Available online at www.sciencedirect.com
ScienceDirect
Energy Reports 9 (2023) 1318–1326
www.elsevier.com/locate/egyr

2022 The 3rd International Conference on Power and Electrical Engineering (ICPEE 2022)
29–31 December, Singapore

DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments

Mohammad Kamrul Hasan[a,*], A.K.M. Ahasan Habib[a,*], Shayla Islam[b,*], Nurhizam Safie[a], Siti Norul Huda Sheikh Abdullah[a], Bishwajeet Pandey[c]

[a] *Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 UKM, Bangi, Selangor, Malaysia*
[b] *Institute of Computer Science and Digital Innovation, UCSI University, Malaysia*
[c] *Jain University, Bangalore, India*

Received 21 April 2023; accepted 20 May 2023
Available online 19 June 2023

Abstract

Smart grid system is evident with control technologies and digital communications systems. The cyber–physical system is a critical infrastructure connected with complex drives and devices. The modern smart grid's prominent communication standard adopts high scalability, supports numerous communication devices' input/outputs, and has multi-vendor interoperability. Cyber-attack leads to an unstable power grid system and enormous economic loss. Throughout different cyber-attack, distributed denial of service attack is mostly destructive to smart grid infrastructure. This paper investigates smart grid cyber security systems and the communication vulnerabilities of other communication protocols. A comprehensive study on distributed denial of service attack techniques and detection approaches is present. Finally, examine a new hybrid machine learning-based distributed denial of service attack detection technique for a sustainable smart grid system.

Peer-review under responsibility of the scientific committee of the 3rd International Conference on Power and Electrical Engineering, ICPEE, 2022.

Keywords: DDoS attack; Smart grid; Communication standard; Cyber security; Machine learning

1. Introduction

Global communication depends on the internet and has significantly increased the internet of things (IoT) based devices integrated with smart grids and people worldwide. More than 3 billion people are actively using the Internet and IoT devices. The growing number of different energy sources are dominated the smart grid system.

* Corresponding authors.
E-mail addresses: mkhasan@ukm.edu.my (M.K. Hasan), ahasan.diu.eee@gmail.com (A.K.M.A. Habib), shayla@ucsiuniversity.edu.my (S. Islam).

https://doi.org/10.1016/j.egyr.2023.05.184

Peer-review under responsibility of the scientific committee of the 3rd International Conference on Power and Electrical Engineering, ICPEE, 2022.

They provide a sufficient amount of power for a stable power grid system. Electric vehicles application is the most prominent source for modern smart grid systems [1–4]. In a smart grid system, a cyber–physical system (CPS) is interdepended and interconnected with cyber and physical domains. The electrical framework is based on Information and commination technology and IoT-based devices with intelligent bidirectional connection with power generation/sources, transmission and distribution, consumer consumption, and energy production for a robust, reliable, secured, sustainable and cost-effective system [5,6].

The smart grid network comprises numerous intelligent electronic devices (IEDs), different appliances, distributed energy resources (DIRs), and facilities. The investment expenses and power consumption are reduced by enabling effective operation. In a smart grid, consumers can generate, store, transfer, and sell energy power in the energy market. This energy market requires real-time communication and monitoring systems with constant data flow facilities [1,3]. Automatic control devices are installed in the smart grid system so that it would be able self-heal faults.

Additionally, a consumer can provide and access bidirectional and real-time grid communication frameworks. Consumer-oriented IEDs support customers or authorized service providers for sustainable power supply and balance between required power consumption and generation. The smart grid must be self-healing, secure, have low latency and real-time communication, have a self-dependable energy market, cyber threat, attack detection, and stand against physical damages [7,8].

The supervisory control and data acquisition (SCADA), phasor measurement unit (PMU), and Phasor data concentrator (PDC) are real-time monitoring devices that provide high-precision management data. The smart grid faces cyber-attacks for real-time monitoring and control nature since control and surveillance appear over the consumer solution and internet protocols [9,10]. Though the conventional power grid is vulnerable, the smart grid faces numerous vulnerabilities to malfunction. In December 2015, Ukraine blacked out the direct cyber-attack [7,11]. There are several vulnerabilities in the security and communication protocols. Attackers know about these vulnerabilities and attack when they get access. There are several attacks done in smart grid networks, like Denial of Service (DoS), Distributed DoS (DDoS), false data injection (FDI), and man-in-the-middle attacks. Among these, DDoS attacks are the most prominent attacks on smart grid security goals. The security goals in the smart grid are considered a CIA triad (confidentiality, integrity, and availability) [1,12]. When the attacker attacks the CIA triad, the user cannot access the network infrastructure and management system. The contribution of this study is bellowed;

- Smart grid cyber security infrastructure and requirements.
- Short review of IEEE C37.119 and IEC 61850 communication standard vulnerabilities for smart grid applications.
- State of the art on DDoS attack techniques and detection approaches.
- Proposed new hybrid detection algorithm.

The rest of the paper organize as flows; Section 2 presents the cyber-security in smart grid. The smart grid Communication Standards and Vulnerabilities are present in Section 3. Section 4 presents the DDoS attack technique in the smart grid. Section 5 describes the DDoS attack detection strategies, and the conclusion is in Section 6.

2. Cyber security

Cyber security (CS) is significant for smart grid infrastructure to achieve a secure power supply, high status, and secure energy trading. The CS protect the network, data, and information against external or internal threat and attacks. This security system ensures authentication than giving access to information [13]. Knowledge about cyber-attack types in the CIA triad is required for the secure smart grid network system. An unauthorized activity in smart grid equipment, techniques, and networks is a cybercrime. This cybercrime is of two types: one is creating a role on an unknown system, and another is a target system. The commonly used cybercrime method presents in Table 1.

This crime affects on CIA triad. The principle of confidentiality is no one accesses the system; only an authorized person can access the system function and sensitive information. Integrity ensures that only authorized people can add, remove, and modify sensitive data and information in the system database. Availability claims that data, functions, and systems must be available at the service level and when needed [1,14,15]. Different types of cyber-attack security systems are shown in Fig. 1. The on-site attack threats are protected by cloud security to save the

Table 1. Cybercrime methods.

Method	Description
DoS [20]	Hackers take control of all of the resources and server control so users cannot access the system
FDI [21]	Attacker injects the false data and changes the control system
Malware [22]	User devices in contact with viruses and worms and automatically affected
MITM [23]	Attacker put himself between the router and the victim's devices, in the meantime, changed the data
Phishing [24]	Attacker sends a link, and when the user discloses their confidential information

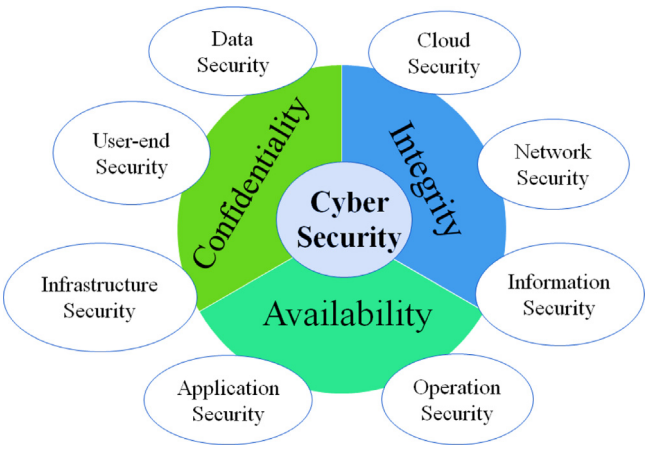


Fig. 1. CIA triad cyber security.

smart grid data information in the cloud [16]. Network security provides the system from disruptors, hacking, or malware. This **network security** solution enables the system to keep the devices out of the reach of malware, organized attackers, and hackers [17]. The **information security** system protects digital and physical data against disclosure, deletion, misuse, unauthorized access, and changes. The **operation security** protects and controls the smart grid decisions and processes data. For example, users can access the process or network to share and store the smart grid data information [18]. Software and hardware-based **application security** such as firewalls, encryption, description, and anti-virus programs protect the system from several cyber threats and attacks [19]. Several security aspects are based on the CIA triad, including infrastructure security, user-end security, and data security prevention.

3. Communication standards and vulnerabilities

Several communication standards protect the smart grid substation for secured operation. The substation communication standards are Modbus, DNP3 (mainly IEC 60870-5 based), IEEE C37.119, IEC 61850, and IEC 60870-6. IEEE C37.119 and IEC 61850 are the latest communication standards used in smart grid systems [25]. One communication standard differs from another, including protocol profile, mode of communication (unicast, multicast, publish–subscribe, peer-to-peer, client–server), communication medium (WAN, Ethernet, serial), factors number, communication bandwidth, security support, inter-operation with multi-vendor.

Smear grid deals with massive data from smart meters, remote terminal units (RTU), PMU, programmable logic controllers (PLC), and data aggregators. Data concentrators (DC) collected the data from the field devices. During the data collection, a DDoS attack happens because the internet design is persecuted by swarm flaws [7]. A single device is considered to compromise electricity outage if the DDoS attack happened in DC in the smart grid [26]. The smart grid vulnerability on different communication standard and devices are present in Table 2.

4. DDoS attack technique in smart grid

DDoS attacks employ smart grids with different strategies that compromise numerous devices. When a DoS/DDoS attack occurs, power or information flow faces restrictions in the physical layer. During the DDoS attack, there are significant effects on smart grid data process skills and history with substantial steps toward defense

Table 2. Consequence and security vulnerabilities.

Consequence	Vulnerabilities	Communication protocols or devices	Ref.
Denied access to measurement data	Information communication security gap	PMU and DC	[27]
Bay level gain access	IEC 61850 GOOSE security vulnerability, including IEDs	IEC 61850/IEDs and PMU	[25]
Unavailable channel gain access	IP network security issues in traffic, resolve service and track services	ANSI C12.22 and smart matter	[28]
Synchro phasor measurement stops working, and system visibility is lost	Authentication approach is not supported	IEEE C37.118/PMU and DC	[29]
Unsolicited event response and the victim forge relay's unresponsive and data aggregator	DNP3 protocols	DNP3 and data aggregator	[30]
Source and destination data communication interrupt	Transportation layer in IEC-104 protocol for SCADA system	IEC-104 and SCADA	[31]

mechanism. Therefore, understanding DoS/DDoS attacks are essential for getting proper knowledge about the impact on the physical grid and cloud layers and more information [7,32,33]. The DDoS attacks are present in Fig. 2. The traditional DoS attack bot in single packet flood and single device compromised.

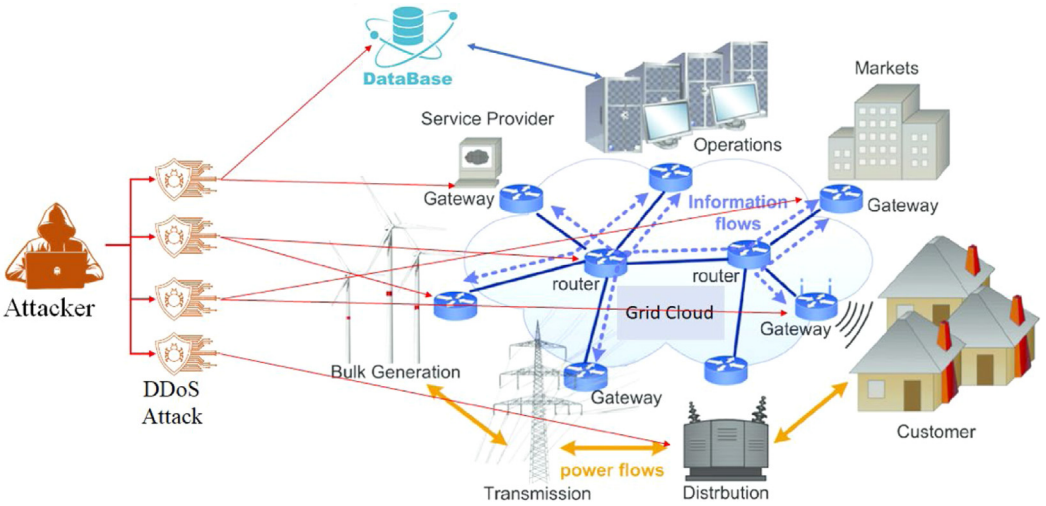


Fig. 2. DDoS attack in smart grid.

In contrast, the attacker (Botmaster) targets multiple packet floods in smart grid applications, and various devices are compromised for DDoS attacks that result in massive destruction. The smart matter is the main target for DDoS attacks because of the vulnerabilities point of security protocols in home networks. Fig. 3 represents the taxonomy of potential DDoS attacks in smart grid applications. The data communication is bidirectional for forwarding and transmitting, and the attacker focuses on this possible point for a DDoS attack.

5. Attack detection strategy

Modern substation automation system flows IEC 61850 GOOSE and IEEE C37.118 communication standards to detect and prevent attacks. The attack detector software modules are; anomaly detector, random data-path selector, spoofing detector, fingerprint detector, and more details in [34]. The PMU simultaneously sends the data to phasor

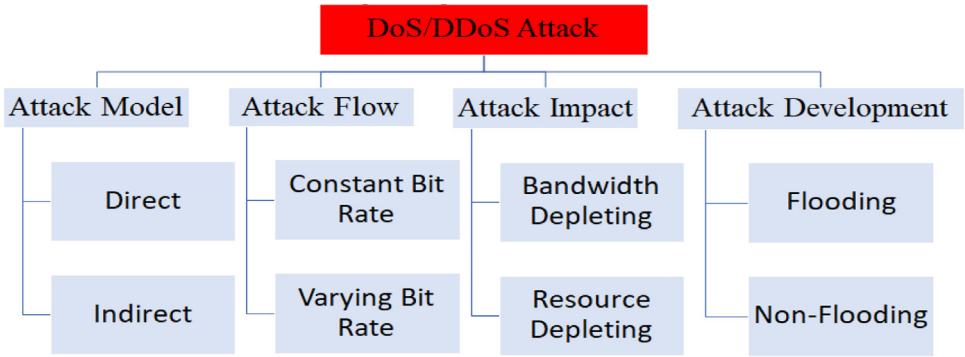


Fig. 3. Taxonomy of DDoS attack [33].

data concentration (PDC). During the DDoS attack, PMU data was sent to healthy PDC command the multiplexer. The spoofing and fingerprint-based DDoS attack detection flowchart is shown in Fig. 4.

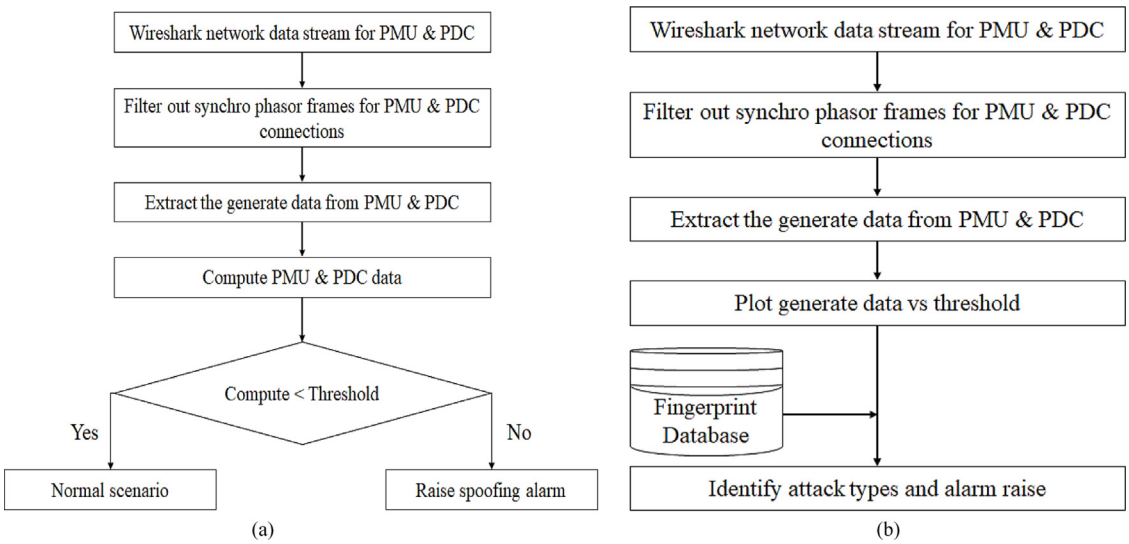


Fig. 4. Flowchart of DDoS attack detection process, (a) Spoofing-based detector, (b) fingerprint-based detector.

The authentication-based solution is another traditional approach to detecting cyber-attacks regarding availability and integrity security goal. When the attacker inserts instructions and erroneous data into the server, a lightweight cryptography algorithm detecting these malicious attacks is considered a powerful tool for rejecting inserts. Trap-based solutions and intrusion detection are also considered to detect attacks [7]. When the attack happens on the GOOSE protocol, the then distributed circuit barker tripped, and no current flowed in the distribution system; moreover, power system frequency fails to cascade and excursion. The power line behavior presents in Fig. 5. Varma et al. [35] present a machine learning-based hybrid approach to detecting DDoS attacks. Here we analyze this machine learning-based DDoS attack detection process.

5.1. WAMS setup and attack model

A public dataset with different classifications is used to overcome the DDoS attack [35]. This data set contains 23 features with statistical information, including packet size of source IP, packet ID, packet rate, packet type, to node, from the node, source address, and destination address. The first 10 000 records of data are randomly sampled

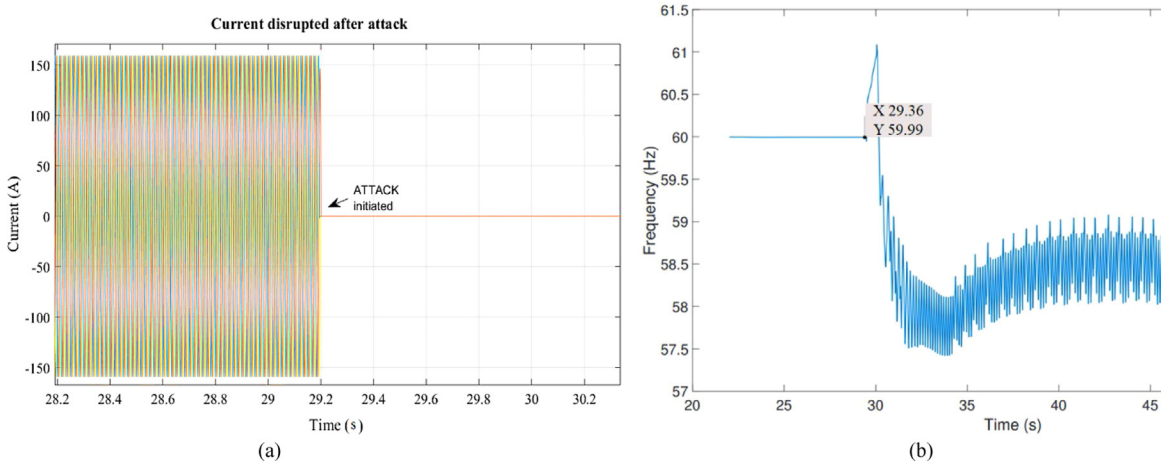


Fig. 5. Power disruption after the attack, (a) current measurement, and (b) frequency excursion [25].

to pre-process the data set. For the same feature, some abnormal data might mislead the trained model. The standard data processing standardization could be as follows;

As $D^{n\times p}$ is the original denoted data matrix, where n is the number of samples and p is the number of features. The mean value of each feature of the sample was calculated;

$$S_j = \sum_{i=1}^{n} \frac{D_i^j}{n} \tag{1}$$

After verifying and pre-processing the data set, the model assumed 80% is train data and 20% is text data, respectively.

5.2. Attack detection algorithm

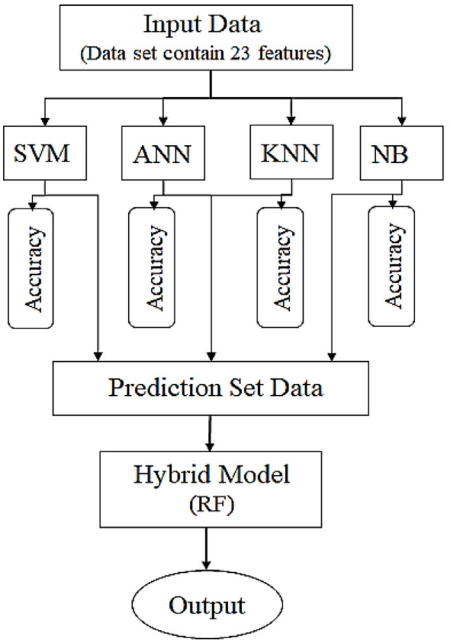
Using the ML algorithms, namely, Support Vector Machine (SVM), Artificial Neural Network (ANN), K-Nearest Neighbors (KNN), Naïve Bayes (NB), and Random Forest (RF) to detect DDoS attack and the proposed model accuracy. Fig. 6a presents the proposed system architecture. Each algorithm offers its attack detection accuracy and prediction set, namely validation and test sets. Finally, each model obtains prediction set data, is trained with an RF model, and makes a hybrid; details are present in [35]. This work is executed in four stages; initially, PMU data is collected from the database and then pre-processed. This pre-processed data is an analysis and evaluated with different algorithms, and finally, these estimated data will train into a hybrid model. This learning model divided the dataset as training: and testing into 80:20, respectively. The hybrid model proposed algorithm result is presented in Fig. 6b.

5.3. Result

For the validation of the proposed hybrid train model, the simulation is conducted in Jupitar Notebook 6.4.8. The program conducts in Intel (R) Core (TM) i7-4790 CPU@3.60 GHz, 16.0 GB RAM, 64-bit operating system, Windows 10 Pro edition desktop computer. Using the algorithm in Fig. 6(b), the proposed system result is presented in Fig. 7. Among the SVM, ANN, KNN, and NB, the ANN algorithm provides better accuracy (77.20%) and the lowest SVM (69.51%) than the other algorithm. The hybrid model (RF) gets better accuracy, which is 81.23%. The future implication will focus on achieving 100% accuracy with real-time DDoS attack detection.

6. Conclusion

Smart grid is a modern and convening power generation and distribution system. IEC 61850 and IEEE C37.118 are the latest communication standard for the smart grid system. DDoS attacks target communication



(a)

Algorithm DDoS Attack Detection: Hybrid Approach

1. **Initialize**:
   Import Python library file
   Import machine learning algorithms
   Import dataset
2. **Data processing**:
   Sampling dataset, as 3000
   Remove empty values, item and dataset processing
3. **Machine learning model**:
   SVM(kernel = 'sigmoid', gamma = 'auto')
   print (accuracy)
   KNN(n-neighbors=5)
   print (accuracy)
   GaussianNB()
   print (accuracy)
4. **Hybrid Model**:
   Blanding SVM, KNN & GaussianNB
   [In]: Validation input and test input data
   [In]: Optimize with Random Forest Classifier
   print (model accuracy)

End
Output

(b)

Fig. 6. Proposed DDoS attack detection, (a) architecture, (b) algorithm.

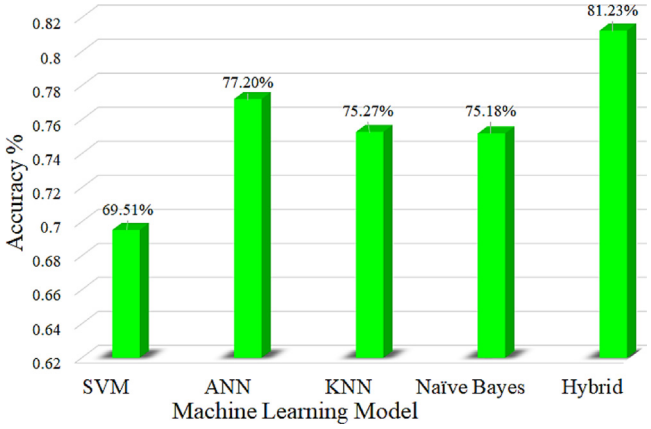


Fig. 7. Model accuracy performance and comparison.

standard protocol vulnerabilities and impose severe attacks on smart grid systems. Cyber security is becoming a significant concern for a secure and reliable power grid system. This paper describes the smear grid cyber security, communication standard vulnerabilities, DDoS attack technique, and detection strategy. This study thoroughly explains how a DDoS attack happens in a smart grid system and prevents it through of hybrid machine learning approach.

Declaration of competing interest

The authors declare no conflict of interest.

Data availability

Data will be made available on request.

Acknowledgments

This work has been supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme, No. FRGS/1/2020/ICT03/UKM/02/6.

References

[1] Hasan MK, et al. Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wirel Commun Mob Comput 2022;2022.
[2] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Rep 2021;7:8176–86.
[3] Akhtaruzzaman M, et al. HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey. IEEE Access 2020;8:222977-223008.
[4] Salamzada K, Shukur Z, Bakar MA. A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. Asia-Pac J Inf Technol Multimed 2015;4(1):1–10.
[5] Habib AA, et al. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. Comput Electr Eng 2023;107:108638.
[6] Hasan MK, et al. Smart grid communication networks for electric vehicles empowering distributed energy generation: Constraints, challenges, and recommendations. Energies 2023;16(3):1140.
[7] Raja DJS, et al. A review on distributed denial of service attack in smart grid. In: 2022 7th international conference on communication and electronics systems. ICCES, IEEE; 2022.
[8] Bagdadee AH, Zhang L. A review of the smart grid concept for electrical power system. In: Research anthology on smart grid and microgrid development. 2022, p. 1361–85.
[9] Hasan MK, et al. Review on cyber–physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. J Netw Comput Appl 2022;103540.
[10] Hasan MK, et al. Timing synchronization framework for wide area measurement system in smart grid computing. In: 2020 global conference on wireless and optical technologies. GCWOT, IEEE; 2020.
[11] Gjesvik L, Szulecki K. Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. Eur Secur 2022;1–21.
[12] Manimegalai M, Sebasthirani K. Performance analysis of smart meters for enabling a new era for power and utilities with securing data transmission and distribution using end-to-end encryption (E2EE) in smart grid. In: Intelligent computing and applications. Springer; 2021, p. 1–12.
[13] amal AA, et al. A review on security analysis of cyber physical systems using Machine learning. Mater Today: Proc 2021.
[14] Ardito C, et al. Revisiting security threat on smart grids: Accurate and interpretable fault location prediction and type classification. In: ITASEC. 2021.
[15] Palmieri M, Shortland N, McGarry P. Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Comput Hum Behav 2021;120:106745.
[16] Li J, et al. Edge-cloud computing systems for smart grid: State-of-the-art, architecture and applications. J Mod Power Syst Clean Energy 2022.
[17] Zhang J. Distributed network security framework of energy internet based on internet of things. Sustain Energy Technol Assess 2021;44:101051.
[18] Ogbanufe O. Enhancing end-user roles in information security: Exploring the setting, situation, and identity. Comput Secur 2021;108:102340.
[19] Alkatheiri MS, Chauhdary SH, Alqarni MA. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. Sustain Energy Technol Assess 2021;45:101219.
[20] Chen X, et al. Distributed resilient control against denial of service attacks in DC microgrids with constant power load. Renew Sustain Energy Rev 2022;153:111792.
[21] Reda HT, Anwar A, Mahmood A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts. Renew Sustain Energy Rev 2022;163:112423.
[22] Abdel Ouahab IB, et al. Towards a new cyberdefense generation: proposition of an intelligent cybersecurity framework for malware attacks. Recent Adv Comput Sci Commun (Former: Recent Pat Comput Sci) 2022;15(8):1026–42.
[23] Al-Shareeda MA, Manickam S. Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation. Symmetry 2022;14(8):1543.
[24] Yoo J, Cho Y. ICSA: Intelligent chatbot security assistant using Text-CNN and multi-phase real-time defense against SNS phishing attacks. Expert Syst Appl 2022;207:117893.
[25] Reda HT, et al. Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in the smart grid. Sensors 2021;21(4):1554.
[26] Risbud P, Gatsis N, Taha A. Vulnerability analysis of smart grids to GPS spoofing. IEEE Trans Smart Grid 2018;10(4):3535–48.
[27] Islam SN, Baig Z, Zeadally S. Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures. IEEE Trans Ind Inf 2019;15(12):6522–30.
[28] Huseinovic A, et al. A taxonomy of the emerging Denial-of-Service attacks in the smart grid and countermeasures. In: 2018 26th telecommunications forum. TELFOR, IEEE; 2018.
[29] Chukkaluru SL, Kumar A, Affijulla S. Tensor-based dynamic phasor estimator suitable for wide area smart grid monitoring applications. J Control Autom Electr Syst 2022;33(3):955–64.

[30] Vosughi A, et al. Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs. Renew Sustain Energy Rev 2022;168:112794.
[31] Grigoriou E, et al. Protecting IEC 60870 − 5 − 104 ICS/SCADA systems with honeypots. In: 2022 IEEE international conference on cyber security and resilience. CSR, IEEE; 2022.
[32] Valdovinos IA, et al. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. J Netw Comput Appl 2021;187:103093.
[33] Eswari DS. A survey on detection of ddos attacks using machine learning approaches. Turk J Comput Math Educ (TURCOMAT) 2021;12(11):4923–31.
[34] Chawla A, et al. Denial-of-service attacks pre-emptive and detection framework for synchrophasor based wide area protection applications. IEEE Syst J 2021;16(1):1570–81.
[35] Varma DA, et al. Detection of DDOS attacks using machine learning techniques: A hybrid approach. In: ICT systems and sustainability. Springer; 2021, p. 439–46.