cybersecurity implementation, most research performed and published on a cyber-attack focusing more on the cyber-attack for industrial fields such as Supervisory Control and Data Acquisition (SCADA), cyber manufacturing systems, nuclear power plants, and cloud services.

Therefore, cyber-attack taxonomy can recommend cybersecurity analysts, IT infrastructure administrators, or security programming developers to anticipate attacks, develop strategies for resistance or incident handling, and evaluate information security systems' implementation.
The paper is organized as follows: Section 2 provides a review of related work in the field. Section 3 describes the methodology followed in conducting this research. The proposed taxonomy and the results are presented in Section 4. Followed by a conclusion in Section 5.

2. Related Works

2.1 Types of Cyber-attack

A cyber-attack is an action that can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks. In general, attacks are active or passive. Active attacks attempt to disrupt or modify information resources or systems to affect the operations of an organization or individual. Active attacks generally alter the flow of data or create false information. Examples of active attack techniques are masquerade, data modification or manipulation, repudiation, replay, denial of service, distributed denial of service, spoofing, ping of the death, ARP poisoning, smurf attack, ping flood, buffer overflow, stack overflow, heap overflow, and format string attack.

Passive attacks try to learn or take advantage of information from a system without affecting system resources; no data has changed from the target. It is eavesdropping or monitoring transmissions. Its purpose is to get the information sent or to open port scans and

Manuscript received July 5, 2021
Manuscript revised July 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.1

vulnerabilities. Passive attacks include active reconnaissance and passive reconnaissance. The types of passive attacks are the release of message content or tapping (wiretapping or fibre tapping), traffic analysis, intercepting encryption, idle scan, port scan, keystroke logging, backdoor, and screen scraping.

In addition to active or passive attacks, in detail, there are several cyber-attack techniques in various ways for individuals or companies on a broader scale. Attackers can organize attacks into two categories: 1. syntactic attacks and 2. semantic attacks. Syntax attack is straightforward and used malware software as a tool to attack, such as viruses, worms, spyware, and trojan horses. Meanwhile, semantic attacks are executed by modifying and disseminating correct and false information. The attacker spreads the issue by fabricating the information to undermine the target's credibility. Examples of this attack are spreading hoax news in which hiding the traces by removing the source. Other forms of semantic attacks are social engineering, email phishing, cloud storage file masquerading, fake Facebook accounts, IM phishing, multimedia masquerading, and phishing websites [1].

In 2016, Magar [2] discussed state of the art in cyber threat models and methodologies. Their research identified the cyber threat characterization elements by dividing the cyber threats into five main elements of threat references, namely Threat Characterization, Threat Taxonomies, Threat Methodologies, Threat frameworks, and Threat Models, as depicted in Fig. 1.

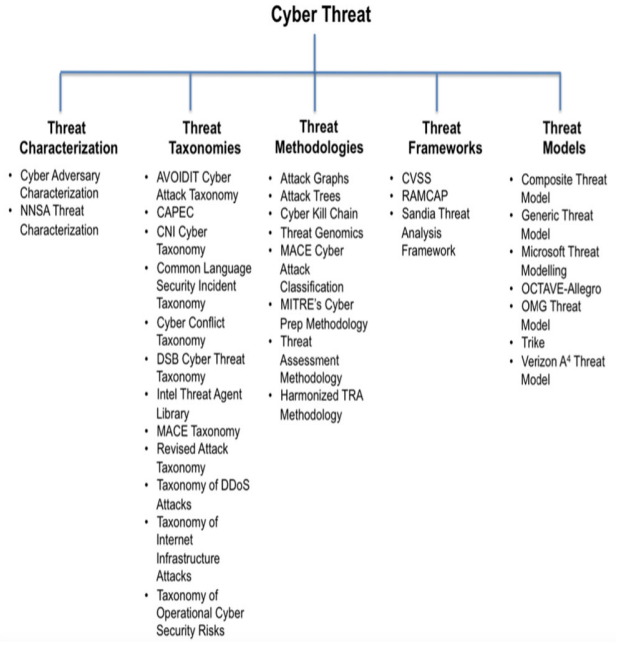

Fig. 1 Cyber-threat References [2]

Fig. 1 depicts the five main cyber threat elements. Threat characterization seeks an understanding of an adversary and the capability to predict it to enhance threat models. Threat taxonomy is referred to as a library that able to classify the information of the threats. Threat methodology is the method to carry out the characterization of threats. A threat framework is a platform to provide a basic structure that consists of threat characterization, taxonomy, and methodology to be used to analyze threats. Finally, the threat model is an approach that is employed to identify the objectives and the vulnerabilities of cybersecurity threats. It is also to determine the best methods to prevent potential attacks and minimize their impacts.

Currently, technological developments have resulted in many operational activities and organizational and business documentation completely digital. In addition, the form of cyberattacks is changing rapidly. The impact of attacks is sometimes uncertain or undetectable, including what or who is the main target of the attack. There is still a lack of valuable tools or technologies, assessment metrics, and frameworks to assess and understand the dangers facing organizations from cyberattacks. Due to that, understanding the behavior of threats or attacks is essential, and this problem can solve by introducing cyber-attack taxonomy.

2.2 Cyber-attack Taxonomy

A taxonomy is a classification system that allows a person to identify something uniquely. In another definition, the taxonomy classifies and categorizes various aspects of the domain for a particular field, which can serve as the basis for describing the domain in a common and consistent language [3]. Taxonomies organize categories hierarchically. Each category has a name and a short description. Sometimes there are relationships between categories or sub-categories, with other categories or sub-categories, such as interrelated interrelationships [4].

For example, when studying a single domain of cyberattack, taxonomies help describe the development of knowledge and describe the relationship of one domain to another. When dealing with security cases or concerns, taxonomies are useful for identifying new security aspects by classifying the problem or source of the problem according to previous similarity cases. Security incidents often occur randomly; the causes are various factors, such as human negligence (accidental or unintentional factors) and environmental or natural factors.

The types of attacks or organizational assets such as computers, networks, information, and all IT equipment and human resources that require security can be categorized using cybersecurity taxonomy to assist administrators on quickly reconstructing, preparing protection to be taken, improving the situation, and preventing the IT

infrastructures if something unexpected happens. This also will provide a secure environment for the future.

Several taxonomies are published in journals and reports. One of them is the threat taxonomy by Louis Marinos and ENISA [5] proposed detailed information about their threat taxonomy, further presented in a report by [6]. It stated that the taxonomy consists of cyber threats, threat agents, and attack vectors.

In 2014, a cyber-attack taxonomy was introduced by [7] called AVOIDIT. AVOIDIT is introduced to identify and defend the cyber-attacks by classifying the nature of attacks. This taxonomy aims to educate the system administrators on preventing their system from any potential cyber-attacks. It consists of five domains: Attack Vector, Operational Impact, Defense, Information Impact, and Target, as shown in Fig. 2.

The security community [8] also developed cyber-attack taxonomy as depicted in Fig. 3 that derived from several existing taxonomies such as AVOID, ADMIT, DDoS Attack, and DDoS Defense Mechanisms.

Fig.3 depicts the taxonomy consists of several domains. The domains are attack vector, operational impact, defense, informational impact, and targets. The number of sub-domains created is also more compared to the taxonomy proposed by [7]. In the Treadstone71 taxonomy [8], there is also a Cyber Adversaries table with the category Adversary class, skill level, maliciousness, motivation, and method, and the Cyber Attack Taxonomy-Glossary table as described in [9] [10]. Glossary cyberattack taxonomy references can help users understand the types of attacks that exist in cyberspace today.

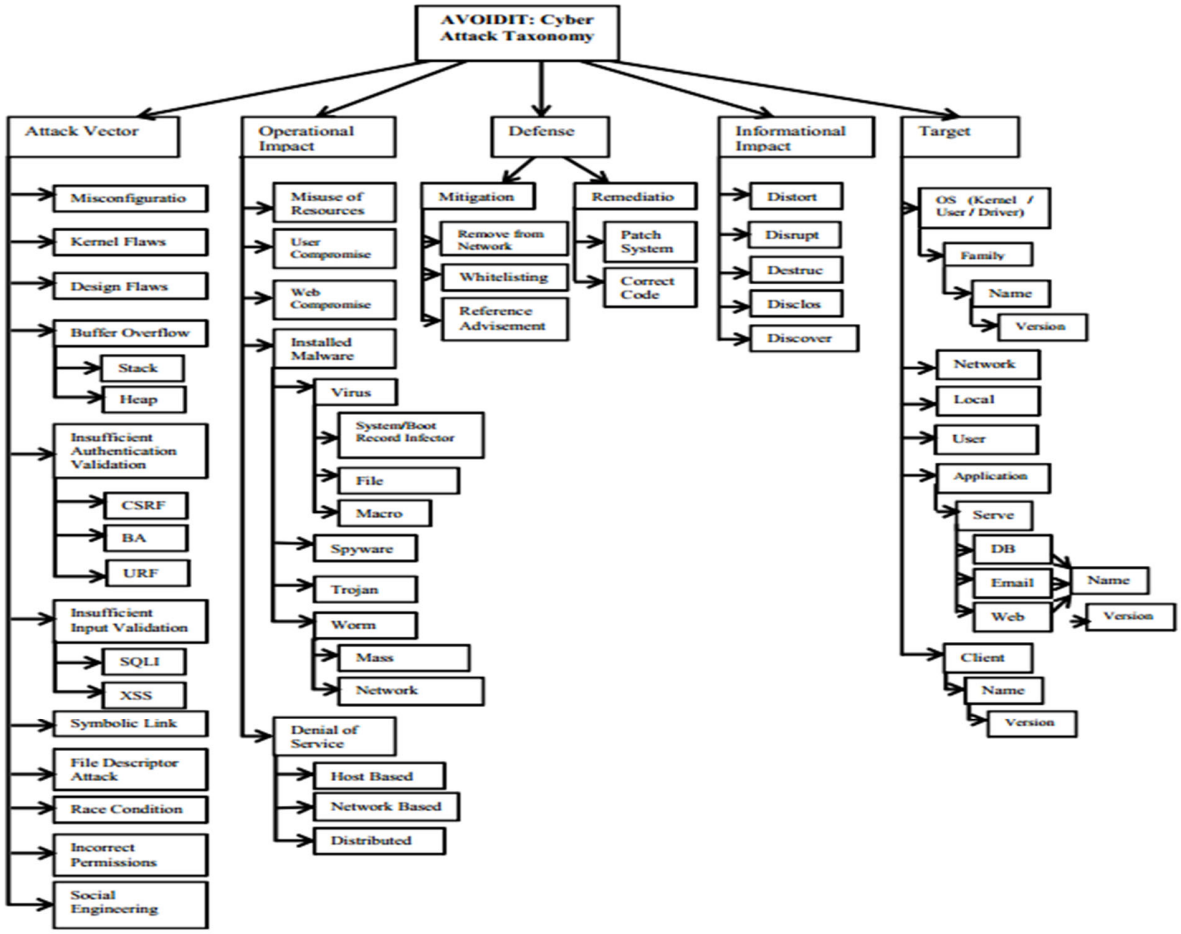

Fig. 2 Cyber-Attack Taxonomy-AVOIDIT

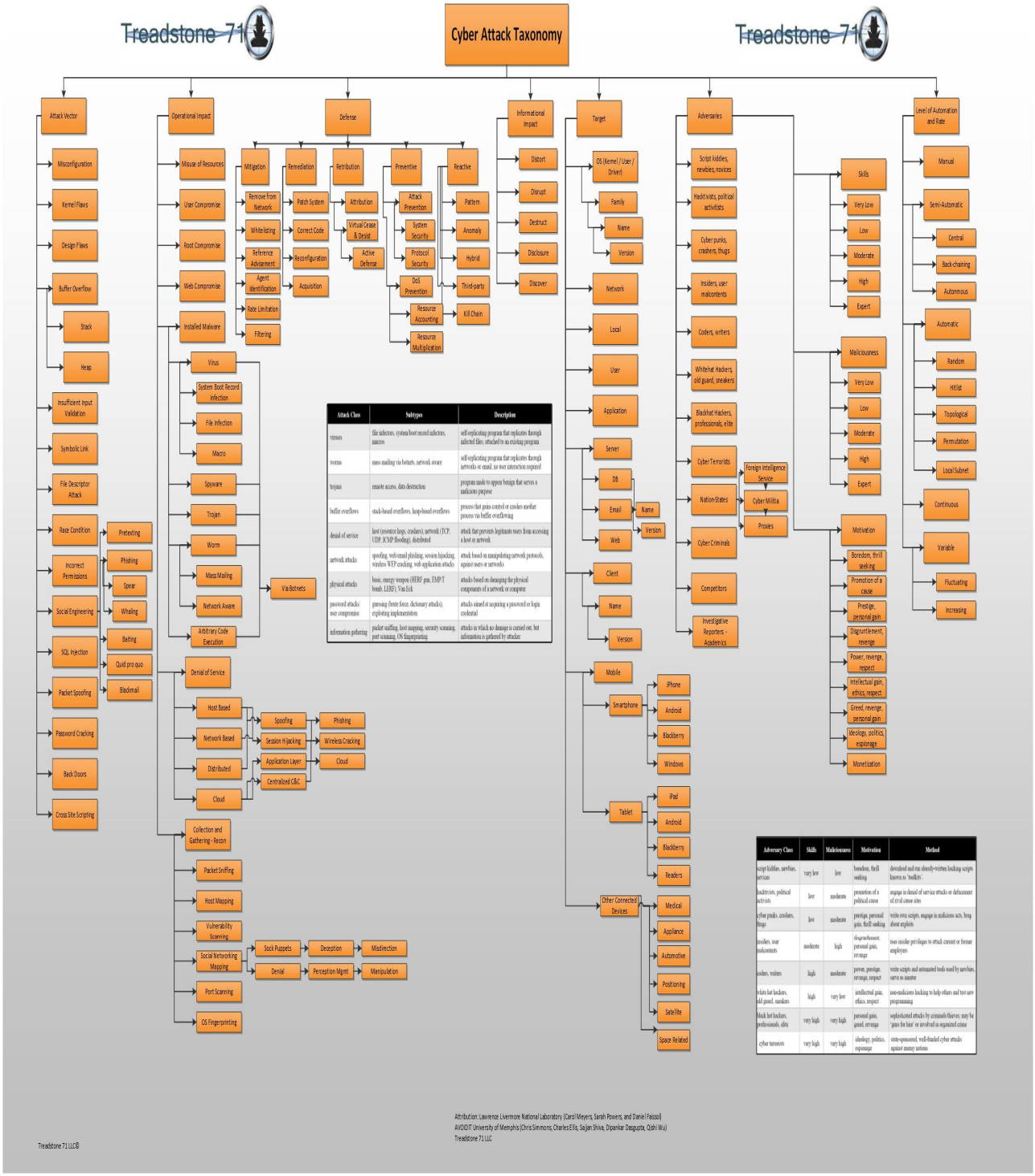

Fig.3 Treadstone71 Cyber Attack Taxonomy [8]

Agrafiotis *et al.* [11] proposed a taxonomy that describes the cyber-harms in organizations. In this study, the domains of cyber threats are focused on the identification of attacks on systems or users. By doing this, users can prepare themselves with various tools and techniques to anticipate various attacks or assess the risk of

the impact of attacks. In this taxonomy, the domains present some of the dangers of cyberspace caused by cyber-attacks and provide an early indication of how the attacks connected, create harm, and spreading.

There are not only [6][7][2][11] and [8] are proposed cyber-attack taxonomies, but there are several studies had been performed and published as listed in Table 1.

Table 1. Analysis of Cyber Attack Taxonomy

Authors	Taxonomy Name & Methods Use	Domain
[12]	Computer and Network Attack Taxonomy – This taxonomy has a broad scope but does not try to analyze all the weaknesses of computer security, or predict all methods of attack that might occur, but only seeks to provide a broad and inclusive framework.	• Attackers • Tools • Results • Access • Objective
[13]	Computer and Network Incident Taxonomy - The researcher developed the term "high level" minimum, with a structure to show relationships between domains (taxonomy), which can be used to classify and understand computer security incidents and vulnerability information. This taxonomy is often the basis for further development of cyberattacks taxonomies.	• Attackers • Tools • Vulnerability • Objective • Action • Target • Unauthorized Result
[14]	VERDICT Taxonomy – This research provides a comprehensive analysis of the types of attacks aimed at computer systems, performing common taxonomy constructs and methodologies that facilitate the design of secure protocols.	• Validation • Exposure • Randomness • Deallocation • Improper Conditions
[15]	A Taxonomy of DDoS Attack and DDoS Defense Mechanisms – This paper describes the taxonomy of DDoS attacks using known and potential attack mechanisms and discusses the important features of each attack category as well as challenges in fighting threats. A taxonomy of defense systems is illustrated using the approaches known today. The aim of this paper is to apply some recommendations into the many existing attack and defense mechanisms to understand the DDoS challenges.	• Manual • Semi-Automatic • Automatic • Protocol • Brute force • Continuous • Variable • Disruptive • Degrading
[16]	Taxonomy for Computer Incidents - *The extended CERT-taxonomy from Howard and Longstaff (1998) with modifications in the categories of attacker, vulnerability, and objective + Result* The author adjust to the environment found in the field of computer security today. The proposed additions include a new set of tools, techniques, and motivations from malicious attacks on computer systems or networks.	• Attackers • Vulnerability • Objective • Result
[9]	A Taxonomy of Cyber Adversaries & A Taxonomy of Cyber Attacks - This research conducts literature survey on cyber enemies, existing taxonomies of different types of enemies and methods, motivation, crime, and appropriate skill levels. Based on the literature survey, this study further do literature on cyber attacks, provide taxonomies of various attack classes, subtypes, and description of threats.	• Viruses, worms, & trojans • buffer overflows • denial of service • network attacks • physical attacks • password attacks/user compromise • information gathering
[17]	A taxonomy of cyber attacks on SCADA systems - The Supervisory Control and Data Acquisition (SCADA) system is firmly embedded in the structure of the critical infrastructure sector. These computerized real-time process control systems, are prone to damage and interference from cyberspace due to their standardization and connec-tivity to other networks and the internet. SCADA systems generally have minimal protection from cyber threats.	• Security Property Goal • Trust Model • Threat Model • Vulnerability • Cyber attacks on hardware • Attacks on software • Attacks on the communication stack
Authors	**Taxonomy Name & Methods Use**	**Domain**
[18]	ADAPT Taxonomy -	• Attacker • Defender

	This study is surveyed the existing game-theory framework, information assurance, and risk assessment framework. Combine this framework, and propose a game theory approach to attack-defense and taxonomy of performance metrics (ADAPT). Furthermore, it offers a game decision system (GDS) that uses ADAPT to compare competing game models. The approach uses a distributed DDoS attack scenario.	• Performance
[19]	Attack taxonomy overview – This research is constructed the ontologies according to taxonomy. In ontology, the concept of attack is included in five dimensions, and the relationships between them are formalized and analyzed in detail. Authors also filled the attack ontology with information about vulnerabilities from national vulnerability databases (NVD), such as CVE, CWE, CVSS, and CPE.	• Attack impact • Attack vector • Attack target • Vulnerability • Defense
[20]	Taxonomy of research in cyber security for emergency management networks - This study proposes existing and potentially relevant research taxonomies in this arrangement, including the types of attacks that have occurred or are likely to happen, and defense mechanisms that have been used or will apply.	Attack Mechanism • by network type • by function affected • by attack vector Defence Mechanisms • by type of defence • by degree of distribution • by organisational element
[7]	The AVOIDIT Cyber Attack Taxonomy - This research is validated the taxonomy of AVOIDIT using a cyber attack scenario and highlighted future work to simulate the use of AVOIDIT within the IRS. They propose an efficient cause, action, defense, analysis and target (CADAT) process that is used to facilitate the classification of attacks.	• Attack Vector • Operational Impact • Defense • Information Impact • Target
[21]	A Taxonomy of Operational Cyber Security Risks – This report presents an operational cybersecurity risk taxonomy that seeks to identify and organize the sources of operational cybersecurity risk into four classes. Each class is broken down into subclasses, which are described by its elements. This report discusses taxonomic harmonization with other security risks and activities, particularly those described by FISMA, NIST SP, and CERT-OCTAVE.	• Actions of People • Systems and Technology Failures • Failed Internal Processes • External Events
[22]	ADMIT Taxonomy - This five-dimensional taxonomy uses five classifications of attack properties. Classification based on attack vectors, defenses, methods, impact and target attacks. The proposed taxonomic classification structure describes the nature of the attack as a whole. Administrators can use the proposed taxonomy to find appropriate strategies to secure their systems from exploitable vulnerabilities. Using ADMIT's taxonomy in network defense strategies can increase the overall level of security.	• Attack vectors • Defenses • Methods • Impact • Target attacks
[23]	TAVI Attack taxonomy - Highly distributed information systems use Industrial control systems (ICS) for monitoring and control critical infrastructures such as nuclear power plants, the oil and gas industry, and others. The main architectural principles of ICS are real-time response, high availability and reliability. The special protocols used are Modbus and DNP3 because they correspond to real-time requirements.	• Threats • Attack • Vulnerability • Impact (CVSS)
[24]	Taxonomy for cyber-attack - This taxonomy is like adopting several pre-existing taxonomies. In this study, it used the Discrete EVent system Specification (DEVS) framework to generalize a case study of buffer overflow with simulation. This framework describes the overall vision of cyber attacks. This case study aims to strengthen the research evidence.	• Attack Vector • Result • Type • Target

Researchers	Taxonomy Name & Methods Use	Domain
[25]	Cloud Attack and Risk Assessment Taxonomy – This taxonomy describes the top two levels of the taxonomy of the cloud attack concept and risk assessment. The top level of the taxonomy consists of five dimensions adopted from the six dimensions of a taxonomy published previously.	• Source • Vector • Target • Impact • Defense
[26]	Taxonomy of attacks Cloud Service Delivery Models - In this study, cloud-based attacks and vulnerabilities were collected, identified, and classified according to the cloud model. It presents the taxonomy of cloud security attacks and potential mitigation strategies with the aim of providing an in-depth understanding of security requirements in the cloud environment. This study also highlighted the importance of intrusion detection and prevention as a service.	• Software as a Service • Platform as a Service • Infrastructure as a Service
[27]	CMS Cross-Domain Attacks Taxonomy In this research, a taxonomy is developed to determine the nature of attacks, especially if the attacks are cross-domain. Taxonomies can help security professionals identify and detect cross-domain attacks on a CMS. The taxonomy is constructed in four dimensions to illustrate how the taxonomy can detect cross-domain attacks on a CMS.	• attack vector • attack impact • attack target • attack consequence
[11]	Organizational cyber-harms taxonomy - In this research, the study reflects on the literature on harm, conceptualized in the field of criminology and economics, and investigates how risks and impacts are related to hazards. Different types of harm are identified, and a taxonomy of cyber hazards faced by organizations is created. This taxonomy consists of five broad themes. In each theme, they present some of the dangers of cyberspace that can be caused by cyber-attacks. This taxonomy is developed to provide an early indication of how these different types of hazards are connected and how cyber harm, in general, can spread.	• physical or digital harm • economic harm • psychological harm • reputational harm • social and societal harm
[28]	Towards a Taxonomy of Cyber Attacks on SCADA System - This paper has a discussion that is almost the same as the discussion of previous studies (Zhu, Joseph and Sastry, 2011). This paper describes network attacks and cyber attacks on hardware, software, and system communication stacks, which are harmful to the system, damaging system control and work speed in SCADA System. The domains discussed in both papers are almost the same, with a few additions and changes in the second paper.	• Security and control execution Goals • Trust Model • Threat Model • Lattice Model • Vulnerability and Threats • Cyber attacks on hardware • Cyber attacks on software • Cyber attacks on communication stack
[29]	Taxonomy of cyber-attacks based on the characteristics of nuclear power plants (NPP) with examples of cyber attacks. This study proposes a systematic countermeasure strategy by matching countermeasures with critical digital assets (CDA). The cyberattack taxonomy is used to investigate cyberattack cases and data for validation/evaluation of cybersecurity suitability for device use as effective prevention and mitigation for cyberattacks against nuclear power plants.	• Attack Procedure • Attack access • Consequence • Vulnerability • Countermeasure
[30]	Researchers present an attack taxonomy that considers the layers of the IoT stack, i.e., devices, infrastructure, communications, and services, with characteristics defined by each layer that the adversary can exploit. They used nine real-world cybersecurity incidents, targeting IoT devices used in the consumer, commercial, and industrial sectors. Researchers describe IoT-related vulnerabilities, exploitation procedures, attacks, impacts, and potential mitigation mechanisms and protection strategies. The proposed taxonomy provides a systematic procedure for categorizing attacks based on the layers affected and the impact accordingly.	• Devices • Infrastructure • Communications • Services

Table 1 indicates some of the taxonomies have similar domains, such as Attackers proposed in [12][13][16] and [18] taxonomies. However, most of the taxonomies proposed are consist of different sub-domains. The

taxonomies proposed are structured based on various purposes of use, coverage area, and depth. Each of them has its advantages and disadvantages according to its aims and objectives. The methods of developing the taxonomies are also different. With the rapid evolution and development of new offensive techniques, the applicability and effectiveness of the taxonomy are sometimes questionable. Hence, a mechanism is needed to develop new categories in cyberattack taxonomy [31].

3. Methodology

There are four phases carried out in this study, as shown in Fig. 4.

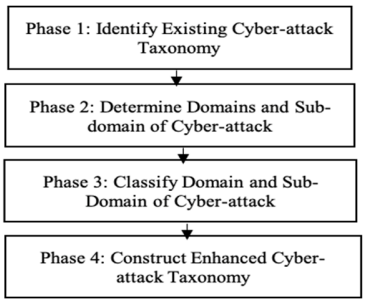

Fig. 4 Research Methodology

In phase 1, the existing cyber-attack taxonomies are identified from several previous research. Various references are collected from published white papers, journals, and conference articles. Digital document sources are obtained through the search engine google.com; or scholar.google.com, ScienceDirect, Scopus, ACM, IEEE Xplore, and Springer. In Phase 2, based on the collected articles, the domains and sub-domains of the cyber-attack are determined. The appropriate domains and sub-domains to be considered in the cyber-attack taxonomy are selected. Then, in Phase 3, the selected domains and sub-domains are classified according to the focus and objectives of the research. Based on this classification, significant domains and sub-domains from the existing taxonomy are selected and improved. Finally, in Phase 4, the enhanced Cyber-attack Taxonomy called AVOIDITAL Cyber-attack Taxonomy is constructed that consists of domains and sub-domains selected and improved in Phase 3 and added one main domain called “Source IP Trackback” to track the source of cyberattacks.

4. Result Analysis and Discussion

Based on Table 1 as discussed in Section 2, it concludes that the number of domains and sub-domains for each taxonomy is proposed based on the focus and objectives of the research as depicted in Table 2.

Table 2. Result Analysis of Cyber-Attack Taxonomy

Authors	No of Domain	No of Sub-domain	Focus on
[12]	5	30	Computer and Network Attack
[13]	7	45	Computer and Network Incident
[14]	7		Computer Attack to Protection Analysis
[15]	9 & 5	14 & 13	DDoS Attack and DDoS Defense Mechanisms
[16]	4	22	Computer Incidents
[9]	2	17	Cyber Adversaries & Cyber Attacks
[17]	7	12	Cyber Attacks in SCADA systems
[18]	3	9	Attack-defense
[19]	5	41	Ontology-based framework for assessing network security and computer systems
[20]	6	18	Cybersecurity for network emergency management
[7]	5	27	Cyber Attack
[21]	4	13	Operational Risk
[22]	5	20	Network and Computer attacks
[23]	4	5	Attacks on Industrial Control Protocol
[24]	4	17	Computer security attack
[25]	5	21	Cloud attack and risk assessment
[26]	3	15	Cloud security attacks
[27]	8	42	Attack of CyberManufacturing System
[11]	5	57	Cyber-harms in organizations
[28]	8	13	Cyber attacks on SCADA system
[29]	5	13	Digital environment in nuclear power plants
[30]	4		Consumer, Commercial and Industrial IoT Attack

Most of the taxonomy proposed is derived from [12]. For example, the taxonomy of cyber-attack proposed by [7][8][13][16] and [22]. However, the best taxonomy has been proposed by [7] that called as AVOIDIT and [8] known as Treadstone71. The AVOIDIT Cyber Attack Taxonomy has 5 domains, 29 sub-domains, 22 sub-sub-

domain, 14 other sub-domain, which are Attack Vector, Operational Impact, Defense, Information Impact, and Target. Whereas Treadstone 71 consists of 7 domains which are Attack Vector, Operational Impact, Defense, Information Impact, Target, Adversaries (A), and Level of Automation and Rate (L). In these domains, they are divided into 67 sub-domains, 95 sub-sub-domains, and 34 other sub-domains.

Based on these two taxonomies and findings in Table 2, this research proposed an enhanced taxonomy by adding one additional domain namely Source IP Trackback (S) domain. The enhanced taxonomy is called AVOIDITALS as shown in Figure 5. Source IP Trackback domain consists of several sub-domain Basic Approaches, Backscatter Traceback Technique, Probabilistic Approaches, Deterministic Approaches, Algebraic-Based Traceback Approach (ATA), Hybrid Packet Marking, Overlay Network for IP Traceback, Log-based Traceback, DNS Logs against Bots, Honeypots and Honeynets, Single-Packet IP Traceback, Singleton Flow Traceback (SFT), Opportunistic Piggyback Marking, Secret Zeckendorf number solution, Hybrid Multilayer Network Traceback, Incrementally Deployable Flow-Based Scheme, Autonomous system based flow marking scheme, Framework for Authentication in Cloud-Based IP Traceback (FACT).

Source IP Traceback (S) domain is proposed in this research as there is a need to identify the attack source to determine a complete attack scenario. Compared to the existing taxonomy, the origin of the cyberattack is difficult to be known as it is only concerned with developing the attacks and their effects, including attackers' categories and motivations. In addition, attackers use various ways to erase their digital traces. Therefore, IP Trackback is the only technique used to determine the origin of the attack.

Fig. shows the domains and sub-domains included in AVOIDITALS. Attack Vector (AV) is a means used by threat actors to access a system or network to commit cybercrimes. Operational Impact (OI) is the impact of cyberattacks on the continuation of operations, which poses a high risk to the business operations of the company or organization. Operational Impact due to misuse of resources, user compromised, root compromised, web compromised, installed malware, denial of service (DoS). The efforts made by the attackers before carrying out the attack including collection and gathering information, gaining access, maintaining access, and clearing tracks. Defense (D) is an effort to tackle cyber-attacks that disrupt defense operations. Defense involves all efforts to carry out mitigation, remediation, retribution, prevention, reaction, detection, notification, containment, restoration, and recovery activities. Preventive and reactive from the DDoS Defense Mechanisms reference. Impact (I) is the effect of an attack that has consequences, both positive and negative. The impact of cyber-attacks presented in this taxonomy includes impacts on informational, business/economic, technical, social/societal, psychological, and physical/digital assets. Targets (T) are targets set for attacks, such as the host and guest OS used by users, local area networks, applications, servers, and clients/workstations on the network, mobile devices, and other connected devices, data center, hypervisor, and accounts. The user as a person can also be the target of attack.

Adversaries (A) or cyber adversaries are threat actors who attack computer network infrastructure, devices used by users or managed by the admin. Adversaries are a person or group of people using their own resources or sponsored by another person or a country who intends to commit a crime against the resources or assets of a person, organization, company, or other cyber resources. These people, with their respective motivations having the potential to become enemies for anyone or any organization because they try to infiltrate illegally, take, modify to damage systems, information, or other digital assets, thereby causing harm to victims. Level of Automation (L) based on the degree of automation of the DDoS attack, differentiate between manual, semi-automatic and automatic DDoS attacks, including the continuous, variable, protocol, and brute-force. Source IP Trackback (S) are methods that can be used (from various journal references) to locate the source IP address of packets on the Internet reliably. Use of a spoofed source IP address allows a denial-of-service (DoS) attack or a one-way attack (where the response from the victim's host is so well known that a return packet does not need to be received to continue the attack).

AVOIDITALS Cyber-attack Taxonomy proposed 8 domains, 105 sub-domains, 142 sub-sub-domains, and 90 other sub-sub-domains, as presented in Fig. 5. This taxonomy can be used as a guideline to facilitate the system or security administrator to determine common cyber-attacks that may occur on computer network infrastructure and devices, including tracking the attack source with IP trackback. This prior understanding and knowledge will help in preventing the system from potential attack and minimize the impact.

4. Result Analysis and Discussion

AVOIDITALS Cyber-attack Taxonomy is proposed based on the AVOIDIT and Treadstone71 taxonomies. AVOIDITALS is an enhanced taxonomy that acts as a guideline to assist administrators in determining cyber-attacks through cyber-attacks pattern identification that commonly occurred on digital infrastructure and provide the best prevention method to minimize impact.

The development of massive information technology has triggered the emergence of various types of new cyber-attacks; the cyberattack landscape will continue to develop

so that further researchers can continue to contribute to compiling cyber-attack taxonomies with new categories or domains that IT infrastructure managers and cybersecurity analyst very much need.

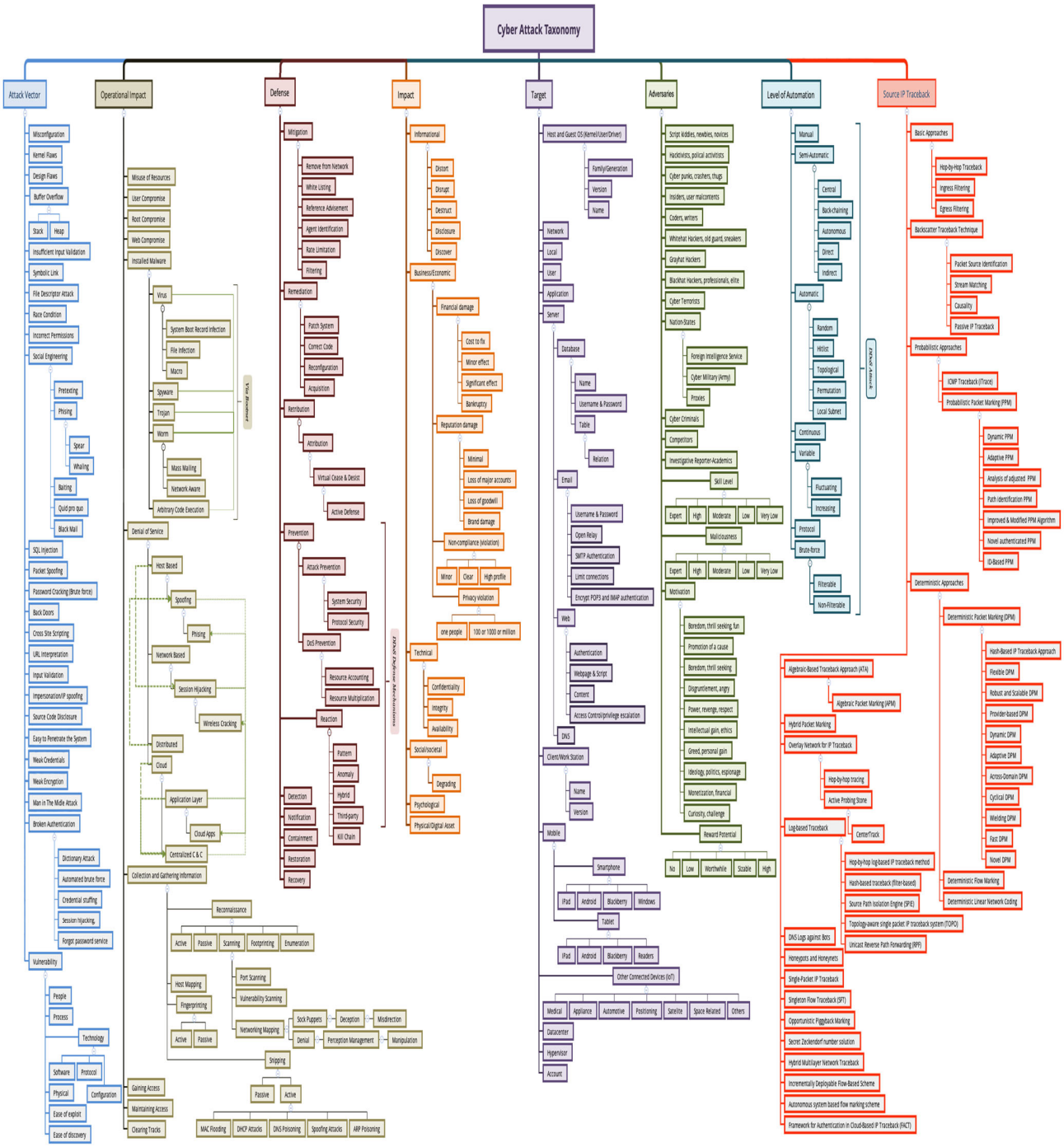

Fig. 5 AVOIDITALS Cyber-attack Taxonomy

Acknowledgments

The authors wish to thank the Universitas Amikom Yogyakarta for providing the financial support and Universiti Teknikal Malaysia Melaka (UTeM) for providing the facilities.

References

[1] Heartfield, R. and Loukas, G.: *Detecting Semantic Social Engineering Attacks with The Weakest Link: Implementation and Empirical Evaluation of a Human-As-A-Security-Sensor Framework.* Computers & Security. Elsevier Ltd. (2018)

[2] Magar, A.: *State-of-the-Art in Cyber Threat Models and Methodologies*, Sphyma Security (2016)

[3] Hansman, S. and Hunt, R.: *A Taxonomy of Network and Computer Attacks.* Computers and Security, 24(1), pp. 31–43 (2005)

[4] Klaper, D. and Hovy, E.: A Taxonomy and A Knowledge Portal for Cybersecurity. In: Proceedings of the 15th Annual International Conference on Digital Government Research, pp. 79–85 (2014)

[5] Louis Marinos and ENISA: *ENISA Threat Taxonomy-A Tool for Structuring Threat Information*. Athens (2016)

[6] ENISA.: *ENISA Threat Landscape Report 2017*. ENISA (2018)

[7] Simmons, C. B. et al.: AVOIDIT: A Cyber Attack Taxonomy. In: 9th Annual Symposium on Information Assurance, (June 3-4), pp. 12–22 (2014)

[8] Treadstone71: *Treadstone 71 Cyber Attack Taxonomy*. In: Website the Cyber Shafarat – Treadstone 71. Available at: https://treadstone71llc.files.wordpress.com/2014/11/cyber-attack-taxonomy-treadstone-71.jpg (Accessed: 4 June 2021).

[9] Myers, C., Powers, S. and Faissol, D.: *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches*. Lawrence Livermore National Laboratory, (August 2007), pp. 1–22 (2009)

[10] Sanjeev Relia, C.: *Cyber Warfare: Its Implication on National Security, Cyber Warfare*. New Delhi: Vij Books India Pvt Ltd. (2015)

[11] Agrafiotis, I. et al.: *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate.* Journal of Cybersecurity, 4(1), pp. 1–15 (2018)

[12] Howard, J. D.: *An Analysis of Security Incidents on The Internet 1989 - 1995*. Carnegie Mellon University. (1997)

[13] John D. Howard and Thomas A Longstaff: *A Common Language for Computer Security Incidents*. Albuquerque, New Mexico; Livermore, California (1998)

[14] Lough, D. L.: *A Taxonomy of Computer Attacks with Applications to Wireless Networks*. In: PhD Thesis. Virginia Polytechnic Institute and State University (2001)

[15] Mirkovic, J. and Reiher, P.: *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*. ACM SIGCOMM Computer Communication Review, 34(2), p. 39-54 (2004)

[16] Kiltz, S., Lang, A. and Dittmann, J.: *Taxonomy for Computer Security Incidents*. In: Cyber Warfare and Cyber Terrorism, pp. 412–417 (2008)

[17] Zhu, B., Joseph, A. and Sastry, S.: *A Taxonomy of Cyber Attacks on SCADA Systems*. In: Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011, pp. 380–388 (2011)

[18] Simmons, C. B. et al.: ADAPT: *A Game Inspired Attack-Defense and Performance Metric Taxonomy*. In: IFIP International Information Security Conference, 405, pp. 344–365 (2013)

[19] Gao, J. B. et al.: *Ontology-Based Model of Network and Computer Attacks for Security Assessment*. Journal of Shanghai Jiaotong University (Science), 18(5), pp. 554–562 (2013)

[20] Loukas, G., Gan, D. and Vuong, T.: *A Taxonomy of Cyber Attack and Defence Mechanisms for Emergency Management Networks*. In: Proc. of 2013 IEEE International Conference on Pervasive Computing and Communications Workshops, March, pp. 534–539 (2013)

[21] Cebula, J. J., Popeck, M. E. and Young, L. R.: *A Taxonomy of Operational Cyber Security Risks Version 2*. In: Technical Report of Carnegie Mellon University Software Engineering Institute, CMU/SEI-2014-TN-006 (2014)

[22] Joshi, C. and Singh, U. K.: *ADMIT- A Five Dimensional Approach Towards Standardization of Network and Computer Attack Taxonomies*. International Journal of Computer Applications, 100(5), pp. 30–36 (2014)

[23] Drias, Z., Serhrouchni, A. and Vogel, O.: *Taxonomy of Attacks on Industrial Control Protocols*. In: Proc. Of International Conference on Protocol Engineering, ICPE 2015 and International Conference on New Technologies of Distributed Systems, NTDS 2015 (2015)

[24] Douad, M. A. and Dahmani, Y.: *ARTT Taxonomy and Cyber-attack Framework*. In: Proc. Of First International Conference on New Technologies of Information and Communication (NTIC), pp. 1–6 (2015)

[25] Juliadotter, N. V. and Choo, K. K. R.: *Cloud Attack and Risk Assessment Taxonomy*. IEEE Cloud Computing, 2(1), pp. 14–20 (2015)

[26] Iqbal, S. et al.: *On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service*. Journal of Network and Computer Applications. Elsevier, 74, pp. 98–120 (2016)

[27] Wu, M. and Moon, Y. B.: *Taxonomy of Cross-Domain Attacks on CyberManufacturing System*. Procedia Computer Science. Elsevier B.V., 114, pp. 367–374 (2017)

[28] Banga, A., Gupta, D. and Bathla, R.: *Towards a Taxonomy of Cyber Attacks on SCADA System*. In: Proc. of 2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019. IEEE, (ICICCS), pp. 343–347 (2019)

[29] Kim, S. et al.: *Cyber Attack Taxonomy for Digital Environment in Nuclear Power Plants*. Nuclear Engineering and Technology. Elsevier Ltd, 52(5), pp. 995–1001 (2020)

[30] Xenofontos, C. et al.: *Consumer, Commercial and Industrial IoT (In) Security: Attack Taxonomy and Case Studies*. IEEE Internet of Things Journal, 4662(c), pp. 1–1 (2021)

[31] Derbyshire, R. et al.: *An Analysis of Cyber Security Attack Taxonomies*. In: Proc. of 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018. IEEE, pp. 153–161 (2018)

Manuscript received July 5, 2021
Manuscript revised July 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.1

Melwin Syafrizal is a PhD. student program at Universiti Teknikal Malaysia (UTeM) Melaka. He is also a lecturer at the Department of Computer Engineering, AMIKOM University, Yogyakarta, Indonesia. His research areas are Computer Networking, Network Security Analysis, Cybersecurity, and Cyber Defense.

Siti Rahayu Selamat is a senior lecturer in the Department of Computer and Communication Systems at the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka. She has a PhD. in Computer Networking, and Forensics. Her research interests in computer science are in the areas of Digital Forensics, Traceability Analysis, Evidence Tracking and Mapping in Forensic Digital Investigation Processes, Trace Patterns, Network Security, IDS, & Malware. Her research group is Forensic Information Security and Computer Networks (INSFORNET).

Nurul Azma Zakaria is currently a lecturer at Universiti Teknik Malaysia Melaka Malaysia at the Center for Advanced Computing Technology. She received his Doctor of Philosophy in Information Science and Mathematics (Saitama University, Japan). Her areas of expertise are in System-Level Design Methodology, Embedded Systems Design, Communication Design for Distributed Embedded Systems, IPv6 Migration, Internet of Things (IoT), Cyber-Physical Systems. Her research group is Forensic Information Security and Computer Networks (INSFORNET).