Computer Networks 169 (2020) 107094

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Cyber-security on smart grid: Threats and potential solutions

Muhammed Zekeriya Gunduz[a], Resul Das[b,*]

[a] Department of Computer Programming, Bingol University, Bingol 12000, Turkey
[b] Department of Software Engineering, Technology Faculty, Firat University, Elazig 23119, Turkey

ARTICLE INFO

Article history:
Received 3 September 2019
Revised 27 November 2019
Accepted 31 December 2019
Available online 3 January 2020

Keywords:
Smart grid
Cyber-security
Cyber-attacks
Internet of Things.

ABSTRACT

The smart grid is one of the most significant applications of the Internet of Things (IoT). As information and communication technologies (ICT) developed and applied in traditional power systems, the improvement of smart grid cyber-physical-systems (CPS) increases too. IoT-based smart grid systems are critical infrastructures, also they have complex architectures and include critical devices. They contain communication systems that can lead to national security deficits, disruption of public order, loss of life or large-scale economic damage when the confidentiality, integrity, or availability of the communication is broken down. These huge systems may be vulnerable to cyber-attacks. Therefore, there is a lot of research effort to enhance smart grid security in industry, government, and academia. The security approaches are important to improve solutions against cyber-attacks in smart grid applications. We present a comprehensive survey supported by a wide review of earlier work. Additionally, recent advances and countermeasures are presented on smart grid cyber-security. In this paper, the threats and potential solutions of the IoT-based smart grid are analyzed. We focus on cyber-attack types and provide an in-depth of the cyber-security state of the smart grid. Particularly, we concentrate on the discussion and examination of network vulnerabilities, attack countermeasures, and security requirements. We aim to supply a deep understanding of cyber-security vulnerabilities and solutions and give a guide on future research directions for cyber-security in smart grid applications.

1. Introduction

Internet of things is the revolution of the Internet and machine-to-machine (M2M) communication. IoT means connecting different devices via the Internet or IP-based solutions. There will be 28.5 billion networked devices by 2022 [1]. A device can be anything like fridge, sensor, air-conditioner, mobile phone, car, personal computer, laptop. Devices can be already connected via non-IP solutions on a small scale. IoT aims to connect all kind of devices through IP-based solutions at a large scale, too [2]. In an IoT network, devices can interact or communicate directly or through a gateway by IP addresses over the Internet [3].

There are a lot of IoT applications such as intelligent transportation, pollution monitoring, smart cities, smart buildings, connected healthcare [2]. The biggest IoT application is smart grid [4]. It has two lines called power line and communication line. The communication line is very important in terms of intercommunication [5]. A smart grid system, from energy generation to the consumer, is equipped with bidirectional smart devices, such as sensors, actuators, and smart meters [6]. This enables to provide a real-time balance, monitor, and control, anywhere and anytime at high granularity and accuracy [7].

Using IoT applications is very convenience for smart grid systems but it may lead to disasters due to some vulnerabilities [8]. Since controlling and monitoring are done on the Internet-based protocols and general public solutions, smart grid may be very attractive to attackers as a critical infrastructure. For example, an attacker can attack the electrical devices, by cutting the real-time balance between energy generation and consumption owing to falsify the data created by the appliances [9]. Because of smart grid's critical nature, it could be the main target of cyber-terrorism, too. So, it is vital to widely examine the components and identify existing vulnerabilities, and all possible cyber-security threats in the smart grid infrastructure [10].

All systems must be designed to ensure security. It means that the main security objectives have to be satisfied. Main security objectives are confidentiality, integrity, and availability (CIA triad). The exact identification of vulnerabilities and kinds of cyber-security threats in smart grid enables describing appropriate countermeasures and counter cyber-attacks [11]. So, we present attack taxonomies according to CIA triad, and network layers. Also, we discuss how to enable secure smart grid communication with high-

* Corresponding author.
E-mail addresses: mzgunduz@bingol.edu.tr (M.Z. Gunduz), rdas@firat.edu.tr, resuldas@gmail.com (R. Das).

https://doi.org/10.1016/j.comnet.2019.107094
1389-1286/

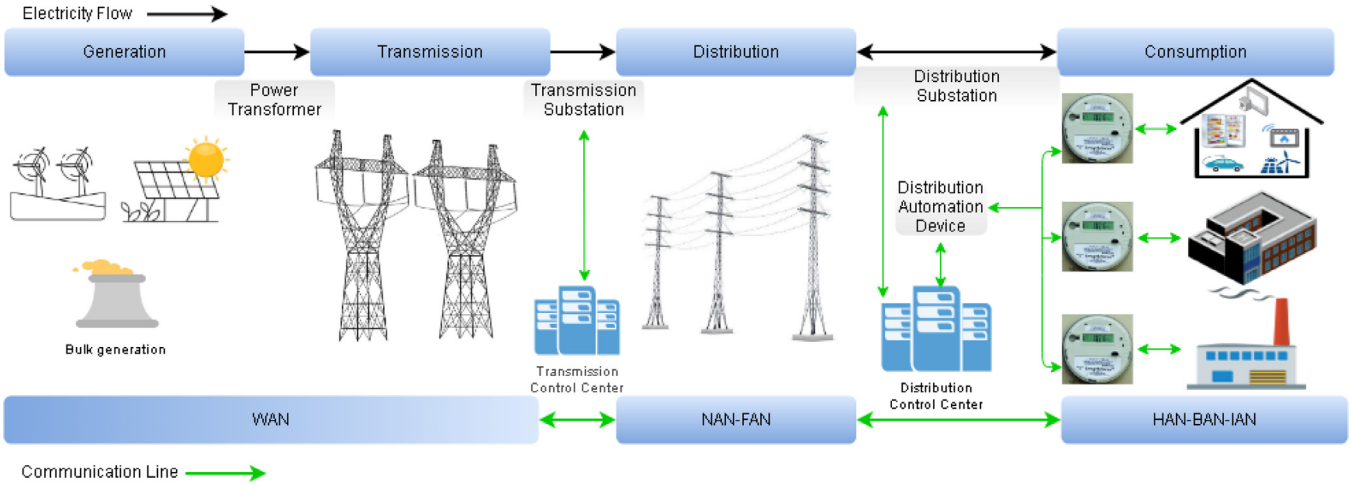

Fig. 1. Smart grid electricity transmission process from generation to consumer.

light some of the latest solutions based on the IoT paradigm. Then we summarize the existing state of the topic and future sights. Additionally, researchers may have a more understanding and the research trends of smart grid security in the study.

The remainder of this paper is organized as follows. In Section 2, the background of smart grid is introduced. In Section 3, cyber-security principles are described. The classification of cyber-security threats and solutions are proposed in Section 4. In Section 5, frameworks for smart grid security analysis are investigated. Future research directions are proposed in Section 6. In Section 7 the work is concluded.

1.1. Main contributions of the paper

Many researchers practice a lot of research effort to enhance cyber-security of smart grid using diverse techniques and also a lot of research, survey and review papers have been published that provide an overview of the widespread cyber security issues in smart grid applications. More than 20 papers have been examined in detail, presented in Table 1 according to content and mentioned attack types. In general, previous studies provide general solutions to cyber-attack types. In this study, we present the types of attacks in smart grid and the security solutions that can be taken against each attack type. Cyber-security has crucial importance in designing information networks. Since smart grid includes many networks, cyber-security has a high priority for smart grid design. So, our objectives are to provide a holistic overview, analyze and review current security solutions, classify cyber-security threats, help to enable deployments with advanced and secured performance, and propose future research directions to enlighten new researchers. The major contributions of the article are as follows:

1. Presenting a detailed background on IoT-based smart grid.
2. Describing smart grid cyber-security objectives and requirements.
3. Providing an evaluation of the existing cyber-attacks according to CIA triad and network layers.
4. Proposing solution approaches and analytic frameworks to help in planning appropriate defence strategies and analyzing the security of smart grid applications.
5. Providing open research issues and future trends that need to be considered while rehabilitating a smart grid system or building a new one.

2. Background on smart grid

Smart grid applications have four main stages shown in Fig. 1. These are generation, transmission, distribution, and consumption. Energy has different types such as geothermal heat, flowing water, solar radiation, wind, hydro plants, chemical combustion, and nuclear fission. Generation of electricity is the process of producing electricity from these kinds of energy. Bulk generation system is connected to the distribution system via the transmission system carrying electricity to far distances. Transmission domain is connected to customer domain by distribution domain which could also supply connection to storage systems and distributed energy resources (DERs) to meet electricity need for customers [22].

2.1. Features of smart grid

Smart grid has a complex infrastructure. It includes a lot of DERs, appliances, and facilities. Enabling efficient operation and maintenance and also optimizing the usage of the assets decrease power consumption and investment costs. A smart grid system is an electricity market that enables to generate, store energy, and shift load for customers. Demand response system helps to balance the load and demand and thus the efficiency of power usage is enhanced. Through bidirectional information and electricity flow, customers can sell their surplus energy to power system when they want. Smart grid applications are expected to have a periodic data flow because of real-time communication and monitoring requirements. Smart grid communication model must be real-time and two-way and thus, customers are better informed [33]. Also, producer and consumer get clarity of electricity consumption readings. Namely, if the bill is not paid, the producer can cut off the power remotely via the Internet.

Smart grid operations include the management of electrical flow, which ensures the reliable, secure and economical transmission of electricity. The fulfillment of these operations contains protection, monitoring, analysis, and control processes. A smart grid system can self-healing the troubles by utilizing technologies such as automatic control devices, timely detection, advanced sensing systems. Also, a smart grid network can effectively resist the problems regardless of kind of cyber attacks, disturbances, and physical damages and it must be designed for real-time, secure, reliable and low latency communication [32].

A smart grid enables new products, services, and markets in their applications. These are necessary to provide green solutions and cost-effectiveness. Authorized service providers or customers

Table 1
A taxonomy of the research papers in smart grid applications.

Reference	Content	Mentioned attack types	Main lesson learned	Results
[12]	A conceptual framework for smart grid security threats identification based on sources of threats	Technical and Non-Technical sources of threats	Various stakeholders must consider security and resiliency issues as a priority in smart grid deployment	Extensive research is required by government agencies, academia, industries, professional bodies and relevant corporate bodies in the evaluation of smart grid security and privacy issues to enhance customers' trust and awareness.
[13]	Smart grid CPS testbeds and main capabilities	MITM, Denial of Service, ARP Spoofing, Eavesdropping, Malformed Packet, Precision Insider, Rogue Software, Database Attacks	Existing smart grid CPS testbeds; Taxonomies, Detailed Features, Targets, Research Areas, Communication Infrastructures	Smart Grid concept compels to develop proper testbeds to test interoperability and cyber-security vulnerabilities.
[14]	Determine the relevant cyber-security and privacy issues to build a reliable smart grid	Black Hole, Route Injection, Denial of Service, Message Modification Attacks	Differences between IT networks and smart grid networks on cyber-security issues, especially privacy issues	Every aspect related to IT in the smart grid has potential vulnerabilities due to inherent security risks in general IT environment.
[15]	Some of the latest solutions for existing cyber-security challenges in smart grid	Denial of Service Attacks	Recommends a new security conceptual model based on the IoT paradigm	Developing standards, conceptual models and techniques that meet the security requirements is vital for smart grid.
[16]	Briefly describes the most important security issues and challenges faced on the IoT-based smart grid	Identity spoofing, availability, privacy, authorization attacks	How can an end-customer actively and securely participate in the energy consumption and generation equilibrium	A lot of security necessities must be taken consideration when a smart grid constructed.
[17]	Briefly describes the most important security vulnerabilities, attack types, solutions and types of attackers	Component-wise, Protocol-wise and Topology-wise attacks	Main security solutions in designing process	Security vision must be taken consideration in communication infrastructure design.
[18]	Cyber-security objectives and requirements along with the risk evaluation process	CIA triad Attacks	Detailed risk evaluation process in smart grid main domains to achieve a road-map of an immune smart grid infrastructure	It is required to enhance the CIA triad of the system by building a robust and efficient smart grid cyber-infrastructure.
[19]	Identifying threats that weaken the smart grid according to network layers	MITM, Denial of Service, ARP Spoofing, Jamming, False Data Injection and Wormhole Attacks	One of the most effective security solutions in mitigating threats is the usage of IDSs that follows a distributed approach	Due to the grid's individual characteristics tailor-made solutions must be designed especially for its own needs.
[20]	A preliminary study case that illustrates the influence of a simple cyber attack which compromised the integrity of power supply data is shown	Attacks against integrity	Feasible approach is to deploy IDS and IPS systems for smart grid applications	One critical aspect of smart grid cyber-security research is insuring sufficient cross disciplinary engagement to formulate optimum approaches and methods.
[21]	Defining smart grid security fundamentals	Network availability, Device, Data and Privacy attacks	The role-based access control scheme, The authentication scheme and IDS approaches to resist the basic cyber attack behaviors in smart grid	Discussing some interesting open problems will trigger more research efforts in this emerging area.
[22]	Security-oriented smart grid testbeds and main capabilities	Nearly all kinds of attacks against CIA triad and security requirements	To succeed the future goals and provide a strong mechanism, further prevention techniques and algorithms should be advanced and confirmed in smart grid testbeds	If cyber-security-oriented testbeds are used effectively, they make significant contributions to the development of smart grid security.
[23]	The possible vulnerabilities in smart grid communication and survey the current solutions	DoS/DDoS, False Data Injection, Replay Attacks	A comprehensive communication architecture with security built in from the very beginning is necessary. A smart grid communication security solution requires a holistic approach including traditional schemes such as PKI technology, trusted computing elements, authentication mechanisms based on industry standards	Securing the smart grid communication infrastructure requires the use of standards-based state-of-the-art security protocols.
[24]	A comprehensive cyber-security study on survey and challenges in smart grid	Nearly all kinds of attacks against CIA triad	Security issues, the communication architecture and security requirements, analyzing security vulnerabilities through case studies, and discussing attack prevention and defense approaches, and the design of secure network protocols to achieve efficient and secure information delivery in the smart grid	The complexity of network architecture, delay constraints on different time scales, scalability, and diversified capabilities of embedded devices, make it impractical to uniformly deploy strong security approaches all over the Smart Grid. So, it requires fine-grained security solutions designed specifically for distinct network applications.
[25]	Current and future threats framework in smart grid	Physical, MAC, Transport and Application Layer Attacks	There are various attacks initiated from the smart home to the smart grid	Due to the smart grids' individual characteristics tailored security solutions must be designed especially for its own network architecture layers.

(*continued on next page*)

Table 1 (*continued*)

Reference	Content	Mentioned attack types	Main lesson learned	Results
[26]	Proposes a cyber attack model for detection of malware-based communication and extrapolates from existing technologies in order to predict future malware types	Nearly all kinds of malware	Existing malware attacks can be generally very destructive on power grids. So, it is important describing generic stages of malware-based cyber attacks	The generic life-cycle model formalizes the stages of malware-based cyber attacks and enables us to investigate existing malware by dissecting it into recurring cycles. This allows a detailed comparison of characteristics in existing malware and provides a useful basis for predicting future developments.
[27]	Using IoT technologies in electric power and energy systems	Interruption, interception, modification, and fabrication attack classes	Using IoT technologies effectively provides fast developing in smart grid applications with some communication challenges	Using IoT technologies securely in smart grid applications is a necessity for digitizing.
[28]	The key threats, the challenges involved in understanding attacks and devising defense strategies against them	Data injection, Time synchronization, Denial of Service, Coordinated and Dynamic system Attacks	Solution approaches that can help mitigate threats, a number of mathematical tools that can help in analyzing and implementing security solutions	Developing appropriate solutions against coordinated attacks which threaten the sustainability of the smart grids are critical for deploying it.
[29]	A detailed survey of the critical challenges in smart grid in terms of ICT, sensing, measurement, control and automation technologies, power electronics and energy storage technologies	Denial of Service, wrapping, phishing, meta-data spoofing and injection attacks	Denial of Service attack detection and mitigation, key management, authentication and encryption still remain as challenging security threats	The fine-grained security solutions should be designed for distinct network applications.
[30]	Reviewing some of the potential attacks, threats, vulnerabilities as well as some proposed solutions to reinforce the smart grid efficiency and reliability	MITM, Denial of Service, False Data Injection, Jamming and Historical Worldwide Attacks	Securing the smart grid infrastructure with encryption and IDS-based solutions is prominent	Examination of historical worldwide cyber-attacks provide more insight on smart grid cyber-security.
[31]	Standardization, Attacks and Security service requirements in smart grid	Attacks against components, systems, and network security	To secure the smart grid, an end to end security architecture has to be addressed	The smart grid is a complex architecture that covers critical devices and systems vulnerable to significant attacks. Hence, security is a crucial factor for the success and the wide deployment of it.
[32]	A comprehensive study of challenges in smart grid security, which is concentrated on the problems and proposed solutions	HAN, NAN, WAN and based-on network layers attacks	Communication networks bring severe security vulnerabilities with them in smart grid applications	Smart grids can be a prime target for cyber terrorism because of their critical nature and socioeconomic impact of blackouts.
[33]	The main security issues and challenges of smart grid, whose main objectives are confidentiality, integrity, authorization, and authentication of the exchanged data	Eavesdropping, Traffic Analysis, Message Modification, Impersonation, and Replay Attacks	The cyber-security countermeasures need to consider heterogeneous devices, networks architectures, different delay constraints, and limited computational resources	Using the same security approach all over the smart grid makes unrealistic to use.
[34]	A cyber-security strategy to detect and counter against cyber attacks in smart grid applications	Nearly all kinds of attacks that take place in a large-scale, like Stuxnet	Attacking cycle steps and details in smart grid	Rather than applying a simple security approach or deploying a specific security technology, they believe that smart grid cyber-attacks may be mitigated more effectively by combining several security mechanisms through a cyber-security strategy.
[35]	Cyber-security issues stunting the development of IoT-based smart grid	Device attacks, Data attacks, Privacy attacks, Network attacks, Organized attacks, APTs, Ransomware attack	Some interesting challenges not mentioned in the literature	The use of IoT-based technologies in smart grid applications is one of the most important challenges in the development of this system in terms of cyber-security.

can remotely control the power usage of intelligent electronic devices (IEDs) by utilizing consumer-oriented IEDs. Markets play role as coordinators who manage some independent network parameters such as service quality, time, total capacity, the capacity ratio of change. When necessary, markets can adjust the parameters to balance the demand and power supply of the entire grid [14].

2.2. Benefits of smart grid

Bidirectional IEDs such as sensors, actuators, smart appliances, and smart meters provides detailed controlling and monitoring of the power line, increasing reliability, quality and maintaining a real-time balance between power generation and consumption [35]. Reliable and economic electricity delivery, optimal utilization of assets, energy conservation, distributed renewable energy generation, reduction of loss, and reduce greenhouse emissions by enabling the integration of electric vehicles and renewable energy sources (RES) are prominent benefits of the smart grid. Also, smart grid executes predictive analysis to maintain the load balance. Additionally, more controllable communication abilities, decreased distribution and transmission loss, instant control capabilities with self-healing, interactive communication, cyber-secure power grid, utilization of RES, large scale energy storage, uninterrupted power supplies, demand management, the integration of consumer devices, electricity pricing based on market, and preven-

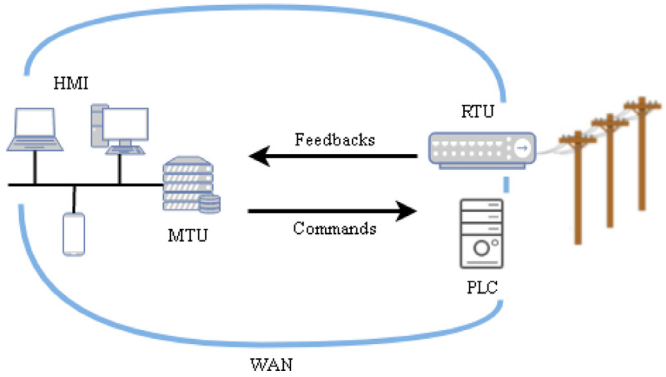

Fig. 2. A typical SCADA architecture.

tive conservation with constant monitoring system in network are some other major benefits of smart grid applications [36,37].

Smart grid provides an active role to consumers by enabling new markets, services, products, and energy usage information for users [33]. This enables flexibility to interact with the electricity market and implement an energy awareness system. Thus, individuals can easily integrate into the microgeneration units, and this allows them to purchase and sell electricity without a license.

Smart grid can capture and analyze data related to power generation, delivery, and usage through control methods and advanced sensing technologies in real-time. It may also supply predictable information and recommendations to all stakeholders (consumers, utilities, suppliers) on optimizing power usage. It can provide services such as better integration of DERs to decrease carbon emissions and device control for energy efficiency, too.

2.3. Key elements of smart grid

A smart grid system has different pieces such as regional control centers, power generation and distribution units, substations, consumers, tap changers, ICT devices, phasor measuring units (PMU), log servers, remote terminal units (RTU), home appliances, protecting relays, IEDs, human-machine interfaces (HMI), circuit breakers, protocol gateways, and smart meters [32]. The aforementioned components are connected to the smart grid for operating, monitoring, and controlling electricity flow and measurement. Existing cyber-security techniques may not be adequate to fulfill the cyber-security requirements of smart grid [32]. Therefore, smart grid systems have unique objectives, goals, and features to provide robust communication architecture and reliable power supply. There are some important assets to consider for efficient operations in smart grid applications.

Supervisory Control and Data Acquisition (SCADA) provides real-time controlling and monitoring of the electricity distribution network. It is generally utilized in large-scale environments [34]. Through decentralized automation management and remote control in medium voltage substations, it can help both ensure the reliability of the power supply and reduce the maintenance and operating costs of the network. Distribution management system (DMS) and energy management system (EMS) are subsystems related to SCADA [38]. SCADA enables the standards for controlling, monitoring and operation of power in industrial processes. A SCADA system consists of four parts [14], as shown in Fig. 2:

1. Data interface appliances like RTU and programmable logic controller (PLC).
2. Communication network such as radio, satellite, cable, telephone.
3. Central master terminal unit (MTU).
4. HMI software or system.

Intercepting or tampering the data damages the grid. Control processes can be performed remotely and automatically with RTUs and PLCs. Various technologies such as VPN, IPSec, firewall, user and device authentication, and intrusion detection system (IDS) are used to secure a SCADA network. Also, access logs and distribution control commands are very vital for a SCADA system. Time-tagged data on the network should be synchronized to ensure the reliability and safety of the SCADA system effectively [39]. Therefore, customers need to have an agreement with their utility companies to use a common time reference such as time-stamped GPS for time synchronization and also ensuring log files and all commands are secure and accurate. So, DERs can be utilized for load support.

Advanced Metering Infrastructure (AMI) is the integration of various technologies that provide advanced connections between the control center and smart meters [31]. The IoT-based smart grid enables that AMI can be implemented easily. AMI is also known as smart metering [40]. HAN, smart meter, operational gateway, and meter data management system are the main components of AMI [14,40]. AMI is responsible for collecting, analyzing, storing and providing measurement data sent by smart meters to authorized parties. So, they can process the data for demand forecasting, outage management, billing. It helps consumers to optimize power utilization knowing the real-time price of electricity. Also, it helps to acquire precious information about consumption of the consumers to maintain the reliability of the power system. Additionally, AMI provides transmitting software updates, commands, requests and pricing-information from authorized parties to smart meters [16]. Smart Metering is a technological solution. Smart metering includes new measuring devices, telecommunication infrastructures and centralized systems for data analysis. Also, it provides data flow bidirectionally, optimizes the operation of electrical networks and contributes to enhancing the safety, reliability, and the quality of service (QoS) requirements such as performance, energy efficiency, security [41]. Smart metering enables bidirectional communication between the central system and smart meters. Smart meters record some valuable information such as energy consumption for management or billing [29]. They can periodically report data on request or in response to certain events to the utility. They can also respond to requests such as power failure, load shedding, real-time pricing, software updates through bidirectional communication capability. Also, they can act as a local EMS by managing the energy usage of smart appliances in the home such as air conditioner, refrigerators, electric vehicles, and ovens.

IoT-based Smart Grid is the empowered form of conventional power lines with IoT technologies. IoT is one of the enabling concepts and plays a fundamental role in the smart grid. The smart grid is considered as one of the most critical infrastructures and is seen as one of the largest IoT applications. Adopting IoT in the smart grid enables large-scale and bidirectional data flow and connectivity throughout the network infrastructure to manage and monitor the energy grid remotely. Through IoT, smart appliances could be efficiently sensed and managed via the Internet. Every device in the network is considered as an object and has a different IP address that could be used to control the devices through the Internet thus connecting numerous devices to create an intelligent, self-sustaining ecosystem. It helps to transfer the high volume of data over the Internet. The communication is made possible due to the massive presence of sensors, actuators and other smart objects alongside the whole system, in addition to the use of smart meters and other smart objects at the customer side. Also, this enables the tracking of real-time energy consumption and demand to the energy supply while assisting consumers to monitor their own usage and adjust behaviors.

Plug-in Hybrid Electric Vehicle (PHEV) contributes to reducing carbon emissions and reducing dependence on fossil fuels,

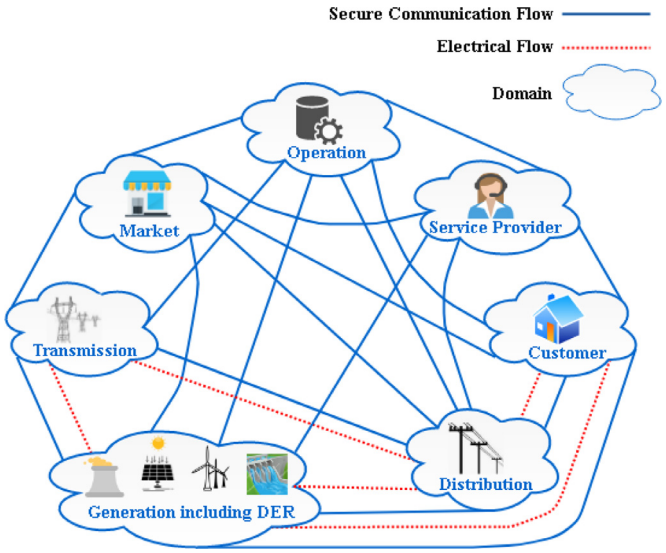

Fig. 3. Smart grid conceptual model [45].

thus providing a means to support DERs in smart grid applications [42]. PHEV can run on gasoline and electricity. PHEV batteries can be recharged by users at home or elsewhere. Since most PHEV batteries are designed for rapid discharge, PHEVs can provide electricity power to the grid [14]. The vehicle-to-grid concept can improve reliability and increase the efficiency of the electricity grid. However, the trade-off between benefits and costs is still unclear [38].

Additionally DER, RES, and communication technologies are other key factors of the smart grid. Communication across the power line happens through wireless, wire cables, fiber-optic links, microwave channels, and ethernet where a wide range of bandwidths are implemented.

2.4. Smart grid conceptual model

Various frameworks have been introduced in academia and industry to describe the architecture of IoT [41], in particular for smart grid applications. National Institute of Standards and Technology (NIST) framework is the most widely utilized untill now [43]. As shown in the Fig. 3, the framework conceptualizes as seven interconnected domains [13,44]. Customers, distribution, transmission and generation domains are responsible for distribution, transmission, and generation of the energy. Market, operation, service provider domains are responsible for service provision, energy distribution management, and energy market management [25]. Generation, transmission and distribution domains include energy substations. Also, operation domain means control systems such as SCADA.

3. Cyber-Security principles on smart grids

The constant advancements in ICT contribute to the development of the traditional electricity grid into the smart grid. However, one of the significant disadvantages of smart grid development is the cyber-security issues involved in. Cyber-security concerns slow down the progress of smart grid applications. Nevertheless, steady improvements will enhance the smart grid experiences in the next years. Smart grid cyber-security issues include ensuring the CIA triad of the control systems and ICT. CIA triad is essential both communication infrastructures and the protection, operation, and management of the energy [22].

3.1. Cyber-security objectives

Cyber-security objectives of smart grid must have precautions securing information with CIA triad [22]. These key security principles have to be met definitely in smart grid systems.

Confidentiality is the protection of data from unauthorized access or disclosure. Confidentiality means that access to information is provided only by authorized people. So, just the authorized users can get access to data and unauthorized ones can't access. A smart grid network can has home devices connected to the power grid with bidirectional and real-time data communication. If attackers get the consumer information, they can abuse the information, keep track of the lifestyle of them, learn what appliances they use, and whether they are at home or not [21]. Confidentiality contains privacy and it is one of the most prominent issues for users [32].

Data never must be tampered by anyone or anything in the system. It's necessary to make sure that all kind of data is correct and non-tampered. Thus, the data must not be changed an unauthorized or undetected manner. Integrity is defined as the prevention of data from unauthorized alteration and destruction. Also, integrity means to maintain and ensure the truth of the data. Integrity helps to provide a secure real-time monitoring system to smart grid.

A power system is expected to be available all of the time. Also, it is important to make sure that timely and reliable accessing and using the information system. Reliability and availability have a direct influence on the control devices of critical infrastructures [46]. Availability is the protection of the information system from breakdown. Availability attacks can corrupt, block or delay information [18]. So, availability means that the information has to be available to authorized parties in the smart grid when needed without compromising security. Data availability generally involves preventing DoS attacks that lead to blackouts [26]. In short, typical cyber-attacks in smart grid applications target at least one of the CIA triad. Malicious users or attackers exploit the information to take advantages or to harm others. Confidentiality attacks aim to allow accessing the information by unauthorized parties [32]. Integrity attacks aim to manipulate original data or insert false data. Availability attacks target to interrupt the power delivery, delay or break the communication.

3.2. Cyber-security requirements

There are also some security requirements in addition to the CIA triad to ensure cyber-security in smart grid applications. Many of these are interrelated. Therefore, to achieve a holistic cyber-security approach, the provision of objectives and requirements should be ensured legally. High level cyber-security objectives and specific cyber-security requirements are shown in Fig. 4.

Authentication and identification are the key processes of confirming the identity of a user or device to defend the smart grid system from unauthorized access. It enables to verify whether the identity of an object is valid. Objects may be users, smart devices, or any components connected to the network. Using a password is a prevalent identification method. Existing authentication protocols can be adapted to design an authentication process in smart grid. However, if the energy systems are not paid enough attention, the authentication design process is vulnerable to significant failures. Authentication and encryption are mandatory cryptographic processes to defend data confidentiality and integrity in smart grid. Also, it is an important identification process to eliminate data integrity attacks. All security requirements require verification of assets to decide whether they are authorized to interact with the data. Integrity and authentication can ensure protection for smart

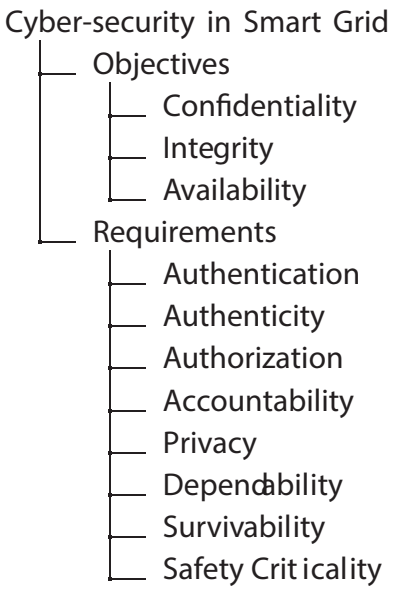

Fig. 4. Smart grid security objectives and requirements.

grid applications against common cyber attacks such as impersonation, MITM, and message modification [23].

Authenticity is necessary to verify that the parties involved are who they claim to be Rawat and Bajracharya [32]. The authenticity of the transmitted data can be ensured by digital signatures. A validation process confirms the parties and messages. Shared secret key management or public key infrastructure (PKI) can be applied to provide authenticity for data transmission across the network [15]. A certificate verifies the identification of the parties. This certificate is provided by a certificate authority. PKI infrastructure is performed before any connection is established between the parties [34].

Access control, also known as authorization, refers to blocking access to the system by unauthorized people or systems without permission [23]. Authorization means to the determination that distinguishes between legitimate and illegitimate parties based on authentication for all other cyber-security requirements. Authorization can lead to safety issues if violated. Access control provides that resources are merely accessed by relevant staff and parties in smart grid that are accurately identified [32]. Stringent access control mechanisms should be implemented to block unauthorized access to sensitive data and critical infrastructures [24]. Access control methods such as Role-Based Access Control, Discretionary Access Control, and Mandatory Access Control can boost system reliability and reduce possible security threats. So, access control is indispensable to restrict a user or device access to the network.

Accountability and auditing provide that smart grid can traceable and recordable [47]. This security requirement is relevant to establish liability. It enables detecting false parties by provable evidence [48]. The assets receiving the data can not later deny it and this is called non-repudiation. Accountability enables non-repudiation. Violation of accountability has typically legal and commercial consequences in smart grid systems. Audit logs are the most common way to ensure accountability [49]. However, it should be noted that audit logs are vulnerable to availability and integrity attacks. Accountability is needed to more secure smart grid applications in terms of confidentiality, integrity, and privacy. If a security problem emerges, accountability operation can determine who is responsible for it. Thanks to accountability the changes in the network traffic can be used as evidence in future judgments. So, the utilities and users can not deny their actions [49].

The electricity bill for homeowners is a case study for accountability. Even though smart meters can determine the real-time cost of power consume, consumers may doubt from its accuracy. The smart meter itself or the utility can modify the transmitted data for someone's advantage or other reasons. As a result, if a smart meter under attack, the user can have two distinct electricity bills, one from the electricity utility and the other from the smart meter [14,34]. An approach is suggested to address this problem in [48]. Moreover, auditability refers to a comprehensive review of all current and past behaviors in a system [23]. It is mostly related to detect causes for faults in a system and to establish the range of the defects or the results of a security event. Auditability without authentication can not ensure accountability. Auditability and authentication should be provided together to ensure exact accountability.

Confidentiality includes privacy and it is the primary issue for confidentiality especially in an AMI system for consumers [49]. A consumer does not want that marketing companies or unauthorized people know their energy usage information, energy usage patterns or other information [14]. Privacy requires that consumer data can not be obtained by unrelated people and used for different purposes without customer's permission, and can merely be utilized for defined permissions [10]. For example, using consumption data for unapproved purposes is a violation of privacy.

Dependability is the capability of a system to achieve its services in time and accurate manner, by avoiding common and serious internal faults. Dependability ensures that services are provided during internal faults. Availability, reliability, maintainability, safety, and security are the essential attributes of dependability. Fault tolerance, fault forecasting, fault prevention, fault detection, fault removal, maintainability, and safety engineering are important measures ensuring dependability [46].

Survivability is the ability of a system to perform its task and thus preventing malicious, intentional or unintentional faults on time. Survivable systems must ensure resilience so that when a part of its security is compromised, it can maintain to meet its services. Survivability aims to provide services both in the existence of malicious intentional actions and external faults. Reliability, availability, fault tolerance, safety, and security are the properties of survivability. Fault prevention, fault detection, fault location, fault forecasting, maintainability, redundancy, security policies, accountability, authentication, authorization, non-repudiation, cryptographic services, isolation of affected areas, and use of heterogeneous security technologies in network design are prominent measures for survivability [46].

Safety is an important security requirement in CPSs and safety criticality is a significant variant of it [46]. Safety criticality refers to systems that can potentially lead to severe outcomes due to the existence of some unexpected situations such as earthquake, flood, tsunami may result in substantial physical damage, human injuries, or even deaths.

In addition to the CIA triad, the aforementioned security requirements must be met strictly to ensure security against cyber-attacks in smart grid applications.

3.3. Cyber-security key components

A lot of cyber-attacks in smart grid may lead to widespread energy blackout and disastrous damage to power resources [27]. Also, they may undermine the cyber-security objectives and requirements. But enumerating all possible attacks is not convenient due to the complexity and large scale of smart grid. Therefore, we classified cyber-attacks based on smart grid security objec-

tives as three types. The aforementioned discussions of security for smart grid show that solutions against threats must consider various constraints, situations, and issues. Therefore, alone security solution, such as encryption, can not block whole cyber-security threats.

Cryptography is not the alone solution, but it plays a very considerable role in enhancing confidentiality and integrity in smart grid [30]. Encryption is the primary cryptographic technique to ensure secure communication. The implementation of encryption schemes is necessary to maintain data integrity and confidentiality in smart grid. Encryption reduces replay and eavesdropping attacks substantially [34]. Many existing authentication schemes and encryption algorithms are adopted in smart grid. Symmetric cryptography, such as symmetric ciphers, DES, AES, and 3DES or public-key cryptography known as asymmetric cryptography are widely used to block possible cyber-threats in smart grid. Also, most electronic appliances in a smart grid are expected to have light-weight cryptographic capabilities.

In addition to cryptographic solutions, the control of the produced effects and their spreading have to be considered across the system life-cycle and several security solutions like expressed below are necessary [46].

1. Confirming hardware-software components through safety engineering approaches.
2. Describing security policies, activation policies, mitigation methods, and preparedness plans by modeling and simulation approaches.
3. Applying cryptographic services and proactive mechanisms.
4. Preparing emergency mechanisms that manage faults such as fault isolation, fault removal, and fault location.
5. Prioritizing services, isolation of areas, and recovery processes.

Smart grid is an application of the IoT. Therefore, IoT-based cyber-security precautions are also valid for smart grid applications. Some of the measures are authentication, encryption, anonymity, risk assessment, data privacy, non-technical measures, sandboxing, securely software updates, single-use passwords [50].

4. Cyber-security threats and solutions

Generation, transmission, distribution, and consumption are the main domains of smart grid. Communication must be met in all domains effectively and securely. Privacy, confidentiality, and authentication of data are crucial for the reliability and also efficiency must be guaranteed to prevent unauthorized modifications throughout the infrastructure and therefore distributed cyber-security systems should be created to maintain data integrity and to monitor the architecture [12]. Smart grid systems have different vulnerabilities and each one owns different characteristics. The vulnerabilities can expose smart grid applications to a lot of distinct cyber-threats that can damage from a low to a high level [19]. The correct identification of the type of security threats and vulnerabilities enable to determinate proper countermeasures.

An attacker can only perform a jamming attack by connecting to the communication channel. Zero-day attacks such as Stuxnet are described as the threat of unknown security vulnerabilities in system applications and may be discovered after the attack finished [26]. An eavesdropping attack is a form of passive attack and the attacker overhears to the messages between the nodes on the communication channel [10]. Traffic analysis, password pilfering, eavesdropping, man-in-the-middle (MITM), and spoofing attacks damage to confidentiality. Data injection, data tampering, wormhole, time synchronization and spoofing attacks damage to integrity. DoS, puppet, buffer overflow, wormhole, jamming and flooding attacks damage to availability in smart grid applications [10].

Especially Advanced Persistent Threats (APTs) are very destructive in critical infrastructures. APTs are a private cyber-attack. Generally, a group or person gets unauthorized access to the system and stays in the system without an undetected manner for a long time. The main target of APTs is generally data theft and APTs are usually supported by nations or large groups. So, APTs involve high-level and complex methods requiring a high degree of stealthy for a long period against the targets [51]. APTs merge various attack methodologies, techniques, and intrusion technologies to compromise interconnected information. In terms of cyber-wars between countries or organizations, an APT has a very damaging effect on the attacked party. Stuxnet, Dragonfly 2.0, Duqu, Red October and Black Energy are the some popular APTs. Honeypots, log analysis methods, hybrid IDS with neural networks, full auditing, cyber-security awareness of users, layered defensive strategies, tight security controls are some prominent defence techniques against APTs.

APTs mainly target the control management system and its components and fulfill some stages before achieving the final goal. APTs mainly target the control management system and its components such as RTU, PLC, PMU, MTU and also fulfill some stages before achieving the final goal. Initial compromise, establishing foothold, escalate privileges, internal reconnaissance, moving laterally, maintaining the presence and completing mission are the stages for an APT in a critical infrastructure respectively [35].

IoT-based security framework solutions for smart infrastructures generally have four layers which are applications, services, network, and end nodes. In the application layer, cyber-attack solutions contain behavior analysis, sensor authentication, lightweight encryption, anti-jamming, and IDS. In the network layer, cyber-attack solutions contain congestion control, authentication, behavior analysis, anti-DoS, intrusion detection, encryption, anti-jamming, and packet filtering. In the services layer, cyber-attack solutions contain intrusion detection, encryption, behavior analysis, authentication, data distortion, selective disclosure, and session identifiers. In the end-nodes layer, cyber-attack solutions contain authentication, encryption, and anomaly behavior analysis of applications and their services [52].

In this section, the types of cyber-attacks that may be used in smart grid applications are described in detail and the precautions that can be taken are identified.

4.1. Classifications of smart grid threats

Malware is the short form of malicious software. Malware attacks compromise the CIA triad of the cyber-infrastructure indirectly or directly [20]. These attacks can lead to many serious results in the smart grid, such as customer information leakage, destruction of the infrastructure or large-scale blackout.

The accuracy of data is crucial for reliable and efficient operation in smart grid. Frequency, current, voltage, or GPS timestamp data can be manipulated. Spoofing attacks, such as identity or data spoofing can cause loss of integrity and availability. Also, they severely degrade smart grid reliability, stability, security, and operation. Spoofing attacks consist of MITM, message replays, and software exploitation attacks. Using multiple devices to monitor the power communication line, collaboration among GPS services, using single data feed, and synchronizing measurements using network timing protocol (NTP) at distinct locations in real-time are some significant solutions against spoofing attacks [27]. Table 2 shows the smart grid cyber-attacks in smart grid according to CIA triad.

Table 2
Classification of Smart Grid Cyber-Attacks according to The CIA triad.

Cyber-Security Objective	Attack Type	References
Confidentiality	Social Engineering, Eavesdropping, Traffic Analysis, Unauthorized Access, Password Pilfering, MITM, Sniffing, Replay, Masquerading, Data Injection Attacks	[10,11,14,19,20,25,34,53]
Integrity	Tampering, Replay, Wormhole, False Data Injection, Spoofing, Data Modification, MITM, Time Synchronization, Masquerading, Load-Drop Attacks	[10,11,14,19,20,23,28,34,54,55]
Availability	Jamming, Wormhole, Denial of Service, LDos(Low-rate Dos), Buffer Overflow, Teardrop, Smurf, Puppet, Time Synchronization, Masquerading, MITM, Spoofing Attacks	[10,11,14,19,20,23,24,28,34,56]

4.2. Confidentiality attacks and solutions

Confidentiality enables to prevent unauthorized access to information. Confidentiality attacks attempt to steal information that should be shared or kept secret merely among the secure parties. Reading memory of devices illegally, spoofing of payload, replay attacks, and changing the control program of smart meters are some examples of such attacks in smart grid. Network coding is used to maintain data privacy. This provides confidentiality in smart grid. Data privacy includes anonymity, unlinkability, unobservability, and undetectability [32,57].

Compared to integrity attacks, confidentiality attacks do not intend to change the transmitted information. They can sniff communication channels in smart grid to obtain the desired information, such as customer's power usage or account number. Traffic analyzing and wiretapping attacks are typical examples [24]. A confidentiality attack may be considered to have a trivial impact on the functionalities of the communication channel in smart grid applications. However, the importance of customer privacy and awareness of privacy has taken more attention in recent years, particularly the possible leakage of many customer information.

Password attacks violate confidentiality. Password guessing, password sniffing, dictionary attacks, and social engineering are common methods used for password attacks. Especially, social engineering is a method to penetrate a system using social skills, rather than technical attacks [20].

An eavesdropping attack is a passive attack type [10] and also it damages to data confidentiality. Eavesdropping attacks sniff IP packets or intercept wireless transmission on local area networks (LAN) in smart grid networks. It includes an attacker who eavesdrops the messages shared between nodes on a communication network. Eavesdropping attacks damage to accountability and integrity of the system as well. Data encryption preserve sensitive data against eavesdropping attacks [53].

Traffic analysis attacks are passive confidentiality attacks. Attackers can sniff and analyze the messages to obtain valuable information about the communication pattern between the nodes.

Masquerading attacks also called impersonation or identity spoofing [33]. Masquerading attacks happen when attackers pretend to a legitimate asset to get privileges. Masquerading attacks harm to CIA triad and accountability. Spoofing attacks such as MAC spoofing, ARP spoofing, IP spoofing are illegal modification of the parameters and they are in masquerading attacks. Identity spoofing attacks such as message replay, MITM and network spoofing [53], enable to imitate an authorized asset without utilizing user password [20]. Authentication processes are essential for every smart grid appliances to avoid these attacks [33].

A side-channel attack targets to obtain the cryptographic keys. Power analysis attack, timing attack, and electromagnetic analysis attack are well-known types of this attack [20,53]. They lead to the violation of passwords, usage information, administrative access, and customer privacy. Home appliances and smart meters are vulnerable to this attack. Detecting saturated channels, saturating communication channel bandwidth, and constructing discrete infrastructure for power grid device communication are pioneer solutions [27].

An attacker can get access to PMU contents or TCP/IP packets of smart meters sent over the network utilizing tools like Wireshark that is used for packet sniffing and analysis [58]. PMU, TCP/IP packets, and smart meters are the main targets of sniffing attacks. Without encryption, attackers may observe and gather critical information. Encryption protects the information from cyber-attacks, makes the network virtual and private. A packet sniffing attack may be mitigated by utilizing a security gateway that transmits IP packets thanks to VPN tunnel, which is designed by embedding an encrypted IP tunnel into the common IP network payload. Communications between VPN tunnels are secured utilizing TLS protocol, and also relations between distinct parties on the smart grid are achieved using X.509 certificates, which authenticate the users and exchange the symmetric keys [27].

4.3. Integrity attacks and solutions

Integrity means to block unauthorized modification or theft of information. Message delay, replay, and injection damage the integrity across the network. Integrity attacks aim to modify the content of original data such as customer account data, billing data, voltage and sensor values, control commands, operating status of the devices, also aim to delay and reorder the stream of the messages illegally [30,39]. Integrity attacks do not include only illegitimate data modification such as false data injection. Besides, device impersonation, sparse, and, replay attacks are considered important integrity attacks. Cryptography algorithms and methods are used to prevent data integrity attacks [15]. Some approaches are proposed to defense against integrity cyber-attacks such as power fingerprinting technique, volt-var control based scheme, and trusted network connect based approach [32]. Authenticity and non-repudiation are important requirements for data integrity, too. Violation of integrity can lead to safety issues that people or equipment may be damaged [23].

Data integrity attacks such as SQL injection and MITM, exploit vulnerabilities to modify, hijack or corrupt legitimate processes in smart grid. Data concentrator unit is connected to HAN's smart meter in smart grid applications. However, an attacker can lead to damage the data transmission between the smart meter and data concentrator unit using MITM or illegal modification of data. Load-drop attacks can be classified in integrity attacks [54].

MITM attacks harm to CIA triad, and accountability of a system. Modified packet source and destinations, route table poisoning, and compromised certificates are some MITM techniques. Network traffic should be encrypted by utilizing security gateways to counter the MITM attacks. Security gateways create VPN tunnels to connect networks. Also, they encrypt the data at the source and decrypt at the target. The efficient encryption processes take place

typically with hardware solutions. Interoperability and secure communication are supported by security gateways with IPsec protocol in smart grid. IPsec ensures confidentiality and unchanged data throughout the communication process to secure the communication line. Additionally, both source and target should be authenticated to block MITM attacks [34]. In other words, authentication of both the source and target nodes, and encryption of network traffic with security gateways are significant solutions. Also, TLS protocols have internal asymmetric cryptographic characteristics that can immediately detect and repair faults to avoid MITM attacks [27].

SQL injection attacks aim to alter databases by injecting script commands. SQL injection attacks inject malicious queries into the database to take control of the system, delete or modify existing data and add manipulated data. It may disturb smart grid operations and eventually result in a blackout. Smart meters continually send power consumption data to store in a database for users and utilities. If queries formed by users are not accurately verified before insertion, SQL injection can happen. In smart grid networks, SQL injection attacks can be reduced by applying measures such as positive pattern matching, static code checking, input type checking, restricting database access to remote users, avoiding dynamic SQL, and implementing penetration tests. Characters such as semicolon, may be abused by attackers and they must be filtered during type checking [27].

A data injection attack means to manipulate data. Feedback signals, sensor readings, and energy consume signals are some examples of data. The effects of such attacks change to depend on targets such as financial benefit or system damage [28]. It uses the information of the system model to inject data led to instability. Data injection attacks generally target state estimator, smart meters, and wide-area protection, monitoring, and control (WAPMC) [53]. State estimator of a power system consists of phase angles and voltage magnitudes at each bus. State estimation provides comprehensive monitoring of current and power flow throughout the smart grid. Therefore, manipulating the monitoring measurements lead to evaluate the operating state of the system incorrectly. Such cases lead to inaccurate operational actions such as causing incorrect pricing, destabilizing the smart grid. As a result, a successful data injection attack prevents to detect of instability that may cause a system crash.

A false data injection attack happens when bad data is injected into smart meters or neighborhood area network measurements. The attack targets to the smart grid infrastructure [59]. Particularly, it aims to damage the integrity of measurement and monitoring sub-systems to manipulate meter and phasor measurements [58]. It impacts the state estimation of SCADA systems. If attackers compromise one or several smart meters, they can inject tampered data into SCADA center successfully, and bypass data integrity check applied in the state estimation process [23].

Replay attacks also known as playback attacks [32]. Replay attacks aim to direct the energy to a different location and damage to the system physically. Replay attacks happen when an attacker obtains the network traffic and then forward it to the destination, acting as the main source. So, replay attacks can have serious effects on system stability. Replay attacks aim to delay or retransmit the messages, after getting them thanks to masquerading attacks. Attackers inject data into the system without causing modifications in measurable outputs. Attackers target non-encrypted sensors to initiate a replay attack. They monitor sensor outputs and repeat them while injecting the attack signal. In addition to inject fake control signals into the network, attackers need to get and analyze the transmitted data between smart meters and devices to obtain the user's characteristics of energy usage and generation. Implementing time-stamps and sequence numbers are effective solutions against replay attacks in smart grid applicatións. Also, a covert attack is a closed-loop version of a replay attack [28].

A time synchronization attack (TSA) targets timing data in smart grid applications. Important processes such as event location estimation and fault detection massively depend on exact timing data in the smart grid. PMU and WAPMC are the main targets of the TSA. Some applications of PMU such as event localization, monitoring voltage stability, fault detection in a transmission line can be affected by TSA [53]. TSA and GPS spoofing aim that GPS signal is imitated by attackers [55]. Therefore, PMU sampling is performed at the wrong time and measurements with incorrect time-stamps are generated. Outcomes in [60] have proved that a TSA may generate wrong location errors and trigger a fake alarm concerning the existence of trouble. The fake alarm can cause an interruption of a communication line. This situation may trigger cascading faults in smart grid. There must be increased usage of PMU to monitor the smart grid more securely.

Authentication schemes and end-to-end encryption are required to eliminate the aforementioned integrity attacks in smart grid networks. Also, attackers must have authenticated access to the communication networks and sensitive information to initiate a confidentiality or integrity attack [24]. Hence, access control and authentication are crucial to prevent the smart grid from integrity attacks.

4.4. Availability attacks and solutions

Availability means that information is accessible by authorized users. Availability attacks prevent and may destabilize authorized access in the smart grid. Availability attacks are also known as DoS attacks [61]. DoS attacks aim to block, damage and delay in data transmission. This causes unavailability in network sources. Availability attacks intend to overload networks by using a variety of techniques, so that the system cannot function properly [56].

Attackers send large volumes of traffic to flood the transmission lines in the network. This causes legitimate data packets in network traffic to be lost and not to be processed. IP-based protocols such as TCP/IP, IEC 61850 are vulnerable to the availability attacks [20]. Since availability is the most important security requirement in the smart grid, advanced and effective countermeasures should be taken against availability attacks. Traffic filtering, big pipes, anomaly detection approaches and applying air-gapped network are some effective solutions [27]. Since DoS attacks are the highest threat to IoT-based smart grid systems, a network layer software solution can be an effective way to mitigate DoS attacks. *IP fast hopping* enables a secure means for a client to conceal the content and destination server of their communication session. IP fast hopping conceals the real IP address of destination server to prevent the identification of network traffic. The server IP address is changed simultaneously in real-time either authorized clients and the server side.

Jamming attacks aim to fill wireless communication lines with noise so that smart meters can not connect to the utility company [53]. This situation adversely affects smart meters in two ways. Firstly, communication channel continuously is seen as busy by routers. Secondly, data packages are blocked from being received. Sending random unauthenticated packets to every wireless station in the network is an effective approach solution to jamming attacks.

Smart grid cyber-attacks are generally coordinated to exploit various components to launch simultaneous attacks. A coordinated attack is the most challenging attack type. Since coordinated attacks can exceed usual defense, they require multilayer security solution with robust approaches. Also, coordinated attacks target all of the security objectives, requirements, and smart grid components. So, the security approaches achieved by analyzing cyber-

security requirements according to network layers will provide effective security solutions for smart grid applications.

4.5. Layer attacks and solutions

MITM attacks aim to sniff and manipulate messages between the control center and field devices [11]. The attacker seems the right destination to both source and target during the protocol session. MITM attacks may be performed in each layer especially in layer 2 and 3, also affects all of the CIA triad and accountability of a system. The cyber-security solutions should include detailed packet analysis software, also robust authentication mechanisms can protect against MITM attacks.

Application layer attacks can easily flood a system that has limited computing sources. Confidentiality and integrity attacks generally initiated in application layer since they attempt to get or manipulate the data in smart grid [24]. DoS attacks can be performed at different layers in smart grid applications [11,31]. DoS attacks in application layer aim to exhaust sources of a system, such as memory, CPU or bandwidth by flooding with intense periods of requests [19]. As communication appliances in smart grid are equipped with limited computational capabilities, they may be potential targets of application layer DoS attacks [24]. A lower layer attack generally targets the bandwidth of communication channels.

Transport layer attacks targeting availability aim to disturb end to end connections by consuming the sources, thereby causing the target device to not receive legitimate traffic after a while [19]. TCP and UDP flooding attacks are some common examples [61]. They are a kind of DoS attacks. Also, IP spoofing is a transport layer attack. MITM attacks can happen during IP spoofing to prevent communication. A MITM attack grants an attacker to sniff a LAN by ARP spoofing [30]. The most prominent defense towards a MITM attack managed through IP spoofing is using encrypted communication. In addition to application layer, using IDS is a very effective cyber-security solution for transport layer, too Radoglou-Grammatikis and Sarigiannidis [62]. Anomaly-based, signature-based and specification-based are three detection modes for IDS/IPSs [66].

Spoofing attacks are detrimental threats in MAC layer because they target both integrity and availability. Spoofing attacks, by exploiting the address fields in a MAC frame, can masquerade themselves to forward false data to other devices. PMUs are the main target of spoofing attacks in smart grid. In power substation networks, malicious nodes may broadcast fake ARP packets to shut down connections of all IEDs to the substation gateway node. It can damage to availability of communication network and the legitimate node cannot recover messages [31].

The most common attack type at physical layer concerning availability is jamming. Jamming attacks occur mainly in wireless networks at the physical layer [53]. Attackers only require to connect to the communication channel to perform a jamming attack [10]. Table 3 shows the attacks according to the network layers. Also, Table 4 shows the cyber-attacks according to network layers and CIA triad in smart grid. Some attacks are active in more than one layer.

Table 3
Classification of Smart Grid Cyber-Attacks according to Network Layers.

Network Layer	Attack Type	References
Application Layer	CPU Exhausting, LDoS, HTTP Flooding, Protocol, Stack Buffer Overflow, Data Injection Attacks	[11,19,32,47,62,63]
Transport Layer	IP Spoofing, Packet Sniffing, Wormhole, Data Injection, Traffic Flooding, Buffer Flooding, Buffer Overflow, DoS/DDoS, MITM, Covert Attack, Replay Attack	[11,19,24,32,47,64]
MAC Layer	Traffic Analysis, Masquerading, ARP Spoofing, MITM, TSA, MAC DoS Attack, Flooding Attacks, Jamming Attack	[11,19,24,32,65]
Physical Layer	Eavesdropping, Smart Meter Tampering Attacks, TSA, Jamming Attacks	[11,19,32,53,65]

Table 4
Demonstration with Network Layers and CIA.

Network Layer	Confidentiality	Integrity	Availability
Application Layer	Data-Injection Attack	-	LDoS, HTTP Flooding, Buffer Overflow
Transport Layer	IP-Spoofing, Data-Injection, Sniffing, MITM, Password Pilfering Attacks	Replay, Covert, Wormhole, Data-Injection, MITM, Spoofing Attacks	Wormhole, MITM, Buffer Overflow, Buffer Flooding, DDoS Attacks
MAC Layer	ARP-Spoofing, Traffic Analysis, MITM Attacks	ARP-Spoofing, TSA, MITM Attacks	Spoofing, TSA, Jamming, DDoS, Flooding, MITM Attacks
Physical Layer	Eavesdropping	Smart Meter Tampering Attacks, TSA	Jamming Attacks, TSA

5. Frameworks for smart grid security analysis

A cyber-security solution should defend all parts of a smart grid system. There are some appropriate countermeasures to avoid the aforementioned typical cyber-attacks. Firewall, encryption, VPN, early warning systems, antivirus software, dynamic reconfiguration systems, access control, IDS, demilitarized zones are for technical solutions [20]. From a security management perspective, solutions should cover risk assessment of assets during-attack and post-attack, security policy exchange, key management [40], security incident, and vulnerability reporting, at least [20]. A robust defense solution integrates various security techniques using artificial intelligence and machine learning, controlled wireless propagation, authentication, network segmentation, certification, proactive real-time IPS-IDS [67], authorization. Also, the solutions should include adaptive, resilient, and scalable security techniques without affecting smart grid operations [32]. The following is required for a secure framework.

1. Authentication and access control strictly enforced for all communication flow throughout the system.
2. Attack detection and countermeasures are essential and must be used everywhere in smart grid.
3. Every node must have basic and light-weight cryptographic functions.
4. Security of network protocols must be designed from the application layer to the MAC layer.
5. Cyber-security testbed platforms must be implemented to investigate the vulnerabilities of the power infrastructures [22].

It can be hard to assure all parts of the smart grid to be secure against cyber-attacks. Therefore, the communication system must detect and identify unusual cases caused by cyber-attacks to monitor the network traffic status. The communication system can monitor the network traffic by profiling, testing, and comparison [68]. Moreover, the network architecture needs to have self-healing ability to sustain network processes, during a cyber-attack. Due to the crucial importance of energy systems, resilience operations in communication networks are vital for keeping system availability [24]. Performing practical security solutions needs an-

alytical frameworks that allow modeling of smart grids applications' cyber and physical environments, the interdependency between many network components, and the decision-making processes more effectively [23]. Analytic tools are quite helpful in modeling and analyzing smart grid cyber-security issues, such as power system protection, control theory, information security, and reliability evaluation [12].

Modeling a networked control system (NCS) combines ICT with control system design to model a smart grid. Communication between sensors, actuators, and controllers in a CPS is achieved by a shared network. An NCS enables to model the cyber-physical structure which enables to analyze possible threats and determine suitable security solutions in smart grid applications.

Game theory is the process of modeling the strategic interaction of players. Players have rules. The game theory includes some mathematical tools. The tools examine strategic interaction and also decision-making between entities. Entities refer to players with interconnected. In the smart grid security game, the attacker tries to plan an attack strategy to increase the damage to the system while the defender (system operator) tries to plan a defense strategy to decrease the damage. Due to opposite purposes of the defender and attacker, game-theoretic methods present valuable tools to model optimal decision-making and discover the best defense strategy against attacker strategy [59].

Vulnerability assessment techniques depend upon probabilistic risk assessment (PRA) for energy control system security levels that are measured by the probability of cyber-security incidents and related energy loss [69]. The possibility is got by historic events and statistical examples. Therefore, a quantitative effect evaluation of energy systems under cyber-attacks can be provided by PRA. However, it is very hard to evaluate the possibility of possible large-scale DoS attacks for PRA against smart grid applications. Because, there is no enough historical data for profiling, and different DoS attacks may have different priorities in the system.

Security-metric-based and graph-based techniques have the scalability issue and may be used in small-scale energy systems such as substation networks. In security-metric-based, each IED has a score. The score depends on all known identifications of cyber-threats and countermeasures in security-metric-based assessment approach. Also, the security-metric for the substation network can be computed depending on the scores of all IEDs.

One of the disadvantages of PRA is the hardship to establish the possibility of possible security events that do not exist in the database. So, graph-based evaluation is applied to model the attack effect on energy systems. This solution identifies the common relationship between attack targets, outcomes, and defense strategies as a graph and utilizes decision-making mechanisms to evaluate the effect and probability of attacks against energy systems.

The smart grid is a networked CPS. So, graph-based techniques may be beneficial to design the network interconnectivity between smart grid devices. A graph includes many vertices, also called nodes, and many edges, also called links, combining the vertices. In smart grid cyber-security applications, the vertices symbolize devices such as smart meters, loads, transformers, generators, routers. Edges represent the interconnectivity between the components. Modeling this interconnectivity may be considered as physical connectivity between those devices or logical connectivity between the devices. Therefore, graph-based techniques are very helpful to explain the nature of smart grid applications, to examine the interconnectivity between the components, and to analyze the propagation of cyber-attacks in smart grid applications.

6. Future research directions

Cyber-security of smart grid against sophisticated cyber attacks is a major challenge hindering the growth of IoT-based smart grid. New attack tactics are continuously discovered and also existing ones evolve making the cyber-security issue to be extremely unpredictable and dynamic.

Differences between the security objectives of smart grid and IT networks require effective security solutions for each of them [17]. Additionally, existing cyber-attack types indicate that energy systems may be vulnerable to potential cyber-security attacks. Therefore, studying cyber-security issues in smart grid applications is a significant engineering task. Active involvement of customers and new technologies can lead to new cyber-security issues. Therefore, tailored solutions should be created for smart grid applications [19].

Thus far, we have examined potential cyber-security threats, analyzed them in terms of the security objectives. We have also evaluated the current literature that offers promising solutions and countermeasures to achieve security objectives. To conclude the overview of smart grid security, trends for future researches are described following.

1. Designing global standardization frameworks for secure communication in smart grid applications.
2. Establishing new protocols or altering old protocols for the requirements of smart grid applications.
3. Exploring new techniques and metrics such as data mining-based, statistical-based, knowledge detection-based, information theory-based, machine learning-based, to evaluate cyber-security methods and proposed solutions for the suitability of smart grid applications.
4. Evaluating cyber-security issues arising from the integration of DERs into the smart grid.
5. Architecting wide-area situational awareness frameworks for cyber-defense solutions [70].
6. Evolving security techniques for zero-day attacks.
7. Creating systems that can assist to log information for forensics analysis and audit controls.
8. Especially for AMI and smart meters, developing dynamic context-aware IDS/IPSs [66] to detect, prevent and alert unexpected changes in the behavior of the system.
9. Developing dynamic self-healing mechanisms such as cloud-based resilience.

When many of the ICT was designed, defending to malware was not a priority and cyber-attacks were rare. But the situation is traverse today. Since IoT-based smart grid is highly dependent on the Internet and ICT, resilient ICT is a prerequisite for reliable operation in smart grid applications. Therefore, embedded ICT must prevent malfunctions, and must not facilitate the intrusion by malicious agents. This is a mandatory requirement for smart grid systems. Furthermore, improvements can only be performed gradually and over time because of the long lifetime of automation systems. The efforts have been made to solve these issues by creating new standards that describe how to augment old systems and protocols. The aim of the efforts is better security regarding malicious attacks.

Several standards have been proposed for worldwide standardization in smart grid systems. These standardization efforts can be utilized to provide well-regulated security assessment methods for smart grid components. So, secure and reliable transactions could be assured. Since the recommendations of standardization are assessed by various professionals in a long-term process, they suggest a high-level assurance that they are secure, well-organized, and complete. These standardization activities deal with cyber and physical security concerns in smart grid applications, facilitate their certification, obtain the credibility of customers and creating a competitive advantage among organizations [35], [71].

Many IoT devices can communicate with each other, but there is no universal language for IoT yet. The lack of standards, espe-

cially for protocols and metrics, has led to a broken set of interconnected solutions rather than a set of easily integrated and combined solutions. Therefore, device producers have to prefer among different frameworks and also users have to decide whether the devices they want are compatible with they have. Since most of the IoT devices have not stringent security protocols and insecure encryption mechanisms it is easy to hack them. Enabling connectivity is the priority for existing IoT devices. So, developing IoT-based smart grid devices and applications without paying much attention to cyber-security is a big challenge.

7. Conclusion

Cyber-security is a major and critical issue for IoT-based smart grid applications. Smart grid security issues include data acquisition, and control devices such as PLC, smart meters, IEDs, RTU, and PMUs. There are also network security challenges, including firewalls, attack scenarios, countermeasures, encryption, intrusion analysis, forensic analysis, and routers. Classification of cyber-attacks for taking into account important factors of information security enables a well-organized and useful way to provide practical solutions for current and future attacks in smart grid applications. Moreover, due to the characteristics of smart grid applications, specific solutions need to be created for their private necessities. Due to security risks in common IT background, we can infer that nearly all aspects associated with IT technology in smart grid applications have potential vulnerabilities. Therefore, cyber-security issues in smart grid applications are under research and need deeper investigations to defend against cyber-attacks and vulnerabilities. In the paper, researchers can find a further understanding of smart grid cyber-security objectives, requirements, and future research trends. Furthermore, we present a compact review of cyber-security threats and defense solutions for smart grid applications. Moreover, we review the recent researches on the smart grid from the security perspective and firstly introduce the background of the smart grid and then discuss the benefits, features and main components. Next, we introduce some solutions against cyber-threats in smart grid applications. Afterward, we analyze the future trends associated with smart grid security. Significant contributions of the survey article are that it presents specific solutions to threats on IoT-based smart grid applications and highlights possible research opportunities for researchers to provide future research directions.

Declaration of Competing Interest

The authors declare that they do not have any financial or non-financial conflict of interests.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.comnet.2019.107094.

References

[1] Cisco Visual Networking Index: Forecast and Trends, 2017/2022 White Paper.
[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: challenges, opportunities, and directions, IEEE Trans. Ind. Inf. 14 (11) (2018) 4724–4734, doi:10.1109/TII.2018.2852491.
[3] M.Z. Gunduz, R. Das, Internet of things (IoT): evolution, components and applications fields, Pamukkale Univ. J. Eng. Sci. 24 (2) (2018) 327–335, doi:10.5505/pajes.2017.89106.
[4] M.M. Raut, R.R. Sable, S.R. Toraskar, Internet of things(IoT) based smart grid, Int. J. Eng. Trend. Technol. 34 (1) (2016) 15–20, doi:10.14445/22315381/IJETT-V34P203.
[5] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G.P. Hancke, Smart grid technologies: communication technologies and standards, IEEE Trans. Ind. Inf. 7 (4) (2011) 529–539, doi:10.1109/TII.2011.2166794.
[6] L. Kotut, L.A. Wahsheh, Survey of cyber security challenges and solutions in smart grids, in: 2016 Cybersecurity Symposium (CYBERSEC), 2016, pp. 32–37, doi:10.1109/CYBERSEC.2016.013.
[7] S. Ahmed, T.M. Gondal, M. Adil, S.A. Malik, R. Qureshi, A survey on communication technologies in smart grid, in: 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), 2019, pp. 7–12, doi:10.1109/GTDAsia.2019.8715993.
[8] J. Fritz, J. Sagisi, J. James, A.S. Leger, K. King, K. Duncan, Simulation of man in the middle attack on smart grid testbed, Proceed. 2019 IEEE SoutheastCon (2019).
[9] R.E. Pérez-Guzmán, Y. Salgueiro-Sicilia, M. Rivera, Communication systems and security issues in smart microgrids, in: 2017 IEEE Southern Power Electronics Conference (SPEC), 2017, pp. 1–6, doi:10.1109/SPEC.2017.8333659.
[10] M.Z. Gunduz, 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, doi:10.1109/IDAP.2018.8620728.
[11] C. Lopez, A. Sargolzaei, H. Santana, C. Huerta, Smart grid cyber security: an overview of threats and countermeasures, J. Energy Power Eng. 9 (7) (2015), doi:10.17265/1934-8975/2015.07.005.
[12] A.O. Otuoze, M.W. Mustafa, R.M. Larik, Smart grids security challenges: classification by sources of threats, J. Electr. Syst. Inf. Technol. 5 (3) (2018) 468–483, doi:10.1016/j.jesit.2018.01.001.
[13] M.H. Cintuglu, O.A. Mohammed, K. Akkaya, A.S. Uluagac, A survey on smart grid cyber-physical system testbeds, IEEE Commun. Surv. Tutor. 19 (1) (2017) 446–464, doi:10.1109/COMST.2016.2627399.
[14] J. Liu, Y. Xiao, S. Li, W. Liang, C.L.P. Chen, Cyber security and privacy issues in smart grids, IEEE Commun. Surv. Tutor. 14 (4) (2012) 981–997, doi:10.1109/SURV.2011.122111.00145.
[15] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, A.R.A. Ali, Smart grid cyber security: Challenges and solutions, in: 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), 2015, pp. 170–175, doi:10.1109/ICSGCE.2015.7454291.
[16] C. Bekara, Security issues and challenges for the IoT-based smart grid, Procedia Comput. Sci. 34 (Supplement C) (2014) 532–537, doi:10.1016/j.procs.2014.07.064.
[17] F. Aloul, A.R. Al-Ali, R. Al-Dalky, M. Al-Mardini, W. El-Hajj, Smart grid security: threats, vulnerabilities and solutions, Int. J. Smart Grid Clean Energy (2012) 1–6, doi:10.12720/sgce.1.1.1-6.
[18] R.K. Pandey, M. Misra, Cyber security threats-Smart grid infrastructure, in: 2016 National Power Systems Conference (NPSC), 2016, pp. 1–6, doi:10.1109/NPSC.2016.7858950.
[19] A. Procopiou, 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, doi:10.1109/CYBER.2015.7288228.
[20] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, H.F. 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, doi:10.1109/ISGTEurope.2011.6162722.
[21] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu, Securing smart grid: cyber attacks, countermeasures, and challenges, IEEE Commun. Mag. 50 (8) (2012) 38–45, doi:10.1109/MCOM.2012.6257525.
[22] M.Z. Gunduz, 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, doi:10.1109/ISDFS.2018.8355329.
[23] Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on cyber security for smart grid communications, IEEE Commun. Surv. Tutor. 14 (4) (2012) 998–1010, doi:10.1109/SURV.2012.010912.00035.
[24] W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges, Comput. Netw. 57 (5) (2013) 1344–1371, doi:10.1016/j.comnet.2012.12.017.
[25] N. Komninos, E. Philippou, A. Pitsillides, Survey in smart grid and smart home security: issues, challenges and countermeasures, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1933–1954, doi:10.1109/COMST.2014.2320093.
[26] P. Eder-Neuhauser, T. Zseby, J. Fabini, G. Vormayr, Cyber attack models for smart grid environments, Sustain. Energy Grid. Netw. 12 (Supplement C) (2017) 10–29, doi:10.1016/j.segan.2017.08.002.
[27] G. Bedi, G.K. Venayagamoorthy, R. Singh, R.R. Brooks, K. Wang, Review of internet of things (IoT) in electric power and energy systems, IEEE Internet Things J. 5 (2) (2018) 847–870, doi:10.1109/JIOT.2018.2802704.
[28] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas. (2016). Smart grid security: Threats, challenges, and solutions. [Online]. Available: arXiv:1606.06992.
[29] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, C.-F. Covrig, A survey on the critical issues in smart grid technologies, Renew. Sustain. Energy Rev. 54 (Supplement C) (2016) 396–405, doi:10.1016/j.rser.2015.10.036.
[30] B. Khelifa, S. Abla, Security concerns in smart grids: Threats, vulnerabilities and countermeasures, in: 2015 3rd International Renewable and Sustainable Energy Conference (IRSEC), 2015, pp. 1–6, doi:10.1109/IRSEC.2015.7454963.
[31] I. Aouini, L.B. Azzouz, Smart grids cyber security issues and challenges, Int. J. Electr. Comput. Energ. Electron. Commun. Eng. 9 (11) (2015).
[32] D.B. Rawat, C. Bajracharya, Cyber security for smart grid systems: Status, challenges and perspectives, in: SoutheastCon 2015, 2015, pp. 1–6, doi:10.1109/SECON.2015.7132891.
[33] V. Delgado-Gomes, J.F. Martins, C. Lima, P.N. Borza, Smart grid security issues, in: 2015 9th International Conference on Compatibility and Power Electronics (CPE), 2015, pp. 534–538, doi:10.1109/CPE.2015.7231132.

[34] Z.E. Mrabet, N. Kaabouch, H.E. Ghazi, H.E. Ghazi, Cyber-security in smart grid: survey and challenges, Comput. Electr. Eng. 67 (2018) 469–482, doi:10.1016/j.compeleceng.2018.01.015.
[35] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks, Int. J. Crit. Infrastruct. Prot. 25 (2019) 36–49, doi:10.1016/j.ijcip.2019.01.001.
[36] C.P. Vineetha, C.A. Babu, Smart grid challenges, issues and solutions, in: 2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG), 2014, pp. 1–4, doi:10.1109/IGBSG.2014.6835208.
[37] M.L. Tuballa, M.L. Abundo, A review of the development of smart grid technologies, Renew. Sustain. Energy Rev. 59 (2016) 710–725, doi:10.1016/j.rser.2016.01.011.
[38] F. Hu, H. Zhen, Cyber-Physical Systems: Integrated Computing and Engineering Design, CRC Press, 2013. Google-Books-ID: AcanAAAAQBAJ.
[39] S. Tan, D. De, W. Song, J. Yang, S.K. Das, Survey of security advances in smart grid: a data driven approach, IEEE Commun. Surv. Tutor. 19 (1) (2017) 397–422, doi:10.1109/COMST.2016.2616442.
[40] A. Ghosal, M. Conti, Key management systems for smart grid advanced metering infrastructure: a survey, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2831–2848, doi:10.1109/COMST.2019.2907650.
[41] L.D. Xu, W. He, S. Li, Internet of things in industries: a survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243, doi:10.1109/TII.2014.2300753.
[42] R.A. Waraich, M.D. Galus, C. Dobler, M. Balmer, G. Andersson, K.W. Axhausen, Plug-in hybrid electric vehicles and smart grids: investigations based on a microsimulation, Transp. Res. Part C 28 (2013) 74–86, doi:10.1016/j.trc.2012.10.011.
[43] Z.A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed, M. Peacock, Future challenges for smart cities: cyber-security and digital forensics, Digit. Invest. 22 (2017) 3–13, doi:10.1016/j.diin.2017.06.015.
[44] NIST Framework and roadmap for smart grid interoperability standards, release 3.0, Spec. Publ. (NIST SP) - 1108r3 (2014).
[45] NIST draft smart grid conceptual model.
[46] C. Alcaraz, J. Lopez, Analysis of requirements for critical control systems, Int. J. Crit. Infrastruct. Prot. 5 (3) (2012) 137–145, doi:10.1016/j.ijcip.2012.08.003.
[47] P. Kumar, Y. Lin, G. Bai, A. Paverd, J.S. Dong, A. Martin, Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues, IEEE Communications Surveys Tutorials (2019), doi:10.1109/COMST.2019.2899354. 1–1.
[48] J. Liu, Y. Xiao, J. Gao, Achieving accountability in smart grid, IEEE Syst. J. 8 (2) (2014) 493–508, doi:10.1109/JSYST.2013.2260697.
[49] F.M. Cleveland, Cyber security issues for Advanced Metering Infrasttructure (AMI), in: 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008, pp. 1–5, doi:10.1109/PES.2008.4596535.
[50] A.S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, Z.Y. Dong, Cyber security framework for internet of things-based energy internet, Future Gener. Comput. Syst. 93 (2019) 849–859, doi:10.1016/j.future.2018.01.029.
[51] J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez, Current cyber-defense trends in industrial control systems, Comput. Secur. 87 (2019) 101561, doi:10.1016/j.cose.2019.06.015.
[52] J. Pacheco, S. Hariri, IoT Security Framework for Smart Cyber Infrastructures, in: 2016IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), 2016, pp. 242–247, doi:10.1109/FAS-W.2016.58. ISSN: null.
[53] Z.A. Baig, A.-R. Amoudi, An analysis of smart grid attacks and countermeasures, J. Commun. 8 (8) (2013) 473–479, doi:10.12720/jcm.8.8.473-479.
[54] E.B. Rice, A. AlMajali, Mitigating the risk of cyber attack on smart grid systems, Procedia Comput Sci 28 (Supplement C) (2014) 575–582, doi:10.1016/j.procs.2014.03.070.
[55] M.S. Al-kahtani, L. Karim, A survey on attacks and defense mechanisms in smart grids, Int. J. Comput. Eng. Inform. Technol. 11 (5) (2019) 7.
[56] R. Kaur, A.L. Sangal, 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, doi:10.1109/SPIN.2014.6776951.
[57] H. Nicanfar, P. Talebifard, A. Alasaad, V.C.M. Leung, Enhanced network coding to maintain privacy in smart grid communication, IEEE Trans. Emerg. Top. Comput. 1 (2) (2013) 286–296, doi:10.1109/TETC.2013.2288275.
[58] T.A. Rizzetti, P. Wessel, A.S. Rodrigues, B.M.d. Silva, R. Milbradt, L.N. Canha, Cyber security and communications network on SCADA systems in the context of Smart Grids, in: 2015 50th International Universities Power Engineering Conference (UPEC), 2015, pp. 1–6, doi:10.1109/UPEC.2015.7339762.
[59] C. Peng, H. Sun, M. Yang, Y. Wang, A survey on security communication and control for smart grids under malicious cyber attacks, IEEE Trans. Syst. Man Cybernet. (2019) 1–16, doi:10.1109/TSMC.2018.2884952.
[60] Z. Zhang, S. Gong, A.D. Dimitrovski, H. Li, Time synchronization attack in smart grid: impact and analysis, IEEE Trans. Smart Grid 4 (1) (2013) 87–98, doi:10.1109/TSG.2012.2227342.
[61] K.I. Sgouras, A.D. Birda, D.P. Labridis, Cyber attack impact on critical Smart Grid infrastructures, in: ISGT 2014, 2014, pp. 1–5, doi:10.1109/ISGT.2014.6816504.
[62] P.I. Radoglou-Grammatikis, P.G. Sarigiannidis, Securing the smart grid: a comprehensive compilation of intrusion detection and prevention systems, IEEE Access 7 (2019) 46595–46620, doi:10.1109/ACCESS.2019.2909807.
[63] M. Yesilbudak, 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, doi:10.1109/ISGWCP.2018.8634478.
[64] Y. Wang, T.T. Gamage, C.H. Hauser, Security implications of transport layer protocols in power grid synchrophasor data communication, IEEE Trans. Smart Grid 7 (2) (2016) 807–816, doi:10.1109/TSG.2015.2499766.
[65] F. Jameel, Network security challenges in smart grid, in: 2016 19th International Multi-Topic Conference (INMIC), 2016, pp. 1–7, doi:10.1109/INMIC.2016.7840156.
[66] C. Alcaraz, L. Cazorla, G. Fernandez, Context-awareness using anomaly-based detectors for smart grid domains, in: International Conference on Risks and Security of Internet and Systems, 2014, pp. 17–34, doi:10.1007/978-3-319-17127-2_2.
[67] P.I. Radoglou-Grammatikis, 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, doi:10.1109/GIIS.2018.8635743.
[68] G. Tuna, R. Das, V.C. Gungor, Communications technologies for smart grid applications: a review of advances and challenges, in: Smart Grid Analytics for Sustainability and Urbanization, 2018, pp. 215–235.
[69] H. Wei, Z. Ling, G. Yajuan, C. Hao, Research on information security testing technology for smart Substations, in: 2014 International Conference on Power System Technology, 2014, pp. 2492–2497, doi:10.1109/POWERCON.2014.6993727.
[70] C. Alcaraz, J. Lopez, Wide-area situational awareness for critical infrastructure protection, Computer (Long Beach Calif) 46 (4) (2013) 30–37, doi:10.1109/MC.2013.72.
[71] R. Leszczyna, Cybersecurity and privacy in standards for smart grids: a comprehensive survey, J. Comput. Stand. Interf. 56 (2018) 62–73, doi:10.1016/j.csi.2017.09.005.

M.Zekeriya Gunduz received the B.S. degree from the Department of Computer Science at the Suleyman Demirel University in 2006. Then he graduated M.S. degree from the Department of Computer Science at the Fórat University in 2013 and currently he is a Ph.D. student in software engineering at the same university. Additionally, he is working as a lecturer at the Department of Computer Programming in Bingol University. His current research areas include IoT applications, communication networks, and smart grid cyber-security.

Resul Das has been working as Associate Professor in the Department of Software Engineering at the University of Firat, where he has been a faculty member since 2011. From 2000 to 2011 he served as both instructor and network administrator at the Department of Informatics at the Firat University. He has been working as instructor and coordinator of Cisco Networking Academy Program since 2002 at this university. He graduated B.S. and M.S. degrees from the Department of Computer Science at the Fórat University in 1999 and 2002 respectively. Then he completed his Ph.D. degree at the Department of Electrical-Electronics Engineering at the same university in 2008. He also worked between September 2017 and June 2018 as a visiting professor at the Department of Computing Science at the University of Alberta, Edmonton, Canada. He has authored more than hundred papers in international conference proceedings and refereed journals and has been actively serving as a reviewer for international journals and conferences. And also he has been serving as Associate Editor for Journal of IEEE Access and Turkish Journal Electrical Engineering and Computer Science. His current research areas include computer networks and network security, cyber-security, software design and architecture, IoT/M2M applications, knowledge discovery, and multi-sensor data fusion.