Chapter 2
A Study of Internet of Things in Smart Grid and Smart Grid Security

Kaushik Kalita, Partha Pratim Borah, and Kankan Kishore Pathak

Abstract The Internet of Things (IoT) may be demarcated as any kind of network that is embedded with sensors, interlinked with software, and other technologies for communication or connectivity of devices over the Internet. IoT is a massive lively global network infrastructure and plays a chief role in smart grid growth and enhances intelligent grid information and communication. Smart grid (SG) is usually a data communication network that is consolidated with a power grid to collect data and information from the substation, consumers, and transmission lines. With IoT, it is like an upgraded version of the network. In this chapter, an attempt has been made to study various applications, communication infrastructures, protocols, and security services of IoT in SG. The importance of securities in the SG for secure communications and prevention of all possible failures or threats is to be discussed thoroughly. Moreover, an attempt has been made to give an idea of cyber security for the SG and its privacy is also to be addressed in this chapter.

2.1 Introduction

A power grid has to be promoted so that it may adjust to variations during growing power outages, demands, and new requirements equipped with the grid and can undergo self-healing. The grid configuration is upgraded for this purpose with the assist of IoT vision. This change is termed as smart grid (SG) which can adjust to changes and self-assist ones. IoT provides SG better and sustainable power and it has proved to be more reliable than the traditional ones. For this purpose, many power companies are taking attempts to initiate the concept of IoT as a futuristic technology, which lead to connection of each device in the grid. It can be implemented

K. Kalita
Department of Electronics and Communication Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati, Assam 781017, India

P. P. Borah · K. K. Pathak (✉)
Department of Mechanical Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati, Assam 781017, India
e-mail: kankan_me@gimt-guwahati.ac.in

B. Das et al. (eds.), *Advances in Smart Energy Systems*, Smart Innovation, Systems and Technologies 301, https://doi.org/10.1007/978-981-19-2412-5_2

along with supervisory control and data acquisition (SCADA) and digital scriber line (DCS) which enables rapid response from the distribution side also. Wired and wireless technologies are available for communication in the smart grid. Wired technology like fiber optics, power line communication (PLC), DCS, and wireless technology involving WLAN and WiMAX are employed presently [33]. IoT-based SG uses as a combination of efficient energy utilization and monitoring and controlling all grid devices and the challenges like security, no connection faults, noises during communication, cost, and information privacy are dealt mostly by software approaches [32].

In IoT-based SG architecture, the equipment shares data with each other through the Internet cloud. In the wireless nodes, resource constraints and shortage of spectrum are major problems. Deployment of SGs has developed the intelligence of grid system interoperation by multi-directional data flow provision between any two or more devices in the networking to achieve a power industry that can revolutionize the industry of power generation, thus, providing adequate data from metering to substation, distributions, transmission, and generation, for increasing security, reliability, and effective control and monitoring of all aspects related to service systems. Ghasempour [15] highlighted that the most crucial application of IoT in SG is data exchanging network which is combined with the power grid to gather and examine data that are acquired from different grid components. Smart grids (SG) have proven protections which are not present in the central control system or the protection schemes for the infrastructure related to power from its value and for smart or advanced homes [34]. The smart grids were introduced for controlling the shortcoming of standard electrical grids using computerized equipment [14]. Since the existence of communication nodes, it has cause to be the expose to attack in the energy sectors, hence, there is a need of a reliable working intelligence of interconnected components for upgraded security protocols, load estimation, demand side management (DSM), cost information, and sustainable use of non-conventional energy systems. There are many challenging issues needed to be addressed and both technology and social knots have to be united before IoT technology being extensively accepted. SGs are a critical infrastructure which attracts cyber-attacks, since monitoring and control can be done over standard Internet-based procedures and solutions relies on public communication infrastructure [16]. This may result in economical loses to the unity and can affect the electric assets, by breaking the real-time balance between energy consumption and production, through operating data produced by smart object or directed from the utility [7].

In this chapter, IoT and its properties in different aspect are described in Sect. 2.2; Sect. 2.3 covers detailed explanation of smart grid, its goals, and challenges. Section 2.4 covers about the applications and services of IoT in SG. In the latter part of this chapter, Sects. 2.5 and 2.6 discuss about the security and cyber security challenges for SG.

2.2 Internet of Things

IoT is the latest upgradation in computer system and electronic engineering which results in enhancing the reliability of the grid that has been the greatest challenge for the technical designers. For enhancing the existing standard grid's utmost reliability and its quick reaction time, the present standard grid with IoT could be introduced. Wortmann and Fluchter [43] have discussed the origin of IoT dated back to more than 15 years. Their work has attributed to the work of the Auto-ID Labs at the Massachusetts Institute of Technology (MIT) on radio-frequency identification (RFID) infrastructure. Assembly manufacturing plot of Intel uses IoT to constantly record the huge amount of data from devices and other framework connected to the grid system for fast leadership action, directed reaction, and insightful results by technically improved hardware operation at minimal cost [28].

2.2.1 Definition

IoT may be stated as the networked interaction of smart devices infrastructure and are embedded with ubiquitous intelligence. IoT may increase the ubiquity of the Internet by assimilating every object for communication via embedded system, which leads to an extremely dispersed network of device communicating with human beings as well as other devices [44]. IoT makes possible the development of a massive number of applications, of which only a very minor part is currently available to the society. IoT application can be assembled under the mention domains:

- *Logistics and transportation domain*—buses, trains, advanced cars, as well as bicycles along with roads and/or rails are mostly embedded with sensors, actuators, and processing power [18]. Real-time data processing technology based on RFID and NFC may realize real-time monitoring of nearly every link of the supply chain, ranging from commodity design [42]. Assisted driving, mobile ticketing, and monitoring environmental parameters like temperature, humidity, and shock during the transportation; the conservation status is monitored, and augmented maps for tourists can be equipped with tags [10] that allow NFC-equipped phones to browse it and provide information about various aspects.
- *Healthcare domain*—IoT technologies in these domain can be grouped mostly into tracking of an individual in motion, this involves both real-time position tracking, and for location and material tracking to prevent left-ins, identification, and authentication for security procedure, and data collection related to integrating RFID technology with other health information, sensing devices enable function centered on patients [42].
- *Smart environment domain*—sensors and actuators associated with the network system in houses and offices can make life comfortable and smarter in several aspects. Industrial plants are automated with maximum employment of RFID

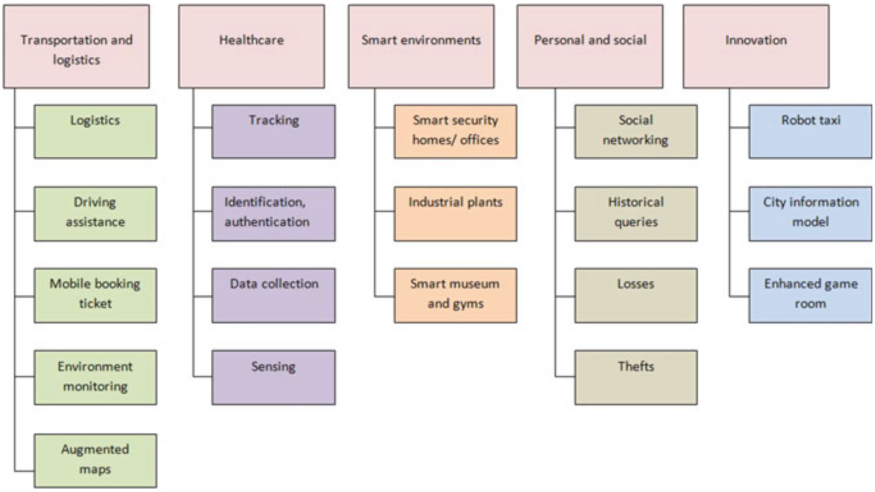

Fig. 2.1 Application domains and relevant major scenarios

tags associated with the production parts [10]. Health parameters are monitored during training session in gyms.

- *Individual and social domain*—the application under this domain is that enable the user to interact with other person to maintain and build social relationship. Historical inquiries about objects and events data let operators study drifts in their activities over time. Search engine for things is been used for searching any object which we cannot remember [22]. For locating the last recorded location of a tagged object a simple web based RFID system is used which act as a search engine for things that we want to locate.
- *Futuristic application domain*—in the future cities, robot taxis swarm together, moving in flocks, providing service where it is needed in a timely and efficient manner. A city information model (CIM) is an idea that keeps the track or monitors the statics and performance of each buildings and urban fabrics by the city government [5] (Fig. 2.1).

2.2.2 *Identification of Radio Frequency*

Radio signal helps in the identification of a particular target and support in acquiring the data for communication purpose. Establishing mechanical or specific optical contact in the specific target is done by RFID technology techniques. The corresponding electronic data can be identified by the electronic reader in the electronic tag by detecting items specific maker information. The most common use of electronic tags is; it is bundled to goods that are to be taken track off. For example, in the shopping mall, electronic mark is often seen. The special communication protocol realizes reading and writing data between the electronic reader and electronic tag [11]. Generally, the electronic reader sends the desired instructions or data to the electronic tag. And when the instructions are received, the electronic tag returns the coded data in memory to the sender [10]. This is a widely used method of communication so far as it uses electromagnetic changes and it does not need contact.

2.2.3 Infrared Sensor Technology

Infrared transducer uses infrared rays to measure temperature sensitive physical properties. Infrared light includes physical properties like reflection, interference, refraction, absorption, and scattering. Anything with temperature above absolute zero, radiation infrared can be applied in it [25]. There is no friction in infrared sensor measurement, since it is done without direct contact with the measured object and therefore has high sensitivity and fast response. The infrared sensor is a combination of optical sensing system, detecting circuit, and a switching circuit [12].

2.2.4 Global Position System

GPS is associated with a space satellite, user signal receiving device, and a ground signal connecting point. It provides the consumer with speed, information, and high precious position in all types of weather condition in real-time application. Application of GPS in power system is advantageous because of its positioning function [29]. We need accurate time standard to acquire accurate synchronization purposes for monitoring and protection system in electrical power system such as microcomputer protection and security automatic equipment monitoring system, dispatching automation system, wave recorder that detects faults. With the expansion and upgradation of power grids, it requires higher standards of accuracy and convenience [25].

2.2.5 Machine/Man to Machine/Mobile

Recent development of communication technologies is gradually advancing toward integration from the upgraded mode of independent parallel. Well known examples of summing of mobile communication infrastructure and IP computer network, TV network, computer network, signal network, power network, satellite communication network are all moving toward integration. Transfer of information from one terminal to another terminal is done in M2M, which can be termed as data exchange between the machines [43]. Generally, M can represent machine or person which can be represented as man and mobile device can be represented as mobile, which represents, M2M as the connection and communication between people or machines and mobile devices [25]. The integration of RFID, M2M, sensing network, and industrial evolution is four major technologies of IoT.

2.3 Smart Grid System

SG technologies all contribute to efficient IoT energy management solution that are currently lacking in the existing framework. What makes the IoT SG better is two-way communication between connected devices and hardware that can sense and respond to user demands. These technologies mean that a SG is more resilient and less costly that the current power infrastructure.

2.3.1 Definition of Smart Grid

SGs are high efficient, reliable, excessive quality, short responsive, and self-sustainable. SGs play a vital position for the improvement of contemporary day towns which is termed as smart cities. Not simply being efficient in transmitting the electricity, however, additionally reduces the carbon emission from electricity saver, which in turn improves the financial condition [33]. Utilization of the assets efficiently to boom the performance of the grid and manages the allotted era efficiently to optimize the electricity intake and offers two-way communiqué among the grid and the consumer [19] (Fig. 2.2).

Few important features are listed below:

- Real-time monitoring

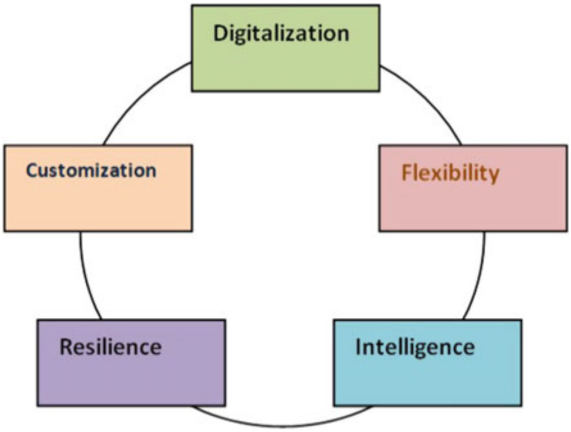

Fig. 2.2 Smart Grid properties

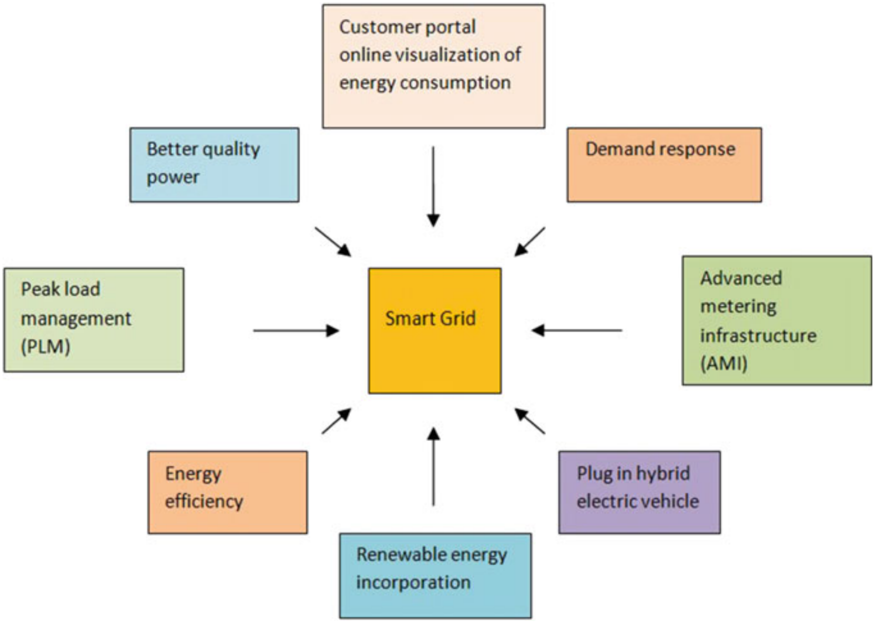
Customer portal online visualization of energy consumption
Better quality power
Demand response
Peak load management (PLM)
Smart Grid
Advanced metering infrastructure (AMI)
Energy efficiency
Plug in hybrid electric vehicle
Renewable energy incorporation

Fig. 2.3 Smart grid benefits

- Quick restoration and automatic outage management
- Energy management
- Tracking and managing of energy usage.

Advantage of smart grid consists of maximal load management, improves device reliability, integration of renewable strength and simplicity of get entry to electricity, and self-sustained grids [33] (Fig. 2.3).

2.3.2 Smart Grid Architecture

The strength shipping community essentially includes subsystems, a transmission system and a distribution system. The grid consists of a tracking gadget and a smart meter which maintains a track of the strength consumed. It consists of superconductive transmission lines which assist to lessen the resistive losses and additionally in like-minded to different asserts of strength like wind, solar, and so forth. The three practical additives of a SG are smart manage centers, advance transmission networks, and intelligent substations. The recent control center plays tracking primarily based totally at the statistics amassed through SCADA and remote terminal units (RTUs). Destiny statistics can be acquired from state management module, which is higher than the prevailing module in phrases of application time and robustness additionally

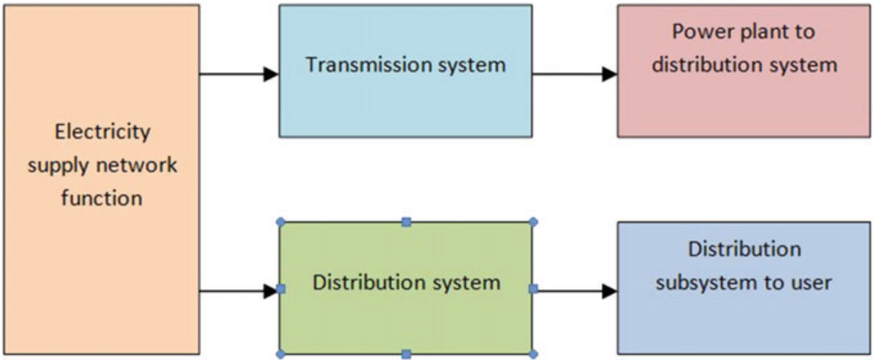
Electricity supply network function
Transmission system
Power plant to distribution system
Distribution system
Distribution subsystem to user

Fig. 2.4 A general model of smart grid

the final results can be blended with a extensive place GIS, and a visible show can be provided [24]. Future is predicted to have online time domain-primarily based totally analysis. These might consist of voltage balance and temporary angular balance. In the future, proactive and adaptive tactic scan be used and there can be coordination so that it will advance a higher manage. There are new functions which is associated with SG, which includes signal processing, sensing, superior materials, electricity electronics, verbal exchange, and computing. For long distance transmission, high-temperature composite conductors and high-temperature superconducting cables are used for electric powered transmission, considering that they have a better present day wearing capacity, low voltage drop, decreased line losses, mild in weight, and higher controllability. Six and twelve section transmission strains are used which offer more electricity transmission with decreased electromagnetic discipline and phase section cancellation. Intelligent sensors are used with superior signal processing to degree the value of line parameters and display the fame with the sensor location. In smart substation, equipments have to be greater dependable and known for capabilities like tracking, controlling, operating, shielding and maintaining [19] (Fig. 2.4).

2.3.3 The Smart Grid Goals and Challenges

2.3.3.1 Goals

The modern power grid of the present time consists of more than 9200 power production units, more than 10 lakh MWs of production capacity, which are linked via 3 lakh miles of transmission lines [39]. The one vital requirement of electricity is its immediate utilization just after its generation which results in blackouts and burnouts. Moreover, efficiency is also an important aspect of the modern power grid. Another cause of major concern is the grid security. The centralized architecture of the present

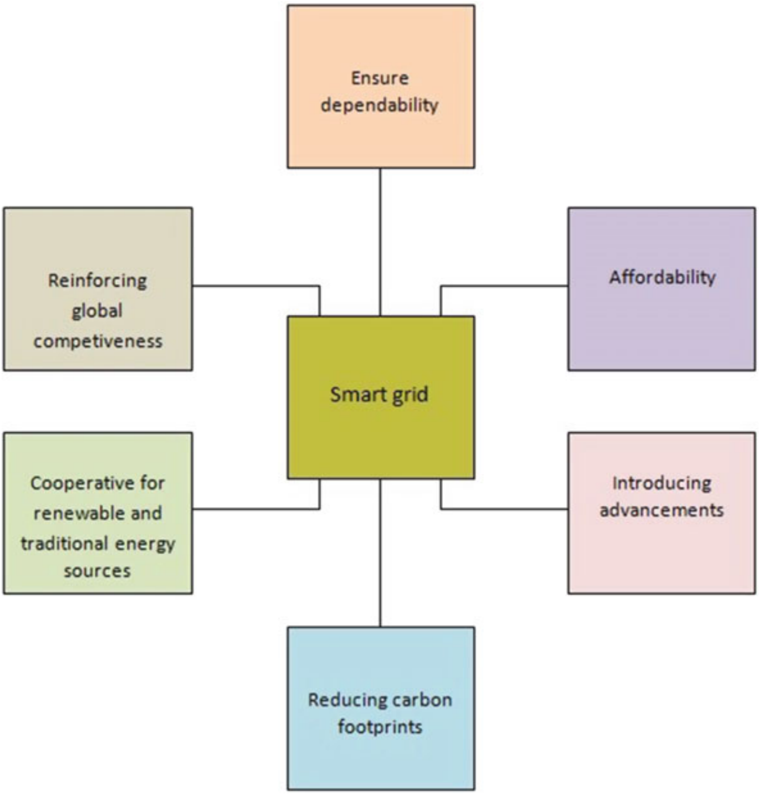
Ensure dependability
Reinforcing global competiveness
Affordability
Smart grid
Cooperative for renewable and traditional energy sources
Introducing advancements
Reducing carbon footprints

Fig. 2.5 Smart grids goals

power grid makes it more susceptible to attacks. Thus, the smart grid system is introduced which integrates power, communication, as well as computer control. It aims in the efficient control of power supply with reduction in the carbon emission [16]. Digital platform is the basic necessity of a smart grid for a fast and reliable system. A SG should be adaptable, compatible, and expandable because of its flexibility. It should inherit intelligent technology which can be reliable and the system should be customizable by the customer [19] (Fig. 2.5).

2.3.3.2 Challenges

Apart from IoT being a promising technology in the smart grid framework, it has certain disadvantages too. It sometimes leads to disaster. Our lifestyle is completely dependent on the energy market, but the present day infrastructure of SG is very complex which is a major challenge. Monitoring and control of the SG is done over the Internet and few are dependent on public communication technologies, so SGs are vulnerable to cyber-attacks. Modification in power industry is directed by the penetration of distributed generation and non-conventional energy sources [3]. Because of the growing electricity demand, electricity should be generated and managed carefully. This results in entrepreneurs and local electric industries at distribution level which is a challenge for the reliability and system efficiency. Some of the challenges of smart grid include:

- Infrastructure of the grid
- Concern over storage and stability
- Communication issues
- Cyber security
- Energy management
- Data management [34].

2.4 IoT Application and Services in Smart Grids

IoT has a large and complicated communication infrastructure. The system is primarily based on transmission, acquiring, processing, and storing of statistics in a dependable or stable and reliable manner. In contrast, SG is related to many technologies on generation, distribution, transmission, and consumption in addition to IoT. Our society has to realize the current state of any era associated with the development in their private existence, and manages their very own micro grid supplies, domestic appliance, EVs, and to manipulate and screen the day by day technical updates on offerings which includes electricity, gas, and water [35]. ICT technologies are regularly utilized by the carrier issuer for management and detection of the fault, monitoring, and goals for troubleshooting the fault. The communication shape is being upgraded with the aid of using the use of IoT era in SG equipments. The networking is related to low-price and low-strength microprocessors, virtual communication infrastructure which has safety and reliability supports, and a smart communication layer which has the ability to evolve and protocol systems to have interaction with diverse software program technology and hardware. Some communication technology which incorporates LTE-A, UMTS, LTE, LPWAN, and slender band IOT (NB-IOT) has been advanced further to BLE for personal area networks and Zigbee within side the use of HEMS [21]. Long-range communication is supplied with the aid of using the stepped forward technology within side the unlicensed bands for SG and IoT programs. The functions of evolving LPWAN permit end-consumer IoT programs that require excessive battery existence, low-price equipments, information transmission, and it is able to be utilized in each subject wherein the cell technology is not always feasible. The IoT and SG infrastructure have a main function in software grid system and generation-transmission-distribution cycles and additionally improves day by day existence elements together with smart metropolis and smart constructing infrastructure [17]. For protection protocols, IoT frameworks which have been proposed with the aid of using many institutes are Arrowhead Framework, Industrial Internet Reference Architecture (IIRA), ETSI structure for M2M, Model Industrie 4.0 (RAMI 4.0), IoT-A, ISO/IEC WD 30141 IoT reference structure (IoT RA), Reference Architecture and the IEEE well-known for an Architecture Framework for IoT [21].

2.4.1 Driving Factors of IoT for Smart Grid

The wireless controlling and monitoring ability of SG networking, which increases the abilities of power plants for more robust DSM and distributed generation (DG) with minimal loses. Hence, demand forecasting (DF) and automatic generation control (AGC) in SG are some control structure required for power generation cycle [23]. The load and supply range as a result of extensive utilization of EVs, non-conventional energy source, strength garage device, and smart clients with their personal distributed energy resources (DERs) adversely have an effect on the not unusual place call for control approaches. The goal of a smart control device may be indexed as strength exceptional and DSM, strength manages, sustainability and fee control, and DG manage. The sluggish and growing integration of supply load to the energy grid calls for strong DF to control the periodic cycle. Another manage technique is AGC which is likewise referred to as secondary frequency manage technique. It addresses troubles reason via means of penetration of intermittent RESs [23]. These manage techniques have been powerful on gradual and restrained modified in load profile. Therefore, they turn out to be insufficient toward the current integration of RESs and distributed generation supply drawing nonlinear dynamics. The AGC manages the strength call by means of monitoring and compensating the frequency of whole structures seeing that a fluctuation at the load reasons equal adjustments at the device frequency, and the weight call is compensated via means of stabilizing the device frequency again [21]. The riding technology of IOT within side the context of SG may be essentially grouped into 3 categories:

- Technologies of data acquisition which produces appropriate information from "things."
- Data processing, ICT and management technologies.
- Security and privacy awareness technologies.

2.4.2 Communication Infrastructure of IoT

Communication technologies were advanced for distinctive utility planes and requirements. Some of those technologies are not unusual place for unique utility planes which includes Bluetooth in private networks and Zigbee in domestic and tool automations, and the other communication technology offers huge utility regions which includes LPWAN, Wi-Fi, and mobile technology. The communication and insurance plans of SG may be categorized into three corporations as NAN, HAN, and WAN. The HAN is important for residential devices with smart appliances, power control systems, electricity manipulate tools, ESSs, PV panels, small-scale wind turbines, electric powered motors, and smart meters [2]. NAN offers with distribution degree of SG in which a set of residential or business masses were aggregated in a substation or transformer while WAN friends numerous NAN regions for control. IEEE 802.11 or IEEE 802.15.4 primarily based totally on communication technology may be good enough for HAN and NANs, while WANs require fiber optic, UMTS, LTE, LTE-A kind large insurance communication technology [37]. The maximum good sized improvement were visible within-side the closing decade with Bluetooth low power, IEEE 802.11 primarily based total community technology, IEEE 802.15.fourprimarily based total superior modems, and cellular communication which includes UMTS, LTE-A, LTE and 5G [21].

Software-defined network (SDN) presents development to decorate flexibility, reliability, scalability, and interoperability of IoT-primarily based totally SG communication infrastructure. SDN gives an open structure version in three ranges with the aid of using isolating manipulate and facts planes, allowing centralized logical manipulate and incorporating community programming capability [29]. Thus, SDN copes with verbal exchange issues came about in traditional structure combining safety manipulating, billing, and tracking facts transmission. Its allows communicating machine for keeping apart decided on gadgets upon detection and safety approach, intrusion detection, reducing excessive visitors, and denial of carrier attacks and far flung manipulate sensors and smart meters.

2.4.3 IoT Protocols

There are main IoT protocol type proposed one is primarily based on records trade protocols as bus-primarily based totally and broker-primarily based totally even as the alternative one lists the protocol into three sections as utility protocol, provider discovery protocol and infrastructure protocol. The bus-primarily based totally protocol allows the customer to transmit a specific message to the assigned developer of that message. The provider discovery protocol consists of Data Distribution Service (DDS), Extensible Messaging and Presence Protocol (XMPP), and Representational State Transfer (REST). The distinguished broker-primarily based on IoT protocols are superior message queuing protocol (AMQP), CoAP, Java messaging provider API (JMS), and MQTT protocols. Another type for those protocols is via means of identifying that if they're message-centric or records-centric. Constrained Application Protocol (CoAP) is a web-primarily based on customer and server version protocol is primarily based on REST structure on HTTP and operates within side the utility layer (APP) [1]. The constrain gadgets inclusive of sensors or sensor nodes are applied as servers for IoT applications. AMQP is likewise a APP protocol as CoAP this is primarily based on message-centric structure. AMQP makes use of TCP and it guarantees the hit message shipping thanks to its authentication and encryption strategies primarily based on SSL/TLS control. The DDS is a latest post/subscribe protocol utilized in M2M communication to allow real-time, excessive overall performance and interoperable records transmission [27]. The protocol consists of records-centric post and subscribes (DCPS) version, and DDS interoperability Wire Protocol (DDSI) that DCPS identifies the DDS structure, and DDSI defines interoperability structure. XMPP is a message-orientated middleware to transmit voice and video records in decentralized customer-subscriber structure. XMPP allows consumer to talk via means of immediate messages on web-primarily based on platform no matter any OS [21].

2.4.4 Future Research Direction

Despite considerable researches for the transformation of traditional software grid to SG had been finished as much as date, there none the less main demanding situations exist to be solved for improving, interoperability, connectivity, reliability and safety of SG CPS [45]. Since the SG infrastructure encompasses complete interplay of energy era, transmission, distribution, and intake environments, it calls for a massive and dependable communication interface to manipulate, control, and reveal this machine. The complexity and heterogeneity of energy and communication structures comprising the SG infrastructure poses demanding situations on interoperability of devices, cyber-architectural safety, resiliency, and statistics control problems. Although the massive operation place of SG attracts a heterogeneous ecosystem, the main demanding situations may be labeled into threefold as manipulate, communication and safety of machine [20]. The demanding situations on manipulate problems are met at era, transmission, distribution, and intake degree that consist of DER integration, far flung tracking, transmission line tracking, PMU and PQ analysis, RES integration, DSM, DR, load control, interoperability, and rising EV programs. It is broadly widespread that maximum of those demanding situations regarding manipulate problems had been solved, and current research have proposed diverse manipulate techniques to conquer energy community deficiencies. However, use of communication machine primarily based on big quantity of various technology and protocols poses numerous demanding situations on interoperability and safety problems.

While the communication networks are essential to enhance the improvement of SG, numerous demanding situations are addressed for robust, secure, resilient, and operational SG communication community. The two-directional communication infrastructure of smart meters is enabled via means of diverse Wi-Fi technology which includes IEEE 802.15.4, IEEE 802.11, cellular, and place community. Therefore, the variety of communication technology running within side the equal infrastructure calls for standardized protocol and alertness interfaces to make certain interoperability of whole machine. To this case, well-known APIs and middleware traits are required to address main demanding situations of heterogeneous infrastructure of communication technology. The particular protocol-primarily based on programs are any other rising studies place within side the context of SG and IoT integration wherein CoAP, AMQP, MQTT, and JMS are the distinguished ones [8]. The safety and privacy researches are also anticipated to be emerge because of numerous special communication protocol, and framework which are applied in IoT, and SG interplays with precise coding and encryption infrastructure. Some researchers surveyed in this subject matter have remarked that public key infrastructure (PKI) utilization might also additionally address the safety problems. The safety problems have additionally expanded the researches on PHY and MAC layer safety, community layer, IEEE802.15.4 cease-to-cease safety, IP and six LoWPAN safety, and routing safety [21]. The studies on energy-efficient IoT architectures are modern day to control sources and communication infrastructure with low-energy intake and surprisingly green. The subtle structure which can be composed via means of sensing and manipulate layers, statistics processing layers, and alertness layers are being broadly researched within side the context of subsequent era IoT architectures. Micro grid control, equipment manipulate, EV manipulate and tracking researches also are ever-evolving structures within side the context of IoT-primarily based totally SG programs [8]. The sensible manipulate capabilities are described as one of the studies guidelines within side the smart constructing control topics.

2.5 Smart Grid Security and Protocol

Three criteria defined by The National Institute of Standards and Technology (NIST) for the maintenance of security of data or information in the SG for its protection are described below [31]:

- *Confidentiality* can be defined as the preservation of authorized restrictions for the disclosure and access of information. It is essential for the protection of both personal and registered information from being disclosed and accessed by individuals, authorized entities, or processes.
- *Availability* can be defined as the assurance of reliable and timely access to information. It is an important security criterion in the SG because the loss of availability creates trouble to access information in a SG.
- *Integrity* in *SG* can be defined as the protection against destruction or inappropriate modification of data.
- *Accountability* assures system manageability and records every task performed by a device, person, or a public authority and ensures that everyone can acknowledge his/her action. The recorded data is accessible and can be used for determining the attacker [31].

2.5.1 Smart Grid Security Threats Classification by Source

The different challenges and threats experienced by SG are identified. It is necessary that the threats are well-defined. A complete approach for the effective security requirements must be established and followed. Hence, a study of the threats' sources is important.

2.5.1.1 Technical Sources of Smart Grid Threats

It is classified based on the diagnosed threats which may be traced to the technical elements of SGs. Three key elements of the technical reasserts of those threats are diagnosed and those are infrastructure safety, technical operation safety and systems' statistics control safety.

- *The infrastructure security*—SGs infrastructure could be very complicated structures which can be geographically, logically, and economically distributed, interconnecting users, electricity plants, utilities, transmission, distribution, substations, transformers, etc. As properly as advanced metering infrastructure (AMI), the related conversation, and ICT gadgets along with aggregate of wireless, fiber optic, power line carrier (PLC), and conventional cable or Ethernet, hence, making SGs, a noticeably smart gadget and as such, the safety of the infrastructure turns into critical [38]. The AMI is extra inclined as it's far important to SG operation. AMI safety (AMI-SEC) project pressure changed into pronounced to have evolved a few constant and preferred safety guidelines, through final replace given that 2009, for implementation of AMI answer consisting of meter statistics control gadget (MDMS) down until smart meter interface [34].
- *Technical operational security*—The complexity of the grid necessitates secured operational schemes. This is due to the fact that disasters might also additionally have extra impact given that essential infrastructure rely upon secured and dependable power operations and components for electricity and manipulation. Some of the coordination within side the operation of the device is below manipulate, however, a few part of the operations additionally require on-subject interest of operators on the software manipulate centers, particularly for the duration of emergencies in a few cases. In a resilient grid device, well timed reputation and analysis of trouble situations are key elements for stopping unfold of disturbances [26]. Since faults may also arise because of failure of protecting devices, there may be want to layout the device to be self-recovery with the aid of making sure perfect fault tolerance degree and provision of considered necessary redundancy to accomplishing a dependable operational security [4].
- *Systems' data management security*—It covers actual time recording, tracking and storing of vital information and information, safety of information toward assaults, guidelines and guidelines guiding information policy, privacy adherence with the aid of using running personnel, customers' delight in phrases of privacy assurance, etc. The developing issues over the opportunities of privateness

breach with the aid of using the application organizations in probable revealing customers' information are predominant challenge for customers. Although SMs have but modified the character of SM information frauds or assaults, compromising the meter with the aid of using far flung penetration and manipulate of recorded and saved information can be a supply of very state-of-the-art assaults able to permitting vague modifications to customer's utilization and falsely indict cantered sufferers or relying on their intention, release large-scale assaults on the principle grid [34].

2.5.1.2 Non-technical Sources of Smart Grids Threats

The non-technical reassets of SGs threats offers with the ones elements that may counter in opposition to the deployment or operation. Such elements encompass herbal or guy initiated additionally surroundings risks inclusive of earthquakes, floods, falling of trees, bush burning, etc. Government regulatory policies, making plans and implementation or maybe marketplace operations and personal zone mobilizations, etc. Although, thinking about the causative mode, a few elements are taken into consideration. Non-technical, however, might also additionally require technical method in tackling it.

- *Environment security*—It could be very crucial in SGs implementation because it enables management and keep away from capable catastrophic results at the infrastructure because of any of the herbal or synthetic inflicted surroundings dangers which include flood, tremors, earthquakes, landslides, falling of trees, burning of bushes, etc. with the aim of using articulating smart reaction. Smart reaction, primarily based on environmental attention, is essentially executed with the aim of using sending suitable hazard alert primarily based on acquired records and imparting change feeder for essential infrastructure in such emergencies. GIS, primarily based on instant records, is fundamental on this evaluation specially in terms of herbal screw ups forecast and evaluation, that is utilized in figuring out environmental threats alert [6].
- *Government regulatory policies and implementation*—As there are opportunities in SGs technologies and services; the conventional utility is facing challenges all due to the requirement of new technologies, policies, increasing demands, and business models involved in upgrading to SGs era. Therefore, governments' collaboration in providing requisite regulatory policies to aid smooth market operations and private sector mobilizations is the key for achieving the set objective of SG deployment. Government has a deep role to play in the areas of investing in research and development [34].

2.5.2 Attack Detection and Counter- Measures

The power grid due to complexity community is at risk of physical attacks. With the smart grid, greater infrastructures are needed for safety in opposition to attackers. Physical safety of power plants, equipment, and community is needed, inclusive of barriers, locks, and video surveillance. Working non-public safety awareness, screening, and schooling also are required measures to save assaults. The worst type of assaults to the SG is the denial of service (DoS) assault, due the impossibility to get right of entry to the gadgets and systems. To come across this assault, four techniques may be used: packet-primarily based, sign-primarily based, proactive, and hybrid. The sign-primarily based detection approach includes measuring the sign strength, evaluating it to a threshold value and elevating an alarm while deviations occur. Packet-primarily based detection approach measures the transmission consequences of every packet. It works by assuming that overall performance degradation is resulting from packet transmission failure, indicating a DoS assault.

The proactive approach tries to become aware of DoS assaults by sending probing packets to check or degree the repute of capacity attackers. Lastly, the hybrid approach combines specific thoughts to enhance assault detection accuracy. For instance, sign-primarily based and packet-primarily based techniques may be utilized in Wi-Fi community to become aware of flooding or jamming assaults. To keep away from cyber assaults on SG there also are cryptographic approach to reap steady communication and statistics safety for any statistics system. Several stages of encryption are preferred because of the restricted computational sources in SG layers. All SG gadgets require an authentication manner to keep away from impersonation assaults. Lastly, key control is primarily based totally on cryptographic primitives and makes use of a public key infrastructure (PKI) to manage strength substations community or AMI community. Key control the usage of a PKI is mentioned as one of the handiest answer for securing the SG communications infrastructure [34].

2.6 Cyber Security a Challenge for Smart Grid

The SG system is a complex system for exchanging the information of an electrical infrastructure. To establish an uninterruptible and secure operation, the understanding of security requirements before providing a complete analysis of cyber security in the context of managing and distributing energy. Here, the need of cyber security in SG is described [41].

2.6.1 Cyber Security Model

Cyber security infrastructure has three main objectives: availability, integrity, and confidentiality, i.e., power availability with information integrity and customer's information confidentiality [39].

Availability: It is the most important basis for SG system. It aims to provide an uninterruptible power supply to the consumer for matching the requirements of the customer.

Confidentiality: The grid infrastructure is responsible for the security of users' data. If the data is not secured, enough informative data will be available for the attacker.

Integrity: The data or information received from the user end should be validated. The network ensures that the data is not altered. Also, authenticity of source is ensured [19].

2.6.2 SCADA System

The cyber communications of SG include communication systems, the electronic information, and services along with the data enclosed in these systems, infrastructure. This involves hardware and software systems information. It basically process, store, and communicate data. SCADA is used for this purpose acts as a control system. The SCADA is also a neutral system [19].

The main blocks of SCADA system are: Human machine interface (HMI) for presenting the processed data, a supervisory computer for collecting the data and using it for the function of processing, remote terminal units (RTUs), programmable logic controller, communication infrastructure [9].

By using the power system communication in the smart grid, the SCADA system connects to other systems like the Internet or by certain dedicated lines. The vendors are using off the shelf products as element of the SCADA systems. These products are similar to the personal computers, and thus are vulnerable to different threats [36].

A SCADA system is an essential element in the grid communications. It is used for two purposes; first the public transport system and second the public control system [19].

2.6.3 Cryptograph

Cryptography is used to secure information for the purpose of cyber-security. It is one of the most trusted and secures exchange of data. In the methodology of cryptography, the design should be robust and the algorithm should be error free.

2.6.4 *Constraints*

2.6.4.1 Computational Constraints

Residential meters have a few boundaries on the subject of computational strength and the cap potential to shop cryptographic materials. The destiny gadgets should have the fundamental cryptographic abilities such as the cap potential to aid symmetric ciphers for authentication. The use of low-cost hardware with embedded cryptography is vital, however, now no longer good enough for the success of excessive availability, integrity, and secrecy within side the SG.

2.6.4.2 Channel Bandwidth

The SG communications take place over different channels having different bandwidths. Advanced encryption standard (AES) is a cipher, which produces the equal number of output bits as input bits. These bits cannot be compressed, since they are random in nature and is encrypted. For compressing this data, we have to compress before encryption. Another factor of concern is the cipher-based message authentication code (CMAC), which is added as a fixed overhead to a message and is usually 64 bits or 96 bits. These overheads are considered important when we are dealing with short messages, since they need large channel bandwidth [19].

2.6.4.3 Connectivity

Standard public key infrastructure-primarily based on peer-to-peer key status quo version, where in any peer may also want to talk with another, is not always applicable from safety factor of view for components. Many gadgets do now no longer incorporate with key server connectivity, online certificates status, certificates authorities, and protocol servers. Many connections among SG gadgets may have longer length than ordinary net connection [19].

2.6.5 *General Cryptographic Issues*

Entropy. An excellent source of entropy is necessary to generate cryptographic solution for creating randomness that is not available for many devices. It is solved by seeding a deterministic random bit generator (RBG) before distributing any key.

Cipher Suite. It is open and is important to establish a secure network connection via transport layer security (TLS). It ensures a secure communication between users and servers by using different algorithms and protocols.

Key Management Issues. Security protocols are dependent on security relations. There are two types for the authentication of security:

- Using secret key
- Using certificate authority

For using secret keys, it is necessary that the keys are transported from one device to another. For the transportation of these keys, a kind key is required for all the communicating devices that should be well coordinated.

Elliptic Curve Cryptography. A Cryptographic interoperability strategy (CIS) is started by National Security Agency (NSA) for government organization by selecting standard cryptography methodology. It incorporates with AES for encryption with 128 or 256 bits. A periodic upgradation of the protection modules is very necessary [19].

2.7 Conclusions

This paper has described about various aspect of IoT in SG and various SG security protocols and challenges. IoT can be considered as the main part of the existing Internet and its future direction relies on its upgradation and improvement. The application of the IoT in grid system includes power equipment installation surveillance, parking and charging of electric vehicles, application of dynamic scheduling for adjustment of home consumption, management of supply and demand of power, equipment maintenance, failure and fault detection. With the application of suitable models, proper verification, analytic stimulation and optimization tools, the network system can adapt to different challenges and it is important that proper care is taken in both operational stage as well as planning for a secured, robust and flexible grid optimization. So that it could respond to threats, source of such threats, also the nature of the threats for proper preventive response, monitoring and control, even before the threat is manifested. The development of SG infrastructure has resulted to reconciling targets for climate change, energy, and safety of the grid. Cyber security is an important aspect in grid security point of view. As the grid develops the number of nodes that will be not susceptible to cyber-attacks. Domain architecture for explaining these challenges has been described in one of the section. Cryptography and key management techniques are used for a secure system against cyber-attacks. We have covered the constraints for cryptography.

Future work may deal in providing models for tracking SG security threats by source classification for the desired resiliency as well as developing a robust simulation tool for threats sensing and response, for a stabilized system. Also researcher will focus on addressing challenges like energy acquisition, congestion, data communication, identify spoofing, and so on.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols and applications. IEEE Commun. Surveys Tutorials **17**(4), 2347–2376 (2015)
2. Ali, Q., Montenegro, S.: Explicit model following distributed control scheme for formation flying of mini UAVs. Dig. Object Identifier **4**, 397–406 (2016)
3. Amin, S.M., Wollenberg, B.F.: Toward a smart grid. IEEE Power Energ. Mag. 34–41 (2005)
4. Arefifar, S.A., Mohamed, Y.A.I., EL-Fouly, T.H.M.: Comprehensive operational planning framework for self-healing control actions in smart distribution grids. IEEE Trans. Power Syst. **28**(4), 4192–4200 (2013)
5. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**, 2787–2805 (2010)
6. AyyoobSharifi, A., Yoshiki Yamagata, Y.: Principles and criteria for assessing urban energy resilience: a literature review. Renew. Sustain. Energ. Rev. **60**, 1654–1677 (2016)
7. Bekara, C.: Security issues and challenges for the IoT-based smart grid. In: International Workshop on Communicating Objects and Machine to Machine for Mission Critical Applications (COMMCA-2104). Procedia Comput. Sci. **34**, 532–537 (2014)
8. Bibri, S.E.: The IoT for smart sustainable cities of the future: an analytical framework for sensor-based big data applications for environmental sustainability. Sustain. Cities Soc. **38**, 230–253 (2018)
9. Boroomand, F., Fereidunian, A., Zamani, M.A., Amozegar, M., Jamalabadi, H.R., Nasrollahi, H., Moghimi, M., Lesani, H., Lucas, C.: Cyber security for smart grid: a human-automation interaction framework. In: Paper published in IEEE PES Innovative Smart Grid Technologies Conference, Europe, 11–13 October 2010
10. Broll, G., Paolucci, M., Wagner, M., Rukzio, E., Schmidt, A., Hubmann, H.: Perci: pervasive service interaction with the internet of things. Internet Things Track **13**(6), 74–81 (2009)
11. Coenen, S., Tenbohlen, S.: Location of PD sources in power transformers by UHF and acoustic measurements. IEEE Trans. Dielectr. Electr. Insul. **19**(6), 1934–1940 (2012)
12. Dada, A., Thiesse, F.: Sensor applications in the supply chain: the example of quality-based issuing of perishables. In: The Internet of Things Lecture Notes in Computer Science, vol. 4952, pp. 140–154
13. Delgado-Gomes, V., Martins, J.F., Lima, C., Borza, P.N.: Smart grid security issues. In: Published in 9th International Conference on Compatibility and Power Electronics, 24–26 June 2015
14. Divakar, P.P., Lakshmi, G.V., Devi, L.: Applications of internet of things on smart grid. IOP Conf. Ser. Mater. Sci. Eng. (2020)
15. Ghasempour, A.: Internet of things in smart grid: architecture, applications, services, key technologies, and challenges. Inventions **4**(1), 22–33 (2019)
16. Goel, S., Hong, Y.: Security challenges in smart grid implementation. In: Smart Grid Security, pp. 1–39. Springer Briefs in Cyber Security (2015)
17. Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J.: Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid. IEEE Internet Things J. **4**(6), 1934–1944 (2015)
18. Ilic, A., Staake, T., Fleisch, E.: Using sensor information to reduce the carbon footprint of perishable goods. IEEE Pervasive Comput. **8**(1), 22–29 (2009)
19. Iyer, S.: Cyber security for smart grid, cryptography, and privacy. Int. J. Dig. Multimedia Broadcast. (2011)
20. Jaradat, M., Jarrah, M., Bousselham, A., Jararweh, Y., Al-Ayyoub, M.: The internet of energy: smart sensor networks and big data management for smart grid. Procedia Comput. Sci. **56**, 592–597 (2015)
21. Kabalci, E., Kabalci, Y.: Internet of things for smart grid application. In: From Smart Grid to Internet of Things, pp. 249–307 (2019)

22. Karpischek, S., Michahelles, F., Resatsch, F., Fleisch, E.: Mobile sales assistant an NFC-based product information system for retailers. In: First International Workshop on Near Field Communication, 24–24 February 2009, pp. 20–23
23. Keyhani, A., Chatterjee, A.: Automatic generation control structure for smart power grids. IEEE Trans. Smart Grid **3**(3), 1310–1316 (2012)
24. Lee, A., Brewer, T.: Smart grid cyber security strategy and requirements. In: Advanced Security Acceleration Project—Smart Grid (2009)
25. Li, B., Lv, S., Pan, Q.: The internet of things and smart grid. In: Published in 3rd International Conference on Advances in Energy Resources and Environmental Engineering, Harbin, China, 8–10 December 2013
26. Li, F., Luo, B., Liu, P.: Secure and privacy-preserving information aggregation for smart grids. Int. J. Sec. Netw. **6**(1), 28–39 (2011)
27. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A Survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
28. Manoj, P., Kumar, Y.B., Gowtham, M., Vishwas, D.B., Ajay, A.V.: Internet of Things for smart grid applications. In: Advances in Smart Grid Power System Network, Control and Society, pp. 159–190 (2021)
29. Mattern, F., Floerkemeier, C.: From the internet of computers to the internet of things. In: Active Data Management to Event-based Systems and More, vol. 6462, pp. 242–259 (2010)
30. Mehrtash, A., Wang, P., Goel, L.: Reliability evaluation of power systems considering restructuring and renewable generators. IEEE Trans. Power Syst. **27**(1), 243–250 (2012)
31. Mrabet, Z.E., Kaabouch, N., Ghazi, H.E., Ghazi, H.E.: Cyber-security in smart grid: survey and challenges. Comput. Electr. Eng. **67**, 469–482 (2018)
32. Mugunthan, S.R., Vijayakumar, T.: Review on IoT based smart grid architecture implementations. J. Electr. Eng. Autom. (EEA) **1**(1), 12–20 (2019)
33. Nandish, B.M., Pushparajesh, V., Girish, V.: Review of internet of things in smart grid. Int. J. Adv. Sci. Technol. **29**(08), 2301–2306 (2020)
34. Otuoze, A.O., Mustafa, M.W., Larik, R.M.: Smart grids security challenges: classification by sources of threats. J. Electr. Syst. Inform. Technol. **5**, 468–483 (2018)
35. Ou, Q., Zhen, Y., Li, X., Zhang, Y., Zeng, L.: Application of internet of things in smart grid power transmission. In: Published in 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, 26–28 June 2012
36. Rawat, D.B., Bajracharya, C.: Cyber security for smart grid systems: status, challenges and perspectives. In: Paper published in Proceedings of the IEEE Southeast Conference, 9–12 April 2015
37. Ray, P.P.: A survey on internet of things architectures. J. King Saud Univ. Comput. Inform. Sci. **30**(3), 291–319 (2018)
38. Ribeiro, I.C.G., Albuquerque, C., de Rocha, A.A.A., Passos, D.: THOR: a framework to build an advanced metering infrastructure resilient to DAP failures in smart grids. Future Gener. Comput. Syst. **99**, 11–26 (2019)
39. Shafiullah, G.M., Oo, M.T., Amanullah, A., Shawkat, A.B.M., Wolfs, P.: Smart grid for a sustainable future. Smart Grid Renew. Energ. **4**(1), 23–34 (2013)
40. Tsolakis, A.C., Moschos, I., Votis, K., Ioannidis, D., Dimitrios, T., Pandey, P., Katsikas, S., Kotsakis, E., García-Castro, R.: A secured and trusted demand response system based on blockchain technologies. In: Published in Innovations in Intelligent Systems and Applications (INISTA), 3–5 July 2018
41. Wang, W., Lu, Z.: Cyber security in the smart grid: survey and challenges. Comput. Netw. **57**, 1344–1371 (2013)
42. Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., Borriello, G.: Building the internet of things using RFID the RFID ecosystem experience. Internet Things Track **13**(3), 48–55 (2009)
43. Wortmann, F., Fluchter, K.: Internet of things technology and value added. Bus. Inform. Syst. Eng. **57**, 221–224 (2015)

44. Xia, F., Yang, L.T., Wang, L., Vinel, A.: Internet of things. Int. J. Commun. Syst. **25**, 1101–1102 (2012)
45. Zanella, A., Vangelista, L.: Internet of things for smart cities. IEEE Internet Things J. **1**(1), 22–32 (2014)
46. Zhang, P., Li, W., Li, S., Wang, Y., Xiao, W.: Reliability assessment of photovoltaic power systems: review of current status and future perspectives. Appl. Energ. **104**, 822–833 (2013)