Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9065768, 26 pages
https://doi.org/10.1155/2022/9065768

Review Article

Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations

Mohammad Kamrul Hasan,[1] **Ali Alkhalifah**,[2] **Shayla Islam**,[3] **Nissrein B. M. Babiker**,[4] **A. K. M. Ahasan Habib**,[1] **Azana Hafizah Mohd Aman**,[1] **and Md. Arif Hossain**[1]

[1]*Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM, Malaysia*
[2]*Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia*
[3]*Institute of Computer Science and Digital Innovations, UCSI University, 56000 Kuala Lumpur, Malaysia*
[4]*Information System Department, College of Science and Arts-Tathleeth, University of Bisha, P.O. Box 551, Bisha 61922, Saudi Arabia*

Correspondence should be addressed to Mohammad Kamrul Hasan; hasankamrul@ieee.org and Shayla Islam; shayla@ucsiuniversity.edu.my

Received 12 August 2021; Accepted 12 November 2021; Published 18 January 2022

Academic Editor: Rajesh Kaluri

The smart grid idea was implemented as a modern interpretation of the traditional power grid to find out the most efficient way to combine renewable energy and storage technologies. Throughout this way, big data and the Internet always provide a revolutionary solution for ensuring that electrical energy linked intelligent grid, also known as the energy Internet. The blockchain has some significant features, making it an applicable technology for smart grid standards to solve the security issues and trust challenges. This study will present a rigorous review of blockchain implementations with the cyber security perception and energy data protections in smart grids. As a result, we describe the major security issues of smart grid scenarios that big data and blockchain can solve. Then, we identify a variety of recent blockchain-based research works published in various literature and discuss security concerns on smart grid systems. We also discuss numerous similar practical designs, experiments, and items that have recently been developed. Finally, we go through some of the most important research problems and possible directions for using blockchain to address smart grid security concerns.

1. Introduction

Internet of Things (IoT) is considered the most uncontrollable innovation in today's world; this improves our ordinary life by reworking the bodily items that surround us into an ecosystem of facts. IoT and big data have numerous applications in day-to-day life, i.e., security, transportation, industrial, retail, healthcare, home automation, military, agriculture, surveillance, and good infrastructure. Indeed, IoT and big data have heavily driven nowadays smart grid developments, and smart meters are progressing by featuring more vital sensing abilities and higher connectivity [1, 2]. The smart electricity generation, transmission, and distribution system and smart buildings/homes are all controlled and explicitly maintained by ICT devices like WAMS, IEDS, and RTUs for service systems, as well as AMIs for smart building/home management in the smart grid (SG) [3]. The IoT-enabled field measurement data can be safely and automatically collected by including the blockchain control and field measurement with smart communication to these ICT devices in HAN/SN, NAN, and WAN [4]. Furthermore, blockchain-enabled AMIs can use DAPPS services to conduct decentralized system capacity, local power management, and trading in a cyber-secured environment [5].

The days are passing. Civilization is also progressing rapidly. Science is becoming more powerful as time passes. Simultaneously with the problems that the modern world presents, scientists and engineers face difficulties in satisfying market demand at various levels for various reasons. The total electricity generation, transmission, and

distribution system are becoming a loss project because of a lack of raw electricity generation raw material supply, corruption on both the transmitting and receiving ends, transmission line and distribution system losses, and other factors. As a result, the SG technology was developed to meet consumer demand, improve the electricity generation and distribution system efficiency, ensure customer protection, and monitor and regulate the entire system through communication (generating and receiving end). As a result, the critical focus of the paper is to include an overview of blockchain (BC) in smart grid and energy trading presented in Figure 1.

Beyond the area of computer vision, this article will contribute as a supplement to an adversarial attacks' summary and protections for SG IoT and big data linked devices and networks. The contribution of this study is discussed below.

(1) *General Working Flow*. We review an overall working flow to describe the Internet-connected devices, protocols, and network infrastructure and its adversarial attacks in SG big data/IoT networks. The integration of the potential BC technology in SG IoT networks is presented. Based on this, a robust classification is provided to organize and structure existing attacks intricately and effectively where the defenses can be possibly accomplished in SG IoT-connected devices and networks.

(2) *Systematic and Comparable Studies*. We classify current attacks based on the above taxonomy into three standard sensor data types: textual, audio, and surveillance sensor data. Here, we also did a quantitative comparison between them based on six technical factors. In addition, we define as well as outline three possible defense strategies for aggressive attacks in CPSs.

(3) *Open Issues and Opportunities*. We highlight several existing research prospects which should be pursued in the future in order to inspire and enhance future follow-up on this research topic.

The overview of this paper's structure is presented in Figure 2. Section 2 discusses the study methodology and the relevant research on IoT security specifications. Section 3 examines the findings, highlighting critical characteristics for understanding IoT and general security criteria related to the entire lot system. Section 4 presents the overview of blockchain technology and its application. Finally, in Section 5, we present the findings of this study, and the conclusion is in Section 6.

2. Research Methodology

2.1. Research Questions. Research questions. The following research questions are to be analyzed and accomplished throughout the paper:

(1) What are the recent features technologies in SG?

(2) What are the security vulnerabilities, threats, and their counter measurement in SG?

(3) What are the blockchain technology and the security mechanism that attracted the researchers to security solutions for SG?

(4) What are the critical success factors of the blockchain that can ensure the security of SG systems (smart metering, energy trading, SG communication systems, etc.)?

(5) What are the issues and challenges of the blockchain- (BC-) based security solutions, and what are the possible enhancements of the blockchain framework that strengthen the security in SG?

2.2. Review Protocol. The specific review protocol of the procedures can be followed during the studies. It is necessary to make assessments almost the review issue, data extractions, data synthesis, inclusion criteria, quality assessment, search strategy, research collection, and dissemination plans. Only full published conferences and journals in the English from 2010 and 2021 were considered. Data sources, data extraction, research collection, and selection strategy process are the main components of the review protocol.

2.3. Data Sources. To assist in answering the research questions, research papers related to blockchain, IoT, and big data were chosen. Related research articles which are not addressed or even endorse with the research questions were rejected. Our primary resources for looking the published research publications are in the following libraries:

(i) Science Direct

(ii) IEEE Xplore Digital Library

(iii) MDPI

(iv) Taylor and Francis

(v) Springer Link

(vi) ACM Digital Library

(vii) Google Scholar

2.4. Search Process. Based on the research methodology, we focused on IoT and blockchain-based keyword patterns to find any research queries. We apply Boolean operators and symbols like "AND," "OR" to find out the following keywords: (block chain OR (block chain technology) OR (block chain security AND block chain issues) OR (IoT security)) OR (big data in SG) AND (study OR Adoption) AND ((requirements AND solution) OR (benchmark AND regulation)) AND ((block chain application AND fields). Figure 3 presents this process.

2.5. Data Selection. The data collection is the deciding process of the appropriate data source and type and perfect implements to collect the data. Data selection precedes the actual repetition of data collection. Data selection criteria were as follows:

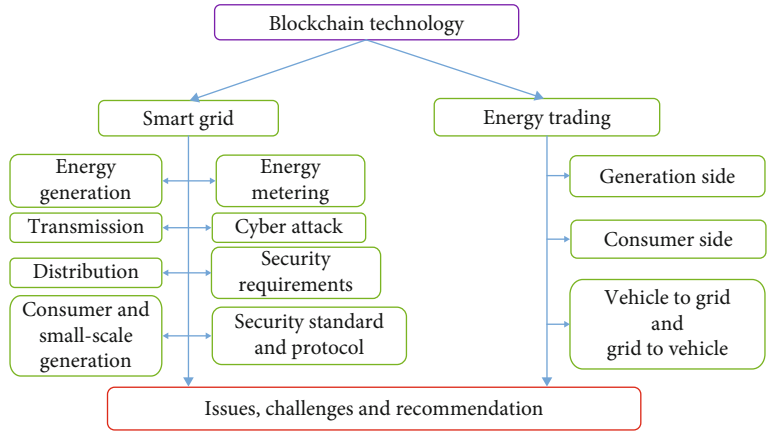

Figure 1: Overview of study.

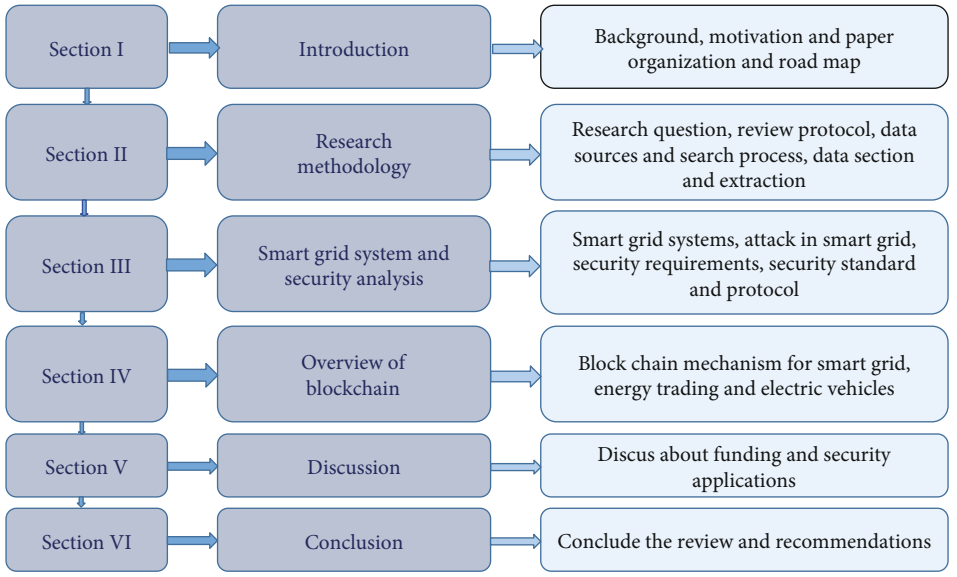

Figure 2: Paper organization

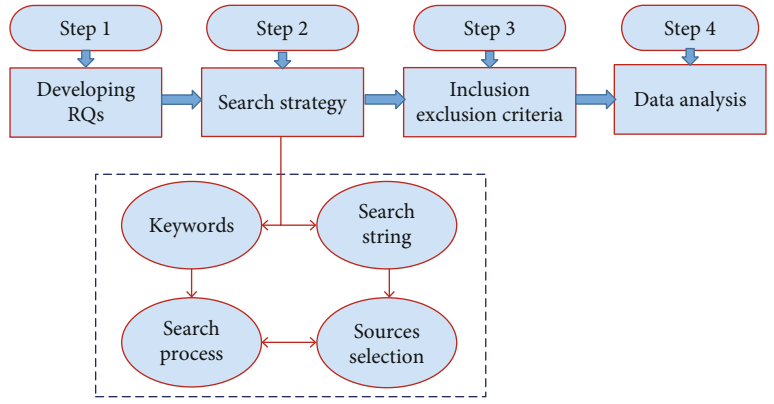

Figure 3: Proposed systematic search process.

(i) Has been the study paper written between 2010 and July 2021?

(ii) Is the research paper published in the well-known/referred data sources?

(iii) Does the research paper reference or address BC/IoT/big data?

(iv) Is there any discussion of security, requirements, or practice in the research paper?

2.6. Data Extraction. In July 2021, we completed the search process and discovered 269 publications and websites. Related research papers were carefully extracted by following the collection and rejection criteria as part of the search process. Finally, preliminary results were found from 142 abstract studies and 57 full-length reviews and research work for studies. The data synthesis and extraction of the selected review papers to find the research question answers and classify the studies shown in Tables 1 and 2 present the IoT and blockchain application field, respectively.

Table 1: Selective articles extraction from primary study sources.

Sources	Found	Candidate	Selected
IEEE Xplore	187	108	64
Elsevier	132	83	43
ACM Digital Library	25	8	3
Hindawi	21	14	9
Google Scholar	200	56	37
Science Direct	87	39	26
Springer Link	42	27	13
MDPI	51	22	14
Website	4	4	4
Total	772	321	213

3. Smart Grid System and Security Analysis

The term "SG" states to a concept that encapsulates the entire electricity generation, transmission, and distribution system in a single edging. In other words, an SG makes smarter the entire system more competent or safer. Clean energy is now in high demand all over the world. As a result, clean energy is also called smart energy. The word "smart grid" was first used in the year 2003 [6]. That was the first time Michael T. Burr used the word in a document. He clarified how the power grid's flaws could be detected and fixed to improve the power flow mechanism from generation to delivery across the whole transmission lines. This SG idea is now a reality, and the SG design objectives are presented in Figure 4. It was becoming a fact through the excellence of executing some one-of-a-kind function that makes things simpler. The SG is prepared smart by exhausting the national grid's security mechanism and central control via the supervisory control and data acquisition (SCADA), transmission equipment monitoring and diagnostic, grid computing, handling the whole power system as a hybrid adaptive power system, and using distributed computer agents to make the self-healing power system network [7].

3.1. Smart Grid Systems. The development of a highly secure, dependable, and eco-friendly national power grid system, termed the SG, is being driven by rising concerns about greenhouse gas emissions like carbon dioxide (CO_2) and the demand for additional efficient and dependable power transmission and distribution [8]. An SG uses two-way digital technology to transmit power between providers and consumers. It monitors and regulates smart appliances in users' homes or buildings to conserve energy, save costs, and improve dependability, efficiency, and transparency (Figure 5) [9]. The legacy power network is intended to be modernized by a smart grid. It automatically monitors, protects, and optimizes the function of the associated pieces. Several of the SG technologies are already in use in different industrial regions, like manufacturing process of wireless and sensor networks in telecommunications, and are starting to be modified for application in the different intelligent fields and linked scenarios such as energy distributions, communication systems, energy metering, and energy trading. The conventional power delivery system focuses on designing technology that improves the power supply's integrity, availability, and secrecy. Until recently, modern communication technology and equipment were thought to be boosting the dependability of the power industry. Nonetheless, the growing connection is becoming more critical for the power system's cyber security. In particular, securing the electrical grid system protects, arranges for, recovers, responds, and mitigates from unexpected cyber system incidents or natural catastrophes [10].

The integration of security system/protocol/algorithm with smart grid (SG) technology is becoming so sophisticated key solutions for facilitating comprehensive security functionality SG technology. The core related interfaces, components, and applications of SG that are critically security dependent are discussed in analyzing the key RQs. The feature of SG is presented in Figure 6.

3.1.1. Smart Meters for Energy Trading. Smart meters (SMs) are distinctive characteristics of SG technology that become a most reliable device for data measurement in electricity generation, transmission, and consumption. The SMs combine use with digital meters and communication systems to allow real-time monitoring of the consumers' energy [2]. In simple terms, a SM is a meter that calculates the amount of electricity used by customers. It usually records the reading at several times during the day. A typical SM assists the customers to understand electricity consumption and billing procedures; therefore, they can easily manage their usage electricity inside their desired budget/billing limit.

On the other hand, the SM measurement aids the suppliers and consumers in calculating accurate bills for customers. SM acts as a contact point between households and the Distribution System Operator (DSO), part of energy transactions. It is crucial to have a secure connection between SM and utility servers because it can affect transactions and billing information. It is essential to maintain track of the transactions in terms of planning the operation and compute invoices. When several parties engage in any kind of trading, trust is a big challenge. Initially, the record of transactions is maintained by a responsible third party. For SM-DSO transactions, blockchain technology can be used to maintain a distributed ledger. As a result, they were implementing blockchain technology to trade energy required to be trusted on their third party [11–15].

3.1.2. Distributed Generations. Smart grid technology relies heavily on distributed generation (DG). The term

Table 2: The use of IoT blockchain technology application field.

Sector	The use or application field
Smart city	Smart transaction and data maintenance, facilitating digital data and data transactions, pollution control data, water management data, and energy management data are all examples of smart service offerings.
Healthcare	Health costs, hospital information systems, medication records, digitizing old medical records, digital case notes, electronic medical records, genome data, and vital signs are all examples of genomic data.
Agriculture	Agriculture big data used for seed processing, agro-seed marketing, sales data, soil data, yields, agro-product shipping, and analytics
Energy	Data on energy generation, demand, resource availability and raw material information, utility condition monitoring, resource tracking, and tariff data maintenance
Manufacturing	Manufacturing packaging data, product output data and management, actuators/sensors, automation, raw material, supplier data monitoring, and transaction data monitoring for product distribution
Transport and logistics	Transport records, vehicle tracking, toll data management, logistic service identifiers, shipment data, and container tracking and accurate distribution are all examples of transportation records.
Others	Virtual nations, voting and government, space development, precious and jewels metals, ownership, economic sharing, and digital content
Distribution	Mining chips, digital currencies, marketplace, sales records, storage records, transport records, used sales, and goods
Business	Import and export data, tech industry digital documents, and transaction processing data have been used for financial analytics.
Finance	Money trading, money deposits, money transfer, crowd funding, smart securities, smart contracts, social banking, digital transaction assets, and crypto currency are all examples of digital transaction assets.

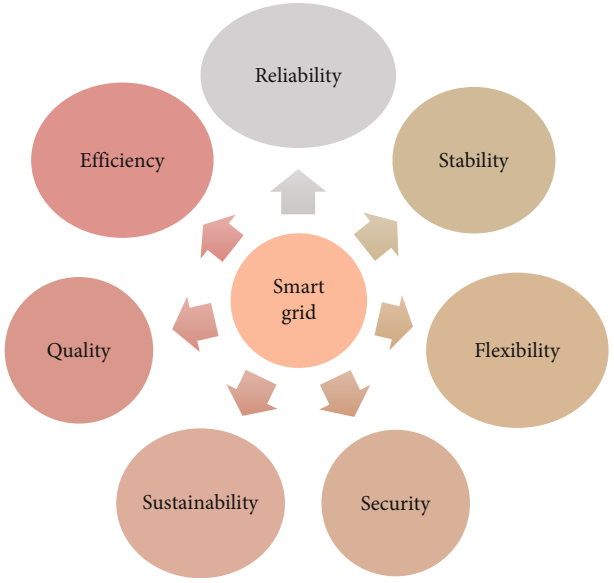

Figure 4: Smart grid design objectives.

"distributed generation" refers to the production of electricity from various small energy sources. Massive power plant generation has inevitable consequences, such as environmental effects on transmission and distribution and a very stable electricity supply via the grid [6]. The present electricity networks are becoming more overburdened as demand rises regularly. As a result, traditional strategies contribute to the complexity of existing networks. To meet customer expectations on the distribution side, such as lower power bills, increased comfort, reliability, and data security, a comprehensive analysis of SG components such as distributed generation is necessary [9, 16]. Integrated minor nonconventional power resources can be utilized to produce electricity at the load end in distributed generation. This technology improves power quality, efficiency, reliability, and security while lowering operational costs and environmental impact [10, 17].

3.1.3. Integration of the Renewable Energy. The interconnection of renewable energy is another critical function of the SG system. Improving the grid's IRE (Integration Renewable Energy) capability allows the national power grid to address customers' increased demand while maintaining future security. Like the DG (distributed generation), IRE will face some difficulties as it integrates into the smart grid.

3.1.4. Two-Way Communication System. The SG system is more straightforward for both suppliers and consumers when the bidirectional communication system is activated. The SG communicates in two-way communication with consumer's alert of the price and energy consumption as well as electricity generation, and suppliers are aware of the simple billing system of usage electricity. Cyberphysical security employs communication interfaces such as Universal Asynchronous Receiver-Transmitter (UART), Ethernet, and WLAN for the complex Internet Connected SACADA and PMU device WAMS in SG networks. The IEEE C37.118, Gateway Exchange Protocol (GEP), SIEGate has been designed and presented to secure cyberphysical communication interface, gateway, and control systems. Furthermore, only this communication device allows for central control of the entire grid. However, one thing to keep in mind is that privacy must be protected when interacting in the SG system, whether multidirectional or bidirectional.

3.1.5. Automatic Healing Capability. Since SG system is a cognitive approach for electricity generating and distributing

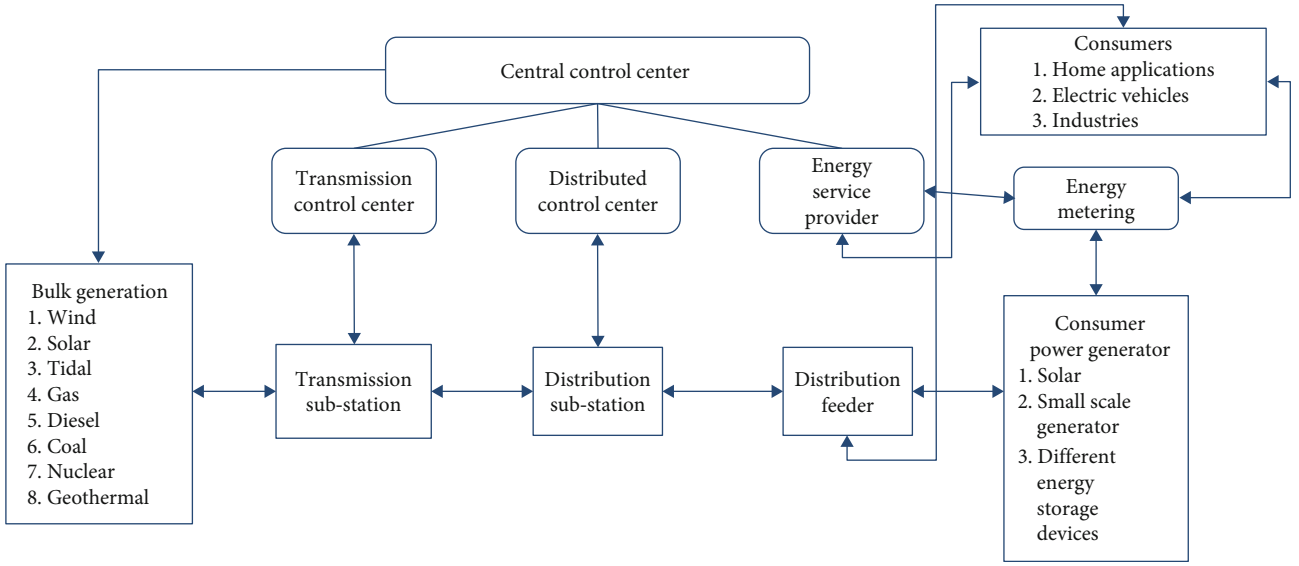

Figure 5: Smart grid communication infrastructures [9].

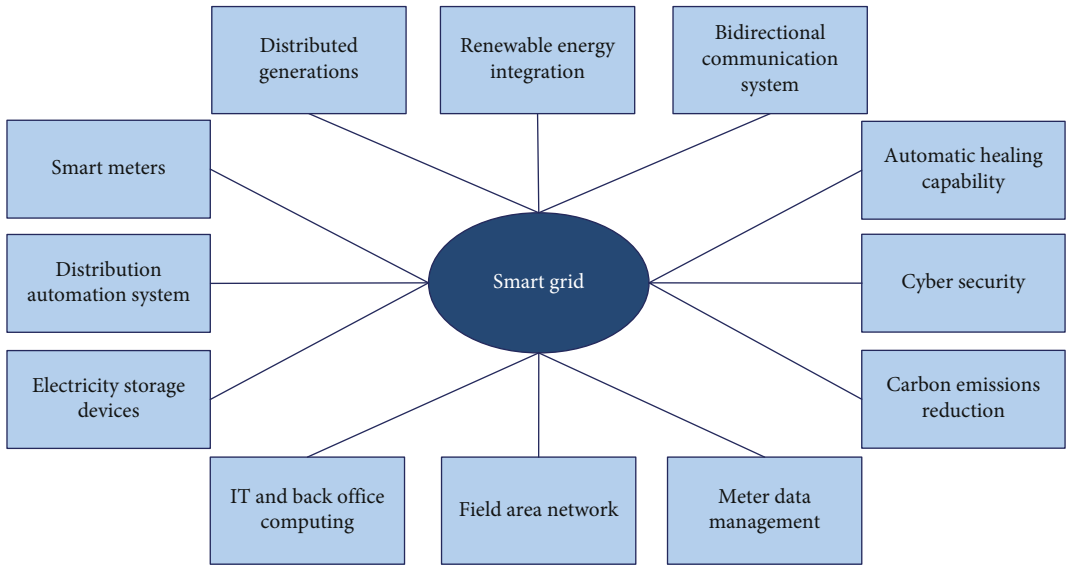

Figure 6: Smart grid features.

with a high level of data protection, convenience, and robustness, the SG must provide one feature: Automatic Healing Capability (AHC). This function comprises automatic identification of unstable system conditions, such as overcurrent, fault current and surge voltage, and information transmission from the central control room and fault or disruption healing/recovery capability.

3.1.6. Carbon Emission Reduction. The SG is called Green Grid. Since it can integrate renewable energy sources into the grid and efficient energy production and distribution, SG technology can help reduce carbon emissions by a significant amount.

3.1.7. Meter Data Management. The key component of Advanced Metering Infrastructure (AMI) is data management systems of the meter [18]. Meter data management (MDM) is a software that stores and manages enormous amounts of generated data by SM systems over time.

3.1.8. Field Area Networks. In power delivery, field networks help build impregnable connectivity between various field equipment, such as transformers, distributors, and smart electronic devices. Near field instruments, several electrical sensors are mounted [19].

3.1.9. Electricity Storage Devices. Energy storage systems in many mobile devices have found excellent applications. Therefore, the environmentally safe products replace the standard battery-acid metal storage equipment, requiring more charging time and less acid use. Based on the SG feature and application, Table 3 presents the contribution of some published work.

Table 3: Comparison survey paper related to smart grid.

Ref	Country	Year	Publication	Sources	Contribution
[6]	USA	2012	J	Science Direct	This article presents an overview of the various network technologies and their contexts. In addition, networking methods, quality of service (QoS), and various optimization problems were briefly addressed.
[8]	Mexico	2012	J	IEEE	The authors discussed the study on the intelligent delivery system and intelligent metering system in this article. In addition, the authors presented feature analysis of distributed asset optimization, alignment, and connectivity sensors of large-scale deployment of AMIs.
[9]	Russia	2013	J	IEEE	The authors of this survey looked at the connectivity required for SG and renewable energy sources. They believe that by using smart grid technology, consumers can reduce the peak to average ratio.
[20]	USA	2011	J	IEEE	The author discus the uses of SMs, benefits, difficulties, and drawbacks according to the energy sector.
[21]	Netherlands	2015	J	Science Direct	The survey proposes the role of SG power electronics component role, control techniques, renewable energy resource integration, intelligent communication, and metering technologies. Additionally, the authors developed the idea and application of electricity inversion systems with the intelligent grid.
[22]	USA	2012	J	Science Direct	A survey of smart grid connectivity architecture routing protocols was addressed. Authors have also outlined QoS, security problems, benefits, and drawbacks of current communication protocols.
[23]	USA	2010	J	Science Direct	This study contains a comprehensive review of integration and the problems associated with hybrid electric vehicles. Different energy control schemes are proposed to mitigate problems relating to hybrid plug-in vehicles (PHEVs).
[24]	USA	2013	J	Science Direct	A discussion of cyber security issues and risks in SG infrastructure is discussed. Additionally, they conducted on contact, security, and protocol specifications.
[25]	Russia	2010	J	IEEE	The paper's various approaches for improving the electric grid are proposed. Different methods are used for a stable power grid system, real-time information transfer, reporting, SM using and automation, and improved transmission control system.
[26]	China	2015	J	Google Scholar	The authors looked at key problems such as communication systems and cyber security issues and possible solutions. They also contribute to potential smart grid research directions.
[27]	USA	2016	J	Science Direct	The authors examined privacy approaches and issues to achieve the most safety of SG system data transfer. They have discussed several issues on vehicle-to-grid (V2G) and their solutions.
[28]	Pakistan	2016	J	Science Direct	A thorough examination of demand side management (DSM) and load forecasting are discussed in this paper. To minimize the peak to average ratio, models and forms of dynamic pricing models and load forecasting are briefly discussed.
[29]	USA	2015	J	energies	This study is focused on V2G network authentication protocols, home and wide area network authentication protocols, and different access control patterns. Also, they discussed the problems of reliable authentication in the smart grid.
[30]	Italy	2014	J	Science Direct	This survey article examines demand response (DR) and SG technologies in depth. The DR would aid in the reduction of capital and operating costs for smart grid technologies.
[31]	Austria	2017	C	IEEE	This study focused on start-up approaches in different technical characteristics and blockchain technology-based standard revelation on microgrid and peer-to-peer trading.
[32]	Pakistan	2017	J	Elsevier	This survey presents the smart grid communication network by a multilayer approach like as Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN).
[33]	Pakistan	2018	J	Elsevier	The goal of this review is to reveal and investigate the current technologies of the smart grid. This study highlights the Architectural Model focusing DR Program (DRP), DSM, and consumer empowerment (CE). Additionally, the study presents a detail discussion on the communication technologies for the power systems like virtual, intergrid, picogrid, nanogrid, and microgrid system.
[34]	China and Singapore	2018	J	MDPI	Blockchain energy Internet and their challenges

Table 3: Continued.

Ref	Country	Year	Publication	Sources	Contribution
[35]	China and USA	2019	J	MDPI	Energy trading in blockchain
[36]	Australia and China	2019	J	IEEE	Theoretical framework and testbed study of blockchain in intelligent grid
[37]	Singapore	2020	J	IEEE	Identify the significant challenges and issues on smart grid addressing blockchain technology
[38]	India	2020	J	Elsevier	Smart grid applicable various technologies, communication system, future, and opportunity of smart grid
[39]	UK	2021	J	IET	Multidimensional blockchain technology in smart-grid
[40]	China	2021	J	Springer	Hybrid blockchain technology (public and private) using 5G network in smart grid

3.2. Attack in Smart Grid. Scanning, surveillance, maintaining, and manipulation are the major four access and measures to use by hackers to target the devices and gain access and control [12]. The attacker collected and gathered information to their target through the first phase, reconnaissance. In the second stage, they take attempts to locate the system's vulnerabilities. These movements are designed to learn and identify the service methods on the open port operating system individually and their flaws. They make an attempt to gain and concession the complete control system during the goal exploitation period. When the target administration access is gained, then the final move must be complete and continuously can access. This is consummate by installing an undetectable and stealthy program, consenting them to simply back to the target system. In SG, security criteria are a concession with attackers [1] following the same steps. They apply various methods to compromise a specific system in the SG at each level. As a result, these steps can be used to classify attacks. The types of attacks that occur during each stage are presented in Figure 7. It depicts the variety of attacks that could occur during the exploitation process. The attacks and the malicious activities have occurred during every step.

3.2.1. Reconnaissance. Attacks such as traffic analysis and social engineering are part of the reconnaissance process. Instead of technological skills, emphasize human interaction and social skills in social engineering (SE). An attacker applies persuasion and communication gain to legitimate the user's confidence to obtain private and credential information, i.e., PIN or passwords to log in to the server. For instance, password and phishing attacks have become well-known methods used in SE [41]. The traffic analysis listens to the attack and analyzes network traffic to decide which computers and hosts connect to the network and their IP addresses. The security of information is primarily jeopardized by social engineering and traffic analysis.

3.2.2. Scanning. The scanning attack is the next move in discovering all of the computers and hosts on the network that are still alive. Scans can be divided into four categories: IP addresses, ports, utilities, and security flaws, which are all things that need to be considered [42]. An intruder usually begins to identify the network with an IP scan in the hosts connected with their won IP addresses. Then, they explore a little deeper by port, checking to see which ones are available. This scan process is run on any host network that has been discovered. After that, the attacker performs a service scan to determine which service or device is running behind each opened port [41]. The final stage is vulnerability scanning to find the flaws, aims, and vulnerabilities associated with every service system on the target devices to be exploited later. Industrial protocols Modbus and DNP3 are also susceptible to scan attacks. The TCP/Modbus was developed to protect the communication system rather than hack by using the scanning Modbus network technique. Attacker entails sending a harmless message to all network-connected computers to collect their information. Mods scan is a well-known scanner on the SCADA Modbus network that can detect and open TCP/Modbus connections and identify system IP addresses and slave IDs.

3.2.3. Exploitation. The SG system components are exploited by malicious activities and attempt to gain control and vulnerabilities over it are included in the third phase, exploitation [41, 43]. Viruses, worms, and Trojan horses popping the human-machine interface (HMI), privacy violations, channel jamming, and integrity breaches, as well as different attacks like denial of service (DOS), man-in-the-middle (MITM), and replay attacks, are all examples of these activities [24]. In the SG, viruses are a program that infects a particular computer or machine. A worm is a program that replicates itself. It spreads across the network, copies itself, and infects the system and other devices. A Trojan horse is a computer program that pretends to do something useful on the target machine. In the context, however, it executes malicious code. An attacker uses this form of malware to infect a computer with a virus or worm.

3.2.4. Maintaining Access. In the final stage, the attacker applies a specific attack form for retaining access, such as backdoors, viruses, and Trojan horses, to obtain permanent access to the target. An undetectable program like a backdoor is mounted for the target invisibly to be quickly and easily accessed. Suppose the attacker is successful in surrounding a backdoor into the SCADA server control. In that case, they will be able to initiate a series of attacks in contradiction of the system, which will significantly affect the

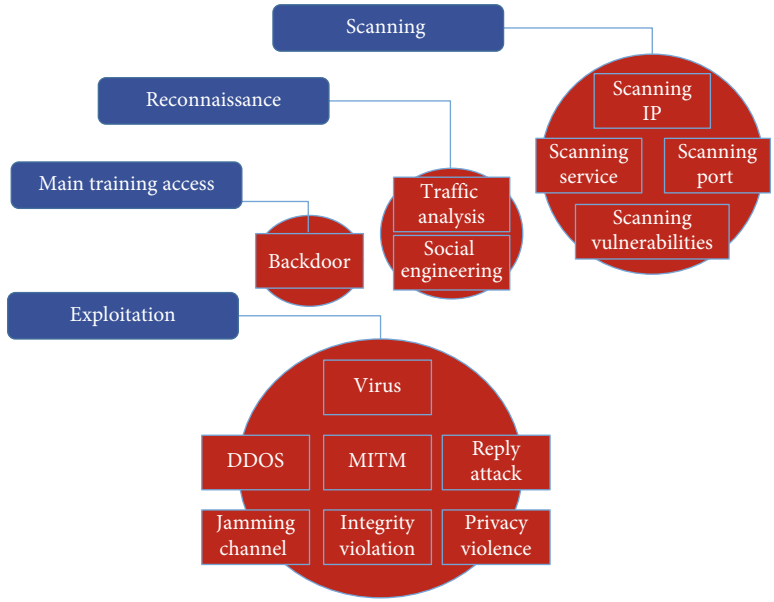

Figure 7: Smart grid-based attacking cycle.

power system [41]. The security criteria on the IT network is defined in the following order based on their importance: confidentiality, honesty, transparency, and availability. They are known as availability, honesty, transparency, and confidentiality in the SG. As a result, attacks that compromise the availability of smart grid networks are considered to be of high severity.

In contrast, attacks that target confidentiality are considered to be of low severity. Every attack has a degree of probability of being carried out in addition to its intensity. Attacks like Stuxnet and Duqu, for example, have a high intensity because they can vandalize industrial control systems and circumvent all security barriers; however, they are complex and complicated [44]. As a result, these viruses are hazardous, but their chances of being spread are poor. The popping HMI attack is another example. It is a highly severe attack requiring specialized networking expertise or extensive experience with industrial and security control systems. While the vulnerability documentation for the devices is publicly accessible, a hacker may quickly launch an attack using open source tools, including Meterpreter and Metasploit. As a result, this attack has a high probability of being carried out.

3.2.5. Impact of the Cyber Attack. Significant impacts can cause cyber attack (CA) on economic and physical/technical impact in SG. Though recent research has concentrated on cyber technical/physical attacks on SG, it is also essential to focus more on CA economic risk. The SG has faced a significant economic problem for CA [45, 46], specifically renewable energy resources with high penetration grid-connection mode. The electricity market is a combination of real-time and day-ahead markets [47, 48]. Mainly, the day-ahead market focused on solving the optimization and load forecasting problem at a minimum cost. The optimization problem explains the location marginal price (LMP) of electricity in different locations at each bus (economic dispatch) since load forecasting is affected by false data injection (FDI) CAs in the day-ahead market.

In contrast, the real-time market estimates the generated power and load power for each bus/line. Each line power is required to calculate to achieve the congestion pattern (when estimated line power exceeds the maximum power limit congested), and real-time LMP can estimate this. Thus, FDI state estimation on CA significantly impacts the real-time market that is briefly discussed in [46–51].

The FDI attacks have significant technical/physical impacts on SG. Typically, SG faces steady-state stability and transient impact for FDI attacks. The FDI attacks on steady-state stability significantly impact SG voltage control (AC/DC voltage control in AC-DC SG), demand current/voltage/power management, and energy management [52–56]. Additionally, the CA has an adverse effect on SG steady-state operation; the FDI attacks have impacted SG dynamic and transient stability. Currently, the SG frequency control system can be affected by FDI, but rotor angle stability will be the target [52, 57–61]. Moreover, all of the attacks were occurred in SG protection system.

3.2.6. Cyber Security. SG infrastructure must be protected against a variety of threats and attacks. Hackers, attackers, organized crimes and cyber terrorists, certain criminal elements, poorly or careless workers, and industrial rivals may all attack the SG. To abuse the vulnerability system, individual criminals, a group of hackers, attackers, organized criminals, and cyber terrorists may target SG systems and networks. Poorly qualified workers running the system carelessly will create the entire system susceptible to physical/cyber security attacks. Since infrastructure is interrelated across the system, if one part of the SG cyber security (CS) network is targeted, the whole system is at risk, resulting in a complete blackout or system failure. As a result, CS must

be robust sufficient to ensure the system's smooth and effective operation. Data privacy, secrecy, and verification are essential for the infrastructure's security and performance of SG applications. Disregarded cyber security strategies must be implemented to protect data security and supervise the infrastructure to prevent unwanted alterations across the infrastructure [41, 62]. There are several security flaws in SG applications, and each has its unique features. SG applications are vulnerable to diversity of cyber threats that might harm the moderate to more comprehensive level [24, 63]. A jamming attack can only be carried out by accessing the data transmission channel. Stuxnet and other zero-day attacks pose the risk of undiscovered data breaches within control systems. These data breaches may only be identified after the attack is executed [42, 64].

The attacker interrogates the communications between the nodes on the data transmission in an eavesdropping attack [20, 65]. Privacy can be compromised by password theft, traffic analysis on MITM, spoofing attacks, and overhearing. Reliability might be affected by data injection, wormhole data injection, task scheduling, spoofing attacks, and data manipulation. DoS, puppet, buffer overrun, wormhole, jammer, and flooding attacks cause security breaches [20, 65]. Services, applications, end nodes, and networks are the four levels of IoT-based information security solutions for smart infrastructures. Cyber attack (CA) countermeasures include intrusion detection systems (IDSs), sensor verification, compact cryptography, causal inference, and antijamming at the application level. Authorization, anti-DoS, pattern detection, intrusion prevention, cryptography, load balancing [47], ant jamming, and packet filtering are all elements of CA remedies at the network layer. Access control, encryption, pattern detection, authentication, information manipulation, controlled disclosures, and session identifiers are all components of cyber attack solutions at the service layer. CA solutions comprise verification, encrypting, and analysis of the anomaly behavior of software and systems at the end-node layer [43, 66]. Figure 8 shows the security solutions for IoT-based information security applications.

3.3. Security Requirements in Smart Grid. CS is a crucial concern due to the risk of CAs and accidents beside this critical industry as it associated with interconnected, according to the EPRI report. Not just malicious threats by malicious workers, corporate espionage, and hackers, but even accidental breaches to the communication system due to software errors, computer faults, and natural disasters must be addressed. Vulnerabilities may enable the attacker to break into a network system, manipulate load conditions and control the gain access in the software to disrupt the power grid in unexpected ways. In the SG system, there are two kinds of data that are shared. Specifically, data and functional data [67]. The logging system, energy trending, power billing, marking, geographical areas' historical reporting, customers' records, and emails are all examples of information. Real-time voltage and current values, capacitor banks, load current, transformer feeder, transformer tap changers, relay position, circuit breakers, and fault positions status are examples of operational information. To secure smart grid networks against any weakness or attack resulting in a power outage, operational data demands a high degree of protection. The smart grid's security criteria and goals are as follows:

3.3.1. Availability. The term "availability" discusses the right to use the information and obtain appropriately and accurately. If the SG's contact information is dislocated, that leads to a loss of availability, so the maximum security criteria are necessary [68, 69]. For example, a lack of availability will disrupt the control system's functioning by preventing network information, and operator systems prevent the network's availability. Availability attacks potentially distort, restrict, or hinder data transmission [11, 70]. Additionally, availability attacks in the smart grid prohibit and may disrupt authorized access. It was challenging to target asset availability in the large-scale conventional power grid. ICT is embedded into the power grid's information assets in the smart grid, allowing them to be attacked and completely inaccessible [12, 71].

The DoS attacks are called availability attacks [13, 72]. DoS attacks attempt to interrupt data transmission by obstructing, corrupting, or stalling it. This makes network sources inaccessible. Availability attacks are designed using several methods to overburden networks to ensure that the system does not operate correctly [14, 73]. Attackers transmit significant volumes of traffic to overwhelm the network's transmission connections. For this, the valid data package's presence is lost and not processed in network traffic. IEC 61850 and IP/TCP are IP-based protocol system, which are subject to availability attacks [15, 74]. The most important security prerequisite in SG technology, robust, and comprehensive remedies against availability attacks must be executed. Some successful methods include traffic filtering, big pipes, air-gapped networks, and anomaly detection methods [16, 75]. In SG system, attacks by DoS pose the biggest threat to big data; integrating software solutions in different network layers may prevent DoS attacks significantly.

3.3.2. Integrity. In the SG, integrity states securing data against unauthorized modification or degradation. The absence of integrity ensues when data is destroyed, modified, or altered deprived of existence identified [43]. For example, power injection is a destructive attack by an opponent who intelligently modifies calculations and state estimator from the power flow and injection meters. To protect the dignity, material authenticity or nonrepudiation is necessary. Integrity threats are not limited to unauthorized data alteration or injection. Integrity attacks include device impersonation, sparse, and replay attacks. Data integrity threats are prevented via cryptography techniques and approaches [17, 76]. SQL injection and MITM attacks use gaps in the SG to alter, takeover, or corrupt authorized operations.

In SG application system, the data concentrators are linked to SM HAN's. On the other hand, an attacker can use unauthorized data alteration or MITM to impair data transmission among the SM and the data concentrator unit. One of the subdivisions of integrity attacks is load-drop

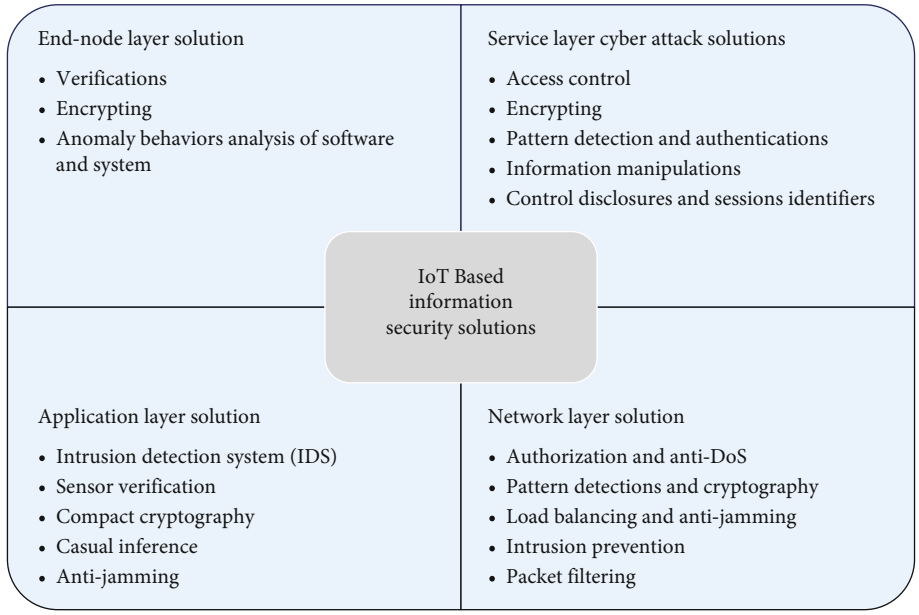

Figure 8: Security solutions for IoT-based applications.

attacks [18, 77]. MITM attacks threaten the systems, and CIA's tried accountability. Security gateways enable the authentication of both target nodes and sources and the confidentiality of data transfer [62, 78]. TLS protocols also include inbuilt asymmetric cryptographic features that can uncover and resolve vulnerabilities efficiently, preventing MITM attacks [63, 75]. By inserting script commands into databases, SQL injection attacks attempt to manipulate databases. SQL injection attacks insert fraudulent demands into the database system to maintain the control system, erase or alter current information, and insert falsified data. SQL injection attacks in the SG network system can be mitigated by using techniques like input type checking, matching the positive pattern, verified static code, database access prevention for remote users, dynamic SQL prevention, and conducting vulnerability scanning. Attackers may use characters such as semicolons; therefore, these characters should be monitored and excluded during type verification [63, 75]. Other kinds of integrity attacks include tampering SCADA systems [64, 79], replay attacks [65, 80], and time synchronization attacks (TSA) [66, 81]. To prevent the mentioned integrity attacks on the SG networks, authentication methods and end-to-end encryption recommendations were used. To launch a confidentiality or integrity attack, attackers can be verified the communication network access and confidential data [19, 24]. As a result, authentication and access control are key to reduce integrity attacks on the SG system.

3.3.3. Confidentiality. In particular, confidentiality protects permitted limits on access to and dissemination of records. In other words, the confidentiality criterion includes preventing unauthorized persons, organizations, or systems from disclosing or accessing proprietary or sensitive details [82]. Confidentiality is compromised if materials are released deprived of permission. For instance, information transmitted among the customer and multiple agencies, i.e., metering use, meter management, and billing information, can be private and protective; else, the customer's information can be exploited and changed, or other uses nefarious purposes [24]. Confidentiality attacks have a negative impact on the communication network's functionality. Confidentiality attacks seek toward obtaining the data that should be kept or disclosed confidential between trusted parties. Accessing device memory unlawfully, replay attacks, spoofing payload, and altering the software control of SG are some instances of confidentiality attacks. Password attacks commonly include the social manipulation, dictionary attacks, password sniffing, and password guessing. Social manipulation is a technique of breaking into a scheme utilizing social skills relatively technical skills [15, 74].

Eavesdropping is a kind of passive attack that also compromises data confidentiality [20, 65]. Eavesdropping attacks on local area networks (LANs) in SG networking systems sniff IP packets or intercept wireless transmissions, causing harm to the system's accountability and transparency. Encryption protects sensitive information from eavesdropping attacks [83]. Traffic analysis attacks are passive confidentiality attacks. Interpreting and sniffing the messages permit the attackers to get crucial data around the communication pattern among the networks. Masquerading attacks, also known as impersonating or identity spoofing, are other confidentiality attacks [84]. Other confidentiality attacks include unauthorized access, MITM, and data injection attacks [10, 63, 78, 84, 85]. To prevent confidentiality attacks, smart grid equipment must include authentication, data encryption, and awareness of privacy protocols.

3.3.4. Authentication. Machine and human authentication is of high importance; besides this, it is also a weakness because it can lead and cause the attacker to gain access to personal and confidential information or illegitimate devices creating

Table 4: General application and assessment details of SG standards and protocols.

No	Standard	Scope	Type	Range	Applicability	CT	Pby	Ref
1	ISO/IEC 27001 & 27002	IS management	General and technical	Worldwide	All components	Yes	2000	[101, 102]
2	The State Grid Corporation of China (SGCC) Framework	Management in electric sector	General and technical	China	All components	Yes	2002	[111]
3	IEEE 1686	Cyber security	Technical	Worldwide	Substations	Yes	2007	[105]
4	IEC 62351	Security of communication protocols	Technical	Worldwide	All components	Yes	2007	[96, 97]
5	AMI-SER	CS requirements for procurement	Technical	US	AMI	Yes	2008	[94]
6	GB/T 22239	IS management	Technical	China	All components	Yes	2008	[103]
7	NIST SP 800-64	CS	Technical	US	Systems in development	yes	2008	[109]
8	NIST SP 800-115	CS testing and assessment	Technical	US	All components	Yes	2008	[108]
9	ISO/IEC 15408 and 18045	Security evaluation criteria	Technical	Worldwide	IT products (hardware and software)	No	2008 (2012)	[104]
10	DHS catalog	IACS security	Technical	US	IACS (SCADA)	Yes	2009	[109]
11	IEC 62443 (ISA99)	Security of IACS	Technical	Worldwide	All components	Yes	2009	[106]
12	IEC Strategic Group 3 SG	Security of communication protocols and IACS	Technical	Worldwide	All components	Yes	2009	[105]
13	SG Interoperability Panel	Communication protocols	Technical	US	All components	Yes	2009	[107, 109]
14	NIST	Cyber and information security, risk management	General and technical	US*	Enterprise and systems in development	Yes	2010	[99, 100]
15	NRC RG 5.71	CS of nuclear infrastructure	General	US	All components	Yes	2010	[107]
16	German Standardization Roadmap E-Energy/SG	Energy storage systems' interoperability	Technical	German	Storage	No	2010	[107, 110]
17	ITU-T Smart Grid Focus Group	Security of communication protocols	Technical	Worldwide	All components	Yes	2010	[107]
18	ISO/IEC 27005	Risk management	General	Worldwide	Enterprise	Yes	2011	[101, 102]
19	European Commission SG Mandate Standardization M/490	Management in electric sector	General and technical	Europe	All components	Yes	2011	[112]
20	Japanese Industrial Standards Committee Roadmap to International Standardization for SG	Management in electric sector	General and technical	Japan	All components	Yes	2012	[107]
21	CEN-CENELEC-ETSI SG Coordination Group	Management in electric sector	Technical	Worldwide	All components	Yes	2012	[95]
22	NIST SP 800-53	Information security management	General	US*	Enterprise	Yes	2013	[109]
23	NIST SP 800-82	IACS security	Technical	US*	IACS (SCADA)	Yes	2013	[99]
24	NERC-CIP	Bulk power system cyber security	General	US	All components	Yes	2013	[98]
25	IEEE Std 2030-2011		Technical	Worldwide	Storage	No	2015	[108]

Table 4: Continued.

No	Standard	Scope	Type	Range	Applicability	CT	Pby	Ref
		Energy storage systems' interoperability						
26	Open SG Security Working Group	Security and communication	General and technical	-	All components	Yes	-	[7]

∗Also it is used world-wide.

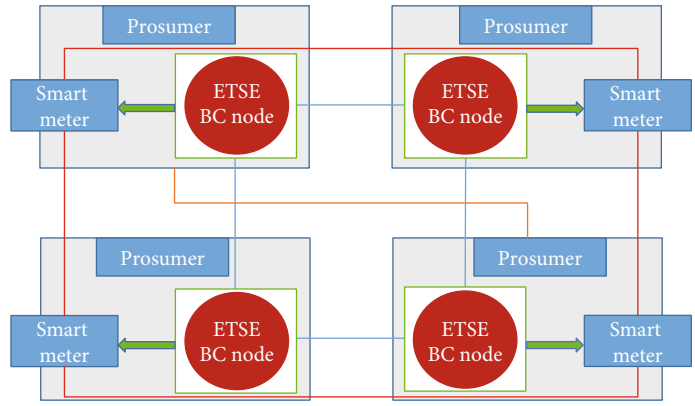

Figure 9: A smart contract enabled permissioned BC in SG [119].

procedure of the SG resources [29]. One of the most challenging aspects of SG communication is authentication. The SCADA systems with communication standards and protocol systems are used in modern SG applications. However, these networks' protocols are often sensitive to MITM attacks, impersonation attacks, and replay attacks. Also, cryptographic keys are applied in the system's different devices that can be exploited. Integrating the SCADA system into Internet communication infrastructure raises security and privacy risks considerably [86]. Mutual authentication between smart devices can be achieved using identity-based authentication and critical public infrastructure (PKI) methods [87]. To avoid authentication attacks, the late-launch dynamic root of trust for measurement (DRTM) technology can be applied to secure the cryptographic key of a specific device [88]. Moreover, to prevent authentication attacks on a mobile RFID-based SG network, an authentication technique can be developed; however, it adds cost and memory [89].

3.3.5. Authorization. They are granting access and permission to the computer (also known as access control). Because of the large number of devices besides these people involved in a SG network system, an authorization system is needed to ensure that information and resources are adequately controlled [29]. Unauthorized individuals or systems are prohibited from access to the system without authorization [79]. For this CS, required authorization refers to a decision differentiating between authorized and illegitimate parties based on authentication. If authorization is breached, it may result in security risks. Access control ensures that resources in the smart grid are only accessible by appropriate personnel and entities who have been properly identified [80]. Strict authentication measures should be established to prevent unwanted access to sensitive data and vital assets [24]. Flexible access control, compulsory access control, and role-based access control are examples of authentication techniques that can improve system performance and minimize security risks. As a result, access controls are required to limit the device's network and user's access.

3.3.6. Nonrepudiation. Attempt to convince that a device or user's operation cannot be reversed later. For example, an IoT system cannot deny sending a message it has already received. When sensitive resources and knowledge are involved, nonrepudiation becomes a major problem [82, 90]. Data integrity relies heavily on nonrepudiation and legitimacy. Accountability attacks are aimed at changing client information such as account information, payment information, or network operation data such as device status and voltage measurements. Such attacks try to interfere with the source information in the communication network process to interrupt vital communication process in the smart grid [91].

3.4. Security Standard and Protocol. There are many security algorithms, standards, and protocols presented to provide the security in the SG system. In an overall standard, generation companies and customers/consumers are linked in distributed ledger and peer-to-peer communication with a trusted third party (TTP) [92]. In SG application, the widely applicable protocol is open smart grid protocol (OSGP) via encryption techniques. However, the rigorous study shows that OSGP encryption mechanism has some weaknesses.

Table 5: Summary of blockchain-based solutions in smart grid.

Ref	Year	Publication	Country	Sources	Methods/Fields	Finding
[15]	2017	J	USA	IEEE	Transactive energy applications	Using a blockchain-based AMI to allow stable and quick energy exchange between DERs
[120]	2018	J	Romania	MDPI	Decentralized demand response program management	A distributed ledger with blockchain technology for storing SM data (also known as energy transactions) and balancing energy demand and supply
[121]	2019	J	Norway	IEEE	Traceable and transparent energy usage	In the SG, a permissioned blockchain ensures anonymity and energy protection (traceable and open energy usage).
[122]	2019	J	China	MDPI	Energy demand and supply information	For energy service providers, a blockchain-based privacy-preserving energy scheduling model
[123]	2017	J	China	IEEE	Peer-to-peer energy trading	A consortium-based energy blockchain
[124]	2020	J	Australia	IEEE	Peer-to-peer energy trading	Next-generation energy management technique with reducing peak demand
[125]	2018	J	China	Springer	Smart grid power trading	A consortium that uses blockchain technology to make energy trading more effective, scalable, and secure
[126]	2019	C	Canada	IEEE	Energy trading in V2G setup	A hierarchical authentication scheme based on the blockchain for privacy-preserving and transferring the energy from V2G and awarding EVs
[127]	2019	J	USA	IEEE	Crowdsourced energy system, P2P energy trading, and energy market	A crowdsourced energy infrastructure and energy sharing model aided by blockchain technology
[128]	2019	J	Singapore	Science Direct	Interconnected cyberphysical systems (CPSs)	ICS-BlockOpS is a blockchain-based industrial control system architecture that ensures organizational data immutability, consistency, and redundancy.
[129]	2018	J	China	IEEE	Smart grid monitoring	Blockchain is being used to map smart grids between power utilities and consumers for data transparency.
[130]	2019	J		IEEE	Industrial CPS	A completely decentralized, blockchain-oriented architecture for a more stable and efficient industrial CPS infrastructure while still addressing the existing shortcomings of cloud-based systems
[131]	2018	J	China	IEEE	Electric vehicle (EV) charging services in smart community	A stable electric vehicle charging system using a blockchain-based approach combined with contract theory, including an efficient scheduling algorithm and innovative energy allocation in the Internet of Things
[132]	2019	C	USA	IEEE	ESU charging coordination in smart grid	A decentralized, open, and privacy-preserving synchronize charging platform for ESUs like EVs and batteries built on blockchain technology
[133]	2018	J	China	IEEE	IoE for EVs and their charging pile management	LNSC, a decentralized security model based on blockchain, has been developed to improve the protection of transactions between EV and charging stations.
[134]	2018	J	Austria	Springer	EVs charging management	To find the best charging station, energy costing and distance to the EVs were used in a blockchain-assisted automated and privacy-preserving protocol.
[135]	2017	C	USA	IEEE	Microgrid optimization and control	To solve market price coercion and privacy leakage issues by microgrid aggregators or operators, a decentralized microgrid operating architecture is built on blockchain and the alternating path system of multipliers (ADMM).
[136]	2018	C	Denmark	IEEE	Voltage control in microgrid	A blockchain-based commensurate management system to reward DERs for their contributions to microgrid voltage regulation
[137]	2019	J		IEEE	Grid operation services for TES	A distributed voltage control algorithm for transactive energy systems (TESs) based on blockchains
[138]	2017	J	China	MDPI	Electricity transactions in microgrid	A decentralized microgrid energy transaction mode based on blockchain and continuous double auction (CDA) to provide autonomous transactions between distributed generations (DGs) and consumers

Table 5: Continued.

Ref	Year	Publication	Country	Sources	Methods/Fields	Finding
[139]	2017	C	USA	IEEE	Resilient networked microgrids	A decentralized transactive microgrid model
[140]	2020	C	USA	IEEE	Utilize cognitive methods and tiered blockchain architecture	Scalable blockchain distributed adaptive protection and network architecture with data exchange security
[141]	2020	C	India	IEEE	Challenges of blockchain technology for rural electrification	Make revenue as per budget using blockchain peer-to-peer trading; smart metering continues accuracy and transparency of energy transactions.
[142]	2020	J	Algeria	Elsevier	Fog-based SCADA systems for cyber security	The security vulnerability and requirement solution system are classified, i.e., authentication solution, intrusion detection and management systems, and privacy-preserving solutions.
[143]	2021	J	China	Hindawi	Authentication and authorization protocol	Blockchain-based power system protocol integrates resource authorization and immutable ledger characteristics and identifies decentralized authentication in smart grid systems.
[144]	2021	J	China	IEEE	Peer-to-peer energy trading	Five-layer design of local energy market based on blockchain

The weakness is generating and transmitting messages by stream cypher encryption with a new key to another customer where only difference is the first 8 bytes of the key. Another issue is using this generate encryption key to use in authentications. After that, when the BC was introduced and used in the SG application, the security issues are solved. Using the existing security protocol in BC architecture became more secure [93]. The existing SG standards and protocols are as follows: AMI-SER [94], CEN-CENELEC-ETSI SG Coordination Group [95], IEC 62351 [96, 97], NERC-CIP [98], IST [99, 100], ISO/IEC 27001 and 27002 [101, 102], GB/T 22239 [103], ISO/IEC 15408 and 18045 [104], IEC Strategic Group 3 SG [105], IEC 62443 (ISA99) [106], IEC 62443 (ISA99) [107], IEEE Std 2030-2011 [108], IEEE 1686 [105], DHS catalog [109], German Standardization Roadmap E-Energy/SG [108, 110], NIST SP 800-82 [99], NRC RG 5.71 [107], NIST SP 800-53 & 800-64 [110], NIST SP 800-115 [108], Open SG Security Working Group [108], ITU-T SG Focus Group [107], SG Interoperability Panel [108, 109], The State Grid Corporation of China (SGCC) Framework [111], European Commission SG Mandate Standardization M/490 [112], and Japanese Industrial Standards Committee (JISC) Roadmap to International Standardization for SG [107].

The SG standard and protocol summary is presented in Table 4, which presents the applicable scope, types, ranges, applicability, communication technologies (CT), and publication year (Pby).

4. Overview of Blockchain (BC)

The BC is a computer network-based archives (big data system), where hackers can access any place worldwide. This is a fully transparent system, where if provisioned for public BC, all service providers and consumers can see the change made and transactions [113]. For this, BC focused on responsiveness in many industries. This is significantly applied in the energy industry, communication, data exchanges, e-treading, and authorization and authentication tamper-proof mechanism. In the point of energy trading, BC technology adopts the grid energy [114].

The block transection of BC is achieved by secure and integrated consensus algorithms [115]. In 2008, the first cryptocurrency, Bitcoin, was introduced in the market and this is the peer-to-peer electronic currency transfer process. In this transection process, without authorization from one party to another party, currency was securely done online transaction by a trusted third party and was first applied in BC technology. This BC technology is significantly and successfully applied in the financial industry, SG, electric vehicle (EV) system, healthcare, IoT, supply chain, etc. [116].

4.1. Blockchain Mechanism for Smart Grid. The integration of BC with SG technology is becoming so sophisticated key solutions for facilitating comprehensive security functionality SG technology. The core related interfaces, components, and applications of SG that are critically security dependent are discussed in analyzing the key RQs. The existing centralized ledger system may be transferred by BC technology into a distributed ledger because of the public key algorithm. It also has end-to-end encryption technology and, due to the distribution processing structure, guarantees low costs. The idea of blockchains is generating a lot of research and functional attention right now. A BC is a cryptographic collection of node blocks, where the headers, corresponding transaction data, and auxiliary protection metadata are secured for each block. Intrinsically, the BC supports free connectivity, incorruptibility, openness and secure storage, and transfer of data [117, 118]. In recent years, several BC implementations have arisen beyond initial cryptocurrency applications, like Bitcoins.

Bitcoin's BC system is a public data database that saves the history of Bitcoin value transfers updated regularly. To avoid forgery, this ledger is created using cryptographic technology.

Table 6: Key findings of the IoT-based paper and their primary studies.

Ref	Publication type	Year	Finding	Types of security applications
[150]	J	2016	Proof of the pseudonymous concept protocol for secure communications among the IoT devices using Bitcoin in blockchain technology	IoT
[151]	J	2016	A broad review of the advantages of blockchain-based IoT devices. For example, instead of distributing firmware patches from the middle, IoT devices from one vendor are connected to the same blockchain firmware and spread peer to peer. It is acknowledged that a token is needed. Alternative solutions are presented.	IoT
[152]	J	2018	Deprived of relying on an essential service like Notary, a blockchain-based system for ensuring the authenticity of Docker images has been developed (offers to defend against denial of service). The importance of a robust blockchain has been recognized.	Internet of Things & Docker
[153]	C	2017	Blockchain is used to build a multilevel network of IoT computers. Rather than entirely autonomous nodes and miners, the blockchain's security is managed by coordination between layers.	IoT
[154]	C	2017	A concept for low-power IoT devices can connect with a proper gateway to allow Ethereum blockchain node communication.	IoT
[155]	C	2018	Introducing "ControlChain," a blockchain-based access power system for IoT devices. Using the same concepts as the Bitcoin blockchain, multiples are proposed. In blockchains, IoT control could be used to handle different aspects.	IoT
[156]	C	2018	IoT data privacy, access, and trading are the main topics of discussion, suggesting a blockchain solution for each to provide anonymity. The Ethereum platform is being used.	IoT
[157]	J	2017	Discussion on blockchain strengths and security, mainly with IoT. Highlighting IoT supply chain from manufacturer to end-user security benefits	IoT
[158]	J	2021	Authentication methods for fog cloud IoT architecture	IoT
[159]	J	2021	Provides a data mining technique based on Fischer linear discrimination and quadratic discrimination analysis	Big data and IoT
[160]	J	2018	A thorough examination of IoT protection. What role could blockchain play in addressing the challenges of reducing current security threats to such devices? Mentioning Ethereum as a possible medium for developing smart contracts in an alternative manner	IoT
[161]	C	2018	Suggestion to create "IoT Chain," a blockchain-based system that allows the authentication to IoT devices and secure access. The Ethereum platform was used to assess the viability of their plan. Authentication servers, key servers, and clients are the three full nodes used by the researchers. The latter serves as the transaction miner, storing data on the blockchain through proof-of-stake and proof-of-work consent mechanisms. The researchers create their Proof-of-Possession system for IoT Chain.	IoT
[162]	C	2019	Blockchain technology based on various technology in smart grid is discussed in this paper, i.e., cost reduction, communication between provider and consumer, machine-to-machine interaction, and security.	IoT
[163]	J	2019	User-friendliness and energy optimization in terms of electronics devices controlling and monitoring. This study focused on the interdisciplinary domain that will be helpful for new researchers.	IoT
[164]	J	2020	Build a green IoT ecosystem based on blockchain technology and discussed the crucial factors and future research direction for a sustainable green IoT ecosystem.	IoT
[165]	J	2020	Blockchain-based IoT architecture for HANs and NANs in SG system	IoT
[166]	J	2021	Blockchain-based access control protocol in IoT-enabled SG system	IoT
[167]	J	2021	IoT-based energy conversion process and inquire on future energy demand on SG system	IoT

The BC technology could help solve a numerous complex matters relating to the transparency and trustworthiness of fast, distributed, and complex data exchanges and energy transactions. Smart contracts built on the BC often exclude the need to negotiate with third parties, constructing it easier toward monetizing distributed and implementing energy transfers and connections, containing both energy flows and financial transactions (Figure 9). Table 5 presents some BC-based SG applicable methods and findings.

4.2. Blockchain Mechanism for Energy Trading. In BC technology, energy trading is necessary for academic research and industrial application with emergency SG electricity generation and distribution. The BC technology is used to reduce the fraudulent act. A certificate is issued for achieving the generators/consumers' trust/guarantee in this energy trading. Implementing BC technology makes the energy trading system easy and helps to reduce the marketing effort and minimize the time. Conventional fossil fuels are diminishing

Table 7: The field of application of the paper.

Title	Year	Topic	Publication type	Ref
Block chain-based…	2016	Smart city	J	[168]
Building a Robust…	2016	Smart energy	J	[169]
Security and privacy in decentralized….	2016	Smart property/smart city/smart energy	J	[170]
PB-PKI: A Privacy-aware……..	2017	Generic application/smart home	J	[171]
Block chain platform for……	2016	Smart manufacturing/smart city/generic application	J	[172]
Securing smart cities……..	2016	Generic application/smart home/smart city	C	[173]
A block chain connected……	2018	Smart manufacturing/generic application	J	[174]
Peer-to-Peer Approaches……	2017	Smart city/smart home	C	[175]
Block chain in Internet of Things……	2016	Generic application/smart home	J	[176]
Block chain for IoT…….	2017	Generic application/smart home	C	[177]
CertCoin:A Name Coin ……..	2014	Generic application	J	[178]
A review on block chain……	2017	Smart property	J	[179]
Cloud-based commissioning……..	2016	Smart city/smart manufacturing	C	[180]
Ethernam blockchain technology	2021	Industry 5.0	J	[181]
A novel method for……..	2015	Smart property	C	[182]
Managing IoT devices…….	2017	Smart home	C	[183]
Authcoin: Validation and Authentication…	2016	Generic application	J	[184]
Integration of the……	2017	Smart city/smart home/smart energy	C	[185]
Towards a novel……	2018	Generic application	J	[186]
Converging block chain……..	2019	Generic application	j	[187]
Towards block chain……..	2017	Generic application	J	[188]
Block chain technology…….	2017	Smart manufacturing	J	[189]
A Peer-to-Peer……..	2014	Smart home	J	[190]
When your sensor…….	2017	Generic Application	C	[191]
A block chain-based……..	2018	Generic application	J	[192]
An IoT electric…….	2015	Smart property	C	[193]
Decentralized Computation…….	2015	Generic application	J	[194]
Decentralized Access…….	2019	Others	J	[195]
Hybrid-IoT: Hybrid……..	2018	Generic application	J	[196]
Managing computation……	2018	Generic application	C	[197]
An out-of-band……..	2018	Smart home	C	[198]
OSCAR: Object security…….	2015	Generic application	J	[199]
Privacy-preserving and……..	2018	Generic application/smart energy	J	[200]
Block chain technologies…….	2016	Generic application	C	[201]
Digital supply chain……	2017	Generic application/ smart manufacturing	C	[202]
Block chain technology……	2016	Generic application	C	[203]
Semantic block chain……..	2017	Generic application	J	[204]
Blockchain in the construction……...	2019	Constriction sector	J	[205]
DeliveryCoin: An IDS and blockchain…….	2019	Automotive industry	J	[206]
Demonstrating blockchain……	2019	Energy trading	J	[207]
Phase offset analysis of asymmetric…….	2019	Smart grid	J	[208]
Dynamic pricing in industrial……..	2020	Smart city	J	[209]
Blockchain outlook for……	2020	Smart home	J	[210]
HSIC bottleneck based distributed…….	2020	Smart grid	J	[211]
A blockchain-enabled secure……..	2020	Energy trading	J	[212]
An approach for applying blockchain……..	2021	Energy trading	J	[213]
Emergence of blockchain-technology…….	2021	Energy trading	J	[214]
Lightweight Cryptographic Algorithms…...	2021	Cyber security	J	[215]

Table 7: Continued.

Title	Year	Topic	Publication type	Ref
Machine Learning Technologies……	2021	Automotive industry	J	[216]
ElStream: An Ensemble Learning……	2021	Machine learning techniques	J	[217]
Blockchain and ANFIS empowered…..…..	2021	Privacy tracing	J	[218]
An improved dynamic thermal…….	2021	Big data	J	[219]
Toward Blockchain for Edge-of-Things…..	2021	Smart grids/big data	J	[220]
A peer-to-peer blockchain……..	2021	Smart grid	J	[221]
Sustainable Security for……	2021	Cyber security/big data	J	[222]

rapidly, and researchers and governments worldwide are looking for suitable alternative energy sources like renewable energy. For this, many smaller generated companies produce energy for smaller grid scale and need to connect in the national grid so that consumers can buy [145, 146].

Additionally, the consumer also produces the energy and sells it on the market. The BC system gives an efficient peer-to-peer trading process for local consumers, which generates a small amount of energy. The peer-to-peer topology automatically handles this data and stores it on the public ledger, where all copies are reflected over the network. The BC technology transmits the data and communicates with SG network in a block node. All nodes are connected where every device shares the address and information with previous devices [115].

4.3. Blockchain Mechanism for Electric Vehicles. Last few years, EV connection with SGs has been an important and hot topic. Primarily, EV charging systems make more concern to connect with the SG. The power grid system can face severe stress for EV irrelevant charging. Thus, BC technology adopted this problem with several approaches. The BC technology in EV charging integration was discussed in [147–149]. Researchers recommended integrating the EV charging system with the BC technology to be able to find out a near charging station so that EVs can charge. Using this BC technology, EV was used easily to find out the low cost and best location for EV charging station to ensure the privacy and security system.

5. Discussion

Since smart grid technology is the most incredible tool for dealing with the complexities of rising energy demand in the future, we should be more mindful of how to use it specifically and wisely. Both underdeveloped and emerging countries, like developed countries, should begin developing policies to make their grid systems smarter and cleaner. There is an adage that says, "cleaner electricity is smarter electricity." And, in this age of environmental degradation, we need a reasonable amount of renewable energy. Smart grid infrastructure assists in the interconnection of national networks. Smart grid systems can transmit energy through a smart web infrastructure, with far-flung transmission and delivery guaranteeing the system's perfection. Under the English Channel, an IF 2000 Under Sea connection creates 2000MW HVDC submarine interconnection that ties up the national grids of France and the United Kingdom. Via a bidirectional transmission and delivery network, this interconnection network assists all countries in meeting their increased energy demand as peak demand rises. Tables 6 and 7 present some funding and application of BC-related published work.

6. Conclusion

A SG infrastructure attack does not only affect consumers; it also affects energy providers' profitability. There are several risks to the SG networks that could turn into attacks depending on the adversary's benefit. To make identifying and analyzing such attacks easier, we have divided them into five categories. The paper also looks at and reports on countermeasures for all types of assaults. Extensive research is also required to ensure that IoT and big data on the SG system can protect against adversarial threats without compromising customer trust in the utility provider or dramatically inconvenience. Based on the survey, we still found some research gaps; those are required more concern and improvement for a sustainable BC-based SG and energy trading system. To address issues and challenges, the further improvements and recommendations are as follows:

(i) The BC in different SG systems needs efficient cryptographic schemes

(ii) BC network required penalty and incentive mechanisms

(iii) Advance privacy, security, and data communication exchanges

(iv) The BC-based SG system is required to keep penalty/reward policies

(v) Interoperability limitation among the SG process

(vi) Game theory, cognitive modeling, and deep learning need to add a standard processing technique for benchmark and validation

(vii) SG energy sources required optimal allocation

(viii) Renewable/storage energy system required communication and advance metering for integration with SG, control, and monitoring

(ix) Energy management systems are required considering the burden and computational complexity to design and implement

(x) SG required more focus to handle uncertainty: source intermittency, weather condition, electric vehicle/plug-in-electric vehicle driving pattern, impulsive human behavior during the load connection, and disconnection

Data Availability

All related data is available in the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This work was supported by the Universiti Kebangsaan Malaysia (UKM) under the FRGS/1/2020/ICT03/UKM/02/6 and GP-2021-K023208.

References

[1] S. Paul, M. S. Rabbani, R. K. Kundu, and S. M. R. Zaman, "A review of smart technology (smart grid) and its features," in *2014 1st International Conference on Non Conventional Energy (ICONCE 2014)*, pp. 200–203, Kalyani, India, 2014.

[2] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, article 106382, 2020.

[3] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[4] D. Zheng, K. Deng, Y. Zhang, J. Zhao, X. Zheng, and X. Ma, *Smart Grid Power Trading Based on Consortium Blockchain in Internet of Things*, vol. 11336 LNCS, Springer International Publishing, 2018.

[5] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5799–5812, 2020.

[6] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391–404, 2012.

[7] B. Zheng, W. Wei, Y. Chen, Q. Wu, and S. Mei, "A peer-to-peer energy trading market embedded with residential shared energy storage units," *Applied Energy*, vol. 308 Article I.D. 118400, 2022.

[8] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: a survey," *IEEE Communication Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[9] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: motivations, requirements and challenges," *IEEE Communication Surveys and Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

[10] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communication Surveys and Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[11] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "Implementation of blockchain technology for energy trading with smart meters," *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, 2019, pp. 1–5, Vellore, India, 2019.

[12] J. A. Abdella and K. Shuaib, "An architecture for blockchain based peer to peer energy trading," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 412–419, Granada, Spain, 2019.

[13] F. S. Ali, M. Aloqaily, O. Alfandi, and Ö. Özkasap, "Cyber-physical blockchain-enabled peer-to-peer energy trading," *Computer*, vol. 53, no. 9, pp. 56–65, 2020.

[14] R. K. Kodali, S. Yerroju, and B. Y. K. Yogi, "Blockchain based energy trading," in *TENCON 2018-2018 IEEE Region 10 Conference*, vol. 1, pp. 1778–1783, Jeju, Korea (South), October 2018.

[15] A. A. Habib, M. K. Hasan, M. Mahmud, S. M. A. Motakabber, M. I. Ibrahimya, and S. Islam, "A review: energy storage system and balancing circuits for electric vehicle application," *IET Power Electronics*, vol. 14, no. 1, pp. 1–13, 2021.

[16] S. Kakran and S. Chanana, "Smart operations of smart grids integrated with distributed generation: a review," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 524–535, 2018.

[17] T. Q. D. Khoa, P. T. T. Binh, and H. B. Tran, "Optimizing location and sizing of distributed generation in distribution systems," in *2006 IEEE PES Power Systems Conference and Exposition*, pp. 725–732, Atlanta, GA, USA, 2006.

[18] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, 2020.

[19] S. Ahmed, T. M. Gondal, M. Adil, S. A. Malik, and R. Qureshi, "A survey on communication technologies in smart grid," in *2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*, pp. 7–12, Bangkok, Thailand, 2019.

[20] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power grid - challenges, issues, advantages and status," in *2011 IEEE/PES Power Systems Conference and Exposition*, pp. 1–7, Phoenix, AZ, USA, 2011.

[21] I. Colak, E. Kabalci, G. Fulli, and S. Lazarou, "A survey on the contributions of power electronics to smart grid systems," *Renewable and Sustainable Energy Reviews*, vol. 47, no. 1, pp. 562–579, 2015.

[22] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, no. 11, pp. 2742–2771, 2012.

[23] H. E. Brown, S. Suryanarayanan, and G. T. Heydt, "Some characteristics of emerging distribution systems considering the smart grid initiative," *The Electricity Journal*, vol. 23, no. 5, pp. 64–75, 2010.

[24] W. Wang and Z. Lu, "Cyber security in the smart grid: survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[25] G. F. Reed, P. A. Philip, A. Barchowsky, C. J. Lippert, and A. R. Sparacino, "Sample survey of smart grid approaches and technology gap analysis," in *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*, pp. 1–10, Gothenburg, Sweden, 2010.

[26] M. H. F. Wen, K. C. Leung, V. O. K. Li, X. He, and C. C. J. Kuo, "A survey on smart grid communication system," *APSIPA Transactions on Signal and Information Processing*, vol. 4, p. 2015, 2015.

[27] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: a survey," *Computer Communications*, vol. 91-92, pp. 17–28, 2016.

[28] A. R. Khan, A. Mahmood, A. Safdar, Z. A. Khan, and N. A. Khan, "Load forecasting, dynamic pricing and DSM in smart grid: a review," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 1311–1322, 2016.

[29] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11883–11915, 2015.

[30] P. Siano, "Demand response and smart grids–a survey," *Renewable and Sustainable Energy Reviews*, vol. 30, pp. 461–478, 2014.

[31] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 6153–6158, Beijing, China, October 2017.

[32] S. Alam, M. F. Sohail, S. A. Ghauri, I. M. Qureshi, and N. Aqdas, "Cognitive radio based smart grid communication network," *Renewable and Sustainable Energy Reviews*, vol. 72, pp. 535–548, 2017.

[33] N. Shaukat, S. M. Ali, C. A. Mehmood et al., "A survey on consumers empowerment, communication technologies, and renewable generation penetration within smart grid," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 1453–1475, 2018.

[34] J. Wu and N. K. Tran, "Application of blockchain technology in sustainable energy systems: an overview," *Sustainability*, vol. 10, no. 9, p. 3067, 2018.

[35] N. Wang, X. Zhou, X. Lu et al., "When energy trading meets blockchain in electrical power system: the state of the art," *Applied Sciences*, vol. 9, no. 8, p. 1561, 2019.

[36] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *Ieee Access*, vol. 7, pp. 86746–86757, 2019.

[37] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for future smart grid: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.

[38] G. Dileep, "A survey on smart grid technologies and applications," *Renewable Energy*, vol. 146, pp. 2589–2625, 2020.

[39] C. Liu, X. Zhang, K. K. Chai, J. Loo, and Y. Chen, "A survey on blockchain-enabled smart grids: advances, applications and challenges," *IET Smart Cities*, vol. 3, no. 2, pp. 56–78, 2021.

[40] D. Wang, H. Wang, and Y. Fu, "Blockchain-based IoT device identification and management in 5G smart grid," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, 19 pages, 2021.

[41] Z. El Mrabet, H. El Ghazi, N. Kaabouch, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 1, no. 67, pp. 469–482, 2018.

[42] Y. Deng and S. Shukla, "Vulnerabilities and countermeasures – a survey on the cyber security issues in the transmission subsystem of a smart grid," vol. 1, pp. 251–276, 2012.

[43] S. Wang, C. Zhang, and Z. Su, "Detecting nondeterministic payment bugs in Ethereum smart contracts," *Proceedings of the ACM on Programming Languages*, vol. 3, no. OOPSLA, pp. 1–29, 2019.

[44] N. Komninos, E. Philippou, A. Pitsillides, and S. Member, "Survey in smart grid and smart home security : issues , challenges and countermeasures," *IEEE Communication Surveys and Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[45] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, 2017.

[46] P. Li, Y. Liu, H. Xin, and X. Jiang, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4343–4352, 2018.

[47] R. M. S. Priya, S. Bhattacharya, P. K. R. Maddikunta et al., "Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything," *Journal of Parallel and Distributed Computing*, vol. 142, pp. 16–26, 2020.

[48] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[49] M. K. Hasan, M. Mahmud, A. K. M. Ahasan Habib, S. M. A. Motakabber, and S. Islam, "Review of electric vehicle energy storage and management system: standards, issues, and challenges," *Journal of Energy Storage*, vol. 41, p. 102940, 2021.

[50] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 226–231, Gaithersburg, MD, USA, October 2010.

[51] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *2012 45th Hawaii International Conference on System Sciences*, pp. 1907–1914, Maui, HI, USA, January 2012.

[52] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2019.

[53] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1330–1339, 2017.

[54] S. Gholami, S. Saha, and M. Aldeen, "A cyber attack resilient control for distributed energy resources," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, Torino, Italy, September 2017.

[55] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[56] J. Hao, E. Kang, J. Sun et al., "An adaptive Markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2398–2408, 2018.

[57] A. Farraj, E. Hammad, and D. Kundur, "On the impact of cyber attacks on data integrity in storage-based transient stability control," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3322–3333, 2017.

[58] A. Farraj, E. Hammad, and D. Kundur, "A systematic approach to delay adaptive control design for smart grids," in *Proceedings of the IEEE International Conference on Smart Grid Communications*, pp. 768–773, Miami, FL, USA, November 2015.

[59] A. Farraj, E. Hammad, and D. Kundur, "Enhancing the performance of controlled distributed energy resources in noisy communication environments," in *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 1–4, Vancouver, BC, Canada, May 2016.

[60] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, pp. 1205–1215, 2018.

[61] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proceedings of the Preprints 1st Workshop Secure Control Systems (CPSWEEK)*, pp. 1–9, Stockholm, Sweden, April 2010.

[62] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: classification by sources of threats," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, 2018.

[63] A. Procopiou and N. Komninos, "Current and future threats framework in smart grid domain," in *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pp. 1852–1857, Shenyang, China, 2015.

[64] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, "Cyber attack models for smart grid environments," *Sustainable Energy, Grids and Networks*, vol. 12, pp. 10–29, 2017.

[65] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1–5, Malatya, Turkey, 2018.

[66] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self-Systems (FAS-W)*, pp. 242–247, Augsburg, Germany, 2016.

[67] T. Bhatt, C. Kotwal, and N. Chaubey, "Survey on smart grid : threats , vulnerabilities and security protocol," *International Journal of Electrical, Electronics and Computer Systems(I-JEECS)*, vol. 6, p. 340, 2017.

[68] N. Nurelmadina, M. K. Hasan, I. Memon et al., "A systematic review on cognitive radio in low power wide area network for industrial IoT applications," *Sustainability*, vol. 13, no. 1, p. 338, 2021.

[69] M. F. Ali, N. A. Abu, and N. Harum, "A novel session payment system via Internet of Things (IOT)," *International Journal of Applied Engineering Research*, vol. 12, no. 23, pp. 13444–13450, 2017.

[70] R. K. Pandey and M. Misra, "Cyber security threats — smart grid infrastructure," in *2016 National Power Systems Conference (NPSC)*, pp. 1–6, Bhubaneswar, India, 2016.

[71] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Computer Science*, vol. 34, pp. 532–537, 2014.

[72] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical smart grid infrastructures," in *ISGT 2014*, pp. 1–5, Washington, DC, USA, 2014.

[73] R. Kaur, A. L. Sangal, and K. Kumar, "Modeling and simulation of DDoS attack using omnet++," in *2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 220–225, Noida, India, 2014.

[74] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on smart grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, pp. 1–7, Manchester, UK, 2011.

[75] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K. C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 847–870, 2018.

[76] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: challenges and solutions," in *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pp. 170–175, Offenburg, Germany, 2015.

[77] E. B. Rice and A. AlMajali, "Mitigating the risk of cyber attack on smart grid systems," *Procedia Computer Science*, vol. 28, pp. 575–582, 2014, 28.

[78] D. Acarali, K. R. Rao, M. Rajarajan, D. Chema, and M. Ginzburg, "Modelling smart grid IT-OT dependencies for DDoS impact propagation," *Computers & Security*, vol. 12, p. 102528, 2022.

[79] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communication Surveys and Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[80] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: status, challenges and perspectives," in *SouthEastCon 2015*, pp. 1–6, Fort Lauderdale, FL, USA, 2015.

[81] Z. A. Baig and A. R. Amoudi, "An analysis of smart grid attacks and countermeasures," *The Journal of Communication*, vol. 8, no. 8, pp. 473–479, 2013.

[82] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1-2, pp. 1–13, 2018.

[83] V. Delgado-gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in *2015 9th International Conference on Compatibility and Power Electronics (CPE)*, pp. 534–538, Costa da Caparica, Portugal, 2015.

[84] Carlos Lopez, Arman Sargolzaei, Hugo Santana, and Carlos Huerta, "Smart grid cyber security: an overview of threats and countermeasures," *Journal of Energy and Power Engineering*, vol. 9, no. 7, pp. 632–647, 2015.

[85] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: issues, challenges and countermeasures," *IEEE Communication Surveys and Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[86] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[87] S. Lee, J. Bong, S. Shin, and Y. Shin, "A security mechanism of smart grid AMI network through smart device mutual authentication," in *The International Conference on Information Networking 2014 (ICOIN2014)*, pp. 592–595, Phuket, Thailand, 2014.

[88] A. J. Paverd and A. P. Martin, "Hardware Security for Device Authentication in the Smart Grid," in *Smart Grid Security. SmartGridSec 2012*, vol. 7823Springer, Berlin, Heidelberg.

[89] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Authentication mechanism for mobile RFID based smart grid network," in *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–6, Toronto, ON, Canada, 2014.

[90] M. Hossain, R. Hasan, and A. Skjellum, "Securing the Internet of Things: a meta-study of challenges, approaches, and open problems," in *2017 IEEE 37th International Conference*

on Distributed Computing Systems Workshops (ICDCSW), pp. 220–225, Atlanta, GA, USA, 2017.

[91] B. Khelifa, "Security concerns in smart grids: threats, vulnerabilities and countermeasures," in *2015 3rd International Renewable and Sustainable Energy Conference (IRSEC)*, pp. 1–6, Marrakech, Morocco, 2015.

[92] R. Das and M. Z. Gündüz, "Analysis of cyber-attacks in IoT-based critical infrastructures," *International Journal of Information Security Science*, vol. 8, no. 4, pp. 122–133, 2020.

[93] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 28, p. 100342, 2020.

[94] F. Nejabatkhah, Y. W. Li, H. Liang, and R. Reza Ahrabi, "Cyber-security of smart microgrids: a survey," *Energies*, vol. 14, no. 1, p. 27, 2021.

[95] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Reference Architecture," pp. 1–107, 2012.

[96] R. Schlegel, S. Obermeier, and J. Schneider, "Assessing the security of IEC 62351," in *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)*, pp. 11–19, Germany, 2015.

[97] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2020.

[98] North American Electric Reliability Corporation, "Critical Infrastructure Protection," April 2021https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States.

[99] Archived NIST Technical Series Publication, "Smart Grid Cyber Security," 2021, https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf.

[100] A. Gopstein, A. R. Goldstein, D. Anand, and P. A. Boynton, "Summary report on NIST smart grid testbeds and collaborations workshops," 2021.

[101] E. Kurniawan and I. Riadi, "Security level analysis of academic information systems based on standard ISO 27002: 2003 using SSE-CMM," 2018, https://arxiv.org/abs/1802.03613.

[102] V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC 27002: 2013 information security controls to personal data protection controls: guidelines for GDPR compliance," in *Computer Security*, pp. 238–257, Springer, Cham, 2019.

[103] M. A. Li, Z. H. U. Guobang, and L. U. Lei, "Baseline for classified protection of cybersecurity (GB/T 22239-2019) standard interpretation," *Netinfo Security*, vol. 19, no. 2, p. 77, 2019.

[104] S. Dotsenko, O. Illiashenko, S. Kamenskyi, and V. Kharchenko, "Integrated model of knowledge management for security of information technologies: standards ISO/IEC 15408 and ISO/IEC 18045," *Information & Security*, vol. 43, no. 3, pp. 305–317, 2019.

[105] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Computers & Security*, vol. 77, pp. 262–276, 2018.

[106] D. Dolezilek, D. Gammel, and W. Fernandes, "Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems," in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, pp. 1–16, Liverpool, UK, 2020.

[107] R. Leszczyna, "Standards on cyber security assessment of smart grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70–89, 2018.

[108] IEEE Guide for Smart Grid, "IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads," 2021, https://www.techstreet.com/standards/ieee/2030_2011?product_id=1781311#full.

[109] R. Leszczyna, "Standards with cybersecurity controls for smart grid—a systematic analysis," *International Journal of Communication Systems*, vol. 32, no. 6, article e3910, 2019.

[110] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids - a comprehensive survey," *Computer Standards & Interfaces*, vol. 56, pp. 62–73, 2018.

[111] X. Yi-chong, "China's giant state-owned enterprises as policy advocates: the case of the state grid corporation of China," *The China Journal*, vol. 79, no. 1, pp. 21–39, 2018.

[112] M. Sanduleac, "Unbundled Smart meters in the new smart grid era: assessment on compatibility with European standardisation efforts and with IoT features," in *2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON)*, pp. 35–41, Marrakech, Morocco, May 2018.

[113] S. Höhne and V. Tiberius, "Powered by blockchain: forecasting blockchain use in the electricity market," *International Journal of Energy Sector Management*, vol. 14, no. 6, pp. 1221–1238, 2020.

[114] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: exchanging distributed energy at speed, scale and security," in *2017 Resilience Week (RWS)*, pp. 18–23, Wilmington, DE, USA, September 2017.

[115] O. Samuel, N. Javaid, T. A. Alghamdi, and N. Kumar, "Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence," *Sustainable Cities and Society*, vol. 76, p. 103371, 2022.

[116] A. Hajizadeh and S. M. Hakimi, "Blockchain in Decentralized Demand-Side Control of Microgrids," in *Blockchain-Based Smart Grids*, pp. 145–167, Academic Press, 2020.

[117] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[118] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: a systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[119] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, p. 6, London, UK, 2018.

[120] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 2, p. 162, 2018.

[121] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[122] S. Tan, X. Wang, and C. Jiang, "Privacy-preserving energy scheduling for ESCOs based on energy blockchain network," *Energies*, vol. 12, no. 8, p. 1530, 2019.

[123] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[124] W. Tushar, T. K. Saha, C. Yuen, D. Smith, and H. V. Poor, "Peer-to-peer trading in electricity networks: An overview," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3185–3200, 2020.

[125] D. Zheng, K. Deng, Y. Zhang, J. Zhao, X. Zheng, and X. Ma, "Smart grid power trading based on consortium blockchain in Internet of Things," in *Algorithms and Architectures for Parallel Processing. ICA3PP 2018*, vol. 11336 of *Lecture Notes in Computer Science*, Cham, 2018.

[126] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. P. C. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Shanghai, China, 2019.

[127] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1612–1623, 2019.

[128] A. Maw, S. Adepu, and A. Mathur, "ICS-BlockOpS: blockchain for operational data security in industrial control system," *Pervasive and Mobile Computing*, vol. 59, p. 101048, 2019.

[129] J. Gao, K. O. Asamoah, E. B. Sifah et al., "GridMonitoring: secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[130] J. Wan, J. Li, M. Imran, D. Li, and Fazal-e-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019.

[131] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601–4613, 2019.

[132] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 504–509, Atlanta, GA, USA, 2019.

[133] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[134] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science - Research and Development*, vol. 33, no. 1–2, pp. 71–79, 2018.

[135] E. Munsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *2017 IEEE Conference on Control Technology and Applications (CCTA)*, pp. 2164–2171, Maui, HI, USA, 2017.

[136] P. Danzi, M. Angjelichinoski, C. Stefanovic, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 45–51, Dresden, Germany, 2017.

[137] S. Saxena, H. Farag, H. K. Turesson, and H. Kim, "Blockchain based grid operation services for transactive energy systems," 2019, https://arxiv.org/abs/1907.08725.

[138] J. Wang, Q. Wang, N. Zhou, and Y. Chi, "A novel electricity transaction mode of microgrids based on blockchain and continuous double auction," *Energies*, vol. 10, no. 12, p. 1971, 2017.

[139] M. Sabounchi and J. Wei, "Towards resilient networked microgrids: blockchain-enabled peer-to-peer electricity trading mechanism," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–5, Beijing, China, 2017.

[140] D. Sikeridis, A. Bidram, M. Devetsikiotis, and M. J. Reno, "A blockchain-based mechanism for secure data exchange in smart grid protection systems," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, Las Vegas, NV, USA, January 2020.

[141] V. Kulkarni and K. Kulkarni, "A Blockchain-based smart grid model for rural electrification in India," in *2020 8th International Conference on Smart Grid (icSmartGrid)*, pp. 133–139, Paris, France, June 2020.

[142] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: solutions and challenges," *Journal of Information Security and Applications*, vol. 52, p. 102500, 2020.

[143] Y. Zhong, M. Zhou, J. Li et al., "Distributed blockchain-based authentication and authorization protocol for smart grid," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5560621, 15 pages, 2021.

[144] Z. Zeng, M. Dong, W. Miao, M. Zhang, and H. Tang, "A data-driven approach for blockchain-based smart grid system," *IEEE Access*, vol. 9, pp. 70061–70070, 2021.

[145] I. Kouveliotis-Lysikatos, I. Kokos, I. Lamprinos, and N. Hatziargyriou, "Blockchain-powered applications for smart transactive grids," in *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pp. 1–5, Bucharest, Romania, September 2019.

[146] I. Petri, M. Barati, Y. Rezgui, and O. F. Rana, "Blockchain for energy sharing and trading in distributed prosumer communities," *Computers in Industry*, vol. 123, p. 103282, 2020.

[147] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[148] S. Chen, J. Ping, Z. Yan, and W. Wei, "Blockchain for decentralized optimization of energy sources: EV charging coordination via blockchain-based charging power quota trading," in *Blockchain-Based Smart Grids*, pp. 169–179, Academic Press, 2020.

[149] P. W. Khan and Y. C. Byun, "Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles," *Sustainability*, vol. 13, no. 14, p. 7962, 2021.

[150] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new blockchain-based access control framework for the Internet of Things," *Security and Communication Networks*, vol. 9, 5964 pages, 2016.

[151] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[152] Q. Xu, C. Jin, M. F. B. M. Rasid, B. Veeravalli, and K. M. M. Aung, "Blockchain-based decentralized content trust for

docker images," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18223–18248, 2018.

[153] C. Li and L. J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *2017 IEEE International Congress on Internet of Things (ICIOT)*, pp. 33–41, Honolulu, HI, USA, 2017.

[154] K. R. Oezyilmaz and A. Yurdakul, *Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress*, EMSOFT Companion, 2017.

[155] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "Controlchain: blockchain as a central enabler for access control authorizations in the IoT," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–6, Singapore, 2017.

[156] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1180–1184, Chengdu, China, 2018.

[157] M. Banerjee, J. Lee, and K. K. R. Choo, "A blockchain future for Internet of Things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[158] S. Amanlou, M. K. Hasan, and K. A. Bakar, "Lightweight and secure authentication scheme for IoT network based on publish- subscribe fog computing model," *Computer Networks*, vol. 199, p. 108465, 2021.

[159] M. K. Hasan, T. M. Ghazal, A. Alkhalifah et al., "Fischer linear discrimination and quadratic discrimination analysis–based data mining technique for Internet of Things framework for healthcare," *Frontiers in Public Health*, vol. 9, 2021.

[160] O. Alphand, M. Amoretti, T. Claeys et al., "IoTChain: a blockchain security architecture for the Internet of Things," *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, Spain, 2018.

[161] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Security and Communication Networks*, vol. 2018, 27 pages, 2018.

[162] D. Orazgaliyev, Y. Lukpanov, I. A. Ukaegbu, and H. S. K. Nunna, "Towards the application of blockchain technology for smart grids in Kazakhstan," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 273–278, PyeongChang, Korea, February 2019.

[163] S. Mugunthan and T. Vijayakumar, "Review on IoT based smart grid architecture implementations," *Journal of Electrical Engineering and Automation*, vol. 10, no. 1, pp. 12–20, 2019.

[164] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain technology toward green IoT: opportunities and challenges," *IEEE Network*, vol. 34, no. 4, pp. 263–269, 2020.

[165] S. Garlapati, "Blockchain for IOT-based NANs and HANs in smart grid," 2020, https://arxiv.org/abs/2001.00230.

[166] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, 2021.

[167] N. Renugadevi, S. Saravanan, and C. M. Naga Sudha, "IoT based smart energy grid for sustainable cites," *Materials Today: Proceedings.*, 2021.

[168] J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services : what blockchain technology can contribute to smart cities," *Financial Innovation*, vol. 2, no. 1, p. 26, 2016.

[169] Y. Symey, S. Sankaranarayanan, and S. S. N. Binti, *Building a Robust Value Mechanism to Facilitate TransActive Energy*, Energy, 2016.

[170] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures , blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.

[171] L. Axon and M. Goldsmith, "PB-PKI : a privacy-aware blockchain-based PKI PB-PKI : a privacy-aware blockchain-based PKI," in *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017)*, vol. 4, pp. 311–318, Madrid, Spain, 2017.

[172] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *Journal of Software Engineering and Applications*, pp. 533–546, 2016.

[173] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 5–7, Sydney, NSW, Australia, 2016.

[174] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A blockchain connected gateway for BLE-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[175] M. Conoscenti and J. C. De Martin, "Peer-to-Peer Approaches for a Decentralized Private-By-Design Internet of Things," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, Buenos Aires, Argentina, 2017.

[176] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things : challenges and solutions," 2016, https://arxiv.org/abs/1608.05187.

[177] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy : the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, 2017.

[178] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Generation Computer Systems*, vol. 107, pp. 805–815, 2020.

[179] P. Ghuli, U. P. Kumar, and R. Shettar, "A review on blockchain application for decentralized decision of ownership of IoT devices," *Advanced Computer Science & Technology*, vol. 10, no. 8, pp. 2449–2456, 2017.

[180] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *IoTPTS '16: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pp. 29–36, 2016.

[181] C. Rupa, D. Midhunchakkaravarthy, M. Kamrul Hasan, H. Alhumyani, and R. A. Saeed, "Industry 5.0: Ethereum blockchain technology based DApp smart contract," *Mathematical Biosciences and Engineering*, vol. 18, no. 5, pp. 7010–7027, 2021.

[182] J. Herbert and A. Litchfield, "A novel method for decentralised peer-to-peer software license validation using

cryptocurrency blockchain technology," in *Proc. 38th Australasian Computer Science Conference (ACSC 2015)*, vol. 159no. January, pp. 27–35, Sydney, Australia, 2015.

[183] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 464–467, PyeongChang, Korea (South), 2017.

[184] B. Leiding, C. H. Cap, T. Mundt, and S. Rashidibajgan, "Authcoin: validation and authentication in decentralized networks," 2016, https://arxiv.org/abs/1609.04955.

[185] A E Commission, "Integration of the blockchain in a smart grid model," in *The 14th International Conference of Young Scientists on Energy Issues (CYSENI) 2017*, pp. 127–134, Kaunas, Lithuania, 2017.

[186] A. Ouaddah, "Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, vol. 520 of Advances in Intelligent Systems and Computing,, Springer, Cham.

[187] D. Nettikadan, R. T. Raphael, and B. D. Paul, "Converging blockchain and Internet of Things," *The International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 662–667, 2019.

[188] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *CCSW '17: Proceedings of the 2017 on Cloud Computing Security Workshop*, pp. 45–50, New York, United States, November 2017.

[189] J. J. Sikorski, J. Haughton, M. Kraft, P. Street, and P. F. Drive, *Blockchain technology in the chemical industry : machine-to-machine electricity market*, University of Cambridge, 2016.

[190] S. Wilkinson, *A Peer-to-Peer Cloud Storage Network*, Finance Magnates, 2014.

[191] S. E. E. Profile, "When Your Sensor Earns Money: Exchanging Data for Cash with Bitcoin," in *2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, Seattle Washington, USA, 2017.

[192] Q. Xu, K. M. M. Aung, Y. Zhu, K. L. Yong, and K. L. Yong, "A Blockchain-Based Storage System for Data Analytics in the Internet of Things," *Studies in Computational Intelligence*, vol. 715, pp. 119–138, 2018.

[193] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *2015 18th International Conference on Intelligence in Next Generation Networks*, pp. 184–191, Paris, France, 2015.

[194] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: decentralized computation platform with guaranteed privacy," 2015, https://arxiv.org/abs/1506.03471.

[195] R. Deters, "Decentralized access control with distributed ledgers using blockchain to manage IoT access," in *IEEE International Conference on Industrial Internet (IEEE ICII)*, pp. 248–257, Orlando, FL, USA, November 2019.

[196] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-IoT: hybrid blockchain architecture for Internet of Things - PoW sub-blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1007–1016, Halifax, NS, Canada, 2018.

[197] R. B. Chakraborty, M. Pandey, and S. S. Rautaray, "Managing computation load on a blockchain - based multi - layered Internet - of - Things network," *Procedia Computer Science*, vol. 132, pp. 469–476, 2018.

[198] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for Internet of Things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 769–773, Maui, HI, USA, 2018.

[199] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: object security architecture for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.

[200] Z. Guan, G. Si, X. Zhang et al., "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[201] M. English, S. Auer, and J. Domingue, "Block chain technologies & the semantic web: a framework for symbiotic development," in *Bonn-Aachen International Center for Information Technology Dahlmannstrasse 2, 53113 Bonn*, pp. 47–61, North Rhine-Westphalia, Germany, May 2016.

[202] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)*, vol. 50, Big Island, Hawaii, USA, January 2017.

[203] M. Mettler and M. A. Hsg, "Blockchain technology in healthcare the revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, Munich, Germany, 2016.

[204] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Semantic blockchain to improve scalability in the Internet of Things," *Open Journal of Internet Of Things (OJIOT)*, vol. 3, no. 1, pp. 46–61, 2017.

[205] J. Li, D. Greenwood, and M. Kassem, "Blockchain in the construction sector: a socio-technical systems framework for the construction industry," in *Advances in informatics and computing in civil and construction engineering*, pp. 51–57, Springer, Cham, 2019.

[206] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and blockchain-based delivery framework for drone-delivered services," *Computer*, vol. 8, no. 3, p. 58, 2019.

[207] O. Jogunola, M. Hammoudeh, B. Adebisi, and K. Anoh, "Demonstrating blockchain-enabled peer-to-peer energy trading and sharing," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pp. 1–4, Edmonton, AB, Canada, May 2019.

[208] M. K. Hasan, S. H. Yousoff, M. M. Ahmed, A. H. A. Hashim, A. F. Ismail, and S. Islam, "Phase offset analysis of asymmetric communications infrastructure in smart grid," *Elektronika ir Elektrotechnika*, vol. 25, no. 2, pp. 67–71, 2019.

[209] H. A. Khattak, K. Tehreem, A. Almogren, Z. Ameer, I. U. Din, and M. Adnan, "Dynamic pricing in industrial Internet of Things: blockchain application for energy management in smart cities," *Journal of Information Security and Applications*, vol. 55, p. 102615, 2020.

[210] H. Hosseinian, H. Shahinzadeh, B. G. Gharehpetian, Z. Azani, and M. Shaneh, "Blockchain outlook for deployment of IoT in distribution networks and smart homes," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 2787–2796, 2020.

[211] M. Akhtaruzzaman, M. K. Hasan, S. R. Kabir, S. N. H. S. Abdullah, M. J. Sadeq, and E. Hossain, "HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey," *IEEE Access*, vol. 8, pp. 222977–223008, 2020.

[212] Z. Liu, D. Wang, J. Wang, X. Wang, and H. Li, "A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks," *IEEE Access*, vol. 8, pp. 177745–177756, 2020.

[213] M. Aybar-Mejía, D. Rosario-Weeks, D. Mariano-Hernández, and M. Domínguez-Garabitos, "An approach for applying blockchain technology in centralized electricity markets," *The Electricity Journal*, vol. 34, no. 3, p. 106918, 2021.

[214] M. K. Thukral, "Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: a review," *Clean Energy*, vol. 5, no. 1, pp. 104–123, 2021.

[215] M. K. Hasan, M. Shafiq, S. Islam et al., "Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things applications," *Complexity*, vol. 2021, Article ID 5540296, 13 pages, 2021.

[216] E. S. Ali, M. K. Hasan, R. Hassan et al., "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications," *Networks*, vol. 2021, article 8868655, 23 pages, 2021.

[217] A. Abbasi, A. R. Javed, C. Chakraborty, J. Nebhen, W. Zehra, and Z. Jalil, "ElStream: an ensemble learning approach for concept drift detection in dynamic social big data stream learning," *IEEE Access*, vol. 9, pp. 66408–66419, 2021.

[218] B. Aslam, A. R. Javed, C. Chakraborty, J. Nebhen, S. Raqib, and M. Rizwan, "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic," *Personal and Ubiquitous Computing*, vol. 1-17, 2021.

[219] M. K. Hasan, M. M. Ahmed, S. S. Musa et al., "An improved dynamic thermal current rating model for PMU-based wide area measurement framework for reliability analysis utilizing sensor cloud system," *IEEE Access*, vol. 9, pp. 14446–14458, 2021.

[220] S. N. Ghorpade, M. Zennaro, B. S. Chaudhari, R. A. Saeed, H. Alhumyani, and S. Abdel-Khalek, "A novel enhanced quantum PSO for optimal network configuration in heterogeneous industrial IoT," *IEEE Access.*, vol. 9, pp. 134022–134036, 2021.

[221] M. M. Ahmed, M. K. Hasan, M. Shafiq et al., "A peer-to-peer blockchain based interconnected power system," *Energy Reports*, vol. 7, pp. 7890–7905, 2021.

[222] C. Iwendi, S. U. Rehman, A. R. Javed, S. Khan, and G. Srivastava, "Sustainable security for the Internet of Things using artificial intelligence architectures," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 3, pp. 1–22, 2021.