IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 23, 2021, accepted March 7, 2021, date of publication March 19, 2021, date of current version April 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3067331

IoT-Enabled Smart Energy Grid: Applications and Challenges

S. M. ABU ADNAN ABIR[1], ADNAN ANWAR[2], (Member, IEEE), JINHO CHOI[3], (Senior Member, IEEE), AND A. S. M. KAYES[4]

[1]IGW Operators Forum, Dhaka 1212, Bangladesh
[2]Centre for Cyber Security Research and Innovation (CSRI), School of Information Technology, Deakin University, Geelong, VIC 3216, Australia
[3]School of Information Technology, Deakin University, Geelong, VIC 3216, Australia
[4]Department of Computer Science and Information Technology, La Trobe University, Melbourne, VIC 3086, Australia

Corresponding author: Adnan Anwar (adnan.anwar@deakin.edu.au)

ABSTRACT The Internet of Things (IoT) is a rapidly emerging field of technologies that delivers numerous cutting-edge solutions in various domains including the critical infrastructures. Thanks to the IoT, the conventional power system network can be transformed into an effective and smarter energy grid. In this article, we review the architecture and functionalities of IoT-enabled smart energy grid systems. Specifically, we focus on different IoT technologies including sensing, communication, computing technologies, and their standards in relation to smart energy grid. This article also presents a comprehensive overview of existing studies on IoT applications to the smart grid system. Based on recent surveys and literature, we observe that the security vulnerabilities related to IoT technologies have been attributed as one of the major concerns of IoT-enabled energy systems. Therefore, we review the existing threat and attack models for IoT-enabled energy systems and summarize mitigation techniques for those security vulnerabilities. Finally, we highlight how advanced technologies (e.g., blockchain, machine learning, and artificial intelligence) can complement IoT-enabled energy systems to be more resilient and secure and overcome the existing difficulties so that they become more effective, robust, and reliable in operation. Precisely, this article will help understand the framework for IoT-enabled smart energy system, associated security vulnerabilities, and prospects of advanced technologies to improve the effectiveness of smart energy systems.

INDEX TERMS Cybersecurity, IoT, smart grid, smart meter.

I. INTRODUCTION

Electricity is considered to be the heart of modern social and economic development. Advances in technology tempted us to use electricity-driven elements in every aspect of our life from commercial to domestic sector for shaping our lives to be more comfortable. However new challenges have arisen where further investigation is necessary on how to manage the supply-demand balance of electricity more effectively, securely and reliably along with ensuring a coordinated multi-way communication for better monitoring and control of the network and user assets. Faster, fuel-efficient and eco-friendly electric transport and smart home setup have become more available and affordable. The Internet of Things (IoT) is a rapidly emerging field of technologies that delivers numerous cutting-edge solutions in various application domains [1]. IoT can resolve those unavoidable challenges by transforming conventional energy grids into modernized Smart Energy Grid system [2], [3].

The IoT-enabled Smart Energy Grid system equipped with intelligent two-way data communication can significantly improve the operation and control of the traditional energy grid system. These improvements address the reliability, flexibility, efficiency of the conventional grid system. In a smart grid environment, the system must provide services including the large-scale integration of distributed renewable energy resources, establishment of live, real-time data communication between consumers and service providers regarding tariff information and energy consumption, facility to collect and transfer statistics of system parameters for analysis and infrastructure to implement necessary actions based on those analyses. Smart Energy grid generates immense data and information that needs to be transferred, processed and stored for intelligent decision making and processing. In this

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

situation, the IoT has appeared to be an empowering set of technologies for the smart energy grid system with substantial perspective due to its multi-dimensional advantages in various sectors [5]. The IoT integration introduces extra precision and competence by the means of intelligent and proactive features and converts the traditional legacy power grid into an efficient smart energy grid [2]–[4].

The big challenges of conventional power grid system are related to the power quality and reliability, which can be resolved with the assistance of Internet of Things (IoT) by providing enhanced management of these challenges [6], [7]. Advanced Metering Infrastructure (AMI) assisted with Smart Metering (SM) technologies can facilitate the transformation of conventional power grid system to a smart grid system by introducing intelligent information processing features during the electricity flow between the service provider and consumers [8], [33], [35]. The IoT delivers great prospective for improving and governing energy consumption through the incorporation of sensing and actuation systems in the AMI [12]. This integrated system gathers a huge amount of data and information regarding different aspects of the grid system such as energy consumption, voltage reading, current reading, phase measurement, etc. The cutting-edge technologies of IoT can trim down those huge data, transmit and process those data in an intelligent manner to achieve effective management of the energy grid system.

IoT technologies can bring significant impacts in numerous field of Smart Energy grid System that includes power generation infrastructure management, SCADA connected system for managing transmission and distribution operation, advanced metering infrastructure, carbon footprint and environmental monitoring, smart home and smart building system and so on. Fog computing based advanced edge computing technology can ensure a local monitoring and control of distributed energy resources and may provide solutions to the cyber vulnerabilities of the traditional centralized SCADA system [15]. The smart home and smart building integrate sensing, data storage, network adaptability, and computing abilities into a household or building elements such as bulb, power outlet, air conditioner, door, window, gas & smoke detector etc. As a result, these elements can be connected in a network via which they can be accessed and controlled from a remote location over the internet [20]. Although IoT has enabled a much improved and efficient energy system monitoring and operation, the deployment of IoT technology also poses some challenges. For example, within IoT framework, cyber-adversaries can initiate cyber-attacks which can bring severe damage like a significant power outage, social security threats, and massive business loss for the utility providers and less severe damages like localize outage or physical damage on consumer end devices [36]. IoT based security vulnerabilities include manipulating energy data analysis [49], energy theft [52], interrupting the process of transactive energy system [53] and energy market [55]. Potential technologies such as blockchain mechanism [10], [58], [67], machine learning and artificial intelligence [56], [71] can be used to encounter those challenges as well as operate the Smart Energy Grid system more efficiently.

A. RESEARCH MOTIVATION AND CONTRIBUTION

The motivation of this survey comes from the recent advances on IoT-enabled Smart Energy Grid system. IoT provides the necessary structure and protocols for sensing, actuating, communication and processing technologies essential for the Smart Energy system. The rapidly growing technological advancements in different sectors of IoT create new opportunities for the smooth operation of the Smart Energy Grid system. This paper will help potential researchers and stakeholders of this sector to understand the architecture of IoT-enabled smart grid system, as well as the different applications of IoT technologies, security vulnerabilities, mitigation of those vulnerabilities and potentials of advanced technologies for smart energy system.

The key contributions of this study are listed as follows:

- We critically review existing survey papers and present key functionalities of the IoT-enabled smart energy grid system. We have highlighted the key technological advancements and compared the essential functionalities of the energy system based on a wide selection of recent surveys and technical works (see Table 1). We illustrate the architecture and technologies of IoT and related software parameters and standards for energy system operation.
- We have analysed and categorized energy grid IoT security vulnerabilities in details and discussed mitigation techniques. Specifically, we focus on how a cyber adversary can take advantage of IoT system vulnerabilities and launch malicious attacks that can compromise the IoT energy system security. Attacks we have explored include energy theft in smart meter data, injection attacks in the IoT home automation system, denial-of-service (DoS) attacks on IoT data analytic, manipulations attacks on transactive energy systems and electricity market, etc. Finally, we review prospective solutions to reduce the threat level, device level vulnerabilities and investigate potential lightweight intrusion detection mechanisms for IoT systems.
- We discuss the prospects of blockchain-based distributed ledger technologies for the end energy users. We highlight how to ensure data privacy during peer-to-peer energy trading and information exchanging. Emerging machine learning technologies for IoT-enabled energy systems have also been discussed to explore the possible opportunities and applications within an IoT-environment.

The organization of the paper is exhibited in figure 1. As illustrated in the figure, motivation towards the adoption of IoT technologies in a smart grid is presented in Section II. A brief description of IoT technologies is presented in Section III, where IoT architecture, software stack, standards and protocols are also summarized. Application

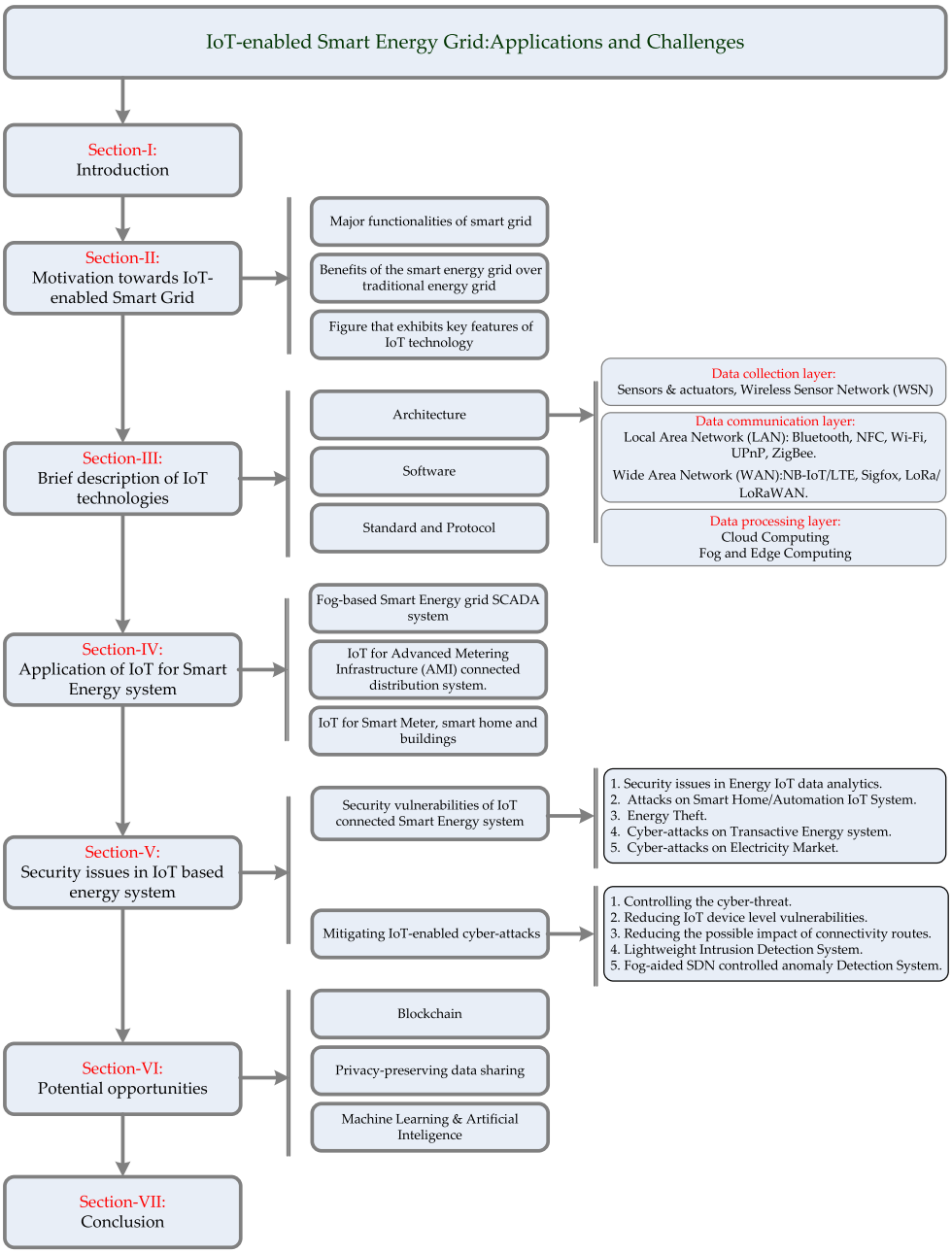

FIGURE 1. **This figure exhibits the organization of this paper.**

of the IoT-enabled smart energy system is presented in Section IV. In this section, the applications have been categorized based on high voltage SCADA system, low voltage AMI system and finally smart home/building level applications. The security aspects of IoT-enabled smart grid are addressed in Section V. Here, both the security vulnerabilities and their mitigation approaches are presented. Section VI demonstrates some potential futuristic research opportunities considering blockchain, privacy-preserving data sharing, and advanced data science and artificial intelligence techniques. Finally, the paper concludes with some brief remarks in Section VII.

B. COMPARISON WITH EXISTING WORKS

Existing review and survey papers on technologies and applications of IoT are compared in Table 1. In the table, we highlighted and compared the essential technologies and functionalities of an IoT-enabled smart energy system based on the existing surveys and literature. We compared how different researches addressed the communication, computing and sensing technologies. We also classified the research works based on their application in the physical energy systems, e.g., whether authors considered the SCADA system, or Advanced Metering Infrastructure or Smart Home. We also compared how emerging technologies

TABLE 1. Comparison with existing literature.

Articles	Type	Sensor technologies	Communication technologies	Computing technologies	Smart Meter/AMI	SCADA system	Cyber Attack	Privacy preservation	Machine Learning	Blockchain	Contribution
[8]	Survey	No	Yes	Yes	Yes	No	No	No	Yes	No	This paper studying the effectiveness of using Smart meter technologies in smart-grids with emphasis on power quality and dependability concerns.
[9]	Survey	No	Yes	Yes	No	No	Yes	No	No	No	This article presents a review of major technologies of IoT-based smart homes including computing technologies and software parameters.
[10]	Survey	No	Yes	Yes	No	No	No	No	No	Yes	This paper reviews existing smart home IoT automation architectures, and evaluates the applicability of blockchain mechanisms.
[12]	Survey	Yes	Yes	Yes	No	No	No	No	No	No	This paper reviews the sensor-based big data applications enabled by the IoT for environmental sustainability and related data processing platforms and computing.
[14]	Survey	No	Yes	Yes	No	No	No	No	No	No	This paper reviewed fog based computing system for smart homes.
[15]	Survey	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	This paper presents a comprehensive survey of existing cybersecurity solutions for fog-based smart grid SCADA systems.
[20]	Survey	No	Yes	Yes	No	No	No	No	No	No	This paper investigates the adoption of IoT for the development of smart buildings.
[28]	Survey	No	No	No	Yes	Yes	Yes	No	No	No	This paper reviewed and explored the major challenges and security issues that hinder the growth of IoT-based smart grid networks.
[29]	Survey	No	Yes	No	Yes	No	Yes	No	No	No	This paper highlights the most significant research works that focus on applying IoT to smart grids.
[36]	Survey	No	Yes	No	Yes	Yes	Yes	No	No	No	This paper survey IoT-enabled cyber-attacks found in different application domains.
[52]	Technical	No	No	No	Yes	Yes	Yes	No	Yes	No	This paper develops an energy detection system called smart energy theft system (SETS) based on machine learning and statistical models.
[56]	Technical	No	Yes	No	No	No	Yes	No	Yes	No	This paper develops a lightweight attack detection strategy utilizing a supervised machine learning-based support vector machine (SVM) to detect an adversary attempting to inject unnecessary data into the IoT network.
[57]	Technical	No	Yes	Yes	No	No	Yes	No	Yes	No	This paper proposes fog-assisted software-defined networking (SDN) driven intrusion detection/prevention system (IDPS) for IoT networks.
[58]	Survey	No	No	No	No	No	Yes	Yes	No	Yes	This paper discusses the privacy issues caused by the integration of blockchain in IoT applications, and the implementation of five privacy preservation strategies in blockchain-based IoT systems.
[67]	Technical	No	No	No	No	No	No	No	No	Yes	This paper proposes a secure Hybrid Industrial IoT framework using the Blockchain technique.
[68]	Technical	No	No	No	Yes	No	Yes	Yes	No	No	This paper considers smart meters as a prominent early instance of the IoT and investigate their privacy protection solutions at customer premises. In particular, it designs a load hiding approach that obscures household consumption with the help of energy storage units.
[69]	Technical	No	Yes	No	No	No	Yes	Yes	Yes	No	This paper addresses the traffic analysis attack to smart homes, where adversaries intercept the Internet traffic from/to the smart home gateway and profile residents' behaviors through digital traces and propose a privacy-preserving traffic obfuscation framework to achieve the goal.
[70]	Technical	No	Yes	No	No	No	No	Yes	No	No	This paper proposes an improved energy-efficient, secure, and privacy-preserving communication protocol.
[71]	Survey	No	No	No	No	No	Yes	No	Yes	No	The objective of this review is to explore the role of artificial intelligence (AI), machine learning (ML), and deep reinforcement learning (DRL) in the evolution of smart cities.
This Paper	Survey	Section-III	SEC-III	SEC-III,IV, V	SEC-IV	SEC-IV	SEC-II,V	SEC-VI	SEC-VI	SEC-VI	This survey is focused on IoT technologies that facilitate the Smart Energy Grid system, includes architecture, related software, standard, applications, security vulnerabilities and opportunities to integrate advanced techniques.

like blockchain, privacy-preserving data sharing and machine learning has been addressed in the existing surveys and literature. Detailed discussion and review are presented in the following sections and subsections.

II. MOTIVATION TOWARDS IoT-ENABLED SMART GRID

Smart grid is the modernized power grid equipped with bi-directional communication capability, the capacity to coordinate information and utilize analytics for an entirely

TABLE 2. Benefits of the smart energy grid over traditional energy grid [30].

Features	Traditional power grid	Smart grid
Communication	One-way and local two way communication	Fully two-way communication with interaction
Power generation	Centralized	Distributed generation, provide support during peak hours when load increases
Topology	Radial	Network
Operation & Maintenance	Manual monitoring, Periodic equipment maintenance	Remote real-time monitoring, prognostic and event-driven maintenance
Power restoration	Manual equipment check, time based maintenance	Self-healing, smart grid can anticipate, identify and respond to faults or outages
Reliability	Prone to failure and cascading outages	Pro-active, real-time protection and islanding
Metering	Electro-mechanical	Advanced metering arrangement that delivers the facility to track and regulate energy consumption
Customer participation	None or limited interaction	Extensive interaction
Power quality control	Less use of sensors, less power quality control	Contains numerous modules for example, sensors, smart meters and technologies on the distribution grid that aids managing the parameters such as voltage and power factor to improve the power quality.
Renewable power source integration	Optimized for non-renewable resources	Offer essential insights and enable automation for renewable power source to supply electricity onto the grids and optimize their use
Operational cost & wastage at peak hour	High at peak hour	Low at peak hour due to distributed generation and control over the power consumption

automated intelligent energy network. Table 2 exhibits some of the main benefits of smart energy grid as compared to the traditional energy grid [30].

Some of the major functionalities of smart grid are as follows [29]:

- Self-healing function that allows smart grid to analyze and identify the major fault in an intelligent way and react quickly.
- It provides an interactive platform to transfer information between the utility and consumers. Consumers have the control of their energy usage and selection of tariff.
- Major issues like cyber-attack and physical attack can be effortlessly resisted in smart power grid system.
- Smart power grid has the prospective to increase the power quality by maintaining a constant voltage with the better coordination of monitoring and control.
- Integration of non-conventional renewable power resources such as solar, wind etc.

IoT can bring a great solution to the recent challenges in transforming traditional power grid into a modernized smart grid [31]. For modern smart grid applications in residential and commercial buildings, adoption of the IoT technologies is gaining popularity. The implementation of sensors and smart metering in smart power grid will enable efficient operation in various stages of power generation, transmission and distribution issue which eventually solves most of the electricity industry challenges. Furthermore, it provides a smart option for the real-time monitoring of power flow throughout the electricity network. IoT, supported by enormous data analysis can assist with vital decision-making in relation to the power sources and end-user demand. Real-time insight analysis can influence new regulations from policy-makers and power generation service provider can react easily to market fluctuation on the similar grounds, which involves implementing a method of when to increase or when to decrease the production, thus elevating the energy efficiency. On the other hand, using these technologies enables the effective analysis of the collected and stored information for future state estimation. With the help of mobile devices enabled with IoT technology, end-user can monitor real-time energy prices and regulate their power uses effectively.

For self-healing function, an enormous number of sensors and actuators are integrated throughout the grid system from power generation to end users for collecting data or information of the system states. Those data sets need to be transferred to a control center for further processing and outcomes are presented to a utility provider or user for further actions. To achieve efficient self-healing, data collection and transmission of this huge amount of data should be accomplished in a coordinated manner without any significant delay. Interactive platforms to represent this data creates bridges between devices, consumers and utility providers. The network operators can monitor their system from those gathered information such as voltage reading, current reading, system states and phase angle measurement and regulate various elements of the grid on the basis of the variations of those parameters. As a result, power quality and reliability can be improved. Customers get information about their energy usage and bill so that they can adjust their usage according to electricity prices. This process also involves a huge amount of bi-directional data transmission between parties in an efficient and reliable manner. For the above discussed scenarios, IoT can play a significant role towards efficient grid automation and control.

Recently, cyber security has become a big factor for every Internet-enabled system as new threats arise which are difficult to counteract [19]. So it is important to make a mitigation plan for such cyber-attacks. This mitigation plan involves prevention and detection methods, including access control, communication encryption, authentication process, intrusion detection systems and so on together with huge data analysis and processing. Physical attacks can also be identified with the help of advanced sensing technologies and data analytics.

Compared to the conventional power grid, smart grid requires more robust intelligent infrastructure to process the enormous data and information effectively. It can become a hindrance to the deployment of the smart grid if an appropriate platform is not provided for bi-directional communication. In these circumstances, the IoT has appeared to be an empowering technologies for the smart energy grid system due to its multi-faceted advantages in various grounds. Figure 2 exhibits the key features of IoT technology, which can benefit the development of smart energy grid. The key features include scalability, heterogeneity, energy-efficiency, dynamic nature and its capability for distributed detection of cyber-attacks through edge computing. The IoT empowers end-devices with real-time operating systems to ease the constraints on huge data transfer requirements and enables powerful intelligent infrastructure to process those data efficiently through edge computing, while being close to the sensing source. IoT integration introduces extra precision and competence by the means of intelligent and proactive features and converts the traditional legacy power grid into an efficient smart energy grid [16].

FIGURE 2. This figure exhibits the key features of IoT technology.

III. A BRIEF DESCRIPTION OF IoT TECHNOLOGIES

In this section, we will discuss about the IoT system architecture which is comprised of various advanced cutting-edge technologies. The software and standard of the technologies will also be discussed in the following sections.

A. ARCHITECTURE

The architecture fully depends on the functionality of the corresponding IoT system, which is connecting components using diverse technologies located in different geographical locations. The architecture is usually distributed on a layer basis and different layers have different requirements [20]. In this paper, we demonstrated a three-layer architecture suitable for the integration to the smart power grid, as shown in figure 3. Such kind of three-layered architecture is more relevant from the application viewpoint of IoT, as well as compliance with the requirements of energy systems [20]. This three-layer of IoT architecture for smart grid consists of,

- Data collection layer,
- Data communication layer and
- Data processing layer.

The data or information collection layer is responsible for sensing and collecting records and information. The data communication layer controls the transportation of those information collected at the data collection layer. Data communication layer is the combination of various communication infrastructure, that's why it is the most vital part of this architecture. Finally, the data processing layer is the upper layer where data is processed and presented to end user and/or service provider. It also stores real-time data for forecast and other decision making.

Various cutting-edge technologies are available for each layer of this architecture [20]. Some key enabling technologies and the state-of-the art standards/protocols are deliberated in the following.

1) DATA COLLECTION LAYER

The data collection layer is in charge of collecting the information from the physical devices with the help of advanced sensing actuation technologies [20]. A sensor can be defined as an element that measures/detects a variation in physical condition or event such as heat, light, sound, pressure, magnetism, motion, etc. and then indicates or react by generating an electronic signal [12]. On the other hand, an actuator can be described as an element that converts an electrical gesture into the act or controls some external device, for example, movement. The output signal of the sensor could be converted to motion by actuator or show in any readable display or transmitted over the network for further processing [12]. This data collection layer is mostly supported by the following attributes:

Sensors and Actuators: The idea behind the 'smart' grid is that it will take action on real time data, to do so, it requires sensors to provide those real-time information. Data sensing process in smart energy grid involves sensing, detecting measures of various factors, for instance, voltage reading, current reading, temperature, phase and continuity measurement etc. Numerous elements of the grid are adjusted based on the variabilities of these parameters. On the other hand, data sensing in the smart home involves factors like temperature & heat, luminous level detection, smoke and gas detection, air quality, movement occupancy to regulate heating, ventilation and air conditioning system (HVAC), metering, security and safety.

Actuators are tools that get input as electrical signal from the energy management system and convert that signal in action and act on machines to control them. Actuators are

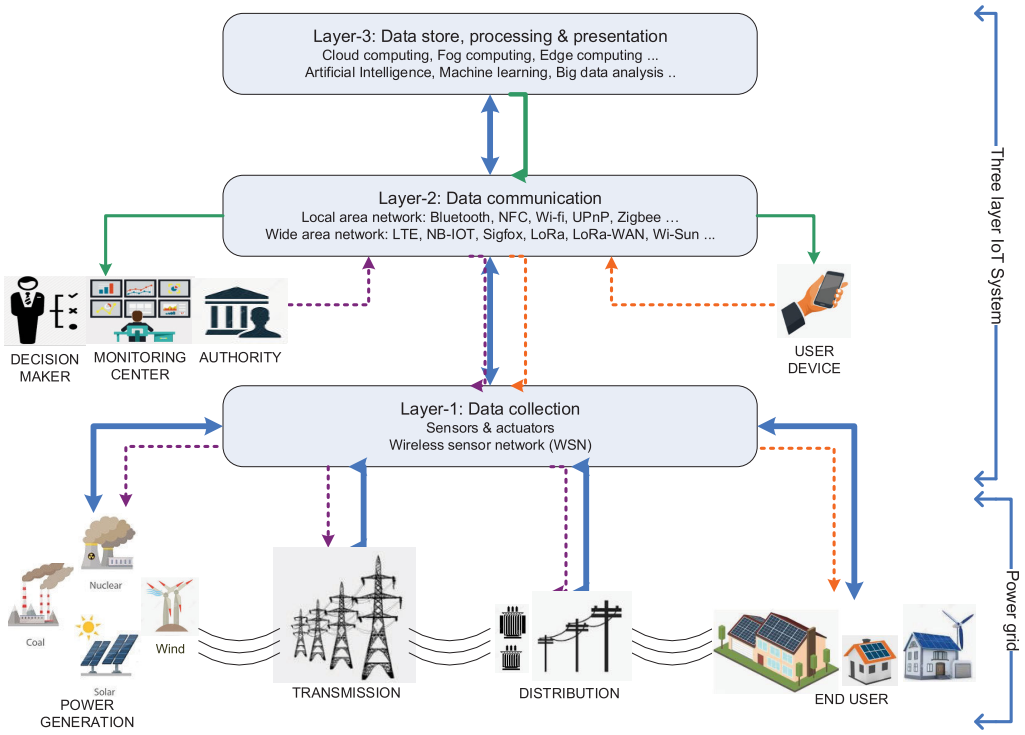

FIGURE 3. This figure shows the three-layer IoT architecture combined with the power grid. The figure is comprised with two-part, the upper part is the three-layer IoT system and the lower part is the power grid. The concept is partially adopted from [20].

classified based on their energy sources, below listed are the kinds of actuators based on the energy source to create motion [13]:

- Pneumatic actuators, they utilize compressed air for creating motion.
- Hydraulic actuators, this type of actuator utilizes hydraulic power to create motion.
- Thermal actuators, they convert thermal energy into kinetic energy, that is, they use heat to create motion.
- Electric actuators, this type of actuator use electricity to create motion, they use external energy source such as battery for the electricity.

Wireless Sensor Networks (WSN): A wireless sensor network (WSN) comprises a diverse class of sensing devices to monitor environmental or physical parameters and to transmit those data through the data communication channel to a remote location for further processing and actions. The scalable characteristics and dynamic reconfiguration features of WSN allow monitoring remotely using sensing and communication technologies among sensor nodes [20].

2) DATA COMMUNICATION LAYER

Data communication layer is responsible for transmitting the raw information or statistics that is acquired from data collection section and transfers them to a remotely located utility for further processing and actions [20]. This can be defined as network of gateway devices. This network can be divided into two main regions. The first is Local Area Network (LAN) which manages the communication between sensors & actuator devices with the local gateway devices at user/facilities end. The second region is the Wide area Network (WAN), which is responsible for transmitting those data from LAN to desired destinations for further processing [8]. For this data communication between networked systems, two types of technologies are used namely wired and wireless. As wireless technology comes with additional advantage over the wired technology in regards to the future expansion of IoT [20], we discuss some key wireless technologies in this paper.

Local Area Network (LAN): Major components of LAN includes:

Bluetooth: Bluetooth is the short distance communication technology for data transmission between devices over the air interface. Bluetooth 5.2 is the latest version of this technology which comes with new features mainly focused on IoT technology. Improved features of this version are Low-Energy (LE) power control, LE Isochronous channels, Enhanced Attribute Protocol (EATT), improved audio etc. The improved data transfer rate is up to 2Mbps and range is up to 240 meters. There are several types of Bluetooth based technologies: Bluetooth Low-Energy (LE), Bluetooth Basic-Rate/Enhanced-Data-Rate (BR/EDR) and Bluetooth Mesh [10]. For point-to-point communication as well as broadcast data in point-to-multipoint situation, power-efficient Bluetooth LE was introduced [10]. For communicating data over point-to-point connections between two devices, Bluetooth BR/EDR was designed. On the other hand Bluetooth Mesh was designed for

multipoint-to-multipoint connection between a relatively large number of Bluetooth devices.

NFC: Near-field communication (NFC) is a type of wireless technology for communicating between two power electronic devices over a short distance of 10 cm. NFC devices can be cast off as electronic-identity document and key-cards. NFC operates at 13.56MHz frequency with the data transmission rates from 106 kbps to 424 kbps. It is suitable for WSNs as it offers low-power and low-cost wireless connectivity [8].

Wi-Fi: For local-area-networking (LAN) between devices, Wireless Fidelity (Wi-Fi) is another communication technology that utilizes radio waves. Nowadays this technology is widely utilized in commercial and domestic entities in various devices like mobile phone, tablet, personal computers and many other daily devices. It uses the frequency of 2.4GHz Ultra High Frequency and 5GHz Super High Frequency ISM radio band in the domain of 0-250m at data transmission rate of 54Mbps. It provides the advantage of scalability with relatively higher rate of data transmission. It also provides security advantage with a robust authentication procedure. Recent developments in Wi-Fi technology can enable appropriate hardware to achieve the data transmission rate of up to 1Gbps. In a smart home environment, many smart electric appliances are adopting this technology for communication.

UPnP: Universal Plug and Play (UPnP) is another technology that allows different devices and access points in the network to seamlessly realize each other's existence and create serviceable way for data communication with zero knowledge of network resources configuration. UPnP was introduced by Microsoft in early 2000 and now supported by many vendors. This technology can be applied to control the small smart home appliances and devices like smart wall switches, dimmers, thermostats, outlets etc. but typically regarded as incompatible for utilization in commercial surroundings for the reason of economy, complexity and reliability [10]. However, recent development in this technology is done to support cloud connectivity and applications.

ZigBee: ZigBee is a cheap, power efficient, short-range improvised wireless networking technology designed for short-term communication of 0-100m with low energy intake as it has ability of creating wireless personal area networks (WPANs) with low-power digital radius and small footprint. Its data transmission rate is approximately 250 kbps on 2.4GHz frequency [24]. ZigBee supports star, mesh or cluster tree topology. There are three types of logical devices in a ZigBee network: Coordinator of the network, network router and end devices. The coordinator device is in charge of activating the networks, management and possession of all the nodes information and data in the network and it is essentially required for every ZigBee network to contain a network coordinator [25].

Wide Area Network (WAN): Major components of WAN includes:

NB-IoT/LTE: Narrow band Internet of Things (NB-IoT) is a Low Power WAN technology that uses a subset of the LTE standard with a single narrow-band window of 200 kHz. It was developed by 3GPP to enable a wide range of cellular services focused on indoor coverage with long battery life and high density of connected devices. Long-Term Evolution (LTE) is based on GSM/EDGE and UMTS/HSPA technologies for wireless broadband communication which increases the capacity and speed of communication using different radio interfaces and improved core network. LTE has been marked as 4G LTE and advanced 4G but it does not meet the 4G wireless service criteria. It is commonly referred as 3.95G and widely used in mobile phone communication industry. This technology has comparatively high power consumption for data transmission.

Sigfox: Sigfox is a narrow or ultra-narrow band technology that creates device to device WAN communication that covers 3-10 km in urban area and 30-50 km rural area with frequency band of 868 to 869 MHz and 902 to 928 MHz and data transfer rate of 100bps and 600bps depending on regions [26]. It uses binary phase-shift keying (BPSK) method for radio transmission. This technology has the advantage of low power consumption for data transmission as compared to NB-IoT technology as well as overcome the short-range limitation of Wi-Fi technology [8].

LoRa/ LoRaWAN: LoRa is the short form of Long-Range, which is derived from Chirp-Spread-Spectrum (CSS) technology as a modulation technique of spread spectrum. This radio frequency technology has a long wireless range, and power-efficient platform that has turned out to be an effective technology for Internet of Things (IoT) networks. LoRa-WAN is a Low-Power Wide-Area-Networking (LPWAN) protocol which is based on LoRa Technology. LoRa-WAN utilizes the unlicensed radio spectrum of the Industrial, Scientific and Medical (ISM) band. This technology operates in different frequency bands in different regions, 915 MHz in USA, 868 MHz in Europe and 865 to 867 MHz, 920 to 923 MHz in Asia. LoRaWAN technology has maximum data transmission rate of 27 kbps using LoRa and 50 kbps using FSK with coverage of 2-5 km in city areas and 10-15 km in countryside areas [27]. Combination of LoRa devices with LoRaWAN protocol empowers smart IoT applications that resolves some of the major obstacles such as energy-management, infrastructure efficiency and more.

3) DATA PROCESSING LAYER

This layer comprises a number of functional modules of the IoT system which operates the task of data management, processing and acts as the primary interface for the users to provide necessary analysis for decision-making tasks. In this layer, artificial intelligence such as predictive analysis, machine learning, computer vision can be used for advanced data analysis. Thus, this segment represents some widely used technologies that contribute to different areas for the purpose of information/data processing and analysis [20].

Cloud Computing: Cloud computing is the on-demand availability of computer system resources such as servers, storage, virtualization, and networking, which allows businesses to build and manage their own applications, data, and

operating systems. Cloud computing is very essential for enabling universal, appropriate, on-demand network access to a distributed group of configurable computing resources such as networks, servers, storage, applications and services, which can be automatically provisioned and released with negligible efforts from service providers. The cloud is commonly used to describe data centers distributed over multiple geographical locations being available to many users over the internet. The cloud technology provides massive data storing facility and highly reliable, scalable and autonomous processing arrangement [9]. In the IoT system, this cloud is utilized for the purpose of aggregating all statistics and information acquired from different elements such as sensors, appliances and other devices, then processing, analyzing and presenting the outcome to end users (consumer or service provider) for further insights.

Fog and Edge Computing:

Fog or Edge computing is a type of distributed computing model that gets data computation and storage closer to the end device with more improvement in response time and bandwidth usage with the capability of decision making. Edge computing advances the localized computation system by making the edge device capable of making a decision by locally processed data. Edge device can take action directly without further analysis from the cloud. Edge computing makes the system more decentralized and decreases the hazard of single-point failure, brings data analysis and decision making to the edge of the network [9].

The amount of IoT enabled entities increases network traffic as they need to transmit to the cloud for further processing and thus require additional bandwidth for the transmission. Therefore it becomes a bottleneck for the cloud based systems as fewer development (such as improving CPU processing power) has been done to increase the bandwidth of data transmission as compared to other technologies [9]. Fog or edge computing addresses this issue by performing computation and storing of data closer to the data generating source and sends the trimmed data to the cloud through the internet. In this way, fog computing reduces the amount of data sent to the cloud, improves the system response time and decreases the network latency. It also has an advantage of preventing single point of failure situation. If the communication link is broken, edge device will still collect and process the collected data from end devices and send them to cloud when the internet connection is resumed.

B. SOFTWARE PLATFORM

IoT software platform is a collection of components integrated with micro-controller-unit (MCU) that is operating over diverse communication technologies. There are two types of devices that are incorporated with this operating system: end-devices and gateways [9].

End devices with MCU can support short-range low power communication protocol and are highly energy efficient. Nowadays MCU has become more complex and powerful that creates opportunities for more features and security for the end devices. As those end devices are resource constrained, data collection and transmission process should be done simultaneously without any buffering, this type of operating-system is called real-time operating system (RTOS) that enables devices to be more productive [9].

Gateway devices are responsible for connecting many IoT enabled end devices with the cloud for data communication, so these devices need to run on more powerful, more protected and robust operating system that can support different communication protocols and secure the network from external attacks. Some example of real-time IoT operating systems are RIOT, FreeRTOS, Nano-RK, LiteOS, Apache Mynewt, Zephyr OS, WindRiver VxWorks, Nucleus RTOS, ExpressLogic ThreadX [9].

C. STANDARD AND PROTOCOL

The standard of data collection layer depends on the devices that are used in that layer. There are so many types of sensors and manufacturers of devices that a number of standards are created by world-wide organisations like ISO, IEC, IEEE. For example, in case of RFID, ISO 18047 standard is used for equipment performance testing, ISO 15459 explains the identification of specific transportation product [21], ISO 18000 for goods tracking, ISO 11784 regulates the RFID data structure used in animal tracking [22]. The Sensor Network Reference Architecture (SNRA) for WSN is defined in ISO/IED 29182 [23]. IEEE802.15.4 represents the communication standard, IEEE 802.15 is the working group for short-range communication [20].

The IEEE standardized Bluetooth is IEEE 802.15.1, but now it is maintained by the Bluetooth special interest group (SIG). NFC is standardized in ECMA-340 and ISO/IEC 18092. Wi-Fi is standardized under IEEE 802.11. The full list of Wi-Fi standards are 802.11a, 802.11b, 802.11g, 802.11n (Wi-Fi 4), 802.11h, 802.11i, 802.11-2007, 802.11-2012, 802.11ac (Wi-Fi 5), 802.11ad, 802.11af, 802.11-2016, 802.11ah, 802.11ai, 802.11aj, 802.11aq, 802.11ax (Wi-Fi 6), 802.11ay. UPnP is now standardized by the Open Connectivity Foundation (OCF) and OCF 1.0 specification has been ratified as an International Standard ISO/IEC 30118. ZigBee is developed according to the IEEE 802.15.4 standard.

The data communication must follow the protocols which are compatible with the IoT system. These protocols are standardized by groups such as IEEE, ETSI, IETF, etc. and widely accepted by the industry. Among that diversity of running protocols, frequently utilized ones are, IPV6, hyper text transfer protocol (HTTP), Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) etc.

IV. APPLICATION OF IoT FOR SMART ENERGY SYSTEM

IoT has potential applications in various areas of Smart Energy System, including power generation infrastructure management, SCADA connected transmission system, advanced metering infrastructure in the distribution system, pollution and environmental monitoring, smart home and

smart building system, etc. Advanced cutting-edge technology of IoT such as fog computing provides huge possibilities for optimizing and managing the SCADA energy transmission system. In recent years, smart home appliances are automated entirely based on Internet of Things (IoT) technology. In this section, we will discuss some of the applications of IoT technology that supports a smarter energy system.

A. FOG OR EDGE NODE-BASED SCADA SYSTEM

The Supervisory Control and Data Acquisition (SCADA) systems are vital for controlling and supervising the electrical energy generation, transmission and distribution systems [15]. The SCADA system collects data and information from the energy grid system and supervising automation procedure to control and regulate different system parameters to run the operation efficiently. The SCADA system has become more efficient with the incorporation of IoT technology such as Fog Computing [17]. The fog-based smart energy grid SCADA system comprises of four major part [15],

- End or terminal devices
- Fog computing devices
- Cloud
- SCADA system

End or terminal devices includes different types of IoT enabled sensors, actuators, appliances which use Wireless Sensor Network (WSN) technology to interconnect with each other for efficient communication. For effective communication among the fog network devices, Wi-Fi, Bluetooth, ZigBee technologies are used.

In the IoT-enabled SCADA system, fog or edge computing devices are comprised of various network devices such as access point, switches, routers to analyze and process a huge amount of data generated from the end or terminal devices [18]. Cloud part is comprised of a cloud data centers, cloud storage and gateway devices located in different geographical locations. These cloud data centres are responsible for aggregating and processing all statistics and information acquired from the field sensors of the SCADA system.

The SCADA interface system includes SCADA Client and SCADA Server. This part is responsible for gathering and analyzing the outcome from cloud analysis. Based on those results, an automated process or system operator takes control decision and regulate different parameters of the energy grid.

The overall architecture of the IoT-based smart energy grid SCADA system is presented in Figure 4.

B. IoT FOR AMI CONNECTED DISTRIBUTION SYSTEM

The advanced metering infrastructure (AMI) is an architecture for programmed, bi-directional communication between the consumer smart meter (having an IP address for communication), and service provider. The objective of an AMI is to deliver real-time statistics regarding power consumption to the utility service providers. It is expected that in near future AMI will let the consumers make up-to-date selections about energy usages based on the real-time tariff. Figure 5 exhibits the schematic representation of AMI [35].

IoT based AMI offers boundless prospective for optimizing and managing of energy consumption via efficient smart meter communication [16]. AMI includes various types of appliances (lights, fans, switches, power outlets, etc.) connected with the smart meter, collect and communicate those in real-time to the utility providers for effective energy management [12]. Moreover, with the help of the smart meter in this infrastructure, the consumer can control their devices remotely thus control their energy utilization effectively. IoT based AMI has a massive prospect for power grid management. The systems become capable of gathering and acting on live statistics of consumer-side small-scale power generation, and utilization from consumers connections (data on service provider's and end user's behavior), and supervising distribution mechanism with the objective to improve the consistency, sustainability and efficiency of energy production and distribution [12].

C. IoT FOR SMART METER, SMART HOME AND BUILDINGS

Smart Metering system is not only a system that collects consumers' energy consumption statistics periodically but also an integrated system combined with hardware, software and communication mechanism that creates a two-way communication between energy devices and users and enable users to observe live data on energy consumption patterns. Ideally, it can be used for monitoring the status of various parameters such as voltage reading, current reading, temperature, moisture status etc. and has the ability to adjust those parameters, energy consumption remotely as per their requirements. Table 3 exhibits the advantages of using Smart Meters in different sector of the energy grid [33].

The term Smart home refers to as the modern homes that have devices and appliances which can be managed remotely by the owner. As an essential element of the IoT, smart homes assist consumers efficiently by interconnecting with numerous advanced devices based on IoT. Smart home technology based on IoT has improved the quality of social life by facilitating connectivity to every person regardless of place and time [34]. Smart web or mobile applications can be used to control the devices within an IoT-connected smart home.

Similar to smart home, the Smart building can be referred as the building in which IoT enabled integration of sensory devices and actuators are applied to observe and regulate the various parameters of electrical, mechanical, environmental and security system applied in those industrial, commercial, public and residential buildings. In a smart Building Management System (BMS), a computer-oriented mechanism used to automatically monitor, control and regulate the electrical and mechanical apparatuses and elements of power systems, lighting systems, heating, ventilation, and air-conditioning (HVAC) systems, home security systems and so on. Its principal objective is the management of the surroundings within

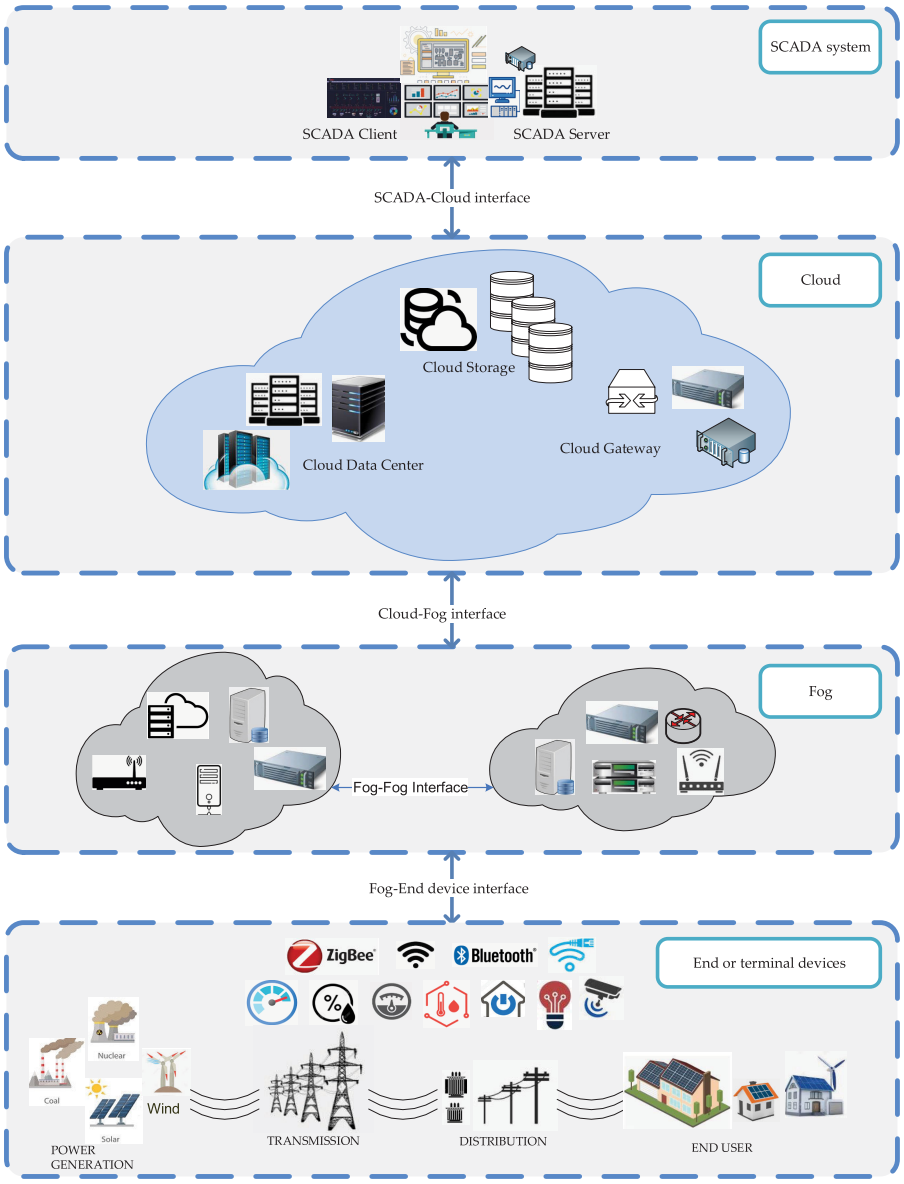

FIGURE 4. This figure exhibits the overall architecture of Fog-based smart energy grid SCADA system. The figure is comprised with four parts of the architecture (from up to down) SCADA system, Cloud, Fog and End or terminal devices with the energy grid. The concept is adopted from [15].

the building, oversee system parameters, manage and control those different parameters, and to reduce carbon emissions [12].

IoT oriented elements in smart homes and buildings are utilized to deliver technology to control and regulate smart systems and lessen energy waste. These elements increase productivity and improves power factor whereas preserving energy efficiency, for example, smart home and buildings lighting system offers programmed lighting regulation through LED lights. These automated structures operate the actions of the lights (e.g., on and off) to manage energy efficiently. Lights of IoT elements spontaneously turn off when occupants left the rooms or leave their homes to curtail the energy ingesting. Preserving energy in smart homes while enlightening the lifestyle of inhabitants is a vital matter. Inhabitants in smart homes use mobile applications to manage consumer energy consumption for financial savings and reduction of expenses. As the temperatures of surrounding of a buildings are continually varying, and the quantity of energy consumed can rise at specific times. For instance, air conditioning systems can adjust the indoor temperature and provide a comfortable atmosphere with the lowest energy ingesting according to the events inside using energy control based on IoT technology [34].

V. SECURITY ISSUES IN IoT BASED ENERGY SYSTEMS

With the assistance of IoT based technologies, the energy grid systems become more intelligent and more interactive to

TABLE 3. Advantages of using smart meters in different sectors of energy grid.

Sectors	Advantages
Energy transmission and distribution sector	Data value regarding efficiency, load and wastages upgraded
	Development in capacitor, condenser banks
	Energy load management upgraded
	Reduce in energy wastage
External Stakeholders	Funding for the Smart Energy Grid Enterprises
	Enhanced environment welfares
Consumers end	Further precised and well-timed billing
	Adequate access and information to manage energy consumption
	Enriched statistics measures and energy quality
Billing , Safety and Securiity sector	Reduction in recurrent billing
	Fast detection of disruptions and energy stealing
	Development in billing accurateness
Client Service and Ground maintenance	Abolishing hand-held metering apparatus
	Reduction in metering expense
	Less call-centre transactions
Service provider	Better-quality in operatives safety and security
	Enhanced consumer premise hazard profile and safety
Decision maker, Forecasting and Marketing	Cost reduction in statistics and information collection

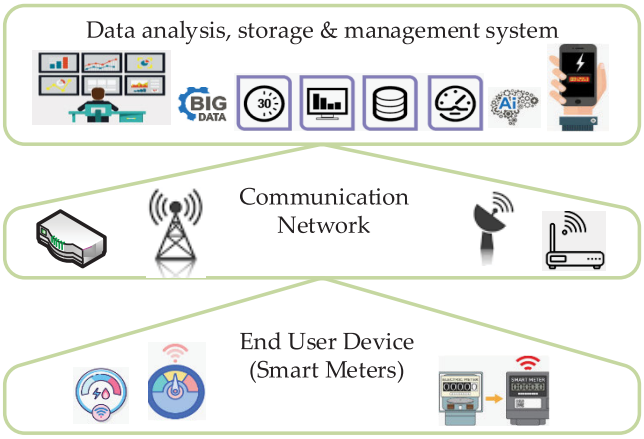

FIGURE 5. This figure exhibits the schematic representation of AMI which includes End-user Devices (Smart Meters), Communication Networks and Data analysis, storage and management system. The concept is adopted from [35].

improve the consistency, efficiency and flexibility of the system. However, cyber-security vulnerabilities increase as well. In this section, we will discuss the security vulnerabilities of IoT connected smart Energy Systems and the corresponding mitigating strategies.

A. SECURITY VULNERABILITIES OF IoT CONNECTED SMART ENERGY SYSTEMS

The research on cybersecurity of Smart Energy System has been done widely to classify cyber-attacks on different sectors of the smart energy system and to recommend security detection and protection procedures [37]–[40]. Cyber crooks, terrorists and state enemies [41] may try to interrupt the energy grid services. An effective cyber-attack may bring severe damage like significant power failure, social security threats, and financial loss for the service providers [36].

Most of the Smart Energy System's security vulnerabilities are related to the communication and networking systems. Because of the increasing amount of various types of devices, appliances and technologies that are integrated into the grid system, new and unique security and privacy concerns are occurring [42]. On top of that, the incorporation of cost-effective, power-effective wireless protocols (such as LoRaWAN, ZigBee) in the smart energy grid system particularly in the distribution infrastructure lead to new and unique types of vulnerabilities [36]. Even more secure protocols like Wi-Fi can be hacked by intelligent cyber-criminal, who cracked the supported encryption scheme and initiate cyber-attacks [43], [44].

As smart energy systems are mostly regulated by SCADA systems, they are more exposed to security threats [50]. Besides, the internal network of SCADA system, the connectivity path that exists between the energy grid system and the utility provider's IT network open opportunities for cyber-criminals to attack this SCADA system. The number of smart home appliances and devices is growing day-by-day, which directly communicates with Smart Meters and therefore, increasing the risk of cyber-attack at the low voltage networks as well [51]. On the other hand, a great number of renewable energy sources are connected and operated, which is distributed throughout the network. All those devices and systems hugely depend on IoT-based technologies to interconnect with each other for communication and management purposes. A successful cyber-injection in any small part can initiate cyber-attack, consequently failure of the system.

In power generation sector, cyber-attack in generators can be done by turning open and close of one or more circuit breakers in a very high-frequency rate within a short time (Aurora attack [36]) to create desynchronization and physical damage of the generator which resulting immediate power failure and generation inefficiency for the long run [45]. On the other hand, attack on the transmission and distribution system can be done by tripping one or more circuit breakers in geographically distributed locations creating power failure in the whole area. This can be done by spreading malware

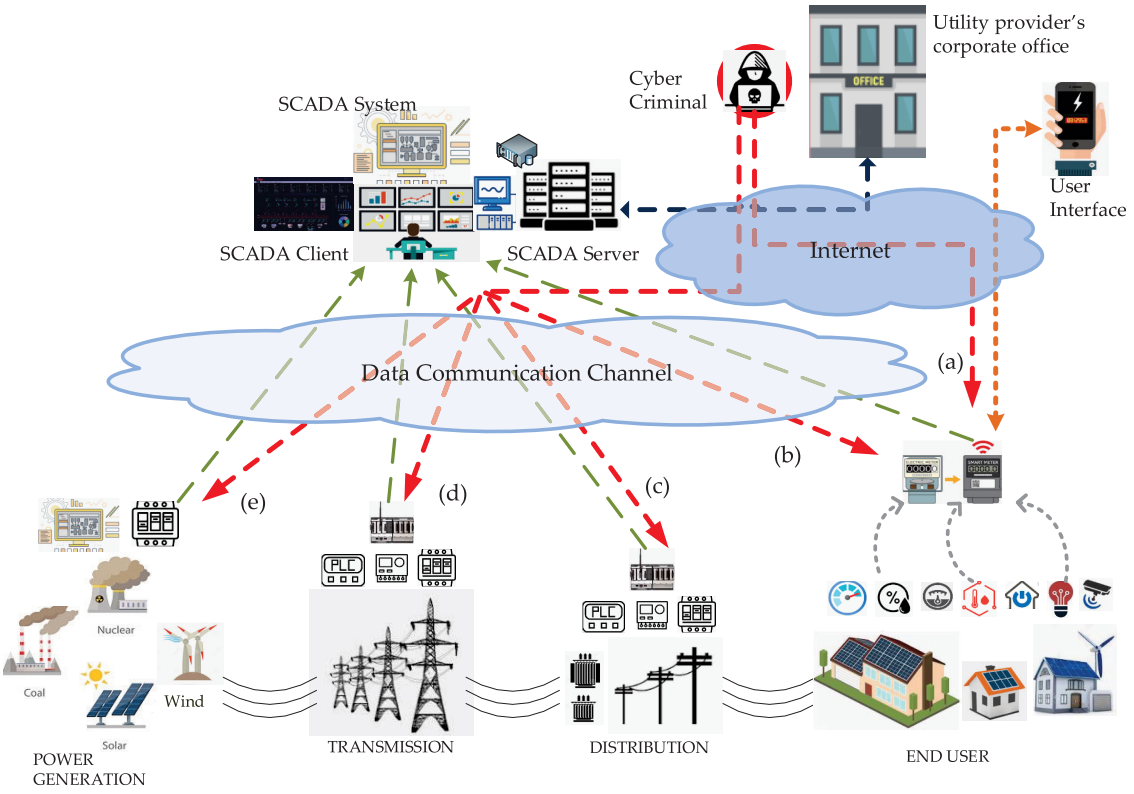

FIGURE 6. This figure exhibits different cyber-attack approaches in IoT based Smart Energy System. From right to left, (a) Cyber-attack at the end-user devices use wireless technology such as Wi-Fi, ZigBee, (b) Cyber-attack at end-user devices/ distributed renewable energy sources through the SCADA system connectivity, (c) at distribution system through the d-SCADA system, (d) at transmission system through the SCADA system, (e) at power generation end through the SCADA system. The concept is adopted from [36].

(e.g., Black Energy and KillDisk Malware in Ukrainian energy industry attack on December 2015 [41], [46]–[48]) using the corporate network and intrude into the private network of SCADA system. Additionally, the cybercriminal may succeed to stop the authentic update of the original firmware of the remote terminal units, and intelligent circuit breakers. Finally, they deactivate the control station's power back-up arrangement and wipe out all the data and information with the help of malware [36]. Figure 6 exhibits cyber-attacks on IoT connected Smart Energy System. More security vulnerabilities of IoT connected Smart Energy Systems will be discussed in the following sections.

1) SECURITY ISSUES IN ENERGY IoT DATA ANALYTICS

The implementation of AMI in IoT-centric Smart Energy system will produce enormous energy data with diverse variety and velocity [49]. The effective operation of this Smart Energy system relies on the perfect analysis of those enormous data. That grid information and statistics can be categorised as follows:

- Grid operational status and equipment monitoring figures
- Energy marketing information
- Energy consumption figures
- Energy management data

All these data must be managed at the same time and in a distributed method to get valuable and beneficial statistics for decision making purposes for effective operation. The whole process of energy data analytics requires an enormous amount of data collecting, transmitting, storing, distributing, and processing. The essential methods include several disciplines, comprising of signal processing, pattern recognition, data mining, machine learning, artificial intelligence optimization and visualization methods.

Security in this critical data analytics has been highlighted as a major concern. Cyber-criminals can manipulate grid operational and equipment data, which may create cascading events of a power outage and leads to entire energy grid failure. Data manipulation or false data injection in energy utilization statistics may create deregulation of the equilibrium between energy supply and demand thus leading to an interruption of the electricity and substantial cost upsurge. In recent years, data-driven techniques are being popular for smart grid applications. Specifically, IoT-enabled smart grid control relies on data-driven analysis for decision making. Authors in [54] shows the impact of adversarial attacks on the machine learning based analysis tool.

2) ATTACKS ON SMART HOME/AUTOMATION IoT SYSTEM

Authors in [36] show that common security vulnerabilities on smart home devices are weak verification

protocols, unauthenticated update procedure of device firmware and due to the usages of unencrypted communications. Moreover, in various remote control applications of the smart home devices are found with major web-based vulnerabilities.

A recent report on smart home devices security revealed a list of just 144 unique user names and password pairs that have been used for more than 1700 smart home devices for their remote telnet access purposes. On the other hand, recent studies shows huge upsurge (280%) in cyber-attacks on smart home devices using telnet access [36].

The IoT based automation devices can experience a varieties of cyber-attacks, as summarized below.

a: CYBER-ATTACKS ON IoT-ENABLED SMART AUTOMATION DEVICES RUNNING IN CRITICAL FACILITIES

Cyber-attacks on automation devices installed in critical facilities can be done to gain below objectives

- To gain initial access, for example, by hacking smart light get the authentication of Wi-Fi and eventually gain the control of the Wi-Fi network devices.
- To create indirect service interruption like using a thermostat to gain remote control over the buildings air conditioning system.
- To gain and leak data. Use a program that hacked smart devices like smart television to act like off mode and use the microphone to record conversation around it and leaks those audio.
- For system misuse like creating light flickering at a specific frequency that can cause people suffering from an epileptic seizure.

b: CYBER-ATTACKS ON IoT-ENABLED SMART AUTOMATION DEVICES RUNNING IN NON-CRITICAL PREMISES

Cyber-attacks can also be done on the IoT enabled devices installed in a non-critical location such as smart homes. The purpose behind those attacks are:

- Cyber-attacks on a huge number of smart home devices to initiate an amplified attack against a critical system
- Cyber-attacks to target a huge number of IoT enable home automation devices at a very short time period to disable those smart home automation systems.

In the following sections, we discuss a few attack scenarios that may be observed in a smart energy grid.

3) ENERGY THEFT

The vast utilization of the IoT assisted AMI in the smart energy grid makes it possible to transmit a huge amount of energy data and information in a faster, dependable and effective way for the management purpose of the smart grid system. It digitalised and swap the old-fashioned analogue system of meter reading and data collection. With the aid of IoT technologies, those enormous amounts of collected data and information are wirelessly communicated for further processing that considerably lessens labour-intensive workings. However, the energy grid becomes vulnerable to energy theft.

Energy theft has to turn out to be a severe concern in the smart energy grid Sector. It has triggered substantial financial losses for both energy service providers and energy consumers. The simplest form of energy theft is to tamper an energy meter in such a way that it cannot record the actual energy consumption any longer so that the energy bill can be manipulated. Energy theft generally involves bypassing the energy meter so that, energy can be used without being recorded for billing.

In a smart energy grid system, smart meters are placed at every distribution point to collect energy consumption data and generates the energy consumption statement remotely. Energy theft methods involve hacking the smart meters through other smart household appliances [52] and communication network. Energy theft is also done by tampering the smart energy meter's operating system, programming and manipulating records on the cloud. Hence, the cyber-criminal can reduce or increase individual's energy consumption records by hacking and manipulating the consumer's smart meters records. Consequently, it affects the billing of the consumers. Figure 7 exhibits energy theft scenario in an energy grid system.

4) CYBER-ATTACKS ON TRANSACTIVE ENERGY SYSTEM

The transactive energy system is a framework that is a combination of the economic strategies and power system control mechanism, used to regulate the flow or transaction of the energy within the existing energy grid system in respect to the commercial and market-centric standard values of the energy. The transactive energy system uses this combined concept of economic and operational mechanism to maintain the demand and supply equilibrium dynamically through the grid system and improve the efficiency and reliability of the energy grid system [53]. The transactive energy control mechanism hugely depends on the cyber system of distributed edge-computing and IoT technologies for decision making and demand response. This system requires an extensive data exchange between diverse market mechanisms like demand requests, capacity availability monitoring, and marketplace statistics. The transactive energy system comprises of several mechanisms, for example, central marketplace mechanism controller, source regulator, communication systems and prosumers. The source regulator at end-point will respond on the tariff information sent by the transactive marketplace and automatically reply data such as bidding price. Information interchange between the prosumers and the immediate marketplace negotiators need to be protected. Robust, secure and dependable communication system needs to be unsured as any physical or cyber-attack can threaten the entire management of the transactive energy system. The transactive structure is vulnerable to the diversity of threats, targeting at various attack surfaces. These potential attacks can target service operation, marketplace negotiators, the communication setup, discussed as follows.

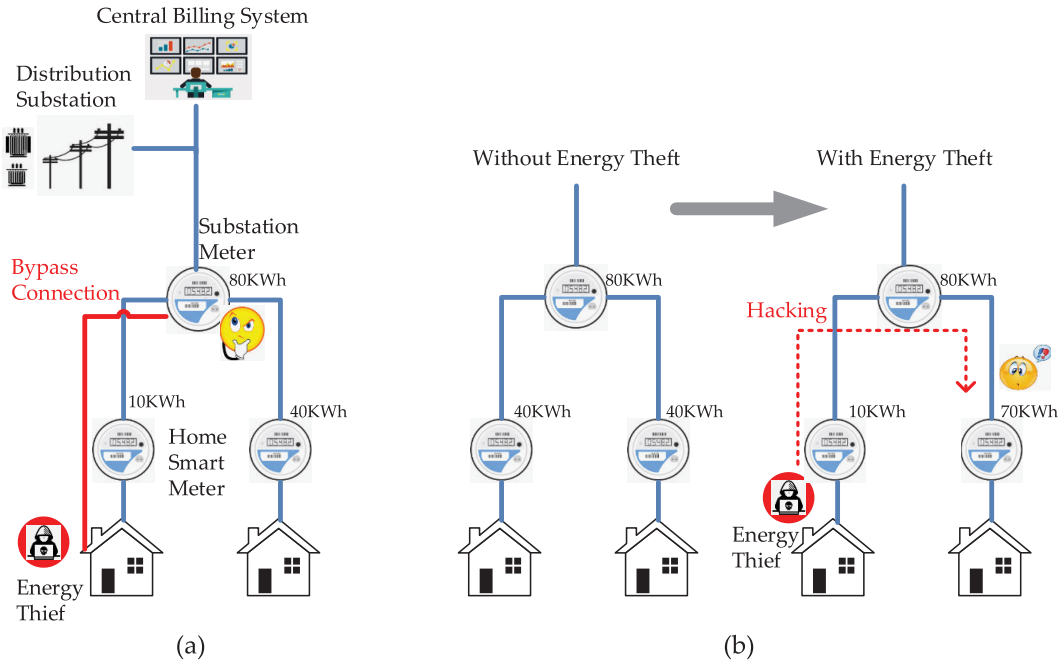

FIGURE 7. This figure exhibits different energy theft situation, (a) energy theft by bypass connection, in this case, substation meter shows more reading than a home level meter, therefore service provider face financial loss, (b) energy theft by hacking smart metering system, in this situation victim consumers face financial loss from manipulated energy consumption. The concept is partially adopted from [52].

a: CYBER-ATTACKS TARGETED AT SERVICE OPERATION AND DEVICES

- Malware injection in the system can create severe power failure or/and data theft.
- Devices such as smart meters can be damaged by cyber-criminals.
- A cyber-attacker can manipulate the control signals of the relay and circuit breaker at the system and create disruption in the transactive system.

b: COMMUNICATION STRUCTURE CENTRIC ATTACKS

- A cyber-criminal can get into the unprotected network of the transactive energy system and modify different parameters such as voltage, current, frequency reading which create rapid fluctuation in those systems and leads to physical destruction to the smart devices and cause a power outage. That cyber-criminal can also manipulate the bidding price and sent to the utilities to gain financial benefits.
- A denial of service attack can be targeted to the utilities and agents that creates unavailability of information, updates, tariff and resource information.
- Spoofing can be done by sending manipulated price signals to agents which increase the locational marginal price as energy sells at much higher expense than proposed.

5) CYBER-ATTACKS ON WHOLESALE ELECTRICITY MARKET

Power system operators attempt to utilize resources in a proficient way to achieve the highest social satisfaction while maintaining the network constraints. For this mission, the energy system practices market mechanisms like auctions. In an auction, the authority first collects bidding prices from different agents, which require the trades that is approved by the agents. Auctions decide marginal estimation and marginal cost functions of energy customers and energy producers, respectively. Therefore, each bid provides figures about the profit that each agent gets from the business. In the next step, the auctioneer decides the market balances, that is, the dealings that maximize the system productivity and minimizes the cost. Electricity markets usually follow social welfare concept, the accumulated profit for all parties. The competitive markets incentivize efficient dispatch that maximizes social welfare because energy generators must offer energy at prices close to their marginal costs. Thus, the demand is attended with the lowest price [55]. If we notice carefully, the whole auction and market settlement procedure is dependent on the effective information exchange among multiple parties. The transformation of the market infrastructure and the introduction of industrial IoT technologies open new threats for the energy grid system. Cyber-criminals can attack the electricity market by manipulating the demand statistics, which creates distortion in demand and supply equilibrium and lessen the effectiveness of the energy system operation. By injecting false bidding price in auction procedure, cyber-criminal creates chaos in the whole process and interrupt the attempt of maximizing the social welfare. False injection attack for SCADA system has been well addressed that shows that energy market can be manipulated using stealthy injection attacks [63]. Similar type of data integrity attack is possible for an IoT-enabled smart grid.

B. MITIGATING IoT-ENABLED CYBER-ATTACKS

The aforementioned analysis of security vulnerabilities demonstrate that some of the cyber-attack patterns are similar in various region, whereas some other cyber-attacks are specific to a particular area. Generally, the lack of improved logical and physical access control in IoT enabled elements increases the vulnerabilities and unguarded the system to threats. In this section, we will discuss some security controls to mitigate the risk factors of the system and later we discuss some detection mechanism.

1) CONTROLLING THE CYBER-THREAT

The objective of these controls is to improve the access and awareness. Execution of these system control parameters generally depends on the system administrators as the threat level are based on the specification of the system settings. Some of the measures are discussed below [36]:

- *Limit the Physical Access to the IoT Devices:* IoT enabled devices should be installed in such places where unauthorised persons cannot access or apply appropriate physical protection to avoid unauthorised access.
- *Monitor Physical Access to the Devices:* IoT devices should be monitored by a surveillance system, particularly which are installed in a location that can be accessible by unauthorised visitors.
- *Avoid Connecting IoT Devices to the Internet Directly:* IoT devices should not be configured with public IP address directly if it is not required essentially. IoT devices should connect to the internet indirectly using private IP address through a gateway or firewall with an appropriate protection scheme.
- *Implement Proxy-Based System Access:* Access should be done through proxy-based access system as those systems offer better authorization and authentication facilities.
- *Secure Remote Access Mechanism:* Secure verification and encryption policies should be applied to protect the remote access of IoT enabled devices. Strong authentication control protocols such as SSL, SSH or VPN protocol should be used while accessing through the internet.
- *Application of Additional Security for Link Layer:* IoT devices located in critical systems should be applied with the highest level of security available in the protocol used in the respective link layer.
- *Regularly Access Logs of Audit Devices:* IoT devices should be regularly logged in and inspect the access log for potential intrusion detection.

2) REDUCING IoT DEVICE LEVEL VULNERABILITIES

The objective of these measures is to lessen the existing security vulnerabilities of IoT enabled devices. The manufacturers are responsible to implement such controls on devices to reduce vulnerabilities. Regulator authorities can set up policies to impose those controls on devices. Sometimes proper configuration on the devices can lessen security vulnerabilities, discussed below [36].

- *Tamper Detection and Prevention Mechanism:* The IoT enabled devices should be facilitated with any kind of alteration detection and prevention mechanism. If an intruder tries to tamper the device, it must detect it and temporarily or permanently disable the access of the intruder.
- *Implemented With Secured and Embedded Crypto Mechanism:* These mechanisms should be implemented on the devices to protect against man-in-the-middle or replay attack.
- *Side-Channel Protection:* Hardware security control should be implemented on devices to protect them from side-channel attacks such as attacks for acquiring sensitive data from the system.
- *Firmware Protection:* Mechanism should be applied to protect the firmware of the devices from unauthorized tampering using methods such as obfuscation, encryption, etc.
- *Secure Update Procedure of Device Firmware:* The device firmware update procedure should be in a secure and authentic way. Device mechanism should prevent any other unauthentic update process.
- *Secure Operating System:* It is not possible to update the operating system of the devices regularly so the operating system architecture should be minimized with least required features and with less exposure to the forthcoming vulnerabilities.
- *Secure Application Programming Interface:* Only well-secured and authenticated application programming interfaces should be used while developing the application software of the device and developed software should be tested with known vulnerabilities.
- *Network Security Protocol Supported Mechanism:* The devices should be implemented with a mechanism that supports the highest available network security protocol to their corresponding layers.
- *Periodical Security Testing Mechanism:* Devices should be implemented with a mechanism that periodically initiates the testing of various security parameters of the device.

3) REDUCING THE POSSIBLE IMPACT OF ATTACK CONNECTIVITY PATHS

In most cases of IoT enabled attacks in the critical area are induced from the devices and spread through the connectivity, we analyse the security control that detects and eliminate the secret and potential ways of cyber-attacks. The following assessment may help to identify and mitigate the possible impact during an IoT attack [36].

- *Detection and Documentation of IoT Dependencies:* Detection and documentation of the dependencies such as communication, control mechanism between IoT

enabled devices and the systems should be done in a systematic approach to reduce possible attack path.

- *Avoid Excessive Physical Vicinity:* IoT devices should not be installed near-critical systems if it is not necessary. If it requires to install physically near the critical components, it is needed to ensure that the IoT device does not create any indirect attack path.
- *Avoiding Cascading Impact With the Utilization of Segmented Network:* Network segmentation needs to be satisfied while designing the network of IoT devices to avoid spreading of cyber-attack like malware injection.
- *Implement Diverse Technologies:* Single unified technology-based system combined of multiple devices and networks can lead to cascading failure with a single self-spreading cyber-attack. So diverse authenticate IoT technologies should be implemented to avoid this type of vulnerabilities.

4) LIGHTWEIGHT INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) plays a major role towards security protection for the IoT technology. The features of IoT systems bound the design of an IDS to be lightweight still competent enough to protect the system from potential cyber-attacks. The definition of lightweight means that the system should have the capabilities to execute its tasks with the existing amount of properties in the sensor nodes of the network so that it can satisfy the real-time or near real-time operational requirements. A lightweight IDS is considerably small, robust and flexible enough to be utilized for the system security arrangement. A lightweight structure targets at saving energy and analytical resources. A lightweight system can describe as one which can execute its operation with limited energy and computation resources irrespective of simplicity. A lightweight attack recognition approach employing a controlled machine learning-based support vector machine (SVM) to detect injection attack into the IoT network has been proposed and evaluated in [56].

5) FOG-AIDED SDN CONTROLLED ANOMALY DETECTION SYSTEM

Distributed fog computing based system provides efficient intrusion detection and protection system against numerous cyber-attacks in near real-time for effective threat detection. The SDN-enabled fog computing can control the process in a distributed manner. Fog based computational arrangements are beneficial to convey computing facilities as near as possible to the edge devices to facilitate latency-sensitive data analytic applications. On the other hand, the Software-Defined Networking (SDN) is an emergent innovative networking standard that dictates parting of the controller plane from data plane of a network.

Edge or Fog computing can get a significant advantage from software-defined networking. The whole system of fog aided anomaly detection structure for an IoT network is restructured with the aid of SDN model. This mechanism influences the mitigation of identified anomalies by mounting suitable flow rules for the altered data plane that separates and removes undesirable attack traffic from normal traffic within the IoT network. Edge computing delivers the necessary computational resources for machine learning-centric anomaly detection structure. Location of this computational concentrated structure over the edge is critical. In some situation, the structure functions from a distant location like cloud, resulting delay in mitigation of anomaly becomes unreasonable. To mitigate detected anomalies, edge computing requires the SDN control which separates normal traffic from attack traffic for an efficient mitigation process [57].

VI. POTENTIAL OPPORTUNITIES

With the integration of IoT based technologies, the smart energy grid becomes more reliable, robust and efficient. However, IoT technologies bring new challenges for the smart energy grid system such as security vulnerabilities. Such kind of challenges can be overcome with the assistance of some new technologies like blockchain, machine intelligence and high performance computing and distributed frameworks. In the following sections, we will discuss some potential opportunities for IoT to improve the overall system performance and security of the smart energy grid.

A. BLOCKCHAIN

Blockchain is a new standard concerning distributed data and storage management, which is based on the concept of a shared, secured, and distributed register that stores and keeps transactions without any centralized administration [59]. In the perspective of IoT, blockchain allows two elements to interconnect and interchange data, information and resources in a distributed peer-to-peer (P2P) network. Blockchain offers a transparent structure in which probabilities of any intruder access is minimum because any information is broadcasted to the entire network, and any acute judgement is approved with a majority votes from the peers on the basis of a consensus algorithm instead of a particular central administrator or server [58].

In the same way, blockchain centric IoT systems are protected from cyber-criminal, who targeted to hack the centralized control server to acquire vital information and/or control the entire system. Surely, the additional expenditure requires for the security surveillance of IoT servers can easily be curtailed utilizing blockchain technology [60]. Moreover, blockchain technology stores IoT elements information in a manner that, in the situation of any data conflict, they can be easily backtracked.

One key feature of blockchain technology for data distribution of IoT elements is encryption. In a P2P network system, each of the communication is equipped with the cryptographic keys exchange mechanism [61]. The process of cryptographic key encryption guarantees the security inside a blockchain system and prevent any intruder to interfere with the information exchange illegally. IoT blockchain applications facilitate with a distributed, reliable and protected information-sharing framework in which data can effortlessly

be outlined and backtracked and therefore, the overall operation of IoT enabled smart grid is improved. In the following section, we briefly discuss some key functionalities of the block chain system that can significantly benefit the IoT integrated smart energy system.

- *Distributed Nature:* The distributed nature of block chain-centric IoT structures will eliminate certain concerns of centralized architecture, for example, centralized failure point [62]. This distributed operation will work in a faster, reliable and efficient way.
- *Security:* The interchange of data and information of IoT elements will keep protected, as all the communications are protected using cryptographic encryption [64].
- *Reliability:* The irreversible nature of blockchain-centric IoT systems improves the confidence of participants, as they can backtrack and authenticate any transaction without any possibility of altering [65]. Furthermore, this facility also improves the traceability of IoT sensors' data.
- *Identity:* Data from any devices in the blockchain aided IoT system can be traced effortlessly, because of unique identifiers for each of the devices are used. In the same way, reliable distributed approval and verification facilities can also be delivered using blockchain in IoT structures [66].

B. PRIVACY-PRESERVING DATA SHARING

A crucial component of the smart energy grid is the advanced metering infrastructure (AMI), which hugely depends on the smart meters for the two-way power transaction and communication process. The bulk integration of smart meters deliver substantial assistance for the management of energy supply and demand for both power service providers and consumers. However, the incorporation of IoT solution increases the threats of privacy violations of enormous data sharing by those smart meters. In the following section, we discuss some potential approaches proposed by the researchers to preserve the privacy of data sharing in a smart energy grid system.

To mitigate the potential privacy leakage of smart meters, information protection schemes like data anonymization and data aggregation can be used [68]. Data anonymization eliminates any attribute information from the meter measurements to hide the private and sensitive information. It depends on a third party as a middle man to pseudonymize meter readings. However, those pseudonymized measurements can still be linked with the home unit that generates those data. On the other hand, data aggregation technique targets to decrease the volume of critical data that can be disclosed. The privacy-preserving aggregation depends on the features of the cryptographic computation [68]. These techniques mainly aim to tackle the processing overhead and storing procedure of the enormous amount of generated information. The aforementioned schemes are planned from the service provider's viewpoint. However, IoT privacy challenges go further than these orthodox approaches in those diverse participants, for example, service providers and consumers. Therefore, consumer-centric resolutions are needed to accommodate separate privacy preferences. One approach to attain consumer-centric privacy protection is done by data perturbation. For example, smart meter readings can be disturbed by inserting arbitrary noise or applying data compression methods [68]. These techniques are known differential private smart meter data analysis. The trade-off between the measured data accuracy and arbitrary noise needs to be analysed. However, altering with smart meter measurements before communications to the service provider may decrease their significance for billing purposes. Another method that uses data perturbation to modify the genuine energy utilization is presented in [68]. The privacy analysis considering renewable energy source or with the assistance of an energy storage system at the consumer locations is addressed in [68].

Network Traffic confidentiality attack is one where cyber-criminals intercept the information traffic from or to the gateway of the smart home system and monitor consumer's usage characteristics over the digital traces. Existing cryptographic techniques may not work effectively because of the effectiveness of cyber-criminals machine learning algorithms in organizing encrypted data flow. Therefore an approach is proposed with a privacy-preserving data flow obfuscation structure to satisfy the privacy objective [69]. To be precise, the approach influences the network system of wirelessly interconnected smart homes and deliberately transfer each smart home's information data flow to another smart home's gateway before transmitting over the Internet. The scheme jointly contemplates the system energy utilization and the resource limitations in IoT devices, while succeeding resilient differential privacy assurance so that cyber-criminal cannot trace any data flow to an exact smart home device. Moreover, the method considers a smart community network system and develop protected multi-hop transmitting protocols to ensure the source/destination non-link facility and fulfil each consumer's personalized privacy requirements [69].

In another approach, authors proposed an enhanced energy-proficient, protected, and privacy-preserving information transmission protocol for the smart home system [70]. In that work, information communication within the smart home systems is protected by asymmetric encryption with secret keys which are created using chaotic system theories. Authors integrate message verification codes to their proposed scheme to assure information reliability and genuineness. Authors also deliver in-depth security exploration and performance assessment in terms of computational complexities, resource budget, and data transmission overhead [70].

C. MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Massive amount of data and information are generated in the IoT enabled smart energy grid system [72], [73]. In the existence of such volumes of immense and complex data, it is challenging to accurately select the most precise and critical information. The best conceivable analysis of this huge data

can be done by using progressive techniques like Artificial intelligence (AI), Machine learning (ML), and Deep Reinforcement Learning (DRL) to get an optimum while scalable output [71], [74], [75]. Those techniques can bring the best probable or approximate optimum control decisions [76]. The accurateness of the these techniques can be more improved by increasing the volume of training samples to reinforce their learning abilities and therefore the improve automatic decision process [77].

The big data is playing an important role in modernizing the functioning structure of a smart energy grid system with efficient energy utilization [78]. In a smart energy grid system, the massive amount of data arrives from diverse sources that needs to be efficiently analysed and presented for suitable administration and operational purposes. Those data and information analytics also requires to satisfy the security goal of power grids [79]. Machine learning based techniques can be used for fault analysis, transient stability analysis, load estimation, valuation of different power generation measurements, and energy grid administration [80]. Researchers proposed a prototype that considers distributed energy resources and ML-based systems as an integrated part of the smart grid system that helps in the complex decision making based on measurement data and information [81]. The ML-based prototype maintains the system performance in an efficient way and navigates the power to critical loads during hostile and unfavourable situations [71].

In an IoT-enabled smart grid, majority of the information is produced by Cloud-centric IoT elements that executes a dynamic role in diverse applications of smart energy grid system. Appropriate use of AI, ML, and DRL techniques can overcome existing challenges of confirming privacy and protection of information, preservation of networks against any potential cyber-attack and encourage developed and accountable data share culture and reliable decision making.

VII. CONCLUSION

IoT deployment of energy systems has opened up tremendous opportunities. However, security vulnerabilities in IoT systems are considered one of the fundamental problems hindering large-scale deployment and application of IoT technologies to the smart energy grid.

In this paper, we review the available IoT technologies and their applications that can solve key issues of a smart energy grid system. In addition, we have highlighted and made a comparison of the existing surveys and literature addressed the computing, sensing and communication technologies to ensure an IoT-connected smart energy system. Next, IoT technologies and their applications to the energy system have been reviewed. We have addressed the key challenges and demonstrated that cybersecurity is a major concern. We analyze and present a comprehensive survey about existing and potential vulnerabilities of IoT enabled smart grid system and discussed the potential mitigation techniques of those vulnerabilities. We also present potential opportunities introduced from the rapid advancement of technologies such as blockchain, machine learning and artificial intelligence to encounter those challenges towards a more effective energy grid operation. Despite these challenges, the utilization of the Internet of Things (IoT) can significantly benefit towards the development of the conventional present grid system to transform in to a smarter grid. Therefore, it is necessary to emphasize security vulnerabilities and the prospects of advance technologies while planning, employing and incorporating of IoT technologies within the smart energy grid system.

REFERENCES

[1] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Jhanjhi, "Secure healthcare data aggregation and transmission in IoT—A survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[2] M. Pau, E. Patti, L. Barbierato, A. Estebsari, E. Pons, F. Ponci, and A. Monti, "A cloud-based smart metering infrastructure for distribution grid services and automation," *Sustain. Energy, Grids Netw.*, vol. 15, pp. 14–25, Sep. 2018.

[3] A. Meloni, P. A. Pegoraro, L. Atzori, A. Benigni, and S. Sulis, "Cloud-based IoT solution for state estimation in smart grids: Exploiting virtualization and edge-intelligence technologies," *Comput. Netw.*, vol. 130, pp. 156–165, Jan. 2018.

[4] Q.-T. Doan, A. S. M. Kayes, W. Rahayu, and K. Nguyen, "Integration of IoT streaming data with efficient indexing and storage optimization," *IEEE Access*, vol. 8, pp. 47456–47467, 2020.

[5] E. Adi, A. Anwar, Z. Baig, and S. Zeadally, "Machine learning and data analytics for the IoT," *Neural Comput. Appl.*, vol. 32, pp. 16205–16233, Oct. 2020.

[6] E. Bejoy, S. N. Islam, and A. M. T. Oo, "Optimal scheduling of appliances through residential energy management," in *Proc. Australas. Universities Power Eng. Conf. (AUPEC)*, Melbourne, VIC, Australia, Nov. 2017, pp. 1–6.

[7] A. S. M. Kayes, W. Rahayu, and T. Dillon, "Critical situation management utilizing IoT-based data resources through dynamic contextual role modeling and activation," *Computing*, vol. 101, no. 7, pp. 743–772, Jul. 2019.

[8] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019.

[9] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet Things*, vols. 1–2, pp. 81–98, Sep. 2018.

[10] D. Minoli, "Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach," *Internet Things*, vol. 10, Jun. 2020, Art. no. 100147.

[11] S. N. Islam, M. A. Mahmud, and A. M. T. Oo, "Secured communication among IoT devices in the presence of cellular interference," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–6.

[12] S. E. Bibri, "The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability," *Sustain. Cities Soc.*, vol. 38, pp. 230–253, Apr. 2018.

[13] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of Things (IoT) and the energy sector," *Energies*, vol. 13, no. 2, p. 494, Jan. 2020, doi: 10.3390/en13020494.

[14] M. Rahimi, M. Songhorabadi, and M. H. Kashani, "Fog-based smart homes: A systematic review," *J. Netw. Comput. Appl.*, vol. 153, Mar. 2020, Art. no. 102531.

[15] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102500.

[16] S. N. Islam, M. A. Mahmud, and A. M. T. Oo, "Relay aided smart meter to smart meter communication in a microgrid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Sydney, NSW, Australia, Nov. 2016, pp. 128–133.

[17] X. Shen, L. Zhu, C. Xu, K. Sharif, and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Inf. Sci.*, vol. 514, pp. 118–130, Apr. 2020.

[18] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "Fog computing for smart grid systems in the 5G environment: Challenges and solutions," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 47–53, Jun. 2019.
[19] A. Anwar and A. N. Mahmood, "Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Boston, MA, USA, Jul. 2016, pp. 1–5.
[20] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, "Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications," *Autom. Construct.*, vol. 101, pp. 111–126, May 2019.
[21] *Information Technology–Automatic Identification and Data Capture Techniques–Unique Identification—Part 1: Individual Transport Units*, document ISO/IEC 15459-1, 2014.
[22] RFID Journal. (2005). *A summary of RFID standards*. [Online]. Available: http://www.rfidjournal.com/article/view/1335/1
[23] A. J. C. Trappey, C. V. Trappey, U. Hareesh Govindarajan, A. C. Chuang, and J. J. Sun, "A review of essential standards and patent landscapes for the Internet of Things: A key enabler for industry 4.0," *Adv. Eng. Informat.*, vol. 33, pp. 208–229, Aug. 2017.
[24] A. Y. Mulla, J. J. Baviskar, F. S. Kazi, and S. R. Wagh, "Implementation of ZigBee/802.15.4 in Smart Grid communication and analysis of power consumption: A case study," in *Proc. Annu. IEEE India Conf. (INDICON)*, Dec. 2014, pp. 1–7.
[25] A. Tomar. (Jul. 2011). *Introduction to Zigbee Technology*. Global Technology Centre 1. Accessed: May 5, 2020. [Online]. Available: https://www.cs.odu.edu/cs752/papers/zigbee-001.pdf
[26] J. de Carvalho Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic, and A. L. L. Aquino, "LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities," in *Proc. 2nd Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech)*, Jul. 2017, pp. 1–6.
[27] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Exp.*, vol. 3, no. 1, pp. 14–21, Mar. 2017.
[28] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Protection*, vol. 25, pp. 36–49, Jun. 2019.
[29] S. S. Reka and T. Dragicevic, "Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid," *Renew. Sustain. Energy Rev.*, vol. 91, pp. 90–108, Aug. 2018.
[30] G. Rahman, M. F. Bin Ramim Chowdhury, A. Al Mamun, R. Hasan, and S. Mahfuz, "Summary of smart grid: Benefits and issues," *Int. J. Sci. Eng. Res.*, vol. 4, no. 3, pp. 1–5, Mar. 2013.
[31] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.
[32] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, "Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings," *Future Gener. Comput. Syst.*, vol. 82, pp. 349–357, May 2018.
[33] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. Al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: A review," *J. Cleaner Prod.*, vol. 217, pp. 702–715, Apr. 2019.
[34] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *J. Netw. Comput. Appl.*, vol. 97, pp. 48–65, Nov. 2017.
[35] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure," *Int. J. Electr. Power Energy Syst.*, vol. 63, pp. 473–484, Dec. 2014.
[36] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.
[37] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.
[38] Z. A. Baig and A.-R. Amoudi, "An analysis of smart grid attacks and countermeasures," *J. Commun.*, vol. 8, no. 8, pp. 473–479, 2013.
[39] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.
[40] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 13–27, Dec. 2016.
[41] D. Goodin. (2017). *Hackers Trigger Yet Another Power Outage in Ukraine*. [Online]. Available: https://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-poweroutage-hits-ukraine/
[42] J. C. Stephens, E. J. Wilson, and T. R. Peterson, *Smart Grid (R) Evolution*. New York, NY, USA: Cambridge Univ. Press, 2015.
[43] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Autom. Conf.*, San Francisco, CA, USA, Jun. 2015, pp. 1–6.
[44] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.
[45] M. Zeller, "Myth or reality—Does the aurora vulnerability pose a risk to my generator?" in *Proc. 64th Annu. Conf. Protective Relay Eng.*, Apr. 2011, pp. 130–136.
[46] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," in *Proc. SANS Ind. Control Syst.*, Bethesda, MD, USA, 2016, pp. 1–29.
[47] L. Robert and C. Anton. (2016). *Blackenergy Trojan Strikes Again: Ukrainian Electric Power Industry*. [Online]. Available: https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikesagain-attacks-ukrainian-electric-power-industry/
[48] C. Anton. (2017). *Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet*. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threatindustrial-control-systems-since-stuxnet/
[49] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.
[50] A. Anwar, A. Mahmood, and M. Pickering, "Data-driven stealthy injection attacks on smart grid with incomplete measurements," in *Intelligence and Security Informatics (PAISI)* (Lecture Notes in Computer Science), vol. 9650. Cham, Switzerland: Springer, 2016, pp. 180–192.
[51] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid," *Inf. Syst.*, vol. 53, pp. 201–212, Oct. 2015.
[52] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5531–5539, Jun. 2019.
[53] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.
[54] I. Niazazari and H. Livani, "Attack on grid event cause analysis: An adversarial machine learning approach," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.
[55] C. Barreto, H. Neema, and X. Koutsoukos, "Attacking electricity markets through IoT devices," *Computer*, vol. 53, no. 5, pp. 55–62, May 2020.
[56] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.
[57] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, "Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network," *IEEE Access*, vol. 6, pp. 73713–73723, 2018.
[58] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.
[59] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 850–880, 1st Quart., 2019.
[60] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, vol. 225. Cheltenham, U.K.: Edward Elgar Publishing, 2016.
[61] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[62] P. Veena, S. Panikkar, S. Nair, and P. Brody, "Empowering the edge-practical insights on a decentralized Internet of Things," in *Empowering EdgePractical Insights a Decentralized Internet Things*, vol. 17. IBM, 2015.
[63] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010, pp. 226–231.

[64] G. Prisco. (Nov. 2015). *Slock. it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy*, Bitcoin Mag. Accessed: May 5, 2020. [Online]. Available: https://bitcoinmagazine.com/articles/sloc-it-tointroduce-smart-locs-lined-to-smart-ethereum contractsdecentralizethe-sharing-economy-1446746719
[65] (2017). *Modum*. Accessed: May 5, 2020. [Online]. Available: https://modum.io
[66] (2017). *Chain of Things*. Accessed: May 5, 2020. [Online]. Available: https://www.blockchainofthings.com
[67] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A secure communicating things network framework for industrial IoT using blockchain technology," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101933.
[68] Y. Sun, L. Lampe, and V. W. S. Wong, "Smart meter privacy: Exploiting the potential of household energy storage units," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 69–78, Feb. 2018.
[69] J. Liu, C. Zhang, and Y. Fang, "EPIC: A differential privacy framework to defend smart homes against Internet traffic analysis," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1206–1217, Apr. 2018.
[70] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.
[71] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Comput. Commun.*, vol. 154, pp. 313–323, Mar. 2020.
[72] F. M. Al-Turjman, "Information-centric sensor networks for cognitive IoT: An overview," *Ann. Telecommun.*, vol. 72, nos. 1–2, pp. 3–18, Feb. 2017.
[73] F. Al-Turjman, "Information-centric framework for the Internet of Things (IoT): Traffic modeling & optimization," *Future Gener. Comput. Syst.*, vol. 80, pp. 63–75, Mar. 2018.
[74] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for IoT-based energy management in smart cities," *IEEE Netw.*, vol. 33, no. 2, pp. 111–117, Mar. 2019.
[75] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, Jun. 2019.
[76] H. Li, T. Wei, A. Ren, Q. Zhu, and Y. Wang, "Deep reinforcement learning: Framework, applications, and embedded implementations: Invited paper," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 847–854.
[77] S. Ramchurn, P. Vytelingum, A. Rogers, and N. R. Jennings, "Putting the 'smarts' into the smart grid: A grand challenge for artificial intelligence," *Commun. ACM*, vol. 55, no. 4, pp. 86–97, 2012.
[78] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi, and M. Abedi, "IoT architecture for smart grids," in *Proc. Int. Conf. Protection Autom. Power Syst. (IPAPS)*, Jan. 2019, pp. 22–30.
[79] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.
[80] N. Zhou *et al.*, "Analysis and prospect of deep learning application in smart grid," *Automat. Electr. Power Syst.*, vol. 43, no. 4, pp. 180–191, 2019.
[81] F. Liang, W. G. Hatcher, G. Xu, J. Nguyen, W. Liao, and W. Yu, "Towards online deep learning-based energy forecasting," in *Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2019, pp. 1–9.

S. M. ABU ADNAN ABIR received the B.Sc. degree in electrical and electronic engineering from the Islamic University of Technology (IUT), Bangladesh, in 2008. He worked as a Manager with the Transmission and Network Operation Centre, IGW Operators Forum (IOF). Before that, he worked for Bangla Telecom Ltd. (ICX of Mir Telecom Ltd.), Huawei Technologies Bangladesh Ltd., Fiber@Home Ltd., and ACI Logistics Ltd. He is a telecommunication professional having more than ten years of technical and managerial experience in telecommunication transmission and data communication network. His research interests include smart grid systems, the Internet of Things, data science, block chain mechanism, machine learning, artificial intelligence, and cyber security.

ADNAN ANWAR (Member, IEEE) worked as a Data Scientist of Flow Power with Energy Management and Solution Company. He is currently a Lecturer and the Deputy Director of the Master of Cybersecurity Course Suites, School of Information Technology, Deakin University. He has over eight years of research and teaching experience in universities and research labs, including NICTA, La Trobe University, and the University of New South Wales. He has authored more than 30 articles, including journal, conference articles, and book chapters in prestigious venues. His research interests include security research for critical infrastructures, including smart energy grid, SCADA systems, and application of machine learning, and optimization techniques to solve cyber security issues for industrial and IoT systems.

JINHO CHOI (Senior Member, IEEE) was born in Seoul, South Korea. He received the B.E. degree *(magna cum laude)* in electronics engineering from Sogang University, Seoul, in 1989, and the M.S.E. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), in 1991 and 1994, respectively. He was a Professor/Chair of Wireless with Swansea University, U.K. He was a Professor with the Gwangju Institute of Science and Technology (GIST), South Korea. He is currently a Professor with the School of Information Technology, Deakin University, Burwood, VIC, Australia. He authored two books published by Cambridge University Press, in 2006 and 2010. His research interests include the Internet of Things (IoT), wireless communications, and statistical signal processing. He received the 1999 Best Paper Award for Signal Processing from EURASIP and the 2009 Best Paper Award from WPMC (Conference). He is also an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS. He is a Division Editor of the *Journal of Communications and Networks* (JCN). He also had served as an Associate Editor or Editor for other journals, including the IEEE COMMUNICATIONS LETTERS, *Journal of Communications and Networks* (JCN), the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and *ETRI Journal*.

A. S. M. KAYES received the Ph.D. degree from the Swinburne University of Technology, Australia, in 2014. He is currently a Lecturer of Cyber Security with the Department of Computer Science and Information Technology, La Trobe University, Bundoora, VIC, Australia. His research interests include information modeling, data privacy and security, context-aware access control, the Internet of Things, and cloud and fog security.