energies

Review

Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions

Mohammad Ahmed Alomari[1,*], Mohammed Nasser Al-Andoli[2,*], Mukhtar Ghaleb[3], Reema Thabit[4], Gamal Alkawsi[5], Jamil Abedalrahim Jamil Alsayaydeh[1], AbdulGuddoos S. A. Gaid[6]

[1] Department of Engineering Technology, Faculty of Technology & Electronic and Computer Engineering (FTKEK), Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka 76100, Malaysia alomari@utem.edu.my (M.A.A), jamil@utem.edu.my (J.A.J.A)
[2] Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia, nasser.alandoli@mmu.edu.my (M.N.A)
[3] College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia, mghaleb@ub.edu.sa (M.G)
[4] Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional (UNITEN), Kajang, Selangor 43000, Malaysia, reema.ahmed@uniten.edu.my (R.T)
[5] Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional (UNITEN), Kajang 43000, Malaysia, gamal.abdulnaser@uniten.edu.my (G.A)
[6] Communication & Computer Engineering Dept., Faculty of Engineering & Information Technology, Taiz University, Taiz, Yemen, quddoos.gaid@taiz.edu.ye (A.G)
* Correspondence: alomari@utem.edu.my (M.A.A) , nasser.alandoli@mmu.edu.my (M.N.A)

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Received: date
Accepted: date
Published: date

Abstract: Despite the fact that countless IoT applications are arising frequently in various fields, such as green cities, Net Zero decarbonization, healthcare systems, and smart vehicles, smart grid is considered the most critical cyber-physical IoT application. With the emerging technologies supporting the much-anticipated smart energy systems, particularly the smart grid, these smart systems will continue to profoundly transform our way of life and the environment. Energy systems have improved over the past ten years in terms of intelligence, efficiency, decentralization, and ICT technology usage. On the other hand, cyber threats and attacks against these systems have greatly expanded as a result of the enormous spread of sensors and smart IoT devices inside the energy sector as well as the traditional power grids. In order to detect and mitigate these vulnerabilities while increasing the security of energy systems and power grids, a thorough investigation and in-depth research are highly required. This study offers a comprehensive overview of the state-of-the-art smart grid cybersecurity research. In this work, we primarily concentrate on examining the numerous threats and cyberattacks that have recently invaded the developing smart energy systems in general and smart grids in particular. The study begins by introducing smart grid architecture, key components, and its security issues. Then we present the spectrum of cyberattacks against energy systems while highlighting the most significant research studies that have been documented in the literature. The categorization of smart grid cyberattacks, while taking into account key information security characteristics, can help making it possible to provide organized and effective solutions for the present and potential attacks in smart grid applications. This cyberattack classification is covered thoroughly in this paper. The study also discusses the historical incidents against energy system which depicts how harsh and disastrous these attacks can go if not detected and mitigated. Finally, we provide a summary of the latest emerging future research trend and open research issues.

Keywords: Cybersecurity, smart grid, Energy Cyberattacks, Energy Security, Cyber-physical systems.

Abbriviations:

AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure.
API	Application Programming Interface.
CPPS	Cyber-Physical Power System.
CPS	Cyber-Physical System.
CPSG	Cyber-Physical Smart Grid.
DDoS	Distributed Denial-of-Service
DER	Distributed Energy Resources
DoS	Denial-of-Service.
DT	Digital Twin
EV	Electric Vehicles
EVCS	Electric Vehicles Charging Station
FDI	False Data Injection attack
GPS	Global Positioning System
ICT	Information & Communications Technology
ICT	Information and Communication Technology.
IT	Information Technology.
ML	Machine Learning
OT	Operational Technology
PMU	Phasor Measurement Unit
RTU	Remote Terminal Unit
SCADA	Supervisory control and data acquisition
SG	Smart Grid
SM	Smart Meter

I. INTRODUCTION

Although various IoT applications, such as smart vehicles, green cities, Net Zero decarbonization, and healthcare systems, are emerging fast and affecting our life drastically, smart grid is still recognized as the most critical cyber-physical IoT application. The current traditional power grid is anticipated to be reorganized as a cyber-physical system with smart devices that may communicate data for sophisticated monitoring and control applications, in addition to the basic feature of carrying power flow [1], [2]. The bidirectional transfer of electricity and information will highly improve the power grid, creating a smart grid that will have intelligent features like self-healing, customer interaction, and adaptive protection and control.

A smart grid is a cutting-edge component of modern electricity systems that offers many advantages, including effective incorporation of distributed energy resources (DER) [3]. The basic goal of smart grid is to distribute automation and control systems over the whole power grid to enable smooth and effective two-way flow of electric power. This bidirectional feature of SG allows electrical and information to flow smoothly from distribution centers and companies to the end consumers and vice versa where selling power is permitted and controlled in both directions. This is accomplished by the incorporation of information and communication technology (ICT) to the traditional grid, which transforms it into a type of cyber-physical system (CPS). A wide range of new technologies, algorithms, and solutions, including artificial intelligence and distributed data processing, can now be developed and applied in the smart grid, thanks to the dynamic integration between the actual and virtual worlds [4], [5], [6] , [7].

Although the introduction of smart energy systems and smart grids came with a plethora of impactful advantages, it also increased the attack surface against energy sector. This opened the door widely for cyber attacker to use their traditional skills against important energy infrastructures such as smart grid. The critical nature of smart grids makes them very attractive to cyberattacks as well as cyberterrorism in worst case scenarios. Cybersecurity is considered one of the largest challenges against smart grids and IoT applications, which need to be well-researched and investigated urgently in the near future. Identifying the types of vulnerabilities that may affect a smart energy system is very important to develop efficient countermeasures against cyber threats [8],[9].

Compared to traditional power grid, smart grid contains huge number of interconnected devices, sensors, and ICT networks, which make it prone to various types of attacks, probing, and espionage. In general, cyberattacks aim to breach the main security pillars of confidentiality, integrity and availability (CIA components) of smart grid network. This can include tapping customer sensitive information, affecting the stability and reliability of grid energy distribution, large electricity blackouts, and infrastructure damage or explosion in severe attacks [10], [11], [12].

Due to its critical nature, there are a number of restrictions associated with how to defend the smart grid against cyberattacks, which prevent the full adoption of some popular IT security techniques. For instance, when an IT system is attacked, the best practices frequently involve the quick disconnection or otherwise isolation of affected devices from the network. A power grid may not be able to use such strategy because the sudden disconnection of grid control devices could result in massive blackouts or other disastrous system failures [13], [14].

Contribution:

Cybersecurity is critical while constructing information networks. Because smart grids incorporate several networks, cybersecurity is a top priority in smart grid architecture [15]. Numerous researches, surveys, and review papers have been published that provide an overview of the prevalent cybersecurity challenges in smart grid applications. Despite many academics work hard to improve smart grid cybersecurity by employing a variety of strategies and research studies, the breaches against these critical systems are very high and more studies and recent reviews are still necessary [16], [17].

In this study, we focus on providing a detailed review of cybersecurity and cyber threats against smart energy systems in general, and smart grid in specific. Our goals are to provide a comprehensive overview, classify cyber-security threats, review and analyze historic smart grid attacks, and suggest future study directions to educate new researchers. Figure 1 explains how the method of this survey is conducted, starting from the identification stage of related articles through the screening process to scrutinize and investigate these articles until reaching the final selection stage with summarized chosen articles.

The contributions and features given in this study are summarized below:

- A state-of-the-art detailed background of smart grid, compared to traditional grid, as well as its key components and security issues are elaborated in this work with up to date analysis of related studies.
- Collecting, studying and providing the latest mechanisms for recognizing different types of cyber-attacks in SG systems. The most common cyber threats targeting smart grid are discussed thoroughly.
- The worldwide historical cyberattacks against critical smart energy systems and smart grids are thoroughly discussed. This can provide academia and industry with a recent vision on how attackers are targeting smart energy systems which helps developing strategies to mitigate such threats.
- The study also summarizes the latest emerging future research trend, current challenges, and open research issues. Addressing these issues can be helpful when rehabilitating current smart grids or even to build a new smarter and more secure one.
- An evaluation of the extant cyberattacks based on the CIA triad and network layers are given.

This manuscript is organized within seven sections. A details background of smart grid architecture, components, and its security issues is presented in Section II. Section III addresses the related works, current research, and previous contributions that aim to mitigate cyberthreats against smart grid

systems. Then, Section IV elaborates on the major worldwide cyberattacks in history that breached the security of critical energy systems. The classification and taxonomy of cyberattacks that targets smart energy systems are illustrated in Section V. Finally, a detailed future directions as well as concluding remarks of this research are presented in Section VI, and section VII respectively.

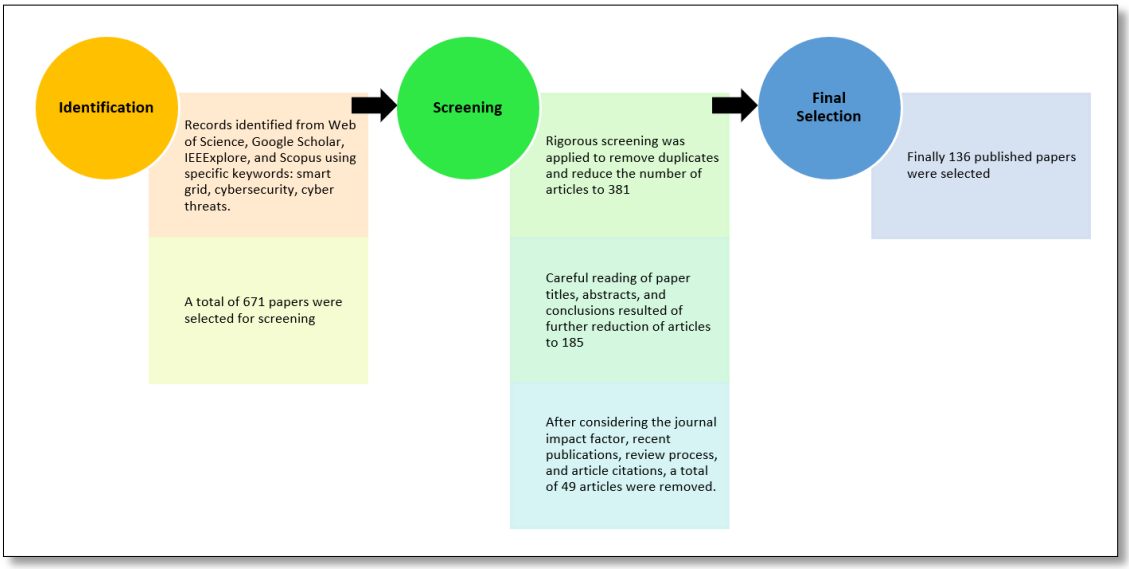

Figure 1: Flowchart of article selection criteria process

II. SMART GIRD BACKGROUND

In the digital age, the notion of a smart power grid has been refined with a few enhancements that explain the hierarchy of a distributed network which may includes smart transformers, transmission lines, distributed substations, and other electric accessories such as smart meters, among others. All of the equipment described above are utilized to deliver electric supplies from generators and plants to business organizations and finally to consumers. However, the ecology between industrial producing units and customer needs to be automated which introduce the need for IoT-based smart grids. The smart grid serves an important function by combining a digital system, operational controls, automation, and ICT to enable bidirectional communication between electricity providers and end customers [18] , [19].

A. *Smart Grid Architecure and Conceptual Model*

Introducing smart grids can be considered as one of the important innovations in energy sector. This innovation is basically a result of a fine blend between the traditional physical power grid and the ICT technologies. Bidirectional smart devices, including smart meters, sensors, and actuators, are included in all domains of smart grid system (from generation to end user side). This makes it possible for the grid to deliver a real-time control, monitor, and energy balance at high accuracy, granularity, and reliability, wherever and whenever needed [20]. According to the National Institute of Standard and Technology (NIST), a smart grid consists of seven domains. The bulk generation (including DER), transmission, distribution domains are responsible for controlling the flow of power, while the rest of domains (service providers, markets, customers, and operations) are responsible for power management and data collection [21]. These domains can be elaborated as follows:

- The Generation domain contains power generation sources - such as nuclear plants, thermal and hydro generators - as well as distributed energy resources (DER) which produce renewable energy like solar, wind, and tidal wave renewable energy installations. The generation domain main role is to produces electricity while it can also store it for later distribution. The generation assets are typically integrated into the smart grid to provide dynamic response to demand and grid conditions. Key components include renewable energy sources, conventional power plants, decentralized power generation, and energy storage systems.
- The Transmission domain is responsible for carrying high voltage power for long distances to hand it over to distribution facilities. In Distribution domain, the electricity is distributed to and from consumers. Transmission Systems carry high-voltage electricity over long distances from power plants to substations. The substations step down the voltage to a lower level suitable for distribution.
- The Distribution System is responsible for delivering electricity from substations to consumers. It includes medium- and low-voltage lines, transformers, and distribution equipment. A smart grid allows for dynamic load balancing and fault detection, making the distribution system more resilient and responsive. The transmission and distribution networks are the conduits through which energy flows from power plants to end-users. The smart grid enables two-way communication and data flow, allowing for better monitoring, optimization, and control of these networks. Key elements include: smart meters and sensors, advanced grid controllers, grid communication infrastructure, and voltage regulation and power flow control [22],.
- The organizations that deliver electrical services to (and from) consumers constitute the Service Provider domain.
- The customer domain is the end user of energy, who in smart grid can also generate and store electricity through DER installations. The customer can be of residential, industrial, or commercial type. Customers, both residential and industrial, are active participants in the smart grid. Through advanced technologies, consumers can engage in demand-side management, shifting energy use based on pricing signals or system needs. Key elements may include smart meters, home energy management systems (hems), demand response, and electric vehicles (EVs).
- The Markets domain contains the players and facilitators in the power markets and other economic systems that encourage action and improve results of the power system. The market layer deals with the economic and regulatory aspects of the smart energy system. This might include real-time pricing, energy trading platforms, incentive programs, and regulatory oversight.
- Finally, in order to manage the movement of electricity, the Operations domain role comes. This domain focuses on the control and analytics of the grid which involves the intelligence and decision-making capabilities that ensure the smart energy system operates optimally. This layer includes grid operation and control systems, advanced analytics, optimization algorithms, and cybersecurity measures [23].

Figure 2 shows the various domains of a smart grid and how they interact with each other.

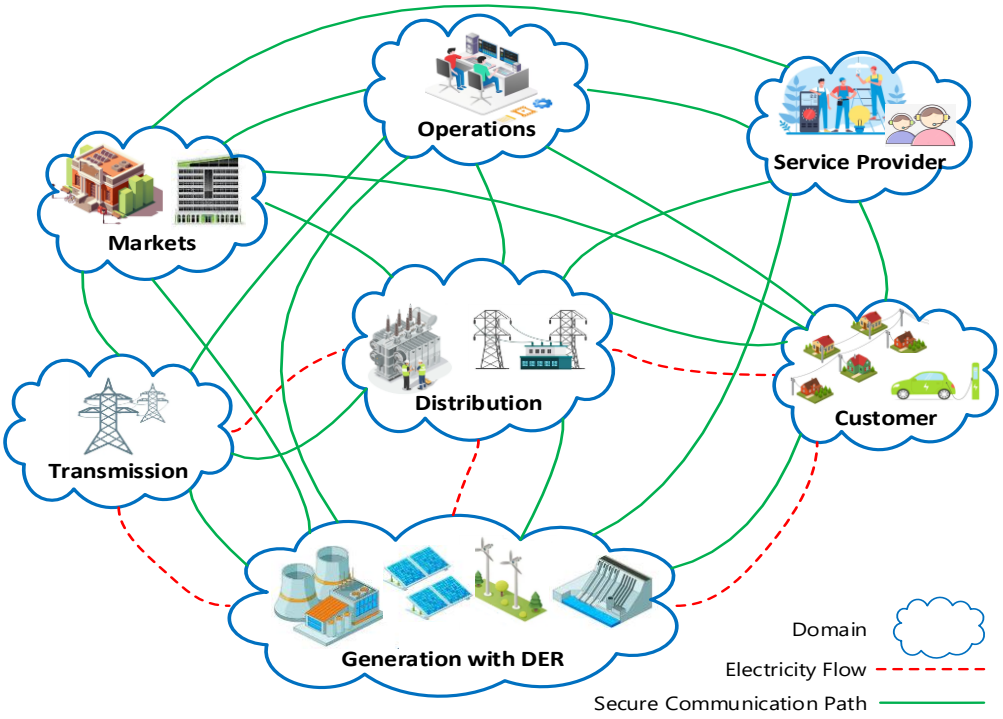

Figure 2: Domains of Smart Grid - Conceptual Model [22]

B. *Key Components of Smart Grid*

Recent SGs are very complex in structure where various subsystems are interconnecting. An IoT-based smart grid might have complex structure with various components such as: ICT devices, power generation, transmission and substations, distribution system, consumer, smart meters and AMIs, regional and central control center, Intelligent Electronic Devices (IEDs), protocol gateways, remote terminal unit (RTU), phasor measuring unit (PMU), SCADA, tap changer, log services, human to machine interface (HMI), circuit breakers, protecting relays, and home appliances [24].

ICT (Information and Communication Technology) devices in a smart grid include sensors, controllers, communication equipment, and computing systems that enable real-time data collection, transmission, and processing. These devices help to monitor system performance, predict failures, and enable the efficient control of the grid. Regional Control Centers (RCCs) and Central Control Centers (CCC) are facilities where operators monitor and control grid operations. They use real-time data to ensure stability, handle emergency situations, and optimize power distribution across the grid. Intelligent Electronic Devices (IEDs) are smart devices used to monitor, protect, and control power system equipment, such as circuit breakers, transformers, and relays. They incorporate microprocessors to provide real-time data processing, protection, and automation. Protocol Gateways facilitate communication between different devices and systems within the grid by translating various communication protocols. For example, they enable interoperability between legacy equipment and newer smart devices. Remote Terminal Units (RTUs) are devices that collect data from remote locations, such as substations or generation plants, and send it to a control center. They also receive commands from the control center to operate equipment like circuit breakers or switches. PMUs

measure the electrical waves on an electricity grid to determine the health of the system. They track phase angle differences, which are key to understanding system stability and managing grid congestion. PMUs feed real-time data into the control center for analysis. Circuit breakers are safety devices that automatically disconnect a section of the grid if there is a fault, preventing damage to equipment and ensuring safety. Protective relays are devices that detect abnormal conditions, such as overcurrent or under-voltage, and initiate protective actions like tripping circuit breakers to isolate faults. Finally, Home Appliances in a smart grid context refer to consumer devices such as HVAC systems, lighting, and home automation systems [24].

The two most important components of a smart grid which are prone for cyber threats are the Supervisory Control and Data Acquisition (SCADA) and the Advanced Metering Infrastructure (AMI).

Supervisory Control and Data Acquisition (SCADA) functions as control systems for industrial process control and monitoring, including electric power grid, oil mining, nuclear facilities, traffic control systems, and water treatment systems. Because they ran on isolated networks, traditional SCADA systems were less vulnerable to Internet threats. Due to this isolated nature, it is argued that original SCADA was developed without any focus on security. Modern SCADA systems, on the other hand, have developed from isolated, relatively simple systems into complex, open, advanced systems that are linked to the Internet [25],[26], [27]. Modern SCADA systems come with many features that make them more complex and challenging to manage. Communication protocols, control logic, security, and user interfaces are a few of the new features. Since they use open access networks to maximize efficiency, these systems have been vulnerable to a variety of cyber threats. A hostile user might take over a power grid of a country, cause a nuclear reactor to malfunction, or shut down the water supply system if SCADA systems are not secured [28].
SCADA networks' architecture has become vulnerable and susceptible for cyberattacks as a result of the use of Internet connectivity, cloud computing, wireless communications, and social engineering. The lack of robust encryption and real-time monitoring is one of the key causes of SCADA's vulnerabilities. From the supervisory level to the field instrumentation level, attacks might happen at any layer. These cyber-attacks can be divided into three categories according to how they affect network connections, software, and hardware [29]. A hardware attack occurs when a hacker gains unauthorised access to the hardware and tampers with it or its functionality. Access control is the main key point for SCADA hardware security. On the other hand, a software attack happens as a result of SCADA's software being implemented inefficiently. The SCADA system uses a range of software to meet the functional requirements and increase efficiency. With software attacks, SCADA is susceptible to SQL injection, Trojan horses, and buffer overflows. Finally, an attack on network layer can occur on various layers such as network layer, transport layer, and the application layer [30], [31].

Advanced Metering Infrastructure (AMI) function is to measure and analyze energy consumption while enabling bidirectional communication between customer and utility company. An essential part of the smart grid technology, which is being quickly adopted in the commercial sector, is the smart electric meter (SM) [32], [33]. Wired or wireless networks can be used to link smart electric meters where these meters achieve their job of remote monitoring and data collections through using different network protocols. These smart meters assist the service provider with remote monitoring and data collection, such as power consumption at a customer premise. Smart meters deliver their data to service providers automatically in almost real-time which make them very efficient and helpful in various ways [34],[35].
Advanced Metering Infrastructure (AMI) security has improved along with the introduction of this technology. AMI is used by energy markets, utility companies, and regulators to make it easier to gather real-time data on electric flow and usage. Utility companies will be able to provide demand-side management, dynamic pricing services, and better grid management as a result, albeit these additional capabilities may increase the attack surface [36]. Smart meters and phasor measuring units

(PMU) are examples of AMI components that are IoT-based and have vulnerabilities similar to those of IoT devices connected to the grid. SMs and PMUs suffer from similar vulnerabilities, such as the lack of appropriate security standards, lack of computing resources for cryptographic algorithms and antivirus software needed for security requirements, and unsecured connections [37], [38].

C. *Security of Smart Grid*

As Smart grids offer a wealth of opportunities and advantages, but they also come with several security risks. The creation of a highly secure information system is vital for maximizing the benefits of smart grids. It is believed that automation and control systems like SCADA were not meant for use in the unsecure and open environment, and neither was Modbus communication protocol, which shares SCADA information to operate industrial processes [39], [40]. The security of smart grid information system must be given top importance since electricity assets are important parts of the country's infrastructure that may attract terrorists. Damaging a power grid due to security intrusions might destabilize large areas or entire cities [41].

Additionally, there are numerous reasons why the IoT-based smart grids are more prone to security issues and threats. Many results from their online accessibility, which makes it possible for data tampering by attackers. The smart grid is more susceptible to attack because of the growing number of IoT devices being employed in it; and here are some of the reasons that make it fragile to breaches [42], [43], [44]:

- The devices in the smart grid exchange private and sensitive data between consumers and utility corporations utilizing an IP-based communication network. These networks can be affected by many security risks, including denial-of-service, man-in-the-middle, replay attacks, and eavesdropping.
- The two-way information flow itself may make the smart grid vulnerable to several threats by permitting unauthorized access.
- It has been asserted that wireless sensor networks, which are used by smart grid to connect smart meters, are vulnerable.
- Employing the IoT components could result in the smart grid to inherit their security issues which might be related to controlling and monitoring these IoT devices.
- As the smart grid contains various components with diverse technologies which require instant interaction between them for smooth functionality of smart grid. This interaction will mandate creating access points between components which increase the vulnerability to security threats.

III. Related Works and Previous Contributions

Cybersecurity in smart grids will be crucial to maintaining power grid stability and delivering dependable, sustainable services. Researchers can use or enhance existing solutions more successfully if they are aware of the various attack types and countermeasures. In an attempt to address the cybersecurity issues related to smart grids and smart energy systems, various studies and researches have been conducted in recent years. Table 1 presents the most recent studies in smart grid cybersecurity field. In the table, we summarized the outcomes from the most significant researches as well as attack vector they covered. However, the current studies still have the following limitations which are to be covered during this review:

- Gathering, researching, and offering the most up-to-date studies which help identifying various cyberattacks in SG systems. This article goes into great detail about the most prevalent cyberthreats that attack smart grids.
- Studying, summarizing, and investigating the major worldwide cyberattacks against smart grids and smart energy systems in the last forty years which helps researchers and community understand attackers' techniques and mentality. This helps new attacks to be eliminated in the future.

- The most recent rising future research trends and present difficulties are also compiled in this study in section VI. Rehabilitating existing smart grids or even creating a new, smarter, and more secure one can benefit from addressing these problems throughout this work.

In addition, Table 2 cover the recent studies of new technologies that may help addressing and improving or even negatively affecting the cybersecurity of smart grid. These edge-cutting technologies may include digital twin, artificial intelligence, blockchain, renewable energy (RE), and electric vehicle (EV) systems. Smart grid cybersecurity is being quickly shaped by these new technologies, which present both possible advantages and challenges. Real-time monitoring and predictive analysis are made possible by the digital twin technology, which builds a virtual version of the actual grid. It aids in vulnerability identification and grid performance optimization. However, there are serious cybersecurity dangers if the digital twin paradigm is compromised since attackers might alter the virtual grid to influence physical operations. The effect of AI is also crucial. By analyzing enormous volumes of data and identifying abnormalities more quickly than conventional techniques, AI helps detect and respond to cyberthreats. AI poses a dual hazard because, although it improves security, cybercriminals may use it as a weapon to automate attacks or get beyond security measures. Decentralized and impenetrable record-keeping provided by blockchain can improve data integrity, strengthen authentication, and safeguard communication between grid components. Blockchain's actual use in large-scale smart grids may be limited by its scalability and energy consumption problems, and implementation flaws could potentially be exploited. Additionally, reducing reliance on centralized electricity and improving grid resilience are two benefits of integrating decentralized renewable energy sources, such as wind and solar. Nevertheless, it makes grid management more difficult and opens up new avenues for cyberattacks, especially if these dispersed systems are not well secured. Finally, in order to charge, store energy, and possibly even distribute electricity, EVs need to communicate with the grid. If these systems are not sufficiently protected, hackers may target EV charges or utilize EVs as gateways to grid infrastructure, which could lead to new vulnerabilities.

Table 1: Recent review studies in the field of smart grid cybersecurity attacks

Ref. Year	Main Contents	Attacks studied /threat Types	Methodology / Defense Method	Results / Research Outcomes	Targeted Infrastructure
[16] 2023	Discusses Past, current, and future threats and defense methods in smart grid. Blockchain and quantum computing in SGs are also introduced. It summarizes different methods and techniques to review corresponding solution approaches in cyber-security in SGs.	Sensor and actuator attacks, Data integrity attacks, DoS, Zero dynamics (ZDA), Resonance (ResA), Time-Delay switch (TDSA), FDIA, MitM attacks	Follows Systematic methodology to review corresponding solution approaches in SG cybersecurity. The decisive problem-solving approaches and defense mechanisms are investigated.	The use of intelligent methods, based on machine learning, will enhance smart grids efficiency and failure prevention. Knowing the different methods of cyberattacks in the power systems and how to deal with them will make the network more resilient.	Smart Grid
[17] 2021	Discusses approaches to defend smart grid through its most vulnerable 4 categories, and identify opportunities to strengthen its cybersecurity	DoS, Injecting False Info, Disconnecting Resources, Insider Attack, Cascading effects	Introducing a defense-in-depth strategy that covers 4 measures: device and application security, network security, physical security, and policies & procedures	The paper identified a set of software and organizational approaches, including IDS, software-defined networking, and awareness training, as ways to secure smart grid. Resulting fundamental security problems and attack vectors in interconnected power grids are investigated.	Power Grid and CPS

[45] 2020	A comprehensive smart grid cybersecurity survey: objectives, requirements, wide spectrum of attacks, solutions to IoT-based threats, future research directions	Most attacks that breach Confidentiality, Integrity, and availability triad are covered in category wise.	Categorizing cyber threats based on two directions: CIA-triad categorization and network layers categorization	Securing the heavily IoT-equipped power grid depends on the examination of network vulnerabilities, attack countermeasures, and security requirements. Analyzing weaknesses of various system layers including IoT infrastructure is crucial.	Smart Grid with IoT
[20] 2021	Investigate microgrid systems: communication protocols, standards, and vulnerabilities with suggestions to enhance their security.	Traffic analysis, Social eng., Scanning ports, Viruses and Worms, DoS, MitM, Reply, Jamming, Masquerade, Backdoor	Layer-wise segregation of microgrid structure is used to identify its cybersecurity risks.	Providing recommendations to enhance the security of microgrid systems by distinguishing their layers. Identifying research gaps and Future work is elaborated.	Microgrids
[3] 2022	A comprehensive study of typical inverter-based smart power grid with DER integration; its vulnerabilities, nature of cyberattacks, and defense strategies.	Mostly focuses on False Data Injection Attack (FDIA), DoS	A comprehensive review analysis of current research	provides an all-inclusive survey at the state-of-the-art smart grid cybersecurity research and elaborate on potential research topics in the future.	Smart Power System (Inverter-based)
[46] 2020	Study mechanisms of the FDIA against smart grids with defense methods	False Data Injection Attack (FDIA)	Model-based defense and data-driven defense methods	The severe consequences of the FDIA show how urgently new detection algorithms must be developed in order to counter these expanding risks.	Smart Grid
[13] 2021	Techniques to defend the smart grid against cyberattacks have been suggested. In order to detect and identify FDI attacks, this paper examines three grid resilience criteria: accuracy, computing complexity, and robustness against external influences.	False Data Injection (FDI) attacks	Quantitative study where the recently proposed cyberattack detection and identification methods (Data-Driven, State Estimation, Game Theory) are quantitatively compared.	A detailed comparison, based on quantifiable criteria, of methods that focus on the detection/identification of cyberattacks against smart grid is given. It shows that no all-inclusive solution to fit all smart energy systems.	Smart Grid
[47] 2019	Introducing an effective and efficient approach to analyze the impacts of cyberattacks on the grid vulnerability to cascading failures. That is analyzed here through high-probability IC screening and a deterministic cascading testing.	FDI attacks	Two-step simulation approach, which consists of a high-probability IC screening and a deterministic cascading Testing.	The simulation results on the IEEE 118-bus systems verify the effectiveness of the proposed approach and highlight the increased risk imposed by cyberattacks which may cause cascading failures to a power grid.	Power Energy Grid
[48] 2023	A thorough study of smart gird cyber-physical and cyber security systems, standard protocols, challenges, and recommendations.	DoS, FDI, and Man-in-the-Middle (MITM), All attacks against CP layers.	A correlation between smart grid CPS communication technology, standards and protocols, and application	Smart grid should be demonstrated rapidly to gather enough state estimation information for assessment. Detecting/mitigating the frequency control in the SG under cyber-attacks requires a proper attention. The power sector has become blockchain technology large applicable field.	Smart Grid
[49] 2018	Bringing in smart grid standards that describe cybersecurity and privacy issues and exploring the information regarding their contents.	privacy-related breaches, Botnets, zero-days, Distributed Denial of Service Attacks (DDoS), Advanced Persistent Threats (APT)	Systematic study is conducted using thirty-six publications on security and eleven on privacy	There are large number of Standards, however can be categorized: 19 documents can be applied to all smart grid components, 3 documents regard substations, 5 Industrial Automation and Control Systems (IACS), 4 AMI, and 5 other selected smart grid components. 12 standards to address privacy.	Smart Grid

[50] 2023	Focusing on information flow cybersecurity by employing technical security controls to combat internet-based risks in IoT-enabled smart grids.	Nearly all types of attacks related to CIA triad	Information security model with 7 security requirements and 45 security controls.	The proposed model demonstrates that it is more practical; and addresses the limitation of the NIST model to improve SG, which is a high-level conceptual model with inadequate details.	Smart Grid
[51] 2023	Studying smart grid security from collaborative factors, emphasizing the situational awareness.	Nearly all major attack types that fit with the nature of smart grids.	A threat modeling framework is used to analyze the nature of cyber-physical attacks, and examine the existing threats detection and defense capabilities	The awareness training for smart grid operators to improve their capabilities in noticing the footprints of attacks is crucial. Examination of the existing threats detection and defense capabilities, such as IDS, and co-simulation techniques, is given; along with discussing the impact of attacks through situational awareness and power system metrics.	Smart Grid
[52] 2019	The challenges and vulnerabilities associated with the control of modern grid-tied power converters due to cyberattacks have been analyzed	Attacks targeting Grid-tied voltage-source converters (VSCs)	Robust and resilient control strategies using watermarking and model verification techniques could be an asset to infiltrate such cyberattacks in real time.	Demonstrated that cyberattacks with minimum sophistication can result in system shutdown, and cause instability and potential damage to the consumer appliances.	Smart grid-tied converters

Table 2: Recent studies of new technologies affecting the cybersecurity of smart grid

Ref. Year	Main Contents	Attacks studied /threat Types	Methodology / Defense Method	Results / Research Outcomes	SG Involved Technology
[53] 2023	Trace the investigation and propose practical ideas in developing digital twin (DT) technology, according to various application domains of power systems.	packet delay, replay, FDIA, DOS attacks, ML-related attacks.	DT-driven model for energy systems	The work proposed solutions to deal with the challenges associated with DT in energy systems; and how DT helps reducing cyber threats through ML technology.	Smart Grid from Digital Twin perspective
[54] 2023	Investigating the impact of AI and blockchain on smart grid security and power distribution automation, including scheduling, management, optimization, and privacy concerns. Introducing three unique pseudo-smart contracts and digital signatures with consensus policies.	Data availability attacks, Control signal attacks, Load redistribution attacks, Measurement attacks, Pricing attacks, Control signal measurement attacks	Framework architecture for a unified and abstracted state-space in which the system analysis includes malicious attacks while maintaining an effective generalized defense hierarchy in real-time.	A secure AI-based blockchain-enabled distributed modular framework for dynamic power distribution automation of smart grids is investigated.	Smart Grid with AI and Blockchain
[55] 2018	Present a soft computing and fuzzy-based system to offer smart grid cybersecurity. This research aims to develop innovative system, towards the optimization of decision-making, aiming to offer enhancement of the design, analysis, management, and support of the digital SG security	Various CIA triad attacks	It employs soft computing approaches, fuzzy cognitive maps, and a Mamdani fuzzy inference system in order to model overall security level.	Based on the manuscript attempt for the fuzzification of a list of Logical Interface Categories (LICs), only 3 LICs are characterized as secure, 21 of them have middle overall security, whereas 3 have low overall security level.	Smart Grid With Fuzzy-based and soft computing system

[56] 2018	Studies cyber threats that affect load balancing which breach stability of smart grid.	Almost all types of attacks against CIA triad. Threat sources: Internet, Vendor, Smart meter, and Energy supplier	The study is based on a load balancing-centered smart grid reference architecture model developed as part of the evaluation using a SCADA system. Threat model is then used.	The biggest threat comes from the Internet and is directly related to the level of internet connection that office users have, as well as their level of access to the OT zone. Supply chain attacks are also a major problem.	Smart grid with renewable energy
[57] 2020	Describe and characterize all backdoors that can be exploited to seriously harm smart power grid due to its connectivity to EV and EVCS equipment.	Demand-side attack vector, all EV/EVCS cyber threats, Spoofing, Tampering, Repudiation, Info Disclosure, DoS	STRIDE threat model (using an attack tree) that summarizes the attack strategies to cause voltage and frequency instability in the power grid	Vulnerabilities must be addressed as the number of EVs continue to grow worldwide and their impact on the smart power grid becomes more viable. Standardizing and unifying protocols for EV charging is of foremost priority	Smart Grid from an EV perspective
[58] 2022	Proposing an algorithm for smart grid DDoS detection based on deep learning	Distributed DoS (DDoS)	A hybrid deep learning algorithm validated through simulations on a cybersecurity benchmark	The proposed algorithm outperforms the current IDS for DDoS attack against communication infrastructure of Smart Grid, with an overall accuracy rate of 99.7%.	Smart Grid with neural networks (deep learning)
[59] 2020	Investigate the resilience and future trends of microgrid	Anomalies and intrusion attacks	Physical-based and cyber-based (classified into network and host-based) method	Monitoring and control functionalities are required for microgrids to operate resiliently in real-time. This monitoring has recently changed in trend from routine situational awareness in forecasting and prediction to the investigation of anomalies and the detection of cyber-physical threats.	Microgrids and Smar Grid

Limitations in current related studies:

While the aforementioned literature studies and review articles in the field of smart grid cybersecurity are valuable resources for understanding the current state of research, they often suffer from various shortcomings. These might include insufficient consideration of dynamic threat landscape, lack of depth analysis on how to integrate emerging technologies (artificial intelligence, machine learning, and blockchain, 5G networks), lack of accounting for the regional and contextual differences, fail to address the importance of human factors (social engineering attacks, operator mistakes, insider threats), a narrow focus on technical aspects, a lack of real-world application and evaluation, and limited integration of interdisciplinary perspectives. Addressing these gaps is crucial for advancing both academic research and the practical deployment of effective cybersecurity solutions in smart grids. Table 3 illustrates a comparison between current literature of smart grid cybersecurity and this review study. It depicts some of the specific shortcomings and limitations in recent studies which created an open gab which need to be covered by new studies.

Table 3: Comparison and limitations of related studies

Categories / Criteria	Reference and Year											
	[16] 2023	[17] 2021	[45] 2020	[20] 2021	[3] 2022	[46] 2020	[13] 2021	[48] 2023	[50] 2023	[51] 2023	[52] 2019	Our study
Review up-to-date related work (recent 5 years)	✓							✓	✓	✓		✓
Consideration of the wide threat landscape	✓	✓	✓	✓		✓			✓	✓	✓	✓
Analysis on how to integrate emerging technologies (AI, Blockchain, ML)	✓				✓	✓	✓	✓		✓		✓
Study of worldwide major cyberattacks						✓						✓
Accounting for the regional and contextual differences		✓			✓			✓	✓			✓
Address the importance of human factors		✓	✓		✓					✓	✓	✓
Attack Types with compromised CIA parameter			✓	✓				✓	✓			✓

IV. Major Worldwide Cyberattacks Against Energy Systems

Many cybersecurity attacks have been reported in the energy sector over the course of the last few decades. This dates back to the early eighties of last century when the first significant attack occurred. Depending on the strength of attack and importance/sensitivity of breached energy system, the impact of these attacks varied greatly. While some have gone completely unnoticed, others have resulted in hefty financial losses, explosions, and even fatalities. The actual threat comes from the rise in these instances [60]. However, over the past few years, these cyber threats have become more threating to the various energy sectors as hackers increasingly attempt to steal data and halt the flow of resources. The third quarter of 2022 saw a substantial increase in cyberattacks against the infrastructure of the energy and commodity sectors, with the number of large events already reaching a record high in 2022. According to the Energy Security Sentinel report [61], since 2017 there have been a total of 46 major cybersecurity attacks that have targeted the energy and commodities infrastructure. The maximum annual level between years 2017 and 2022 has been reached with thirteen attacks so far in 2022. Additionally, the majority of attacks during this period targeted the oil infrastructure, which has a share of about 30% of all incidents. The next most exposed area was electricity networks, which accounted for roughly 25% of these attacks. The gas sector have experienced a moderate amount of cyberattacks compared to other energy sectors [61]. Figure 3 summarizes and illustrates a timeline of major worldwide cyberattacks against energy systems.

A. *Siberian Gas pipeline explosion*

The 1982 explosion of the gas pipeline in the Siberian wilderness (Soviet Union), is considered to be the first suspected cyberattack on an energy facility. The breach is thought to have been brought on by a Trojan inserted to control software prior to its deployment. The pipeline control software was altered by the attackers, which caused the valves to act improperly, severely exceeded pressure limits, and eventually caused a large explosion. The explosion took place during the Cold War, a time of intense tension between the United States and the Soviet Union. According to United States retired officials, the CIA intentionally hacked and manipulated the software that controls the gas pipeline [62],[63].

B. *USA DavidBesse nuclear plant*

In January 2003, the well-known Slammer worm infiltrated the DavidBesse nuclear plant's control system in Ohio, USA, using a denial of service (DoS) attack. Through the contractor's network, the worm sneaked into the plant network. The impact of this intrusion made the supervisory system inoperable for 5 hours. As a result, it was impossible for the control room engineers to keep track of critical parameters like the reactor's core temperature. A backdoor access into the power plant's network, through the Internet, has served as an entry point for the attack, even though the worm was not designed to particularly target the power plant. The Safety Parameter Display System (SPDS), a safety monitoring system at the facility, was used to track and manage the safety of equipment there. The SPDS was connected to the plant's network, which was protected by a firewall against external network threats. However, a contractor in the plant had a bridge connection to connect him/her to the plant while bypassing the firewall, and allowing them to provide certain application services for the plant. Through this bridge, the contractor’s vulnerable network was breached by the Slammer worm, which then accessed the plant's network and rendered the plant SPDS supervisory system useless [64],[65].

C. *USA national Idaho laboratory*

Back in 2007, the US Department of Homeland Security investigated an Aurora cyberattack against test generator, which is used extensively throughout the USA. The Idaho National Laboratory has been assigned to study the Aurora vulnerability which damaged a generator costing a million dollars. The vulnerability allowed an attacker to deliberately open and close a generator's circuit breaker by injecting a number of tampered control commands. A hacker broke into the test generator's control system during this attack, flipping its circuit breaker on and off quickly in succession. As a result, the generator became desynchronized when it is cut off from the power grid. The aurora attack is built to manipulate the breaker when the generator and system slip out of synchronism; and fast enough before the safety control system responds to the breach. Attackers often have a 15cycle window to reclose the breaker before any protection device kicks in since generator protection features are purposefully delayed to prevent unwanted tripping. Manipulating the circuit breaker caused the large generator to cease functioning and explode as a result of a major desynchronization between the mechanical inertia of the generator and the electrical inertia of the grid [66].

D. *Turkey BTC oil pipeline explosion*

A cyberattack on the control and safety systems of the BTC (Baku Tbilisi Ceyhan) pipeline in Refahiye, eastern Turkey, resulted in an explosion in 2008. The attack raised the pipeline's pressure, which in turn triggered the explosion. At that time, the event was blamed on a technical issue, but PKK anti-Turkey militants claimed involvement. Later, the incident was suspected to be a consequence of a cyberattack, most likely by Russian state or criminal hacker networks. The incident happened in a tense time of Georgian war where Russia was involved. The following Investigations indicated that hackers sneaked into the pipeline's surveillance systems and valve stations, then over pressurized the crude oil inside the pipeline which led to pipeline explosion. Investigators from the governments of Turkey, Azerbaijan, and the United Kingdom have examined why the security controls, intended to detect oil spills or fires, didn't function before the explosion. Investigators eventually learned that hackers entered the system through the surveillance cameras, using the cameras' communications software to access the internal network of the system. Upon getting into the network, the intruders may have altered the pipeline pressure by breaking into industrial computers at the valve stations while avoiding detection by the central control room[67] [68].

E. *Germany WinCC SCADA system*

This attack occurred in 2010 on WinCC SCADA Software in Germany using the infamous Stuxnet virus. When struck, the virus was detected in fifteen chemical, power, and industrial control plants in Germany that use SCADA and Siemens software. The complex virus was intended to alter the functionality of Siemens Simatic process logic controller computers, which were used in production

lines, power plants, and other heavy industry. The attacker leveraged on a number of previously undiscovered Windows flaws known as zeroday exploits. The virus has the ability to conceal its presence while running and controlling over the computers it infected. The infection targeted the PCS 7 and Simatic WinCC software, however it was found and patched before it could have impacted any business or realtime data aggregation operations [69].

*F. **Iran Nueclear power plant***

The Iranian authorities acknowledged that the Natanz nuclear power station had been targeted in 2011. This complex attack is accomplished by a malicious code called Stuxnet. PLCs, which are commonly used to automate business operations and power systems, were the main target of this sophisticated computer malware. Stuxnet is a unique type of malware since it is the most intricate, sophisticated, and potent malware to date. It was created to attack certain SCADA systems utilising a number of operating system flaws, and as a result, it destroyed more than a thousand Iranian nuclear centrifuges. The attack's primary goal was to shorten the lifetime of centrifuges in order to eliminate Iran's nuclear program. Given how destructive a cyber weapon can be, this attack on Iran's nuclear power plants has highlighted the significance of cybersecurity. It has established itself as the first malware capable of directly harming a crucial energy infrastructure through the manipulation of control systems [70].

The cyberattack was accomplished on the physical layer of the plant's control system through manipulating the centrifuge rotors' weaknesses and changing their speed and pressure. It was carried out using zeroday exploits, and physically delivered by human using a USB storage device. The sophisticated level of the attack as well as thorough investigation has led to the assumption that it was sponsored by nationstate hackers from US and Israel in order to limit Iran nuclear program. At early stages, attackers infected Iranian critical infrastructure management facilities with the Stuxnet, which gathered realtime data from industrial systems. Later, they made the uranium centrifuges spin erratically and severely disrupt the entire plant electrical grid. As a result, centrifuges used to refine nuclear material were physically destroyed due to rotors' overspinning and increase of pressure [65].

*G. **Saudia Aramco Cyberattack***

The largest oil and gas firm in the world, Saudi Aramco, which supplies about 10% of the world's oil, was hit by a virus in August 2012. Due to its massive scale, this attack was regarded as the country's most serious attack. The attacks, which were caused by a malware known as Shamoon (also known as Disstrack), erased 30,000 computers' hard drives, or 85% of the oil giant's equipment, and forced the corporation to cease operations for roughly two weeks. Although viruses routinely infect the networks of multinational corporations, the fact that an attack of this magnitude was launched against a company so vital to the world's energy markets is concerning. The aggressive wipe out of data from computer hard drives appears to have been Shamoon's primary task. Although there was no oil spill, explosion, or other significant malfunction in Aramco operations as a result of this, the attack had large impact on the company's business operations, and it is possible that some production and drilling data were destroyed. Over US$15 million was predicted to be spent on replacement and incident response costs. This incident occurred after years of warning about the dangers of cyberattacks against country's critical infrastructure. The Shamoon malware apparently attempted to assault the oil and gas flow networks several months after the initial strikes in an effort to sabotage global supplies [65] [69].

*H. **Qatar RasGas***

RasGas company is the secondlargest LNG producer in Qatar after Qatargas. In year 2012, Qatar RasGas was impacted by the Disstrack malware, which resulted in major network outages and the shutdown of the company's website and computer servers. Before infecting personal computers in a company's network, Disstrack seized control of a computer machine connected to the Internet. In its second stage, the malware overwrites files and the master boot record of victim's machine, which prevents the staff personal computer from booting. After the initial attacks in midAugust, and although

oil and gas production were unaffected, RasGas' computer systems were shut down for weeks into September. The cyberattacks against Qatar's RasGas and Aramco attacks were attributed to the Iranian government, according to U.S. officials and Middle Eastbased private sources [71] [72].

I. Ukraine power grid attack

The increased usage of energy generators SCADA systems on personal devices like smartphones or tablets, which are used for private and corporate purposes, makes the threats of cyberattacks against energy infrastructure more tangible. This increases the possibility that a third party could acquire unauthorized access to a SCADA system (a power generator unit or transformer station) and take over the device's fundamental control features. One such attack targeted the Ukrainian energy infrastructure on Dec 2015, more specifically hitting the electricity distribution firm Kyivoblenergo. The attackers sent emails with infected files to the company's employees. The remote access malware known as BlackEnergy3 was installed on company workstations as a result of opening the files, allowing remote access to these Internetconnected workstations. Therefore, large sections of the power grid (three major distribution companies) were isolated and shut down as a result of the attackers' access to the power company's SCADA, leaving around 230,000 consumers without power for nearly 6 hours. This attack is known to be one of the first publicly recognized cyberattacks on power system automation software. The attack was launched against Ukraine grid through the use of spearphishing techniques to implant malware, resulting in the widespread blackout. The malware got through a bad data detection system and linked remotely with workers' computers to shut down 30 substations (seven 110 kV and 23 35 kV) for several hours [73].

After months of investigating the attack, it has been determined that a foreign cyberattack was involved. After breaking into the SCADA system, the hackers began to open circuit breakers throughout the distribution network. The operators were consequently obliged to manually reset the circuit breakers because they were unable to access the SCADA system. Following the 2015 breach, a second attack targeting Kiev occurred in 2016. In this attack, 200 MW of the generation capacity, about 20% of the city's nighttime electrical energy consumption, was shut down by the hackers [65].

J. Norway Norsk Hydro

A significant cyberattack targeted Norsk Hydro, a Norwegian aluminum and renewable energy firm, in March 2019.

The business unit Extruded Solutions (a division that transforms aluminum slabs into finished products) suffered the most substantial operational difficulties and monetary losses as a result of the attack, which had an impact on the entire worldwide organisation. About 35,000 Norsk Hydro personnel from 40 different countries have been impacted by the breach, which has locked the files on thousands of servers and PCs. The total financial impact would be close to $71 million. Despite the attack, the majority of the company's business units, including energy, bauxite and alumina, and primary metal, were still able to produce at or slightly above normal levels, albeit with laborintensive workarounds and manual processes. Norsk Hydro insisted that they would not pay a ransom to get access to its servers and computers, preferring to restore data from backup systems instead [63].

The main reason behind the attack is that an employee inadvertently opened an infected email from a reliable customer, which led to the intrusion. That made it possible for hackers to sneakily introduce their infection into the company’s IT systems.

According to the Norwegian national cybersecurity agency, the attack employed a virus dubbed LockerGoga, a fresh variant of ransomware that encrypts computer files and demands payment to decrypt them. Similarities exist between LockerGoga and other recent widespread ransomware outbreaks like Gorgon or CottleAkela. These malicious software programmes are made to access and encrypt private user data stored on infected devices, either by sending phishing emails or other forms of social engineering to persuade victims to visit a link or download a harmful file. The ransomware encrypts the data with AES algorithm or a comparable encryption technique as soon as the victim

opens the malicious attachment. In the LockerGoga incident, attackers employed the RSA4096 and AES256 encryption techniques [74].

K. *US Colonial Oil Pipeline*

The Colonial Pipeline, the largest fuel pipeline company that runs from the Gulf of Mexico to New York and considered to be a main fuelsupply artery, was the target of a ransomware cyberattack in 2021. As a result of the attack, supply of gasoline and jet fuel to the USA's East Coast were disrupted where the company proactively shut down its pipeline system in response to the attack. The main reason of the shutdown was that the company wanted to ensure the ransomware did not spread to the OT (operational technology) environment. In addition, the injected malware locked up large number of corporate systems including billing systems which complicated the mechanism to produce bills and receive payments [75].

Using authentic credentials belonging to a Colonial Pipeline employee, cybercriminals accessed a company's VPN on May 6 (one day before the attack). Although the VPN account was dormant and not intended for usage, the credentials were still valid and allowed the hackers to access the network. The employee probably used the same login information on different websites, and the perpetrators got hold of the password through a different data breach. It is uncertain how the VPN login came into the hands of the cybercriminals. Another measure that made the breach easier is that multifactor authentication (MFA) was not supported by the VPN. According to incident investigation, the attack was the result of a single compromised password which allowed them to inject a type of malware (ransomware) that encrypted company's computer data and kept it hostage until the ransom cryptocurrency is transferred. Additionally, the hack group (called Darkside) also exfiltrated more than 100GB of company's sensitive data. So, they used a double extortion tactic by stealing data and threatening to leak it while asking for a ransom [76] [77].

To mitigate the breach consequences, Colonial Pipeline started negotiating with Darkside hack group and paid hackers a $4.4 million ransom, in the bitcoin cryptocurrency, a day after finding the malware on its systems. Even with this fast response and paying the ransom, Colonial Pipeline took one week to restarted their entire pipeline system and product delivery commenced to all markets [78].

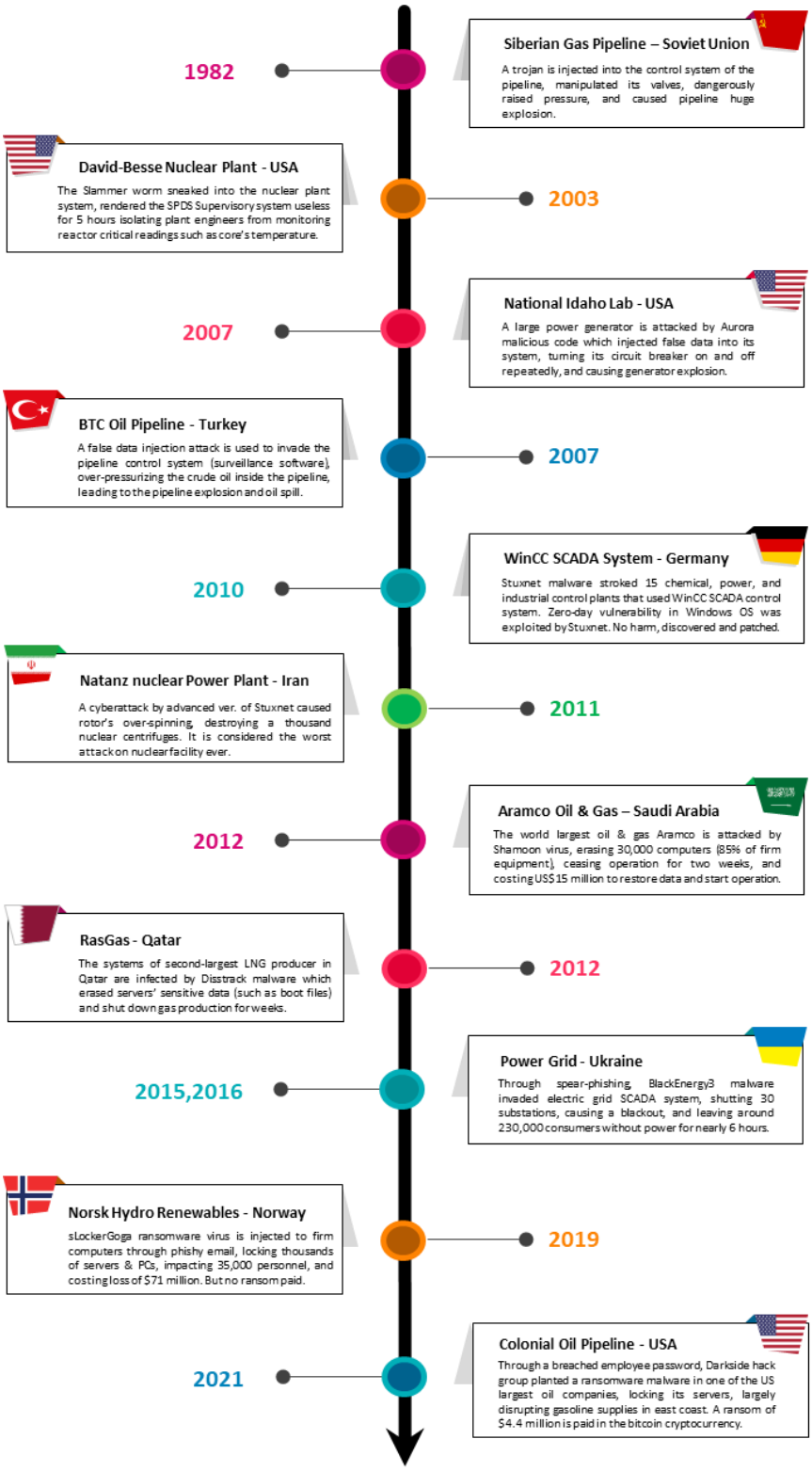

Figure 3: Timeline of Major Worldwide Cyberattacks Against Energy Systems

V. Classification of Smart Grid Cyberattack

Securing the CIA triad of the control systems and ICT in an IoT-based smart grids is one of the most crucial cybersecurity issues. The security, operation, and management of the energy sector as well as the communication infrastructures depend on the CIA triad. The wide range of cyberattacks against energy systems in general and smart grid in specific can be categorized according to the CIA security triad. This can organize the threats into three categories: Data Availability Attacks, Data Secrecy Attacks, and Data Integrity Attacks. Availability refers to the ability of the smart grid system to function as expected under normal and fault conditions. Integrity in the context of the smart grid refers to the accuracy and reliability of data and control information while Confidentiality involves protecting sensitive data from unauthorized access or disclosure [79], [80].

Suitability of CIA triad as classification Framework for smart grid cybersecurity:

The CIA triad represents important cybersecurity principles that are essential for assessing and fighting against cyberattacks in various critical infrastructures, including smart grids. To demonstrate the suitability of using the CIA triad to classify smart grid cyberattacks, we may go over each component of the triad and how it pertains to smart grid vulnerabilities [55], [48]:

- **Confidentiality/Secrecy**: Maintaining confidentiality makes sure that private data isn't viewed or shared without permission. Confidentiality in a smart grid refers to safeguarding sensitive data, including communication protocols, grid setup details, and customer information (such as usage trends and payment data). Targeted assaults, business espionage, or privacy violations could result from unauthorized access to this data. Operational concerns and privacy violations could result from a cyberattack that undermines the security of smart grid communications by leaking consumer data or intercepting control signals between power plants and SG control centers.
- **Integrity**: Integrity guarantees that data is reliable and correct, i.e., that no unauthorized parties have changed or interfered with it. For a smart grid to function reliably, data integrity must be maintained. To guarantee appropriate decision-making and grid stability, for instance, sensitive data from power meters, grid status reports, and control signals must be preserved. Inaccurate decision-making could lead to blackouts or even system failures if this data is altered, whether intentionally or inadvertently. The infrastructure of the grid could be harmed by a cyberattack that aims to change sensor readings or control commands (for example, by fabricating the grid's load data). This could result in operational failures including overloading transformers or misdirecting power flows.
- **Availability**: Availability guarantees that data and systems are usable and available when required. Availability is essential for sustaining continuous operations in the context of smart grids. Service disruptions, delays, or even total blackouts could result from a denial of service (DoS) attack or other disruptive tactics that target the availability of vital components (such as communication networks, control systems, or power generation facilities). Grid performance and public safety could be seriously impacted by Distributed Denial of Service (DDoS) attack that can overwhelm control centers or communication systems, making it impossible for operators to manage the grid.

The CIA triad classification is considered very suitable for smart grid cybersecurity. First, a thorough framework for assessing cyberattacks on smart grids is offered by the CIA triad. The availability and integrity of the grid's control systems are just as important as maintaining the secrecy of sensitive data because these grids rely on the constant flow of reliable data. Second, the goals of cybersecurity are in line with the CIA triad. Any cybersecurity plan, particularly those for smart grids, must prioritize protecting the CIA attributes. By grouping cyberattacks into different categories, it becomes easier to

comprehend their causes and effects and create effective defenses. Lastly, communication is made easier by the CIA triad classification. The CIA triad is a well-known concept that makes it simpler to debate and rank cybersecurity measures for smart grids by facilitating clearer communication regarding risks, incidents, and defenses. Despite several drawbacks, the CIA triad provides a well-defined, organized, and generally recognized paradigm for categorizing and comprehending cyberattacks on smart grids. By emphasizing availability, secrecy, and integrity, this model offers a simple and practical method for determining and reducing the risks endangering the functionality and safety of contemporary smart grids [24].

A. *Data Availability Attacks:*

DoS and DDoS:

Denial of Service (DoS) attack is one of the most common cyberattacks against smart grids and smart energy systems in general. Attacks of this type work by jamming communication lines and causing delays through targeting routing protocols and electronic maneuvers. Therefore, a DoS attack can restrict authorized users' access to resources and services by oversaturating the communication network bandwidth with traffic. Regarding smart energy systems, DoS has the potential to paralyze communication between smart power electronics in a smart grid and can interfere with communication between the control system and all agents within a system, delaying distributed control framework for microgrids. However, if the source of DoS attack is known and can be found, it is simple to protect the system from a DoS attack by blocking the malicious website [81].

DoS attacks on smart grids SCADA systems keeps on rise in last years. A complex piece of malware called Industroyer, was deployed in the 2015 BlackEnergy attack against Ukraine power grid. The malware was designed to disrupt the operation of Industrial Control System (ICS) used in electrical substations by launching DoS attack and temporarily blocking serial COM lines, causing a large denial of control. This resulted in an energy blackout that affected about 225,000 customers for several hours [82] . Compared to DoS, the Distributed DoS (DDoS) attack is a more severe form of DoS in which numerous hosts simultaneously attack the victim site. By taking advantage of a widespread vulnerability to hack numerous hosts throughout the communication infrastructure, DDoS attackers prepare their breach in advance by recruiting these hosts. Then they flood the victim site with all compromised hosts [83].

Jamming:

Jamming techniques can be used to disrupt the smart grid's availability principle and add noise to the communication channel. For a jamming attack, the attacker simply needs to establish a connection to the communication channel in order to launch the attack. Due to their shared medium, wireless networks in energy systems are vulnerable to jamming-type attacks. When the radio frequency transmissions of two legitimate communicating nodes are interfered by an attacking node, the communication can suffer greatly. Jamming in the physical layer of the grid's communication networks is one sort of DoS attack. In a cyberattack, a jammer sends out noise signals to disrupt data transmission over the communication channel which forces the nodes to increase the power transmission and increase the energy consumption. Therefore, it is crucial to guarantee the robustness against jamming attacks [84].

Flooding:

Attackers bombard a system with a large volume of traffic during a flood attack to prevent it from inspecting and allowing authorized network traffic. Energy depletion and message delays are two efficient effects of flooding attacks. In power grid's electric substations, a lot of communication messages must be transmitted very fast. However, flooding attacks can increase the delay and affect how quickly these messages are delivered. In such scenario, a network attacker (such as a compromised

device) floods the system with false messages to consume the available CPU and network resources. This causes the delivery times of legitimate messages to increase, causing them to miss the delivery time. Therefore, flooding attacks have the potential to seriously harm smart grid applications' availability. Another effect of flooding attacks is energy depletion. The attacker may insert malware into a smart grid network to raise the transmission power and, consequently, the energy consumption of legitimate network devices [85].

DoS and flooding attacks have many factors in common where the flooding attacks sometimes put as one category of DoS. Application layer DoS attacks try to deplete a system's resources, such as memory, CPU, or bandwidth, by flooding them with a large volume of requests. Attacks on the transport layer that target availability try to break up end-to-end connections by draining the sources, which eventually prevents the target device from receiving genuine traffic. flooding Attacks that targets TCP and UDP traffic are two typical examples [86].

Buffer Overflow:

A buffer overflow occurs when a program overruns the buffer's boundary during the writing of data to it and that results in overwriting nearby memory. The existence of a buffer overflow attack cannot be easily detected by passive IDSs. A typical buffer overflow attack cyberattack takes advantage of a vulnerability known as a "buffer overflow" while user-controlled data is written to memory. The attacker can overwrite data in other areas of memory by sending more data than can fit in the allotted memory block. Inputs intended to run code or change how the software behaves can cause buffer overflow attacks. This might lead to a denial-of-service attack that would impair availability and impact data integrity and confidentiality. Attacks such as buffer overflow, jamming, and flooding have the potential to negatively impact the availability of smart grid applications either directly or indirectly [87] [88].

Masquerading:

In a masquerade attack, the attacker impersonates another person or a device ID using a false identity to acquire legitimate but unauthorized access to the victim's personal information. Masquerading attacks also called identity spoofing or impersonation. Attackers may do this to gain access to privileges that could compromise the CIA's parameters and accountability. An attacker may potentially pose as a router, or a DER device in energy system in order to access confidential data or communication details. False trip is an example of masquerading disruptive impact in which a device manipulation, such as PV, can masquerade as a fault. As a result, the attacker may be able to false trip a protective relay and turn off power to numerous consumers [89].

CPU Exhaustion:

In this attack, bogus data overloads the target CPU, which causes wasting of both computation time and power. It can be accomplished by executing heavy mathematical calculations across several threads exhausting CPU cores. Attacks on the CPU make it too busy with needless calculations. These attacks are carried out by hackers who introduce malware and virus code into the victimized systems. This attack falls under the category of Denial of Service (DoS), and the attacker's main goal is to deplete the computational resources of the smart grid and deteriorate the grid's network communication performance. DoS attacks in the application layer target the exhaustion of system resources such as memory, CPU, or bandwidth by flooding them with short bursts of requests or bogus data [35].

B. *Data Secrecy Attacks:*

Attacks against confidentiality aim to obtain data that should be shared or kept secret only between secure parties. Such attacks against smart grid may include: illegally reading memory from devices or smart meters, altering the control program of SMI devices, spoofing payloads, and replay attacks.

Eavesdropping:

Eavesdropping is a type of passive attack in which the attacker taps on the communications between the nodes on a channel. They resemble MitM and impersonation attacks, where a malicious party secretly disrupts lawful peers' communication on a network and steals their important data. The impact of eavesdropping attacks can reach to integrity and accountability of the system as well. In smart grid communication, eavesdropping attacks affect data confidentiality either by intercepting wireless communication in a home area network or sniffing IP packets on the LAN. Eavesdropping intrusion occurs when an unauthorized user gets access to a cyber system and gains unauthorized access to crucial backend servers. There are several countermeasures for eavesdropping attacks: message encryption, access control, anti-virus programs, firewall, VPN, and IDS. Encryption reduces eavesdropping attacks substantially. Many existing authentication schemes and encryption algorithms are adopted in smart grid [90] [91].

Spoofing:

Spoofing is a method used by cybercriminals to pretend as a legitimate or known source. Spoofing can take many different forms, including IP spoofing, email spoofing, DNS spoofing, GPS spoofing, and website spoofing. Additionally, spoofing may also involve software exploitation assaults, message replays, and man-in-the-middle (MITM) attacks [92]. The integrity and confidentiality of an energy smart system can be compromised by spoofing attacks. For the smart grid to operate reliably and efficiently, data accuracy is essential. Data from GPS timestamps, currents, voltages, or frequencies can all be breached. Loss of integrity and availability can result from spoofing attacks such as identity or data spoofing. Such attacks can seriously impair the functioning, stability, security, and reliability of smart grid. Furthermore, GPS location data can be subjected to cyberattacks in a variety of ways. One such method is Global Position System (GPS) spoofing, in which the attacker creates fake GPS signals to provide false location data. Some of the most effective defenses against spoofing attacks are: the use of several devices to monitor the power communication line, cooperation between GPS services, a single data feed, and the synchronization of measurements through NTP (network timing protocol) at various locations in realtime [93] [94].

Replay:

Replay attacks is a well-known communication-based attacks where it can be classified as one type of spoofing or DoS attacks. Replay attacks occur when a hacker connects to a secure network, intercepts data, and then deliberately delays or resends it in an attempt to deceive the target into completing the hacker's requested actions. [95]. In DoS type of replay attack, the attacker intercepts packets sent over the network and resends them to the target nodes which can greatly waste the energy of these nodes under attack. This could cause network fragmentation as a result of exhaustion of nodes' energy. Additionally, the rapid replay of packets has the ability to drain resources in a manner akin to DoS attack. Since the authentication strategy requires a multi-hop approach before reaching the main authentication server, the effect is clear. Each packet is partially processed by the intermediate nodes before being forwarded, which increases end-to-end delays and leads to energy depletion. The primary cryptographic technique used to guarantee secure communication is encryption, which greatly reduces replay and eavesdropping threats. Encryption techniques must be implemented in a smart grid to ensure data integrity and confidentiality [96], [97].

Traffic Analysis:

Traffic analysis cyberattack is an example of passive attacks that do not alter data but it violates their confidentiality principle. Attackers can sniff and examine the messages to gather important details about the nodes' communication patterns. In a smart grid traffic analysis attack, the traffic is monitored and examined to identify the hosts and devices connected to the network, as well as their IP addresses.

An adversary could collect crucial data about the identity, location, and functionality of nodes using network traffic analysis. The traffic patterns of network's wireless sensor devices can provide a wealth of contextual data, including the location of important nodes. Sensing data, for instance, is sent through relatively set pathways that connect source nodes and sinks. This results in pretty clearly discernible traffic patterns that pinpoint the position of sinks. Traffic analysis attacks can be of various types such as those based on monitoring traffic volumes, traffic rates, and traffic patterns [98] [99].

Unauthorized Access:

An abandoned employee password or a weak one can be some of the various vulnerabilities that may enable an attacker to gain unauthorized access privileges and launch cyberattacks on smart grids. Data tampering, information leakage, and denial of service (DoS) attacks are just a few examples of such cyberattacks. Confidentiality protects private information from unauthorized access. A crucial unauthorized access against smart grid systems is the one that can breach to the supervisory SCADA system in a generation unit or transformer station, and hence taking control of the unit basic functions. Some examples of cyberattacks based on unauthorized access are Ukrainian power grid blackout and U.S. Colonial oil pipeline shutdown occurred in 2015 and 2021 respectively [39] [77].

Password Pilfering:

Password pilfering attacks refers to any means or technique that leads an attacker to get a user or employee legitimate password, and that consequently leads to a violation of confidentiality. Some examples of popular techniques to pilfer a user password is through social engineering. There are other various methods to hack a password including guessing, social engineering, dictionary attacks, and password sniffing, brute force, phishing, using malware and keyloggers [40].

Man in the Middle (MITM):

The goal of MITM attacks is to intercept and change communications between field devices and the control center. This allows attacker to pass false data into the victim device or system. During the protocol session, the attacker seems to be the intended destination for both the source and the target. The three CIA parameters are all impacted by MITM attacks, which can be conducted in various layers, particularly the Transport and MAC layers. Comprehensive packet analysis software should be a part of cyber security systems, and strong authentication procedures can thwart MITM breaches [100].
In smart grid systems the primary goal of authentication is to stop harmful, unauthorized components, like fraudulent smart meters, from imitating real components and launching MITM attacks that can grant specific access to the smart grid. Getting access to smart grid components' data during exchange can causes various vulnerabilities, such as corrupting or dropping data packets, decreasing or stopping the performance of the smart grid network, or starting additional attacks against the system, such as DoS and flooding attacks. MITM can be of various types such as ARP (Address Resolution Protocol) spoofing based man-in-the-middle attack which can be used to breach a smart grid SCADA control system [9].

Sniffing:

With this attack, data on communications between a sender and a receiver can be unlawfully intercepted. Examples of sniffing attacks may include packet sniffing and password sniffing. Sniffing is a network based attack which, due to it spy based nature, can be used as a preparatory step for other more aggressive attacks such as FDIA. In smart grid, sniffing AMI (Advance Metering Infrastructure) networks allows attackers to tap on the communication line or protocol to read smart meter important data illegally. The main targets of sniffer attacks include PMU (phasor measurement unit), TCP/IP packets, and smart meters. Without efficient protection such as encryption, sniffing can collect crucial information about the victim smart energy system. To reduce secret key/password theft possibility, it is advisable to replace them frequently while using stronger credentials [90] [101].

Social Engineering:

A social engineering cyberattack is one that penetrates a system by employing social techniques, such as psychological tricks, and usually without using technological skills. Confidential data, such a password or login PIN, is typically compromised in this kind of attack. Social engineering depends more on interpersonal communication and social skills than it does on technical expertise. The attacker employs communication and persuasion in this phase to gain the trust of an authorized user. In order to log on to a specific system, this attack is accomplished to obtain the user's credentials and private information, such as passwords or PIN numbers. Phishing and password pilfering are two popular approaches employed in social engineering [98].

Regardless of the strength of smart grid firewalls, cryptographic techniques, intrusion detection systems, and antivirus software systems, social engineering poses a threat to the security of its networks. Compared to computers or other technologies, people are more likely to trust other people which makes them the weakest link in the security chain. Malicious actions carried out through interpersonal interactions might psychologically persuade a person to reveal sensitive information or violate security protocols. Social engineering attacks are the most effective attacks since they harm all systems and networks as a result of these human interactions [102].

C. ***Data Integrity Attacks:***

The main cryptographic method for guaranteeing safe communication is encryption. Encryption techniques must be put in place for the smart grid to preserve data integrity and confidentiality.

FDIA:

One of the most common and widespread attacks on energy smart systems and smart grids is false data injection attack (FDIA). Usually, this kind of attack modifies the data without changing the system's code. FDIA may have wide range of types: physical-based FDIA, communication-based FDIA, cyber-based FDIA, and network-based FDIA. GPS spoofing is a type of FDIA in which the adversary imitates the GPS signal and inserts false data into it before sending it to the system [46].

In the context of smart grid technology, an FDIA attack is one in which an adversary manipulates sensor readings to introduce undiscovered errors into calculations of state variables and values. As a result, the attacker has the ability to tamper with state estimate procedures and trick the network administrator. Depending on the goal of the intrusion, the FDIA can result in a number of different consequences, such as energy theft, injecting errors in LMP (locational marginal pricing) for illicit market profits, and physical damage to the network [36]. By complicating the state estimate process and accidentally involving the contingency analysis procedures, FDIA can have severe effect on the LMP. FDIA is carried on by the insertion of auxiliary signals or by altering the data included in the measurements that the smart grid sensors report [103].

Tampering, SM Tampering

Malicious tampering and alteration of vital data in sensors, meters, and command centres might be extremely dangerous to smart grids and energy infrastructures. Tampering refers to an illegal change or obliteration of information or a procedure. This attack may fall under data injection attacks, in which attackers take advantage of flaws in devices and communication lines to be able to manipulate them and alter their data. It is possible to intentionally alter the data measured by SCADA field units, such as PMU and RTU devices, to produce incorrect control signals and irregular grid schedules [57].

Tampering of smart meter can occur when the utility meters' readings are altered and inaccurate. One instance of this is when the readings from the meters do not accurately reflect the consumption. An example of tampering attack against smart meters can be based on ping flood attack. In this type of attack, the smart meter is continuously pinged with traffic, and when the smart meter replies, the traffic

on the smart meter is overloaded. As a result of this, low power consumption data is read, and that causes utility income loss. Smart grids and energy systems can be damaged by intercepting or altering the data; hence all system data must be properly secured against alteration. To ensure security and confidentiality, proper mechanisms should be used to protect against tampering [104].

Time Synchronization:

Precise timing information is necessary for many smart grid functions, including fault detection and event location estimation. Due to that, a Time Synchronization Attack (TSA) can be launched to target the smart grid's timing data. It is highly possible to attack the measurement system by faking the GPS (Global positioning system) because many smart grid applications use synchronous measurements and the majority of measurement equipment include GPS for exact timing [105].
In addition, TSA may target the Wide area measurement systems (WAMSs) in smart grid. The monitoring equipment is dispersed throughout the entire power grid network, where the control centre receives their measurements data with different transmission delays. The control centre must time-synchronise all acquired measurements in order to obtain an accurate picture of the state of the system operation. GPS-based time-synchronisation monitoring devices have been widely used in smart grid monitoring systems because the GPS signal is highly accurate and reliable for timing without the need for additional communication infrastructure [106].

Wormhole:

Mobile ad-hoc networks are becoming more and more common and significant in the smart grid. However, due to their limited capabilities, functionality needs, and deployment scenarios, they are exposed to a variety of attacks, including wormhole attacks. In this attack, two or more malicious nodes are used, and data packets are tunneled from one end of one malicious node to the other malicious node before being broadcast. Wormhole attacks can have an impact on the smart grid's availability as well as its integrity principles [43].

Covert Attack:

The covert attack, when an attacker modifies the system inputs and influences secretly the system outputs, is one of the most complex attacks on grid systems. In covert attacks, the details regarding the operational and informational architecture, such as the protocol, system model, and device details are exploited. In order to seize control of the victim systems, the attacker needs to injects its malicious codes. A covert attack is sometimes referred to as a closed-loop replay attack. The GLRT (Generalized Likelihood Ratio Test) can distinguish between infected and healthy operational technology (OT) devices which qualify it to be used as a protection mechanism against covert attacks [107].

LoadDrop Attacks

A loaddrop is a cyberattack against metering infrastructure (AMI) of smart grid. It is a scenario in which an adversary gains access to the control functions of a trusted utility system (such as AMI) within the smart grid in order to issue a series of service disconnect commands to each consumer smart meter. This type of attack has the potential to cause a load loss in the corresponding power network. The failure consequences of a loaddrop attack can be deduced from the relevant regulatory standards for the stability and reliability of the power system. There are various failure effects for this attack such as system shutdown, power quality violation, anomalous operation, and normal operations effect. Studying the intersystem interactions between a metering network and the power system during a loaddrop attack is necessary to reduce the impact of the attack [108, 109].

D. *Cyberattacks According to Vulnerable Network Layer*

This section presents the taxonomy of smart grid cyberattacks with focus given to the targeted network layer: application, transport, MAC, and physical. The security procedures developed through the

analysis of cybersecurity requirements according to network layers will provide effective security solutions for smart grid applications. Understanding what attacks targets what network layer can help us find the suitable mitigation and solution for the attack. These mitigations can range from encryption (lightweight and heavyweight), anti-jamming, congestion control, authentication, IDS, behavior analysis, anti-DoS, and packet filtering. Table 3 shows what are the specific network layers each cyberattack targets in general. However, it is common to see some attacks to be active and efficient in more than one layer. The table also shows the attack taxonomy according to the CIA triad.

Table 3: Cyberattacks against smart grid with compromised CIA parameter and vulnerable grid network layer

No.	Attack Types/category	Compromised CIA Parameter	Vulnerable Network Layer	Ref.
1	Denial of Service (DoS)	Availability	Transport, MAC	[83] [81] [82]
2	Jamming	Availability	MAC, Physical	[84] [110]
3	Spoofing	Availability, Integrity, Confidentiality	Transport, MAC	[93] [94]
4	Flooding, Buffer Flooding, HTTP Flooding	Availability	Application, Transport, MAC	[85] [86]
5	Lowrate DoS (LDoS),	Availability	Application	[81]
6	Buffer Overflow	Availability	Application, Transport	[87] [88]
7	Masquerading	Confidentiality, Integrity, Availability	MAC	[35]
8	Distributed Denial of Service (DDoS)	Availability	Transport, MAC	[111]
9	CPU Exhausting	Availability	Application	[35]
10	Eavesdropping	Confidentiality	Physical	[90] [91]
11	Traffic Analysis	Confidentiality	MAC	[98] [99]
12	Unauthorized Access	Confidentiality	Application	[39] [77]
13	Password Pilfering	Confidentiality	Transport	[40]
14	Man in the Middle (MitM)	Confidentiality, Integrity, Availability	Transport, MAC	[100] [112]
15	Sniffing	Confidentiality	Transport	[90] [101]
16	Replay	Confidentiality, Integrity	Transport	[96] [97]
17	Social Engineering	Confidentiality	Transport	[102]
18	Data Injection Attacks, FDIA	Confidentiality, Integrity	Application, Transport	[46] [103]
19	Tampering/ Smart Meter Tampering	Integrity	Physical	[57] [104]
20	Wormhole	Availability, Integrity	Transport	[43] [113]
21	Time Synchronization (TSA)	Integrity, Availability	MAC, Physical	[106] [105]
22	LoadDrop Attacks	Integrity	Application, Transport	[108, 109]
23	Covert	Integrity	Transport	[107]

VI. Future Directions

As IoT-based smart grids and smart energy systems are getting more complex (with ICTs as the backbone), so do the security issues of these systems when they get more exposed to cyber space and Internet. As smart grid initiatives grow, it is important to highlight that there are numerous research areas that need be studied in order to help improving smart grid security. It is important to note that the integration of various technologies to smart energy systems has led to cybersecurity issues which opened a spectrum of research areas. Each of these technologies has joined energy systems bringing its benefits as well as its cyberthreats. Allowing customers to be involved actively in smart energy systems through buying and selling electricity as well as other activities, has also led to cybersecurity issues which need to be studied. Due to all these reasons, proper future directions need to be investigated to tailor specific solutions for smart grids systems.

Blockchain, artificial intelligence (AI), and digital twins are example of future directions that can play a critical role in enhancing the security of smart grids against cyberattacks while addressing the core principles of the CIA triad—Confidentiality, Integrity, and Availability. With blockchain, data integrity is preserved, ensuring that unauthorized changes can be detected and reverted. AI can identify unusual patterns (e.g., sudden control system changes) and trigger defenses, while digital twins can simulate the grid's response, enabling recovery and continuity during the attack. Follows are detailed discussions on the main future directions that are of great importance which need to be researched and investigated to ensure smart grid high protection against cyber threats:

- **Blockchain:** In a smart grid environment, a plenty of problems emerge that are related to the security of the distributed data in various sections of smart grid. Data management of a centralized server-based storage system can cut the cost but sacrifice with the security and privacy of protecting the ledger (system data) [114]. This can be mitigated by the use of blockchain distributed ledger technology, where data can travel from one node to the other in a secure way. Integrity, transparency, provenance, and trustworthiness can be achieved by blockchain hyperledger-enabled modular infrastructure through continuously simulating distributed node transactions and including energy-related data management logs. Additionally, blockchain technology is also useful for authentication issues, while the development of blockchain platform for smart grid and microgrid can be of significant contribution in commercialization. In general, smart grids can benefit from the use of blockchain and distributed ledger technologies for secure and transparent data management. These technologies can be used for data integrity verification, secure transaction recording, and identity management within the smart grid system [115].

  Blockchain is a powerful technology that can greatly improve smart grids' resistance to cyberattacks. By offering decentralized, unchangeable ledgers for data transactions, blockchain can safeguard smart grids. This ensures the integrity of control systems by making it harder for attackers to change or modify grid data. From a perspective of authentication and access control, blockchain makes it possible for safe, transparent authentication procedures, which guarantee that only authorized individuals and devices may access grid systems, lowering the possibility of unauthorized access. Blockchain's distributed ledgers minimize the possibility of a single point of failure. The grid keeps working even if one node is compromised or attacked since other nodes keep operating [116], [117].

- **Artificial Intelligence-enabled Machine Learning:** AI-enabled machine learning (ML) approaches, such as supervised, semi-supervised, and unsupervised learning, can be used to analyze the lack of efficiency and reliability in smart grids. By enabling ML developments and tailoring operational executions and reactions to the needs, it will be possible to broaden the scope of dynamic monitoring and controlling of smart grid technologies. Furthermore, the combination of artificial intelligence and power distribution technology establishes an entirely novel approach for the development of real-time generation, control, distribution, and monitoring of electric power supplies. Machine learning can also be efficient in smart grid automated vulnerability assessment, gathering threat intelligence, and predicting threat and risk. In addition, machine learning and artificial intelligence can be used in real-

time to detect and mitigate security issues. Integrating AI-powered security solutions with cryptographic approaches may become a smart grid security trend [107].

AI is a potent instrument that can greatly improve smart grid security against cyberattacks. Artificial intelligence (AI) can monitor and analyze enormous volumes of grid data in real-time in anomaly detection, spotting odd patterns that can point to possible vulnerabilities or cyberattacks. By detecting new threats and vulnerabilities, machine learning algorithms may anticipate and proactively reduce cyber risks from the standpoint of predictive threat modeling, enabling quicker incident reaction times. Intrusion detection systems with AI capabilities are able to continuously scan the grid for suspicious activity. For example, AI systems can promptly identify and notify security teams if an intruder modifies power flow data in an attempt to interfere with operations. AI can also provide quick response to cyber disasters, guaranteeing that even if a cyberattack, such as a DDoS attack, systems can adjust in real time, rerouting or isolating impacted areas of the grid [54].

- **Cryptographic Algorithms and Protocols**: The fundamental cryptographic approach for ensuring safe communication in smart energy systems is encryption. Although encryption is not the only remedy, it plays a significant role in improving smart grid security. To guarantee data integrity and secrecy in these systems, encryption algorithms must be implemented. Encryption significantly decreases replay, FDIA, and eavesdropping attacks. Public key cryptography is an important tool for identifying cyberattacks in smart power systems, particularly FDIA. In smart grid, many existing authentication techniques and encryption algorithms are used. Symmetric cryptography, such as symmetric cyphers AES and DES, as well as asymmetric cryptography, are commonly employed to prevent cyber-threats in smart grids. Furthermore, most smart grid electronic gadgets are supposed to feature lightweight cryptographic capabilities in future. Cryptographic techniques are frequently used in Wireless Sensor Network (WSN). Such cryptography approaches, however, are becoming more applicable than ever with the integration of smart metering devices and smart inverters with ICT elements. Another major problem in smart grids is privacy, as precise energy consumption data can reveal sensitive information. Future encryption approaches may prioritize consumer privacy while allowing utilities to collect necessary data for grid management [26], [95], [118].

  Furthermore, the security of many existing cryptography techniques is jeopardized by the advent of quantum computing. To maintain the long-term security of grid communications, future directions in smart grid cryptography may include the use of quantum-resistant cryptographic algorithms. While the National Institute of Standards and Technology (NIST) works on standardizing post-quantum cryptography methods, the smart grid industry will need to follow by adopting these new protocols and standards to protect against quantum attacks. Cryptographic protocols provide promising solutions for vulnerabilities in the communication protocols of the smart grid. It is critical to provide cryptographic standards and protocols that enable interoperability among smart grid components and systems. The standardization initiatives in this area will most likely continue to evolve [48], [28].
- **Investigating new cyber threats:** Potential cybersecurity flaws can show the need for research to strengthen the cybersecurity of a smart grid, which can help preventing unidentified cyberattacks. Because there are no mitigation strategies in place, jamming attacks pose a hazard to wireless communication by weakening the connectivity of smart grid components. The time-based synchronization needed for PMU data may be impacted by spoofing attacks on GPS signals. Another thing that needs to be looked into is evolving security tactics for zero-day attacks. It is absolutely necessary to conduct further research on coordinated cyberattacks. Additionally, it's important to assess the cybersecurity concerns brought on by the inclusion of DERs into the smart grid [3], [16].
- **Standards and Protocols:** Because the IoT-based smart grids are relatively new systems, they suffer the lack of tight standards and protocols which are needed to be more security oriented. As an example, the necessary standards to evaluate the IDSs/IPSs of these systems are not available. The absence of regulatory standards for sustainable energy management and dispatching is caused by a number of smart grid domains and sub-systems, including power distribution and related automation. From generation to customer, the distributed network's current lifetime for the process layer is ineffective and unstable. Frameworks for international standardization must be developed for secure

communication in smart grid applications. Additionally, new protocols need to be developed while the existing ones need to be updated to suit the current requirements of smart grid applications [48], [116]. To quantify the quality of a smart grid, several key metrics need to be considered, as smart grids are complex systems that integrate information technology, communications, and automation with traditional electrical grids. These metrics can be categorized into different aspects like reliability, efficiency, sustainability, security, and resilience. Reliability is one of the most important aspects of a smart grid since it ensures the grid can meet demand consistently without interruptions. Additionally, Smart grids aim to improve both operational and energy efficiency through real-time data, automation, and demand-side management [119] [120]. Given the increased reliance on digital systems and IoT devices, smart grid security is paramount. That includes the ability to track and lower the number of cybersecurity incidents, measures how well the grid can continue to operate or recover after a cyberattack, ensures that the communication infrastructure that supports smart grid operations remains secure and operational. Resilience metric also play a significant role in understanding the complex interplay between the behaviours and operational characteristics of interdependent critical infrastructures such as smart grids [121].

- **Digital Twin (DT):** With the expansion of contemporary cities, several energy layers—such as microgrids, smart grids, and transportation systems—have appeared, presenting a variety of difficulties for the multidimensional energy management system. As an example, traffic is a major problem in transportation systems that requires real-time planning, monitoring, and management. Remote data transfer within the electric grid and various analyses requiring real-time data are only a few of the current issues in this sector. These issues can be solved by presenting and analyzing a genuine digital twin DT framework in each area. As a result, it is vital to consider numerous applications of DT in the development of various areas of energy management, such as smart grids, transportation systems, and microgrids [122], [53]. Digital twins have the potential to significantly improve smart grid security against cyberattacks while also addressing the CIA triad. Digital twins generate real-time virtual replicas of the smart grid, allowing for continuous monitoring of the system's operation and security. In the event of an attack, digital twins can enable operators to simulate reactions and assess consequences before acting on the actual grid. Operators can use digital twins to test cyberattack scenarios in a secure, virtual environment, assessing the grid's resilience and developing effective remedies. During an attack, digital twins can provide backup simulations, allowing for operational awareness even if parts of the smart grid are affected, reducing grid downtime and ensuring system availability [123].

VII. Concluding Remarks

Internet connectivity used to be pretty remote from traditional grids which is no longer the case for the current IoT-based smart grids. The huge integration of ICT technologies and components into the smart grids has exposed them into a number of vulnerabilities that can breach grid security. In recent years, a plethora of cyberattacks have affected the energy sector, which could have been avoided if proper security measures were developed. These emerging threats require urgent attention and in-depth studies by the academia. This can be accomplished by researching fresh vulnerabilities and developing suitable solutions for the grid's cyber and physical layers. It is very important to notice that almost all parts of IT technology used in smart grid applications have potential weaknesses due to security threats associated with the traditional IT history. Also, due to the features of smart grid applications, unique solutions must be developed for their individual needs. As an example, solutions need to avoid any possibility of restart/shutdown of grid system which causes blackout to huge areas and leaves millions of people without electricity.

In order to protect against cyberattacks and vulnerabilities, research is being done on cybersecurity challenges in smart grid applications. In this work, a comprehensive overview of cybersecurity threats and detailed classification of cyberattacks against smart grid applications is provided. Researchers may learn more about the goals, needs, and upcoming research trends for smart grid cybersecurity in the study. We also provided a brief overview of cybersecurity concerns for smart grid applications, as well as introducing the historical incidents against smart grid. Additionally, we evaluated recent studies on

it from the perspective of security, and discussed its advantages, features, and key components. Then, we examined future possibilities in smart grid security which shed a light on open research directions in the field. The survey paper makes significant contributions by presenting a wide range of cyberthreats that affect IoT-based smart grid applications; and by suggesting potential research opportunities that could help researchers shape future research directions. This review can also enlighten researchers about the smart grid cybersecurity goals and requirements. To give comprehensive and complete details, the recent studies on the smart grid have been covered from a security angle. This paper offers a comprehensive overview of the state-of-the-art smart grid cybersecurity research while giving detailed classification/organization of the cyberattacks emerging in recent years. Attack categorization can aid in the provision of organized and effective solutions for current and potential attacks in smart grid applications.

Author Contributions: Conceptualization, Mohammad Alomari, Gamal Alkawsi and AbdulGuddoos Gaid; Methodology, Reema Thabit and AbdulGuddoos Gaid; Resources, Mohammed Al-Andoli, Mukhtar Ghaleb and Reema Thabit; Supervision, Jamil Abedalrahim Jamil Alsayaydeh and AbdulGuddoos Gaid; Writing – original draft, Mohammad Alomari, Mohammed Al-Andoli and Mukhtar Ghaleb; Writing – review & editing, Mohammad Alomari, Mohammed Al-Andoli, Gamal Alkawsi and Jamil Abedalrahim Jamil Alsayaydeh. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: The authors express their gratitude to the Research Management Center (RMC), Multimedia University, and the Centre for Research and Innovation Management (CRIM), Universiti Teknikal Malaysia Melaka (UTeM) for their valuable support in this research.
The authors also are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for supporting this work through the Fast-Track Research Support Program.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES:

[1] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf, and D. Kundur, "A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids," *IEEE Access*, 2024.
[2] Y. Jiang, S. Yin, and O. Kaynak, "Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond," *IEEE Access*, vol. 6, pp. 47374-47384, 2018.
[3] N. D. Tuyen, N. S. Quan, V. B. Linh, T. V. Vu, and G. Fujita, "A Comprehensive Review of Cybersecurity in Inverter-based Smart Power System amid the Boom of Renewable Energy," *IEEE Access*, 2022.
[4] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 446-464, 2016.
[5] M. Ravinder and V. Kulkarni, "A Review on Cyber Security and Anomaly Detection Perspectives of Smart Grid," in *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2023, pp. 692-697: IEEE.
[6] H. Harkat, L. M. Camarinha-Matos, J. Goes, and H. F. Ahmed, "Cyber-physical systems security: A systematic review," *Computers Industrial Engineering* p. 109891, 2024.
[7] M. K. Hasan, R. A. Abdulkadir, S. Islam, T. R. Gadekallu, and N. Safie, "A review on machine learning techniques for secured cyber-physical systems in smart grid networks," *Energy Reports*, vol. 11, pp. 1268-1290, 2024.
[8] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5244-5257, 2021.
[9] T. S. Ustun and S. S. Hussain, "A review of cybersecurity issues in smartgrid communication networks," in *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*, 2019, pp. 1-6: IEEE.
[10] M. Z. Gunduz and R. Das, "A comparison of cyber-security oriented testbeds for IoT-based smart grids," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, pp. 1-6: IEEE.
[11] K. Aygul, M. Mohammadpourfard, M. Kesici, F. Kucuktezcan, and I. Genc, "Benchmark of machine learning algorithms on transient stability prediction in renewable rich power grids under cyber-attacks," *Internet of Things*, vol. 25, p. 101012, 2024.
[12] S. Abdelkader *et al.*, "Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks," *Results in Engineering*, p. 102647, 2024.

[13] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, no. 5, p. 1380, 2021.
[14] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "An anomaly-based intrusion detection system for the smart grid based on cart decision tree," in *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, 2018, pp. 1-5: IEEE.
[15] M. Yesilbudak and I. Colak, "Main Barriers and solution proposals for communication networks and information security in smart grids," in *2018 International Conference on Smart Grid (icSmartGrid)*, 2018, pp. 58-63: IEEE.
[16] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023.
[17] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors Journal*, vol. 21, no. 18, p. 6225, 2021.
[18] F. Jameel, "Network security challenges in smart grid," in *2016 19th International Multi-Topic Conference (INMIC)*, 2016, pp. 1-7: IEEE.
[19] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46595-46620, 2019.
[20] N. Jamil, Q. S. Qassim, F. A. Bohani, M. Mansor, and V. K. Ramachandaramurthy, "Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research," *Applied Sciences*, vol. 11, no. 21, p. 9812, 2021.
[21] N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities," *Journal of Information Security*, vol. 43, no. 1, pp. 21-33, 2019.
[22] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, and D. Wollman, *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology, 2021.
[23] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," *SoutheastCon*, pp. 1-6, 2015.
[24] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 2018, pp. 1-5: IEEE.
[25] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100433, 2021.
[26] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges," *IEEE Access*, vol. 7, pp. 135812-135831, 2019.
[27] G. S. OV, A. Karthikeyan, K. Karthikeyan, P. Sanjeevikumar, S. K. Thomas, and A. Babu, "Critical review Of SCADA And PLC in smart buildings and energy sector," *Energy Reports*, vol. 12, pp. 1518-1530, 2024.
[28] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1942-1976, 2020.
[29] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, "Smart grid security: Threats, challenges, and solutions," *arXiv preprint arXiv:.06992*, 2016.
[30] M. S. Al-kahtani and L. Karim, "A survey on attacks and defense mechanisms in smart grids," *International Journal of Computer Engineering Information Technology*, vol. 11, no. 5, pp. 94-100, 2019.
[31] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Transactions on smart grid*, vol. 7, no. 2, pp. 807-816, 2015.
[32] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Transactions on Information Forensics Security*, vol. 13, no. 1, pp. 129-142, 2017.
[33] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2886-2927, 2019.
[34] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2831-2848, 2019.
[35] C.-C. Sun, D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 612-622, 2020.
[36] E. U. Haq, C. Pei, R. Zhang, H. Jianjun, and F. Ahmad, "Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach," *Energy Reports*, vol. 9, pp. 634-643, 2023.
[37] W. Luan, J. Peng, M. Maras, J. Lo, and B. Harapnuk, "Smart meter data analytics for distribution network connectivity verification," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1964-1971, 2015.
[38] C. Cuijpers and B.-J. Koops, "Smart metering and privacy in Europe: Lessons from the Dutch case," *European data protection: Coming of age*, pp. 269-293, 2013.
[39] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933-1954, 2014.
[40] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of cyber-security issues on smart grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, pp. 1-7: IEEE.
[41] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications surveys tutorials*, vol. 14, no. 4, pp. 981-997, 2012.

[42] C. Lopez, A. Sargolzaei, H. Santana, and C. Huerta, "Smart grid cyber security: An overview of threats and countermeasures," *Journal of Energy Power Engineering*, vol. 9, no. 7, pp. 632-647, 2015.
[43] A. Procopiou and N. Komninos, "Current and future threats framework in smart grid domain," in *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2015, pp. 1852-1857: IEEE.
[44] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE communications surveys tutorials*, vol. 14, no. 4, pp. 998-1010, 2012.
[45] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.
[46] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218-2234, 2020.
[47] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing impacts of cyber attacks on power grids vulnerability to cascading failures," *IEEE Transactions on Circuits Systems II: Express Briefs*, vol. 66, no. 6, pp. 1058-1062, 2018.
[48] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network Computer Applications*, vol. 209, p. 103540, 2023.
[49] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids–A comprehensive survey," *Computer Standards & Interfaces*, vol. 56, pp. 62-73, 2018.
[50] A. Akkad, G. Wills, and A. Rezazadeh, "An information security model for an IoT-enabled Smart Grid in the Saudi energy sector," *Computers Electrical Engineering*, vol. 105, p. 108491, 2023.
[51] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, "Smart grid cyber-physical situational awareness of complex operational technology attacks: A review," *ACM Computing Surveys*, vol. 55, no. 10, pp. 1-36, 2023.
[52] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE Journal of Emerging Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326-5340, 2019.
[53] M. Jafari, A. Kavousi-Fard, T. Chen, and M. Karimi, "A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future," *IEEE Access*, 2023.
[54] A. A. Khan, A. A. Laghari, M. Rashid, H. Li, A. R. Javed, and T. R. Gadekallu, "Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review," *Sustainable Energy Technologies Assessments*, vol. 57, p. 103282, 2023.
[55] K. Demertzis, L. S. Iliadis, and V.-D. Anezakis, "An innovative soft computing system for smart energy grids cybersecurity," *Advances in Building Energy Research*, vol. 12, no. 1, pp. 3-24, 2018.
[56] A. Vernotte, M. Välja, M. Korman, G. Björkman, M. Ekstedt, and R. Lagerström, "Load balancing of renewable energy: a cyber security analysis," *Energy Informatics*, vol. 1, no. 1, pp. 1-41, 2018.
[57] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434-214453, 2020.
[58] S. Y. Diaba and M. Elmusrati, "Proposed algorithm for smart grid DDoS detection based on deep learning," *Neural Networks*, vol. 159, pp. 175-184, 2022.
[59] T. V. Vu, B. L. Nguyen, Z. Cheng, M.-Y. Chow, and B. Zhang, "Cyber-physical microgrids: Toward future resilient communities," *IEEE Industrial Electronics Magazine*, vol. 14, no. 3, pp. 4-17, 2020.
[60] C.-T. Lin, S.-L. Wu, and M.-L. Lee, "Cyber attack and defense on industry control systems," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017, pp. 524-526: IEEE.
[61] S. P. Global". (2022). *Energy Security Sentinel: An interactive study of geopolitical risk and energy prices*. Available: https://www.spglobal.com/commodityinsights/PlattsContent/_assets/_files/en/specialreports/oil/oil-security-sentinel.html
[62] T. C. Reed, *At the abyss: an insider's history of the Cold War*. Presidio Press, 2005.
[63] N. E. Oueslati, H. Mrabet, A. Jemai, and A. Alhomoud, "Comparative study of the common cyber-physical attacks in industry 4.0," in *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, 2019, pp. 1-7: IEEE.
[64] T. L. Hardy, "Software and System Safety: Accidents," *Incidents, Lessons Learned, AuthorHouse*, 2012.
[65] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Computer Communications*, vol. 155, pp. 1-8, 2020.
[66] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641-29659, 2021.
[67] M. Krzykowski, "Legal Aspects of Cybersecurity in the Energy Sector—Current State and Latest Proposals of Legislative Changes by the EU," *Energies*, vol. 14, no. 23, p. 7836, 2021.
[68] K. E. Hemsley and E. Fisher, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States)2018.
[69] C. Bronk and E. Tikk-Ringas, "The cyber attack on Saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81-96, 2013.
[70] S. K. Venkatachary, J. Prasad, and R. Samikannu, "Cybersecurity and cyber terrorism-in energy sector–a review," *Journal of Cyber Security Technology*, vol. 2, no. 3-4, pp. 111-130, 2018.
[71] N. Kshetri, "Cybersecurity in gulf cooperation council economies," in *The Quest to Cyber Superiority*: Springer, 2016, pp. 183-194.
[72] A. Henni, "Middle East Attacks Raise Cyber Security Questions," *Journal of petroleum technology*, vol. 64, no. 10, pp. 68-69, 2012.

[73] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing Analysis Center*, vol. 388, pp. 1-29, 2016.
[74] *Norsk Hydro*, https://www.hydro.com/en/media/on-the-agenda/cyber-attack/
[75] " Cybersecurity, Energy Security, and Emergency Response, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident, Accessed Jan 2024."
[76] "Hackers Breached Colonial Pipeline Using Compromised Password, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [Accessed 13 Oct 2023]."
[77] R. L. Grubbs, J. T. Stoddard, S. G. Freeman, and R. E. Fisher, "Evolution and Trends of Industrial Control System Cyber Incidents since 2017," *Journal of Critical Infrastructure Policy*, vol. 2, no. INL/JOU-21-65119-Rev000, 2021.
[78] J. Voas, N. Kshetri, and J. F. DeFranco, "Scarcity and global insecurity: the semiconductor shortage," *IT Professional*, vol. 23, no. 5, pp. 78-82, 2021.
[79] R. K. Jha, "Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability," *Recent Research Reviews Journal*, vol. 2, no. 2, pp. 215-241, 2023.
[80] T. Mazhar *et al.*, "Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods," *Future Internet*, vol. 15, no. 2, p. 83, 2023.
[81] A. Y. Nur and M. E. Tozal, "Defending cyber-physical systems against dos attacks," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2016, pp. 1-3: IEEE.
[82] A. Cherepanov, "WIN32/INDUSTROYER: A new threat for industrial control systems," *White paper, ESET*, 2017.
[83] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3616-3626, 2019.
[84] E. Bout, V. Loscri, and A. Gallais, "Energy and Distance evaluation for Jamming Attacks in wireless networks," in *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, 2020, pp. 1-5: IEEE.
[85] Q. Li, C. Ross, J. Yang, J. Di, J. C. Balda, and H. A. Mantooth, "The effects of flooding attacks on time-critical communications in the smart grid," in *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015, pp. 1-5: IEEE.
[86] F. Zhang, M. Mahler, and Q. Li, "Flooding attacks against secure time-critical communications in the power grid," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2017, pp. 449-454: IEEE.
[87] H. Ying *et al.*, "Detecting buffer-overflow vulnerabilities in smart grid devices via automatic static analysis," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2019, pp. 813-817: IEEE.
[88] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM based DoS attacks using data mining in smart grid," *Energies*, vol. 5, no. 10, pp. 4091-4109, 2012.
[89] Z. Xiang, H. Guangyu, and W. Zhigong, "Masquerade detection using support vector machines in the smart grid," in *2014 Seventh International Joint Conference on Computational Sciences and Optimization*, 2014, pp. 30-34: IEEE.
[90] Z. A. Baig and A.-R. J. J. C. Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures," *J. Commun.*, vol. 8, no. 8, pp. 473-479, 2013.
[91] C. Valli *et al.*, "Eavesdropping on the smart grid," 2012.
[92] Y. Cui, F. Bai, Y. Liu, P. L. Fuhr, and M. E. Morales-Rodriguez, "Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5807-5818, 2019.
[93] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344-1371, 2013.
[94] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 847-870, 2018.
[95] M. Qasaimeh, R. Turab, and R. Al-Qassas, "Authentication techniques in smart grid: a systematic review," *TELKOMNIKA*, vol. 17, no. 3, pp. 1584-1594, 2019.
[96] A. Ghosal, A. Saha, and S. Das Bit, "Energy Saving Replay Attack Prevention in Clustered Wireless Sensor Networks," in *Pacific-Asia Workshop on Intelligence and Security Informatics*, 2013, pp. 82-96: Springer.
[97] B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, "Replay attack impact on advanced metering infrastructure (AMI)," in *Smart Grid Inspired Future Technologies*: Springer, 2017, pp. 52-59.
[98] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers Electrical Engineering*, vol. 67, pp. 469-482, 2018.
[99] B. Di Ying, D. Makrakis, and H. T. Mouftah, "Anti-traffic analysis attack for location privacy in WSNs," *EURASIP Journal on Wireless Communications Networking*, vol. 2014, no. 1, pp. 1-15, 2014.
[100] J. J. Fritz, J. Sagisi, J. James, A. S. Leger, K. King, and K. J. Duncan, "Simulation of man in the middle attack on smart grid testbed," in *2019 SoutheastCon*, 2019, pp. 1-6: IEEE.
[101] B. Roberts, K. Akkaya, E. Bulut, and M. Kisacikoglu, "An authentication framework for electric vehicle-to-electric vehicle charging applications," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2017, pp. 565-569: IEEE.
[102] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019.
[103] K. Jhala, P. Pradhan, and B. Natarajan, "Perturbation-based diagnosis of false data injection attack using distributed energy resources," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1589-1601, 2020.

[104] S. Kumar, H. Kumar, and G. R. Gunnam, "Security integrity of data collection from smart electric meter under a cyber attack," in *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, 2019, pp. 9-13: IEEE.
[105] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87-98, 2013.
[106] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1952-1973, 2016.
[107] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Transactions on Information Forensics Security*, vol. 14, no. 10, pp. 2765-2777, 2019.
[108] E. B. Rice and A. AlMajali, "Mitigating the risk of cyber attack on smart grid systems," *Procedia Computer Science*, vol. 28, pp. 575-582, 2014.
[109] A. AlMajali, E. Rice, A. Viswanathan, K. Tan, and C. Neuman, "A systems approach to analysing cyber-physical threats in the Smart Grid," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2013, pp. 456-461: IEEE.
[110] S. Savadatti, S. Kuldeep Dhariwal, S. Krishnamoorthy, and R. Delhibabu, "An Extensive Classification of 5G Network Jamming Attacks," *Security Communication Networks*, vol. 2024, no. 1, p. 2883082, 2024.
[111] R. Kaur, A. L. Sangal, and K. Kumar, "Modeling and simulation of DDoS attack using Omnet++," in *2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, 2014, pp. 220-225: IEEE.
[112] A. Kosugi, K. Teranishi, and K. Kogiso, "Experimental Validation of the Attack-Detection Capability of Encrypted Control Systems Using Man-in-the-Middle Attacks," *IEEE Access*, 2024.
[113] D. Kumari and K. Singh, "Smart Gird Reliability Evaluation Considering Worm Contamination in SCADA," in *2024 International Conference on Automation and Computation (AUTOCOM)*, 2024, pp. 600-605: IEEE.
[114] A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts," *IEEE Access*, vol. 10, pp. 78887-78898, 2022.
[115] M. Faheem, M. A. Al-Khasawneh, A. A. Khan, and S. H. H. Madni, "Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: a study on big datasets," *Data in Brief*, p. 110212, 2024.
[116] Y. Zhong *et al.*, "Distributed blockchain-based authentication and authorization protocol for smart grid," *Wireless Communications Mobile Computing*, vol. 2021, pp. 1-15, 2021.
[117] Z. A. Shaikh *et al.*, "Blockchain hyperledger with non-linear machine learning: A novel and secure educational accreditation registration and distributed ledger preservation architecture," *Applied Sciences*, vol. 12, no. 5, p. 2534, 2022.
[118] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: A survey of current solutions and research challenges," *IEEE Communications Surveys Tutorials*, vol. 22, no. 4, pp. 2658-2693, 2020.
[119] I. Mashal, "Smart grid reliability evaluation and assessment," *Kybernetes*, vol. 52, no. 9, pp. 3261-3291, 2023.
[120] S. A. Ebad, "On Quantifying of IoT Security Parameters-An Assessment Framework," *IEEE Access*, 2023.
[121] A. Almaleh, "Measuring resilience in smart infrastructures: A comprehensive review of metrics and methods," *Applied Sciences*, vol. 13, no. 11, p. 6452, 2023.
[122] H. Rødseth and R. J. Eleftheriadis, "Successful asset management strategy implementation of cyber-physical systems," in *Engineering Assets and Public Infrastructures in the Age of Digitalization: Proceedings of the 13th World Congress on Engineering Asset Management*, 2020, pp. 15-22: Springer.
[123] F. B. Ismail, H. Al-Faiz, H. Hasini, A. Al-Bazi, and H. A. Kazem, "A comprehensive review of the dynamic applications of the digital twin technology across diverse energy sectors," *Energy Strategy Reviews*, vol. 52, p. 101334, 2024.

MOHAMMAD AHMED ALOMARI is affiliated to Faculty of Technology & Electronic and Computer Engineering (FTKEK), Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia, where he is currently working as a senior lecturer. He received his M.Sc. and PhD in Computer Systems Engineering from Universiti Putra Malaysia (UPM), Malaysia. This author became a member (M) of IEEE in 2010, a Senior Member (SM) in 2020. Dr. Mohammad major research interests include data storage encryption in mobiles, security of smart renewable energy and smart grid, embedded systems, and cryptography. He is currently extending his research to Internet of Things (IOT), blockchain Technology, and cloud computing. Dr. Mohammad has authored and co-authored several national and international publications in journals and international conferences, while he is working as a reviewer for worldwide reputable journals in Springer and SAI organization. Dr. Mohammad is a member of organizing and technical committees of many international conferences and workshops in Malaysia and Japan. He is also a member of International Association of Engineers (IAENG), and the Malaysian Society for Engineering & Technology (MySET).

MOHAMMED NASSER AL-ANDOLI received the B.Sc. degree in computer information systems from Mutah University, Jordan, in 2011, the M.Sc. degree in computer science from Jordan Univer- sity of Science and Technology, Jordan, in 2016, and the Ph.D. degree in information technology from Multimedia University, Malaysia, in 2022. From 20122 to 2023, he was a Postdoctoral Researcher at Faculty of Engineering and Technology, Multimedia University, Malaysia. In 2023, he was a Senior Lecturer with the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia. He curruntly a Senior Lecturer with Faculty of Computing and Informatics, Multimedia University, Malaysia. His research interests include malware analysis, complex network analysis, inter- active media, machine learning, high-performance computing, deep learning, and parallel computing.

MUKHTAR GHALEB is an assistant professor of computer networks at the University of Bisha, Saudi Arabia. He received his B.S. degree in computer information systems from Zarka private university, Jordan, in 2004. He received his M.S. degree in networking and distributed computation from University Putra Malaysia (UPM), Malaysia, in 2008. He began the pursuit of his career with an appointment at Sana'a University, Yemen. He received his Ph.D. degree in computer networks from UPM, in 2014. Currently, his research interests are mobile data gathering, routing protocols, power consumption, performance modeling and simulation, Terrestrial and underwater Sensor Networks, AI, and sentimental analysis.

Dr. **REEMA** earned a Ph.D. degree in computer science from Universiti Putra Malaysia (UPM), Malaysia, in 2022. She also holds an M.Sc. degree in information technology from Universiti Utara Malaysia (UUM), Malaysia, which she received in 2016. Her educational background includes a B.Sc. degree in computer science and engineering from Aden University, Yemen, obtained in 2004. With a research focus in the field of data privacy, Dr. Reema specializes in steganography, cryptography, watermarking, and IoT security using machine learning. Prior to her current position, Dr. Reema Thabit served as a lecturer at Aden Community College in Yemen from 2005 to 2013. Currently, she has held the position of senior lecturer in cybersecurity within the computing department of Universiti Tenaga Nasional (UNITEN) in Malaysia since 2023. In this role, she teaches various subjects in the cybersecurity program for degree students and supervises undergraduate and postgraduate students in their projects and theses.

GAMAL ABDULNASER ALKAWSI was born in Yemen. He received his B.S. degree in software engineering, master's degree in management information on systems from Coventry University, INTI, Malaysia; and Ph.D. degree in information communication technology from The Energy University (UNITEN), Malaysia, in 2019. He is currently a Postdoctoral Researcher with The Energy University (UNITEN), and has published in journals and conferences. His research interests include emerging technology acceptance, user behavior, adoption of information systems in organizations, the IoT, artificial intelligence, and machine learning.

JAMIL ABEDALRAHIM JAMIL ALSAYAYDEH (Member, IEEE) received a degree in computer engineering from Zaporizhzhya National Technical University, Ukraine, in 2009, an M.S. degree in computer systems and networks from Zaporizhzhya National Technical University, Ukraine, in 2010 and Ph.D in Engineering Sciences with a specialization in Automation of Control Processes from National Mining University, Ukraine, in 2014. He is currently a Senior Lecturer at the Department of Engineering Technology, Faculty of Electronic and Computer Engineering and Technology, Universiti Teknikal Malaysia Melaka (UTeM) since 2015. His teaching portfolio includes a range of courses such as Computer Network & Security, Internet Technology & Multimedia, Software Engineering, Computer System Engineering, Data Communications & Computer Network, Computer Network & System, Real Time System, Programming Fundamental, Digital Signal Processing, Advanced Programming. He is a research member at Center for Advanced Computing Technology, his research interests are formal methods, simulation, Internet of Things, Computing Technology, Artificial Intelligence, Machine Learning, Computer Architecture, Algorithms, and Applications. Dr. Alsayaydeh has more than 57 research publications to his credit that are indexed in SSCI, SCIE, and Scopus, which cited by over 220 documents. He supervised undergraduate and postgraduate students and he is a reviewing member of various reputed journals. Currently he actively publishes research articles, received grants from the government and private sectors, universities and international collaboration. He is also as a Member of Board of Engineers Malaysia (BEM).

ABDULGUDDOOS S. A. GAID obtained a B.Eng in Electronics Engineering from the Sudan University for Science and Technology (SUST), Khartoum, Sudan, in 2000. He pursued an M.Eng and a PhD in Electrical, Electronic, and Systems Engineering from Universiti Kebangsaan Malaysia (UKM) in 2004 and 2010, respectively. After joining Taylor's University in September 2010, he served as a lecturer until August 2012. From September 2012 onward, Dr. Gaid has been a faculty member at the Communication and Computer Department, Faculty of Engineering, Taiz University. He teaches various courses in electrical, electronics, and communications. His primary research areas include wireless communications and microstrip patch antennas for wireless communication networks. Dr. Gaid has a publication record of over 30 conference and journal papers and has actively contributed to organizing committees for conferences such as the International Conference on Technology, Science, and Administration (ICTSA 2021) and the 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA 2023) held at Taiz University.