Significance and Research Challenges of Defensive and Offensive Cybersecurity in Smart Grid

Hana Mujlid
hmujlid@tu.edu.sa
Department of Computer Engineering, Taif University, Taif, Saudi Arabia

Summary
Smart grid (SG) software platforms and communication networks that run and manage the entire grid are increasingly concerned about cyber security. Characteristics of the smart grid networks, including heterogeneity, time restrictions, bandwidth, scalability, and other factors make it difficult to secure. The age-old strategy of "building bigger walls" is no longer sufficient given the rise in the quantity and size of cyberattacks as well as the sophisticated methods threat actor uses to hide their actions. Cyber security experts utilize technologies and procedures to defend IT systems and data from intruders. The primary objective of every organization's cybersecurity team is to safeguard data and information technology (IT) infrastructure. Consequently, further research is required to create guidelines and methods that are compatible with smart grid security. In this study, we have discussed objectives of of smart grid security, challenges of smart grid security, defensive cybersecurity techniques, offensive cybersecurity techniques and open research challenges of cybersecurity.

Keywords:
Smart grid; IT infrastructure; Cyber attacks; Defensive cyber security; Offensive cyber security; Cyber challenges

1. Introduction

Research and development into smart grids (SG) are accelerating quickly as the traditional grid moves from a conceptual model to a deployment phase. The national institute of standards and technology (NIST) defines a smart grid as the incorporation of information and communication technologies (ICT) into the electrical grid [1-2]. Utilities, ICT developers, and consumers can utilize and operate the modern grid in an efficient and economical manner by installing and integrating distributed and mixed renewable energy resources closer to the consumption premises [3-8].

Power flow in the smart grid is bidirectional, allowing utility companies and consumers to share power over two-way communication networks [9-12]. The electrical grid is no longer primarily owned by utilities. According to the NIST conceptual model, there are seven domains that make up the smart grid: markets, service providers, operations, transmission, consumption, and bulk generation [2], [13], [14]. To effectively operate the smart grid, technical shareholders use a number of communication networks and software programs. Various shareholders of smart grid and the attacker's observation on communication channel among them, is depicted in figure 1.

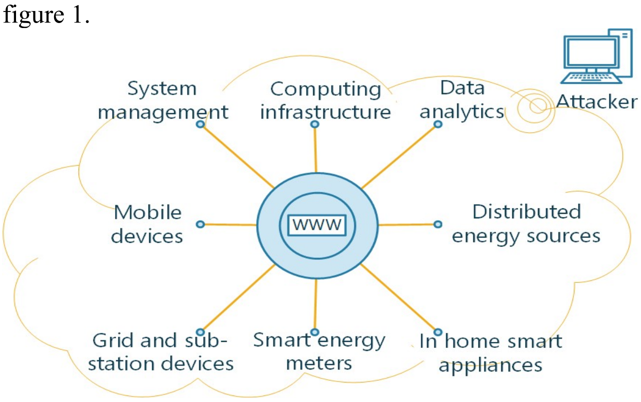

Fig. 1: Attacker's observation on communication system of power network

Over the past two decades, cybersecurity has developed into one of any organization's most crucial components. The world has changed, bringing with it new technological developments and perils. Malware assaults and account theft account for more than 55% of all cyberattacks [15-16]. Malware injection makes up one of the most prevalent types of cyberattacks, making up 39.3% of all cyberattacks in 2019 [15]. In order to safeguard the smart grid infrastructure from both internal and external threats, electric utilities need to invest more in developing a robust, reliable, efficient and effective cybersecurity infrastructure. Data protection for businesses is more crucial than ever, so they should give greater consideration to all aspects of cybersecurity. These include all around cybersecurity, offensive cybersecurity, and defensive cybersecurity. Various sources of cyber security threats are shown in figure 2 and a few prominent cybersecurity threats are shown in figure 3.

Two main categories of cybersecurity measures for smart grid are defensive cybersecurity and offensive cybersecurity. In this study, we have summarized objectives of smart grid security, pertinent literature on defensive and offensive cybersecurity and open research

Manuscript received December 5, 2022
Manuscript revised December 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.12.4

challenges for implementation of cybersecurity in smart grid domain. Main contributions of this study are mentioned below.

1) Security objectives of smart grid
2) Defensive cybersecurity techniques
3) Offensive cybersecurity techniques
4) Limitations of defensive and offensive cyber security techniques
5) Open research challenges of cybersecurity in smart grid

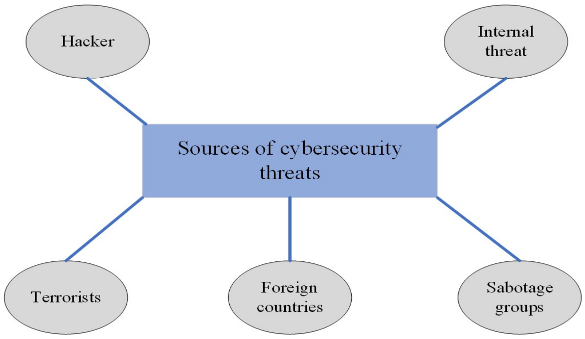

Fig. 2: Prominent cyber security threats to smart grid

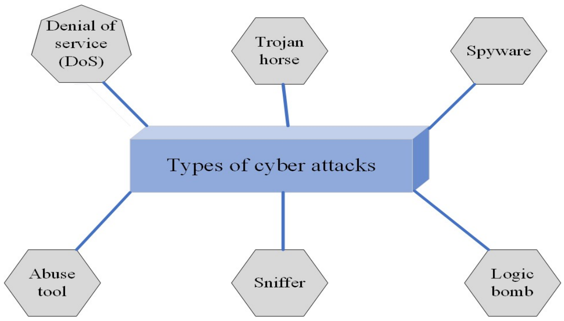

Fig. 3: Types of cyber security threats to smart grid

Rest of the paper is organized as follows. Section 2 discusses the objectives of smart grid security. State-of-the-art literature on defensive and offensive cyber security is presented in section 3. Critical analysis defensive and offensive cyber security techniques and open cybersecurity research challenges of smart grid are discussed in section 4. Finally, section 5 concludes this study along with future research directions.

2. Security Objectives of Smart Grid

A vast number of interconnected devices make up a smart grid. The smart grid exchanges two types of data: information and operational data. Where; the information could be the power consumption bill, historical data, logging, and reporting etc. and the operational data could be related to electric supply companies, capacitor banks, transformer's data, current load, voltages, circuit breakers, relays status etc. [17-19]. A high level of cyber security is required to protect the power system against potential deficiencies of the power system and blackouts. Main security objectives of a modern power system are briefly described below.

2.1 Confidentiality

Smart grid networks facilitate the information with varying levels of privacy and sensitivity, ranging from consumption data to personally identifiable information about consumers. Preventing unauthorized individuals from accessing data in order to safeguard individual security and privacy is called confidentiality.

2.2 Integrity

The smart grid's loss of integrity could alter sensor data and product formulas, which could have an impact on power management. Preventing unauthorized users from changing information or a system is known as integrity.

2.3 Availability

Timely information access within modern grid system is described as availability. Loss of availability could have an impact on electricity delivery since authorized people might not be allowed to access. Denial of service (DoS) attacks may hamper availability.

2.4 Authentication

Authentication is related to communicating entities that are consumer and utility (electric supply company). A gap in the authentication of humans and machines could allow an attacker to obtain sensitive data or allow unauthorized devices to exploit the smart grid's resources.

2.5 Authorization

An authorization system is necessary to ensure proper management of information and resources. Granting system access and requesting permission (also known as access control) to the variety of devices and people is known as authorization.

2.6 Non-Repudiation

Ensuring that a system's or user's performance of a certain action cannot later be revoked is known as non-repudiation. When important assets and data are at stake, non-repudiation becomes a serious problem.

3. Literature Review

Research community has put in a lot of efforts in cybersecurity domain to protect IT asset throughout the world. Many cyber security techniques have been proposed which can be used to protect smart grid infrastructure. Main categories of cybersecurity techniques are described below whereas; taxonomy of cybersecurity literature is shown in figure 4.

1) Defensive cyber security techniques
2) Offensive cyber security techniques

3.1 Defensive cybersecurity techniques

Defensive cybersecurity is a strategy to lessen the effects of assaults and keep attackers away from the network. The IT system must have the fewest feasible network vulnerabilities for defensive cybersecurity to perform well and prevent interference from outsiders. Many network attacks have gone undetected for days or even months because to defensive cyber security's inability to stop zero-day malware and sophisticated persistent attacks in real time. Table 1 summarizes the pertinent literature on defensive cyber security techniques.

The authors of [20] presented a paradigm based on AI that mimics adversarial, competitive co-evolution processes for cybersecurity scenarios. In order to combat an aggressor, the authors have created defense tactics. Simple application situations have been addressed by the authors, but complicated ones are not provided.

A study on the variety of attack persistent threats (APTs) to penetrate corporate ecosystems has been published in [21]. In order to safeguard the supervisory control and data acquisition (SCADA) system, authors have suggested combining multiple security measures. The impact of APTs on SCADA systems has only been studied by the authors.

In [22], use of artificial intelligence is considered in the context of cybersecurity protective measures. The application of AI in antivirus systems, APT, intrusion detection, spam and phishing detection, etc., has been discussed by authors. This research is useful for evaluating the use of AI to defensive measures, but the authors did not suggest any novel artificial intelligence-based defensive strategy.

The goal of study at [23] was to analyze the big data generated by cyber incidents in order to find patterns, correlations, and other pertinent evidence for cyber occurrences. The authors have shown how big data analysis and AI work together to strengthen cyber defense. Only an overview of the use of AI and big data in cyber protection is given in this study.

The management and support tool for cyber security exercises has been described by the authors of [24] for those working in cyber defense of any domain. The Swedish Defense Research Agency's CRATE Exercise Control (CEC) instrument is utilized in this work to demonstrate its application and requirement. This research demonstrated the actual use of a training tool for cyber defense specialists.

3.2 Offensive cyber security techniques

Main objectives of offensive cybersecurity techniques are to use deliberate, well-thought-out, and exact arrangements to conceal the real network, to learn about the intruder's thinking and delay his attempts to establish situational awareness. Offensive cybersecurity techniques are being widely used in the world and these can also be efficiently and effectively applied to safeguard power system against cybersecurity threats. Table 2 summarizes the pertinent literature on offensive cybersecurity techniques.

An Active Deception Framework (ADF) that offers an open environment for creating advanced cyber deception applications has been presented by authors of [25]. ADF offers sensors that track adversary activity in real-time, assisting in the development of active deception tactics. Additionally, the management application programming interface (API) facilitates automated low-level network setups. Real-time response of ADF makes it suitable to be applied in smart grid domain.

For industrial control systems that can be utilized to secure power systems, the Decepti-SCADA framework is proposed in [26]. The purpose of the Decepti-SCADA framework is to trick a network thief into thinking they are speaking with genuine supervisory control and data acquisition (SCADA) systems. Consequently, slowing them down and simultaneously alerting security analysts to the existence of an intruder.

Table 1: State-of-the-art literature on defensive cybersecurity

Paper	year	Description of Research	Approach	Limitations
[20]	2018	AI based framework to recreate adversarial competitive co-evolutionary processes	Proposed defensive strategies	Considered simple use case scenarios but didn't include complex ones
[21]	2019	Study about the spectrum of attack vectors and analysis of pertinence of IDS	Proposed multiple security solutions to secure the SCADA system	Only investigated the impact of Advanced Pertinent Threats APTs for SCADA
[22]	2020	A survey paper about the use of artificial intelligence in cybersecurity defensive measures	Discussed application of AI in Antivirus systems, APT, intrusion detection, spam and phishing detection etc.	Did not proposed any new defensive technique with AI
[23]	2019	To detect patterns, correlations, and other useful evidence for cyber events collected through cyber incidents	Demonstrated that big data analytics and AI collectively can improve cyber defense	Only overview of of the AI and big data in cyber defense
[24]	2020	Described cyber security exercise management and support tool	Used CRATE exercise control (CEC) tool	Only implementation of a training tool, no

Cyber deception is used in [27] to re-balance the actions of attackers and defenders. Authors have modeled the use of cyber-deception by the defender on the perception of the attacker using notions from game theory. Despite the employment of AI in this research, the authors failed to demonstrate how game theory actually works. The ability of honeypots to fool intruders may be improved by the method for creating phoney data described in [28]. Authors have suggested a Deferentially Private Synthetic Data Generation (DpSyn) methodology to produce synthetic data using deep learning. The suggested model is incapable of learning on its own.

In [29], it is shown how a player's perception influences their decision-making when selecting the optimum strategy based on hyper game theory. Stochastic Petri Nets were used by the authors to simulate a straightforward cyber game scenario and provide an example probability model. The proposed paradigm did not enhance the powers of cyber deception. Authors have conducted a thorough analysis for cyber deception methods in [30]. Authors have studied high-level deception plans and tactics and talked about cyber defensive tactics using game theory modeling. They came to the conclusion that cyber deception is still in its infancy and faces a number of difficult problems that must be resolved.

The authors of [31] analyze some significant cyber-deception tactics. A rigorous analysis of cyber deception has been offered by authors. The differences between deception-based and nondeception-based defense tactics have been examined. It is suggested in [32] that supervised machine learning techniques be used to identify a covert cyber-deception assault in smart grid (SG) communications networks. The test's configuration was created by the authors using the MATPOWER 6.0 toolbox. Automatic decision boundary learning occurs in the support vector machine (SVM). The attack recognition effectiveness of the suggested system decreases with system size and rises with it.

4. Critical Analysis and Research Challenges of Cybersecurity Techniques in Smart Grid

Survey of defensive and offensive cyber security techniques for power system would not be completed without critically examining the both techniques. Following discussion of future research topics focuses on the drawbacks and limitations of both types of cyber security. Open research challenges are also described afterwards.

4.1 Shortcoming of defensive cyber security techniques

Various services aimed at long-term assurance for your company will be offered as part of a cyber defense engagement. Cyber attack prevention is the focus of defensive cybersecurity. Although defensive tactics are important for every firm, they are insufficient to shield a company from all dangers, especially zero-day attack.

4.2 Shortcoming of offensive cyber security techniques

Although offensive cyber security tactics won't completely remove the hazards of an attack, they will lessen its likelihood by maintaining a constant state of readiness. The network of a power system can be searched for sophisticated enemies using offensive cyber tactics. The possibility of launching an error-prone attack is the main issue with any offensive cybersecurity plan. A well-planned cyber attack might cause damage on a level with conventional warfare or nuclear weapons. Additionally, an offensive strategy may intensify and produce unneeded vulnerabilities.

Table 2: State-of-the-art literature on offensive cybersecurity

Paper	year	Description of Research	Approach	Limitations
[25]	2020	Presented an Active Deception Framework (ADF)	Implemented deception framework using the Open Daylight SDN controller	No collaboration between cyber deception units
[26]	2020	Presented decepti-SCADA framework, for industrial control system	Introduced a high interaction honeypot system for networked critical infrastructure	No collaboration among cyber deception units
[27]	2019	Actions of attackers and defenders are rebalanced using cyber deception	Used game theory concepts	AI used, real working of game theory is missing
[28]	2019	Generate fake data to enhance the capability of Honey pots	Proposed a Deferentially Private Synthetic Data Generation (DpSyn) model to generate synthetic data	Proposed model do not have any self-learning capability
[29]	2019	Hyper game theory to examine player's perception	Modeled a simple cyber game scenario	Proposed model made insignificant improvement in cyber deception capabilities
[30]	2020	Performed a detailed investigation for cyber deception techniques	Reviewed high-level deception schemes and actions	No cyber deception model is proposed
[31]	2018	Analyzed some strategies for cyber deception and concluded that there is a need for more research for cyber deception	Discussed difference between deception and non-deception defense strategies	Insisted on more research and proposed no solution
[32]	2018	Proposed a supervised machine learning method to detect a concealed cyber deception attack	Used MATPOWER 6.0 tool-box	Proposed system has very low attack recognition efficacy

4.3 Open research challenges of cybersecurity in smart grid

A few prominent open research challenges regarding cybersecurity issues of smart grid are described in the following.

4.3.1 Collaboration among heterogeneous devices:

The Internet of Things (IoT) includes many interconnected heterogeneous devices that require authentication and authorization mechanisms to ensure overall system security. Confidentiality, integrity, and availability are the fundamental characteristics that must be ensured in this regard. Data aggregation of heterogeneous devices is another open research challenge in this context.

4.3.2 Resource constrained devices:

Resource-constrained devices face a lack of battery, computing, and storage power. Therefore, these devices are more vulnerable to cyber attacks such as eavesdropping, hacking, identity forgery, phishing, tampering, denial of service, probing, reconnaissance, etc., which can lead to large-scale security breaches. Lightweight security solutions are needed for such devices.

4.3.3 Connectivity:

Communication network of any power system is complicated since it integrates several interconnected devices. The decentralized nature of the smart grid environment necessitates a high level of protection for the systems against threats and weaknesses. Attacks may result in bodily harm, blackouts, and ineffectiveness. This is due to system takeover by attackers.

4.3.4 Increased industrial automation:

To meet the daily needs of humanity, electric power industry is becoming increasingly automated. Industrial automation relies on the communication of devices that are vulnerable to cyberattacks. In this context, data protection is the first line of defense to prevent such attacks. Moreover, deceptive cybersecurity is a proactive approach to attract, understand and combat the attacker.

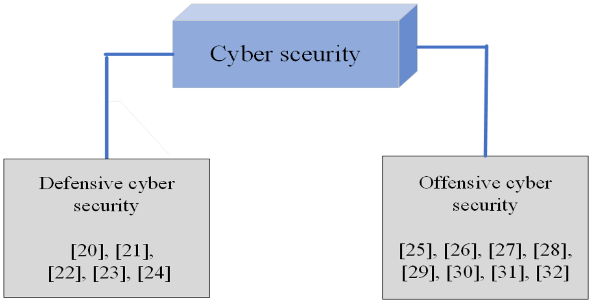

Fig. 4: Taxonomy of state-of-the-art literature on defensive and offensive cyber security

4.3.5 Trust:

Consumers are no longer considered as trustworthy due to the robust inter-connectivity of the smart grid systems (modern power system), which had an impact on the design decisions. Some clients won't abide by the terms and conditions. To offer false information about the amount of the electricity bill in order to make savings, users can, for example, purposely damage the smart meter of the power system.

4.3.6 Software Vulnerabilities:

Malware is one of the many flaws that adversely affect the software. SCADA systems use general-purpose technology, which increases the danger of malware and harmful updates. A general purpose system has a number of well-known vulnerabilities that need to be patched in order to ensure the power system availability.

4.3.7 Customer's Privacy:

Consumer privacy protection is a crucial component of any system, including the smart grid, and should be carefully secured. Many issues relating to user privacy were raised by the installation of smart meters into the smart grid. A smart meter may threaten the user's privacy, which is crucial, in addition to providing some important information about the user's power use. Since, it may deduce user behavior from the data collected by the service provider. Information regarding clients' availability at home or when travelling is among the data gathered about them. Even information on some regular behaviors, like sleeping and watching TV, as well as the appliances people use, can be extracted. The gathered data may be of interest to businesses, marketers looking to promote competitors, or criminals planning crimes. To prevent illegal access to data and safeguard the privacy of the user, data should be safeguarded both during transmission and during storage.

4.3.8 Cyber-enabled activities:
4.3.9

Globalization is leading to cyber-based activities that involve a large amount of Internet based transactions. Cyber criminals target such transactions to steal financial and intellectual data, which can lead to economic losses of electricity consumers, national security problems, and foreign policy violations. In this context, the role of cybersecurity is very important to counter the spread and severity of malicious cyber activities against power system.

4.3.10 Skilled cybersecurity professionals:

Every field requires a skilled and knowledgeable workforce for its effective implementation, and cybersecurity is no exception. Since, it is a relatively new paradigm; there is a lack of professionals for effective implementation, training, and awareness.

4.3.11 Cyberwarfare:

Cyber attack on critical infrastructure is another emerging area that involves power stations, computer networks, military installation, baking system etc. In future, the war dynamics may get change to cyberwarfare and economies may be controlled via cyber attacks/control. Offensive cybersecurity may be helpful in understanding the attacker behaviors and take counter measures prior to launch of actual cyber attack.

5. Conclusion and Future Work

Advanced attackers constantly create destructive tactics, techniques, and processes to get through reactive, rule-based cybersecurity measures and live in the noise of networks. These innovations, which include file less malware, dynamic infrastructure, polymorphic and disguised malware, and hijacking legal operations of power systems, all circumvent conventional protections of any power system. Researchers and business experts have focused on the crucial issue of cyber security in the power system. In this work, we presented security objectives of a power system, reviewed state-of-the-art literature on defensive and offensive cybersecurity and discussed open research challenges of cybersecurity for smart grid.

Given the sophisticated techniques threat actors utilize to hide their activity, the traditional approach of "building bigger walls" will no longer be sufficient. Only through aggressive cyberattacks, which this study refers to as offensive cybersecurity, power system organizers can uncover sophisticated adversaries on their networks and defend their power network. The field of cybersecurity is developing and getting better every day to keep up with the changing needs of today's internet. Everyone, but notably businesses, should educate themselves on the methods available to safeguard their data and guarantee the provision of energy services.

References

[1] Apel, R. “Smart grid architecture model: methodology and practical application,” presented at Workshop of Electrical Power Control Centers, 2013.

[2] NIST, Introduction to NISTTR 7628 Guidelines for Smart Grid Cyber Security. [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628 total.pdf

[3] Aslam, S., Herodotou, H., Mohsin, S. M., Javaid, N., Ashraf, N., & Aslam, S. ”A survey on deep learning methods for power load and renewable energy forecasting in smart microgrids,” Renewable and Sustainable Energy Reviews, 144, 110992, 2021.

[4] Mohsin, S. M., Javaid, N., Madani, S. A., Abbas, S. K., Akber, S. M. A., & Khan, Z. A. (2018, May). Appliance scheduling in smart homes with harmony search algorithm for different operation time intervals. In 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA) (pp. 51-60). IEEE.

[5] Iqbal, Z., Javaid, N., Mohsin, S. M., Akber, S. M. A., Afzal, M. K., & Ishmanov, F. (2018). Performance analysis of hybridization of heuristic techniques for residential load scheduling. Energies, 11(10), 2861.

[6] Mohsin, S. M., Javaid, N., Madani, S. A., Akber, S. M. A., Manzoor, S., & Ahmad, J. (2018, May). Implementing elephant herding optimization algorithm with different operation time intervals for appliance scheduling in smart grid. In 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA) (pp. 240-249). IEEE.

[7] Aslam, S., Javaid, S., Javaid, N,. Mohsin, S. M., Khan, S. S., & Akbar, M. (2018, July). An efficient home energy management and power trading in smart grid. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 231-241). Springer, Cham.

[8] Aslam, S., Aslam, S., Herodotou, H., Mohsin, S. M., & Aurangzeb, A. (2020, February). Towards energy efficiency and power trading exploiting renewable energy in cloud data centers. In 2019 International Conference on Advances in the Emerging Computing Technologies (AECT) (pp. 1-6). IEEE.

[9] Wang, W. & Lu. Z., (2013) ”Cyber security in the Smart Grid: Survey and challenges,” Computer Networks, vol. 57, no. 7, pp. 1344-1371.

[10] Wang, W. ”A survey on the communication architectures in smart grid,” Computer Networks, vol. 55, no. 15, pp. 3604-3629,2011

[11] Line, M. B., Tondel I. A., & Jaatun, M. G. ”Cyber security challenges in Smart Grids,” presented at the 2nd IEEE PES International Conference and Exhibition, Innovative Smart Grid Technologies (ISGT Europe), Manchester, 2011.

[12] Khurana, H., Hadley, M., Ning, L., & Frincke, D. A., ”Smart grid security issues,” iEEE Security & Privacy, vol. 7, no. I, pp. 81-85, 2010.

[13] Reed, G. F., Philip, P. A., Barchowsky, A., & Lippert, C. J.. (2010). “Sample survey of smart grid approaches and technology gap analysis,” presented at Innovative Smart Grid Technologies Conference Europe.

[14] Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., & Al Ali, A. R. (2015, October). Smart grid cyber security: Challenges and solutions. In 2015 international conference on smart grid and clean energy technologies (ICSGCE) (pp. 170-175). IEEE.

[15] Mehrfeld, J. (2020, July). Cyber security threats and incidents in industrial control systems. In International Conference on Human-Computer Interaction (pp. 599-608). Springer, Cham.

[16] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973- 993.

[17] Naidua, H., & Thanushkodib, K. ”Recent trends in SCADA power distribution automation systems,” Journal of Scientific and industrial Research, vol. 45, no. 3, pp. 205-218, 2010.

[18] Rezai, A., Keshavarzi, P., & Moravej, Z., ”Secure SCADA communication by using a modified key management scheme,” iSA Transactions, vol. 52, no. 4, pp. 517-524, July 2013.

[19] E. Knapp & R. Samani, ”Security models for SCADA, ICS, and smart grid,” Applied Cyber Security and the Smart Grid, pp. 101-123, 2013.

[20] O’Reilly, U. M., & Hemberg, E. (2018). An Artificial Coevolutionary Framework for Adversarial AI. In AAAI Fall Symposium: ALEC (pp. 50-55).

[21] Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyberdefense trends in industrial control systems. Computers & Security, 87, 101561.

[22] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3), 410.

[23] Leenen, L., & Meyer, T. (2021). Artificial intelligence and big data analytics in support of cyber defense. In Research Anthology on Artificial Intelligence Applications in Security (pp. 1738-1753). IGI Global.

[24] Almroth, J., & Gustafsson, T. (2020, September). CRATE Exercise Control–A cyber defense exercise management and support tool. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 37-45). IEEE.

[25] Islam, M. M., & Al-Shaer, E. (2020, September). Active deception framework: An extensible development environment for adaptive cyber deception. In 2020 IEEE Secure Development (SecDev) (pp. 41-48). IEEE.

[26] Cifranic, N., Hallman, R. A., Romero-Mariona, J., Souza, B., Calton, T., & Coca, G. (2020). Decepti-SCADA: A cyber deception framework for active defense of networked critical infrastructures. Internet of Things, 12, 100320.

[27] Fugate, S., & Ferguson-Walter, K. (2019). Artificial intelligence and game theory models for defending critical networks with cyber deception. AI Magazine, 40(1), 49-62.

[28] Abay, N. C., Akcora, C. G., Zhou, Y., Kantarcioglu, M., & Thuraisingham, B. (2019). Using deep learning to generate relational honeydata. In Autonomous Cyber Deception (pp. 3-19). Springer, Cham.

[29] Cho, J. H., Zhu, M., & Singh, M. (2019). Modeling and analysis of deception games based on hypergame theory. In Autonomous Cyber Deception (pp. 49-74). Springer, Cham.

[30] Lu, Z., Wang, C., & Zhao, S. (2020). Cyber deception for computer and network security: Survey and challenges. arXiv preprint arXiv:2007.14497.

[31] Wang, C., & Lu, Z. (2018). Cyber deception: Overview and the road ahead. IEEE Security & Privacy, 16(2), 80-85.

[32] Ahmed, S., Lee, Y., Hyun, S. H., & Koo, I. (2018). Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning. IEEE Access, 6, 27518-27529.

Hana Mujlid (Member, IEEE) received her Bachelor degree from the College of Science, Faculty of Science, Um Al-Qura University, Makkah, KSA in 2005, and the M.Sc. and Ph.D. degrees from Florida Institute of Technology, Melbourne, USA in 2012 and 2016, respectively. Currently, she is working as an Assistant Professor with the Faculty of Computer and Information Technology, Department of Computer Engineering, Taif University, Taif, KSA. She worked as a Dean of deanship of library in TU, KSA from 2019 to 2021, and as a Vice-Dean of Society College at 2018. In addition, she worked as lab researcher at Florida Institute of technology, FL, USA in 2016. She enjoyed being a Mathematics instructor at Elementary school in the Ministry of education, KSA in 2012. She worked as a Manager of communication and network department Om AL-Qura University, Makkah, KSA in 2010, and as Computer Engineer at Computer Technology Company in 2007.