Cybersecurity challenges in IoT-based smart renewable energy

Alexandre Rekeraho (alexandre.rekeraho@unitbv.ro)
Transilvania University of Brasov
Daniel Tudor Cotfas
Transilvania University of Brasov
Petru Adrian Cotfas
Transilvania University of Brasov
Titus Constantin Bălan
Transilvania University of Brasov
Emmanuel Tuyishime
Transilvania University of Brasov
Rebecca Acheampong
Transilvania University of Brasov

Research Article

Keywords: IoT, Renewable energy, Cybersecurity, vulnerabilities, threats

Posted Date: April 25th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2840528/v1

Version of Record: A version of this preprint was published at International Journal of Information Security on August 1st, 2023. See the published version at https://doi.org/10.1007/s10207-023-00732-9.

Abstract

The Internet of Things (IoT) makes it possible to collect data from, and issue commands to, devices via the internet, eliminating the need for humans in the process while increasing productivity, accuracy, and economic value. Therefore, the integration of IoT plays a crucial role in achieving high efficiency and sustainability in the production of renewable energy that could be used to meet future electricity needs. While this approach has many significant benefits, it also opens smart renewable energy to cyber-attacks, giving hackers a new window of opportunity to take advantage of renewable energy's vulnerabilities. This obviously affects the financial and physical functioning of smart renewable energy. This article reviews the literature on cybersecurity threats and vulnerabilities in IoT-based smart renewable energy and cyber-attacks on power systems. False data injection, replay, denial of service (DoS), and brute force credential attacks have been identified as the main threats to IoT based smart renewable energy. These threats exploit IoT based smart renewable energy's vulnerabilities such as the usage of insecure communication protocols, poor encryption techniques, poor hash algorithms, lack of access control, lack of parameter sanitization, and the inappropriate use of authentication alongside encryption. The findings of this review will assist researchers in better understanding the issues surrounding the cybersecurity of IoT-based smart renewable energy and the needs for grid security in light of the exponential growth in the number of renewable energy sources connected to the grid.

1. Introduction

Global climate changes caused by human activities raise concerns about environmental preservation because the consequences would be disastrous if no action was taken. Following these concerns, developing renewable energy becomes important, and notably in recent years, substantial emphasis has been placed on renewable energy consumption [1]. As traditional energy sources deplete, renewable energy sources are expected to be the largest power generators [2]. The largest portion of renewable energy being used today is provided by wind and solar when compared to biomass, geothermal, and any other existing renewable energy sources. Solar radiation contributes to the generation of electricity on the power system on both a large scale (via utility-scale installations and solar farms) and a small scale (via rooftop installations, microgrids or nanogrids, distributed energy resources (DER), and storage systems). Wind speed, temperature, dust, humidity and light intensity are some of the environmental elements that affect renewable energy generation. These variables have an impact on the efficiency of energy conversion from renewable energy sources. Since our future generations will rely on renewable energy, researchers must incorporate IoT to deliver reliable and economical energy [3].

IoT technologies enable operators to remotely manage and monitor equipment in real time. Furthermore, they can automate particular system operations and give greater control to the workforce, allowing for lower operating expenses and less reliance on fossil fuels in the energy industry [4].Traditionally, electrical grids were built to deliver uniform electricity in a one-way flow from the power plants to the endpoints of consumption. Therefore, this obsolete system cannot support the variable supply of smart renewable energy[5]. Hence, IoT enabled smart grids support the switching between renewable energy sources and

existing power stations to ensure a continuous supply of electrical energy [6]. With this switching capability, smart grids can handle the dynamic nature of renewable energy while providing users with an uninterrupted electricity supply. Therefore, the integration of IoT plays a crucial role in achieving high efficiency and sustainability in the production of renewable energy that could be used to meet future electricity needs.

While this method has many significant benefits, it also opens smart renewable energy to cyber-attacks, giving hackers a new window of opportunity to take advantage of renewable energy vulnerabilities [7]. This obviously affects the financial and physical functioning of the grid [8], [9]. Furthermore, due to the growing prevalence of DER like wind and photovoltaic (PV) assets, as well as the communication and advanced technologies they employ [10], the cyber-physical security of these smart renewable energy assets requires urgent attention. Due to the advancements in PV system digitalization and the proliferation of IoT devices used in PV plant communication, transmission, and data collection, cybercriminals can [11]:

- compromise a monitoring and control platform by using replay attacks to re-create the actions of a previously running system
- coordinate cyberattacks that spread across the supply chain, for example, digital parts, faulty electronic components. Microcontrollers, digital signal processors, and intelligent application-specific integrated circuits are just a few of the cutting-edge electronic components used in PV inverters. Malicious malware hidden in these parts can compromise inverter functionality and lead to failure
- damage the plant or shut it down by attacking the inventor algorithms or controller and/or the plant supervisory system, or by getting into the inverter controller software and the unit controller and changing them.
- Hardware-level attacks, such as tampering with photovoltaic modules, wires, combiner boxes, and inverters [12],
- target the grid with the ability to dramatically affect plant operation and general safety, including activities like manipulating energy demand and cutting the plant off from the grid. Cybercriminals can cut off electricity from PV inverters to the grid by tripping the circuit breakers or by creating high, low, or zero voltage levels.

The findings of this review will assist researchers in better understanding the issues surrounding cyberattacks on IoT-based smart renewable energy and the needs for grid security in light of the exponential growth in the number of renewable energy sources connected to the grid. Methodology used for the research is presented in section 2. The research discusses previous work in Section 3., introduces the architecture of IoT-based renewable energy in Section 4. Section 5 presents the vulnerabilities and threats in renewable energy, and Section 6 presents the recent cyber-attacks on power systems. The discussion and conclusion are presented in Section 7, with the emphasis on the current trends in cybersecurity for renewable energy systems.

2. Methodology

While conducting our studies, a systematic approach was deemed essential to ensure that all relevant studies are identified, and that high-quality evidence is included in the analysis. This involved a thorough search process that was carefully executed, following the literature search guidelines outlined in [13], [14] and adhering to the recommendations for the Preferred Reporting Items for Systematic Reviews (PRISMA) as detailed in [15].

To begin with, a search was conducted in the Scopus database to identify relevant scientific literature. The Scopus database was chosen for its ability to provide a systematic evaluation of the literature and ensure comparability of documents across different research domains. English language documents were exclusively included in the search, with no limitations on geographical distribution. However, emphasis was placed on scrutinizing literature that was published from the year 2015 up to the present.

To perform the search query, specified keyword strings were used in the title, abstract, and keywords fields of the documents for the relevant fields. This helped in ensuring that the search was focused on the areas of interest. After identifying the documents, a visual inspection was performed to eliminate any duplicates or those that had no substantial evidence for the study objectives. This helped in removing irrelevant documents and ensuring that the analysis was based on high-quality evidence.

After filtering out the irrelevant documents, the remaining ones underwent both qualitative and quantitative analysis. This rigorous process entailed an exhaustive examination of the documents to extract pertinent information, which was then summarized and analyzed. The analysis was carried out using appropriate statistical tools to draw meaningful conclusions.

Table. 1 outlines the conclusive keywords selection for the bibliometric analysis. The corresponding number of documents detected in the Scopus database are showcased for each respective case. Likewise, the graphical illustration depicted in Fig. 1 showcases the yearly distribution of the documents discovered in relation to each respective search query case, While Fig. 2 represents the distribution of research documents type and Fig. 3 illustrate the percentage distribution of retrieved research documents by subject areas.

Table 1
Searched keywords string and corresponding number of documents

Search case	Keyword string	Retrieved documents
Q1	(“cybersecurity" OR "vulnerab*") AND ("IoT" OR "smart") AND ("microgrid" OR "nanogrid" OR "renewable")	375
Q2	("cyber attack" OR "cyber-attack") AND ("IoT" OR "smart”) AND ("microgrid" OR "nanogrid" OR "renewable")	200
Q3	"cyber threat" AND ("IoT" OR "smart") AND ("renewable" OR "microgrid" OR "nanogrid")	34

Upon analyzing the data presented in Fig. 1, it becomes apparent that the number of articles and conference papers related to the keyword string Q1 "Cybersecurity or Vulnerab*" in IoT-based Smart Renewable Energy is significantly higher than those related to the keyword string Q2 and Q3 ("Cyber-attack or Cyber Threats") respectively. Moreover, it can be observed that the number of published papers, as per their yearly distribution, exhibits a similar increasing trend regardless of the keyword string utilized, indicating a rising interest in the subject matter. The observed declining trend in the 2023 data can be accounted for by the limitation that the data is based solely on the first months of the year.

By analyzing the data presented in Fig. 2, it becomes evident that the most common publication types in this research area, for each search case, are conference papers, articles, and book chapters. However, the relatively low quantity of review papers suggests that further attention should be given to this type of publication, as their insights could be useful in identifying potential areas of focus and informing future research directions.

Based on the data presented in Fig. 3, it can be observed that the highest number of published documents are concentrated in the research areas of engineering, computer science, and energy, respectively. Conversely, a small percentage of papers are distributed across other scientific disciplines. This information was instrumental in enabling us to filter out papers that were not relevant to our area of interest.

3. Review On Previous Work

The authors of [16] conducted a cybersecurity analysis of a photovoltaic (PV)-based home nanogrid deployment and exploit protocols like Domain Name Service (DNS) and Secure Shell (SSH). The paper gives a detailed explanation of the criteria that smart microgrids must meet to make them more secure and less vulnerable to cyberattacks. It also presented a new method for assessing cybersecurity concerns in PV-based distributed energy resource (DER) implementations for homes, in addition to a categorization of standards published in the scholarly literature based on their applicability to the security of smart grids. Assessment of PV systems for residential use was the primary emphasis of the work. The research [17] examines cybersecurity attacks on the smart microgrids' data confidentiality, integrity, and availability. The focus, however, was on a false data injection attack which aimed to compromise data integrity. Authors in [18], assessed the risks and potential remedies associated with IoT-based smart grids. They concentrated on the study and investigation of current network vulnerabilities, defenses against attacks, and security standards that smart grids must achieve. Many challenges to the confidentiality, integrity, and availability of smart grids—the primary security goals—are taken into account in [19]. The most widely used communications protocols in the realm of industrial control systems are the subject of a qualitative cybersecurity investigation in [20]. Such protocols encompass DNP3, Modbus, TASE.2, IEC 60870-5-104, IEC 61850, IEC 60870-5-101, OPC UA, and OPC UA. The authors provide a standardized approach based on protocol flaws for comparison.

The authors in [21] offered a thorough analysis of the security issues plaguing IoT-based smart grids, along with some potential approaches to those problems. The study's overarching objective was to evaluate the repercussions of security breaches, smart grid vulnerabilities, and proposed countermeasures. However, the study did not include renewable energy research. The paper [7] laid the groundwork for future nanogrids to better catalog their assets, assess potential dangers, calculate potential risks, and implement safeguards. To demonstrate the framework's use, researchers examined the cybersecurity of a working prototype of a nanogrid that uses PV modules and load regulation. The nano grid incorporated a blockchain-powered energy trading platform and a weather station that broadcasts temperature and humidity data according to a predefined protocol. The data is utilized to make predictions, which are then used to make suggestions for consumption and generation. Furthermore, an expense analysis was conducted to offer a systematic evaluation of the protection measures and determine a trade-off between the costs of establishing security measures and the damages brought on by unauthorized breaches.

Most of the literature review focused on the cybersecurity of the smart grid and neglected the part of renewable energy that is growing rapidly. The main objective of this research is to review cybersecurity threats and vulnerabilities in IoT-based smart renewable energy and cyber-attacks on power systems. The findings of this review will assist researchers in better understanding the issues surrounding cyberattacks on IoT-based smart renewable energy and the needs for grid security in light of the growing number of renewable energy sources that are linked to the grid.

4. Architecture Of Iot-based Smart Renewable Energy

IoT covers a wide variety of items equipped with sensors and actuators for data collection, processing, and dissemination to other devices, software, and platforms. The Internet of Things (IoT) is the most exciting new development in technology today [22]. The term "Internet of Things" (IoT) is defined in [23] as a specific type of network that links any physical item to the Internet using a standard protocol and gathers data in real time using a variety of information sensing devices. IoT is also defined as a network of interconnected electronic devices, software, and services that enables the transmission and interaction of data for the purposes of intelligent identification, precise locating, tracking, and controlling data. The IoT idea offers a framework that makes intelligent data exchange possible for operations including monitoring, controlling, and communicating [24]. Through a network connection, IoT enables physical equipment to be monitored and managed remotely [25]. This establishes real-time connectivity between cloud-based computer systems and physical devices (like controllers, actuators, and sensors) [26]. IoT technologies have given rise to a number of ground-breaking ideas that have changed the way numerous industries conduct their daily business [27].

IoT-enabled sensors are used at every stage of smart renewable energy supply chain, from generation, transmission to distribution. These resources help firms to remotely monitor and control renewable energy equipment in real time [28]. Smart renewable energy is the result of the bidirectional power flow that necessitates bidirectional information flow between consumers and the utility, and the usage of IoT

as a key technology. This is achieved by integration of sensors, actuators and communication technologies in renewable energy as shown in Fig. 4.

- **Sensor**: These devices are deployed in the field to collect and transmit information in real time. The role of these sensors is to help operators remotely monitor and control energy generation, transmission, and distribution processes.
- **Actuators**: Actuators are devices that turn a certain kind of energy into motion. They produce a variety of motion patterns, including oscillatory, linear, and rotational movements. To deliver useful services in the energy industry, actuators interact with other nearby equipment.
- **Communication technologies**: End-to-end data connections can be initiated in the environment by connecting sensors to IoT gateways through wireless technologies. Wind and solar power plants are typically located in difficult-to-reach locations. Deploying IoT devices guarantees green energy efficiency and real-time data transmission.

Perception (the lowest), Network (the next), Middleware (the next), and Application (the highest) are the layers engaged in controlling and monitoring renewable energy sources [29]. The perceptual layer is the data-gathering one. It gathers data on physical parameters for use in environmental monitoring and management. This layer can be equipped with a wide variety of sensors and other components to accommodate a wide range of configurations and user needs. The network layer follows the perception layer. Through the transport and access network, it transports data and information. Unlike transport networks, which operate over long distances, access networks, such as Wi-Fi, ZigBee, and sensor area networks, operate over short distances. Wired and wireless area networks both belong to transport networks.

Middleware is responsible for bridging the gap between the network layer and the application layer; it extracts data and transforms it into the needed format. By breaking down a large system into smaller pieces, middleware makes it easier to manage and, therefore, more service-oriented. In the application layer, we find the application platform and the cloud computing platform. Data sent from the perception layer through the gateway is received and stored in the application layer, which then analyzes, organizes, and performs computations on the data. As a result, the application layer is in charge of sending data obtained from the web server about the monitored parameters to the end user via graphical representations or reports. Figure 5 depicts the mentioned layers involved in the execution of different functions in smart renewable energy systems.

Four layers of IoT-based architecture for RE systems were defined in the study [30]: the power layer, the data acquisition layer, the communication network layer, and the application layer. The locations where energy is produced and consumed make up the power layer. On the generation side, there are RE sources such as wind and solar, as well as energy storage solution like batteries. The power layer also includes buses, transformers, and loads. The energy load is consumed in places where there are buildings with a variety of energy consumption applications, such as electric cars, machinery, lights, and other appliances. To ensure efficient energy use, loads are classified as residential, commercial, or industrial. Moreover, the

power system layer has several sensor nodes and measurement devices that form the data acquisition layer when interconnected with renewable energy sources.

Information gathered by measuring devices and various sensor nodes is sent into the application layer via the communication network layer. RE system can be controlled using information gathered from a variety of sources, including wind power and solar panels, depending on whether you're operating off the grid or in grid-connected mode. Table. 2 illustrates the sensors used in PV and wind renewable energy. The control center receives data from the power layer's sensor nodes and measuring equipment through the communication network layer. Depending on the technology employed, this layer can be broken down into wireless (LoRa, ZigBee, cellular, WiMAX, Wi-Fi, etc.) and wired (optical fibers, Ethernet, PLCs, etc.) solutions. Through the use of remote terminal units and intelligent electronic devices, the communication network layer collects and transmits data from all parts of the system. In [31] they constructed an IEC 61850-compliant communication network architecture for monitoring PV power plants remotely. A variety of services, including web servers, databases, historians, application servers, and human-machine interfaces (HMI), are kept in the control center. Monitoring and controlling processes in real-time are two of the primary responsibilities of the application layer. The local control center provides stores, and processes monitoring status and data information for various services. The control center has a LAN for communicating with other control and protection devices, including remote terminal units and IEDs.

5. Security Vulnerabilities And Threats In Iot Based Smart Renewable Energy

The smart RE integrates two-way communication technology and computational intelligence across the whole energy system, from the generation to the consumption endpoints. Despite the numerous benefits, this method leaves renewable energy vulnerable to security threats, giving hackers a new opportunity to take advantage of vulnerabilities in smart renewable energy. Moreover, perpetrators target smart renewable energy since its monitoring and management rely on public solutions and Internet-based protocols. These attacks can cause both physical and financial damages, which may lead to the power system's services being disrupted. This has physical and financial effects on the functioning of the power system.

A total of 23 vulnerabilities in photovoltaic systems were discovered in the study [32], and their root causes were investigated. All of the vulnerabilities were taken from the vulnerability databases [33], [34]. These vulnerabilities include insecure communication protocols (the problems include the usage of poor encryption techniques, poor hash algorithms, and inappropriate utilization of authentication alongside encryption.), lack of access control, Lack of parameter sanitization, Backdoor and hard-coded accounts (developers frequently employ hidden and backdoor accounts for testing purposes, but they forget to delete them before a product is given to a consumer.), cross-site scripting.

The following is a list of the most well-recognized security threats that target smart IoT-based RE system, as gathered from a survey of the relevant literature [35],[36],[37],[38],[39],[40],[41],[42],[43]:

False Data Injection (FDI)

Once intruders can alter or manipulate the original measurements given by the sensors, a sort of cyberattack known as a false data injection attack can be planned, impacting the control center's computing capacity [44], [45], [46], [47]. In this way, the adversary can tamper with the network operator's state estimation algorithms and cause them to draw incorrect conclusions[48], [49]. It can be either cyber-based or physical-based [50]. One of the most dangerous types of attacks on distributed energy resources based on false data injection is energy theft[51]. The theft is the result of a falsified meter reading that provides inaccurate information.

Table 2
Sensors in PV and Wind energy system [30]

Unit	Part	Sensing Device
PV System	PV Array	power, current, module temperature, tracker
	Grid	Current from grid, current to grid, power to grid, power from grid, utility voltage
	Meteo mast	Wind direction, wind speed, ambient air temperature, irradiance
Wind Turbine System	Generator	Power, Voltage, Current, status, temperature
	Converter	Voltage, current, torque, frequency, power factor, temperature, status
	Transformer	Status, temperature, voltage, current, oil level
	Rotor	Status, rotor speed, rotor position, pitch angle, pressure temperature
	Transmission	Status, pressure, grease level, temperature, vibration, oil level
	nacelle	Status, wind speed, wind direction, orientation, displacement
	yaw	Temperature, speed, position, grease level
	meteorological	Humidity, temperature, pressure, wind speed, wind direction

The reading from the smart meter must be precise because it is used for billing and accounting. Customers who aren't trustworthy could give false information to get a discount or ask for a high payment [52]. The effects of the FDI were investigated in [53]. The overvoltage and its effects on the grid-connected PV were brought on by the successful attack that altered sensor readings at the level of the PV system. The authors presented the economic impact of the attack as well.

Investigation of a power system integrity compromise is presented in [54]. The article [55] presented a scenario in which an FDI attack is carried out on PV system meter data being utilized for fifteen-minute forecasting. As a result of the attack, the command-and-control center provided the grid with the incorrect

operational parameters, and the research shows that the FDI could lead to catastrophic failures. To solve this problem, research [56] suggests a novel FDI attack detection technique suitable for power grids with a high proportion of renewable energy sources. Using multiple attack scenarios, the created framework is tested on an IEEE 14-bus system incorporating numerous renewable energy sources. The proposed detection method performs better in a renewable energy grid-connected setting, according to numerical findings. The authors of [57] proposed a detection technique for PV grid-connected systems' voltage sensors' measurement change. Encryption techniques have generally been shown to offer significant advantages for FDI attack prevention [58], [59], [52], [60]. Unfortunately, these approaches still have a considerable computational cost. Hence, additional study is required to decrease lower computational costs, as well as improve the algorithm's efficiency, precision, and processing speed.

Man-in-the-Middle (MITM)

As part of a MITM attack, an intrusive party inserts itself into a dialogue taking place between two communicating devices to either pose as one of the devices or eavesdrop, making it seem as if the information is being exchanged normally [61]. Consequently, false command injections and false data injection assaults by the attacker might endanger power system activities including load forecasting, automatic generation management, economic dispatch, and state estimation. The Metasploit framework is used in work [62] to conduct a man-in-the-middle cyberattack on a PV plant that is connected to the grid. In [63], it is shown that a MITM assault on a power factor correction unit may overwhelm a distributing feeder, resulting in the deliberate tripping of the whole feeder as well as a subsequent blackout throughout a wide area. To show the efficacy of this approach, an experiment was implemented in a laboratory model utilizing commercial power equipment with varying loading situations. The study [64] shows that a commercial PV inverter that offers auxiliary services to the grid may be the target of a MITM attack, resulting in the deliberate collapse of the whole feeder and the subsequent blackout of a large area. The attack's efficacy and potential danger were exposed by its successful experimental execution. PV inverter capability and feeder loads are only two of the many variables taken into account to determine the overall viability of the planned attack.

Replay

Replay attacks take place when an attacker captures network traffic and acts as the main source by forwarding it to the target [18]. The threat actor either causes a delay in the data transfer or causes it to be retransmitted. An attacker can impersonate the legitimate sender of data by resending it to its intended recipient after intercepting it. The recipient of the legitimate communication is duped into thinking it was delivered from a trusted source. The message is delivered twice, which is why it is termed a replay assault. The cybercriminal who launches a replay attack doesn't even need to decode the message they're resending, making it all the more dangerous. But they can still trick the recipient into thinking the communication is genuine. Cybercriminals can gain access to otherwise inaccessible data by using networks that have been compromised through replay attacks. Replay attacks were identified as one of the attacks on renewable energy systems by the authors [65]. One of the most popular protocols for IoT

devices, ZigBee, is used to transmit data between devices via a network. However, the study [66]showed that ZigBee is vulnerable to replay attacks, and the authors showcased a replay attack method that can be executed with just an open-source KillerBee and the commercially available API-Mote. Messages sent across ZigBee gadgets can be recovered with the help of a suggested noise-removal approach. The HMAC-MD5 technique was proposed by [67] as a means of detecting replay attacks in the isolated smart grid. Research [68] described a new authentication technique that combines robust cryptography with a random key method for maximum security. The study demonstrates that it has the potential to provide mutual anonymity, authentication, forward and reverse security, and resilience to replay attacks.

Denial of service (DoS): Routing protocols and electronic movements are the primary targets of DoS attacks, which overload communication channels and slow down network speeds. By overwhelming the system with extra data packets, a denial-of-service attack can effectively restrict what regular users can do [69]. In [70], two types of denial-of-service attacks were launched against the IoT-based PV system, and their performance was evaluated (in terms of both the time it took to launch the attacks and the percentage of times they were successful). The distributed denial of service (DDoS) cyberattack, in contrast, is a more severe kind of cyberattack in which several hosts attack a target simultaneously. Threat actors prepare a cyberattack ahead of time by exploiting a vulnerability to hack several hosts across communications networks; hackers then overwhelm the target site with all hacked hosts. In the case of inverter-based smart energy systems, DoS can obstruct information exchange between all devices and the control system. DDoS can be grouped into three types: volume-based [71], protocol-based DDoS [72], and application-layer DDoS [73]. The authors in [74] analyzed the impact of DOS attack on the PV system. Simulation of DOS on PV inverter is presented in [75]. The analysis of DOS impact against microgrid is presented in [76], [77], [78]. Hybrid intrusion detection system was suggested by [79] as the prevention of DOS in distributed energy resources.

Brute force credentials

The goal of this attack is to guess passwords, usernames, and encryption keys through repeated attempts and error. Before gaining access, the hacker tries several login identities and passwords. Once they're in, the criminal may stay in the system as long as no one notices that they aren't the real user. During this period, they can set up back doors, spread laterally, understand the system for the purpose of later assaults, and steal information. The optical ports of a smart meter can be accessed with brute-force password cracking using a program like termineter[80]. As a second phase of an assault, malware may be installed on the smart meter to steal the power.

6. Cyber-attacks On Power System.

In this section, we discussed the major cyber-attacks that have jeopardized the power industry in recent years.

The first high-profile documented cyber-attack on the power grid occurred in Ukraine on December 23, 2015 [81]. It affected a regional electricity distribution company, and it is considered the first of its kind to

be a case in point for the security and safety of the electric grid everywhere. The investigation report [82] states that the threat actors employed remote industrial control system (ICS) client software or pre-existing operating system-level remote administration tools through virtual private network (VPN) connections to carry out malicious remote actions on the circuit breakers. It is thought that the perpetrators obtained legitimate credentials in advance to make remote access administration easier. The attack resulted in a six-hour blackout that affected over 225,000 consumers in and around Kyiv, the capital city of Ukraine [83].

On December 17, 2016, a second cyber-attack happened in Ukraine, almost one year after the previous attack. This time around, the actors attacked the Pivnichna electricity substation outside the capital city of Ukraine. It subsequently caused a blackout that lasted for over an hour, and one-fifth of Kiev's power consumption was lost due to this power outage [84]. The analysis report [85] proved that malware termed "CRASHOVERRIDE" was used in this attack, and its framework has modules for specific ICS protocol stacks; however, it also includes non-ICS-specific modules, such as a wiper, which deletes files and processes from the running system in order to launch a destructive attack on operational technology equipment.

On March 5, 2019, a renewable energy development company based in the USA suffered a denial-of-service attack [32]. The incident caused the grid operators to lose communication with the solar and wind generation sites totaling 500 megawatts; it left operators blinded to the generation systems for about twelve hours [86]. A cyber-attack paralyzed a German wind turbine operator in February 2022. They reported that the remote monitoring and control of thousands of wind turbines had failed because of a fault in the satellite connection to their systems [87]. The computer emergency response team of Ukraine (CERT-AU) reported on April 12, 2022 [88], that they faced a cyberattack on the Ukrainian energy firm. The attackers targeted several critical infrastructure elements, including high-voltage electrical substations, using a malicious program termed Industroyer2 (a variant of Crashoverride used in 2016). The attack was detected and promptly mitigated before it caused greater damage; otherwise, a blackout would have impacted approximately two million people [89]. Moreover, on October 26, 2022, one of Germany’s largest municipal energy suppliers confirmed on its site [90]that it had been targeted by a cyberattack. This hack has impacted customer service availability as a result of an IT malfunction in their system. However, the immediate reaction prevented the attack from causing greater damage; hence, the critical infrastructure of the facility was not affected.

7. Discussion And Conclusion

Many industries have embraced the IoT in recent years to boost productivity and effectiveness. Its use is also being optimized in the energy industry to enhance sustainability. As a result of the IoT's standardized networks and protocols, firms can remotely troubleshoot malfunctioning machinery, monitor their devices, and maximize the production of renewable energy. On the other hand, "cyber security" refers to the tools, procedures, and controls put in place to prevent harm to computerized infrastructures such as computers, devices, networks, and stored information. Near the power plants, where renewable energy is generated,

many systems employ sophisticated controls, digital sensors, and network designs. Each control that may be accessed either physically or online is a potential entry point for hackers targeting renewable energy installations. And accessibility must be managed, and data confidentiality, integrity, and availability must be maintained. Security solutions have been recommended in the literature:

Several power systems communication protocols, such as IEC 61968, IEC 61970, IEC 61850, IEC 60870-6, and IEC 60870-5 series, are covered by the IEC 62351 Standard, which was created to offer security recommendations [17]. Security measures such as intrusion detection system, digital signatures to ensure authentication, and prevent spoofing and eavesdropping are all included. The research [91] provided a detailed examination of the IEC 61850 messaging architecture and the associated cybersecurity issues. It demonstrated how the application of IEC 6185 has grown from transmitting electrical measurements across a single LAN to multiple LANs, WANs, and the transmission of highly confidential information like financial transactions. Each form of the IEC 61850 message was reviewed in light of the cybersecurity suggestions made in IEC 62351 Standard. Nevertheless, the time efficiency of the IEC 62351-recommended security measures was investigated for power system that employ IEC 61850-based communication. Several shortcomings, including IEC 61850 time requirements, were discovered when RSA digital signatures are employed to secure generic object-oriented substation events (GOOSE) and Sampled Values (SV) in accordance with the IEC 62351-6 Standard [92],[93]. The authors in [94] defined roles and responsibilities for PV suppliers, standards development organizations, the government, and grid operators throughout the course of a five-year time frame to improve cybersecurity for communication-enabled photovoltaic systems [94].

Password authentication systems against brute force, access control lists, and encryption mechanisms against vulnerabilities in Message Queue Telemetry Transport (MQTT) between IoT devices in advanced nonogrid composed by DER and weather station have been implemented in [95]. MQTT is a commonly used protocol for Internet of Things communication [96]. Authentication techniques, message encryption, and data integrity checks have been recommended by [97] for man-in-the-middle and false data injection attack prevention. These precautions might, however, have a detrimental effect on the microgrid's functioning if not taken appropriately. For example, improper encryption may have an impact on the payload data and authentication, and an inadequate authentication process may not offer the needed authentication for particular microgrid applications, making it easier for MITM and DoS attacks to succeed [97]. In 2020, the United States Department of Energy (DOE) issued a Plan for Enhancing Cybersecurity in Renewable Energy to lead cybersecurity research and development (R&D) for Energy Efficiency and Renewable Energy (EERE) technologies [98]. However, the National Renewable Energy Laboratory and Underwriter Laboratories (UL) identified gaps in the PV industry's cybersecurity standards [99].

Artificial intelligence (AI) is becoming more popular in cybersecurity because it can protect systems in real time from cyberattacks. The most common application of artificial intelligence in security is intrusion detection, which entails monitoring network activity for suspicious behavior. The rise of the Internet of Things has sparked widespread interest in AI. The review paper [100] provided an analysis of the current

literature on the topic of artificial intelligence (AI) approaches used for power grid stability, security issues, defect detection, load forecasting, and in smart grids. The research showed that using AI could make smart grids more resilient and reliable. Smart renewable energy can use algorithms based on machine learning and artificial intelligence (ML/AI) to train systems to spot anomalies and sound alarms before cyberattacks on renewable energy. On the other hand, Blockchains "keep a continually expanding set of organized records, known as blocks". Cryptography links these blocks. Each block includes a cryptographic hash of the preceding block, transaction data, and a timestamp. In other words, tampering with even a single block in a single chain will be instantly detectable. Changes to a blockchain ought to be made to each block in the chain. IoT devices handle vast amounts of data, which is sent in a chain and is vulnerable to cyberattacks from hackers. In this context, blockchain technology is capable of standardizing, securing, and validating the adoption of device data. The blockchain can do monitoring of the sensor data collected for IoT security, prohibiting unauthorized change. With blockchain technology, sensors may transfer data without the requirement for a trustworthy third party. Thus, adopting blockchain technology to IoT-based smart renewable energy can enhance its security.

This article reviewed the literature on cybersecurity threats and vulnerabilities in IoT-based smart renewable energy and cyber-attacks on power systems. False data injection, replay, denial of service (DoS), and brute force credentials attacks have been identified as the main threats to the IoT-based smart RE, exploiting its vulnerabilities such as the usage of insecure communication protocols, poor encryption techniques, poor hash algorithms, a lack of access control, a lack of parameter sanitization, and inappropriate use of authentication alongside encryption. The findings of this review will assist researchers in better understanding the issues surrounding cyberattacks on IoT-based smart renewable energy and the need for the grid security in light of the exponential growth in the number of renewable energy sources connected to the grid. Despite the considerable study discussed in this research, it is still important to thoroughly analyze the security and vulnerabilities of a significant number of IoT-based smart RE components in light of the existence of advanced cyber threats.

Declarations

Funding: No funding was received to assist with the preparation of this manuscript.

Conflict of interests: The Authors declares that they do not have conflict of interest

Ethics approval**:** Not applicable

Data availability:

Data sharing not applicable to this article as no datasets were generated.

References

1. P. A. Cotfas and D. T. Cotfas, “Solar Hybrid System Component Study in Low Concentrated Sunlight,” *International Journal of Photoenergy*, vol. 2021, pp. 1–13, 2021, doi: 10.1155/2021/6677473.
2. B. Yu, D. Fang, K. Xiao, and Y. Pan, “Drivers of renewable energy penetration and its role in power sector’s deep decarbonization towards carbon peak,” *Renewable and Sustainable Energy Reviews*, vol. 178, p. 113247, May 2023, doi: 10.1016/j.rser.2023.113247.
3. S. Ding, J. Zeng, Z. Hu, and Y. Yang, “IOT-based social-economic management of distribution system with the high penetration of renewable energy sources,” *Sustainable Cities and Society*, vol. 76, p. 103439, Jan. 2022, doi: 10.1016/j.scs.2021.103439.
4. D. P. Rani, D. Suresh, P. R. Kapula, C. M. Akram, N. Hemalatha, and P. K. Soni, “IoT based smart solar energy monitoring systems,” *Materials Today: Proceedings*, 2021, doi: 10.1016/j.matpr.2021.07.293.
5. A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, and I. Traore, “A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook,” *Energies*, vol. 15, no. 19, p. 6984, 2022, doi: 10.3390/en15196984.
6. Q. N. Minh, V.-H. Nguyen, V. K. Quy, L. A. Ngoc, A. Chehri, and G. Jeon, “Edge Computing for IoT-Enabled Smart Grid: The Future of Energy,” *Energies*, vol. 15, no. 17, Art. no. 17, Jan. 2022, doi: 10.3390/en15176140.
7. P. J. Hueros-Barrios, F. J. Rodríguez Sánchez, P. Martín, C. Jiménez, and I. Fernández, “Addressing the cybersecurity vulnerabilities of advanced nanogrids: A practical framework,” *Internet of Things*, vol. 20, p. 100620, Nov. 2022, doi: 10.1016/j.iot.2022.100620.
8. 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, Oct. 2018, doi: 10.1109/TII.2017.2788868.
9. J. J. Q. Yu, Y. Hou, and V. O. K. Li, “Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018, doi: 10.1109/TII.2018.2825243.
10. J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, “Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things,” *IEEE Power Electronics Magazine*, vol. 4, no. 4, pp. 37–43, Dec. 2017, doi: 10.1109/MPEL.2017.2761422.
11. J. Ye *et al.*, “A Review of Cyber–Physical Security for Photovoltaic Systems,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022, doi: 10.1109/JESTPE.2021.3111728.
12. “How to Protect Your Solar Panels from Thieves? | LEDwatcher.” https://www.ledwatcher.com/how-to-protect-your-solar-panels-from-thieves/ (accessed Feb. 03, 2023).
13. H. Kraus, “LibGuides: Topic: Systematic Searching for Evidence Synthesis: Searching Scopus.” https://guides.lib.uconn.edu/systematic_searching/scopus (accessed Feb. 16, 2023).
14. E. Ferrier, “LibGuides: Guide to Searching: Citation Searching.” https://libguides.brown.edu/searching/citation (accessed Feb. 16, 2023).

15. D. Moher *et al.*, “Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement,” *Systematic Reviews*, vol. 4, no. 1, p. 1, Jan. 2015, doi: 10.1186/2046-4053-4-1.
16. “Prosumer Nanogrids: A Cybersecurity Assessment | IEEE Journals & Magazine | IEEE Xplore.” https://ieeexplore.ieee.org/abstract/document/9141261 (accessed Feb. 03, 2023).
17. F. Nejabatkhah, Y. W. Li, H. Liang, and R. Reza Ahrabi, “Cyber-Security of Smart Microgrids: A Survey,” *Energies*, vol. 14, no. 1, Art. no. 1, Jan. 2021, doi: 10.3390/en14010027.
18. M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
19. D. Faquir, N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras, “Cybersecurity in smart grids, challenges and solutions,” *AIMS Electronics and Electrical Engineering*, vol. 5, no. 1, pp. 24–37, 2021, doi: 10.3934/electreng.2021002.
20. A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, “Security Challenges in Control Network Protocols: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 619–639, 2019, doi: 10.1109/COMST.2018.2872114.
21. M. Ouaissa and M. Ouaissa, “Cyber Security Issues for IoT based Smart Grid Infrastructure,” *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 937, no. 1, p. 012001, Sep. 2020, doi: 10.1088/1757-899X/937/1/012001.
22. A. Koohang, C. S. Sargent, J. H. Nord, and J. Paliszkiewicz, “Internet of Things (IoT): From awareness to continued use,” *International Journal of Information Management*, vol. 62, p. 102442, Feb. 2022, doi: 10.1016/j.ijinfomgt.2021.102442.
23. H. Kopetz and W. Steiner, “Internet of Things,” in *Real-Time Systems: Design Principles for Distributed Embedded Applications*, H. Kopetz and W. Steiner, Eds. Cham: Springer International Publishing, 2022, pp. 325–341. doi: 10.1007/978-3-031-11992-7_13.
24. A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, “A Review and State of Art of Internet of Things (IoT),” *Arch Computat Methods Eng*, vol. 29, no. 3, pp. 1395–1413, May 2022, doi: 10.1007/s11831-021-09622-6.
25. M. Biegańska, “IoT-Based Decentralized Energy Systems,” *Energies*, vol. 15, no. 21, Art. no. 21, Jan. 2022, doi: 10.3390/en15217830.
26. M. Rupesh and N. A. Selvan, “Design of IoT Based Smart Energy Meter for Home Appliances,” *J. Phys.: Conf. Ser.*, vol. 1964, no. 5, p. 052001, Jul. 2021, doi: 10.1088/1742-6596/1964/5/052001.
27. O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, “Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey,” *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, Feb. 2018, doi: 10.1109/JIOT.2017.2773600.
28. “The use of IoT in renewable energy generation,” Oct. 24, 2019. https://www.allerin.com/blog/the-use-of-iot-in-renewable-energy-generation (accessed Feb. 04, 2023).
29. S. Ponnalagarsamy, V. Geetha, M. Pushpavalli, and P. Abirami, “Impact of IoT on Renewable Energy,” in *IoT Applications Computing*, I. Singh, Z. Gao, and C. Massarelli, Eds. IntechOpen, 2022. doi:

10.5772/intechopen.98320.

30. A. M. Eltamaly, M. A. Alotaibi, A. I. Alolah, and M. A. Ahmed, “IoT-Based Hybrid Renewable Energy System for Smart Campus,” *Sustainability*, vol. 13, no. 15, p. 8555, Jul. 2021, doi: 10.3390/su13158555.
31. M. A. Ahmed, A. M. Eltamaly, M. A. Alotaibi, A. I. Alolah, and Y.-C. Kim, “Wireless Network Architecture for Cyber Physical Wind Energy System,” *IEEE Access*, vol. 8, pp. 40180–40197, 2020, doi: 10.1109/ACCESS.2020.2976742.
32. Y. Dubasi, A. Khan, Q. Li, and A. Mantooth, “Security Vulnerability and Mitigation in Photovoltaic Systems,” in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Jun. 2021, pp. 1–7. doi: 10.1109/PEDG51384.2021.9494252.
33. “NATIONAL VULNERABILITY DATABASE.” https://nvd.nist.gov/ (accessed Feb. 04, 2023).
34. “Search Engine for Security Intelligence | Vulners.” https://vulners.com/ (accessed Feb. 04, 2023).
35. M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, “Detection of False Data Injection Cyber-Attacks in DC Microgrids Based on Recurrent Neural Networks,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, Oct. 2021, doi: 10.1109/JESTPE.2020.2968243.
36. N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, “A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy,” *IEEE Access*, vol. 10, pp. 35846–35875, 2022, doi: 10.1109/ACCESS.2022.3163551.
37. C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, “Cyber Security Assessment of Distributed Energy Resources,” in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, Jun. 2017, pp. 2135–2140. doi: 10.1109/PVSC.2017.8366503.
38. Z. Li, M. Shahidehpour, and F. Aminifar, “Cybersecurity in Distributed Power Systems,” *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017, doi: 10.1109/JPROC.2017.2687865.
39. A. Sundararajan, T. Khan, A. Moghadasi, and A. I. Sarwat, “Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies,” *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 449–467, May 2019, doi: 10.1007/s40565-018-0473-6.
40. A. Sundararajan, A. Chavan, D. Saleem, and A. Sarwat, “A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security,” *Energies*, vol. 11, no. 9, p. 2360, Sep. 2018, doi: 10.3390/en11092360.
41. D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat, and B. Kroposki, “A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems,” *IEEE Systems Journal*, vol. 14, no. 1, pp. 17–27, Mar. 2020, doi: 10.1109/JSYST.2019.2919464.
42. N. Jacobs *et al.*, “Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources,” in *2019 IEEE Power and Energy Conference at Illinois (PECI)*, Feb. 2019, pp. 1–8. doi: 10.1109/PECI.2019.8698915.
43. 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)*, Sep. 2017,

pp. 1–6. doi: 10.1109/ISGTEurope.2017.8260213.

44. F. Cai and X. Koutsoukos, “Real-time detection of deception attacks in cyber-physical systems,” *International Journal of Information Security*, Mar. 2023, doi: 10.1007/s10207-023-00677-z.
45. A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, and A. Youssef, “Attack Detection for Load Frequency Control Systems Using Stochastic Unknown Input Estimators,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2575–2590, Oct. 2018, doi: 10.1109/TIFS.2018.2824253.
46. M. Higgins, W. Xu, F. Teng, and T. Parisini, “Cyber–physical risk assessment for false data injection attacks considering moving target defences,” *International Journal of Information Security*, Nov. 2022, doi: 10.1007/s10207-022-00621-7.
47. R. Tan *et al.*, “Modeling and Mitigating Impact of False Data Injection Attacks on Automatic Generation Control,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017, doi: 10.1109/TIFS.2017.2676721.
48. G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A Review of False Data Injection Attacks Against Modern Power Systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017, doi: 10.1109/TSG.2015.2495133.
49. 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, Oct. 2017, doi: 10.1109/TII.2017.2656905.
50. C. Konstantinou and M. Maniatakos, “Hardware-Layer Intelligence Collection for Smart Grid Embedded Systems,” *J Hardw Syst Secur*, vol. 3, no. 2, pp. 132–146, Jun. 2019, doi: 10.1007/s41635-018-0063-0.
51. S. N. Islam, M. A. Mahmud, and A. M. T. Oo, “Impact of optimal false data injection attacks on local energy trading in a residential microgrid,” *ICT Express*, vol. 4, no. 1, pp. 30–34, Mar. 2018, doi: 10.1016/j.icte.2018.01.015.
52. S. Aoufı, A. Derhab, and M. Guerroumi, “Survey of false data injection in smart power grid: Attacks, countermeasures and challenges,” *Journal of Information Security and Applications*, vol. 54, p. 102518, Oct. 2020, doi: 10.1016/j.jisa.2020.102518.
53. A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, “Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability,” in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, Oct. 2018, pp. 2872–2877. doi: 10.1109/IECON.2018.8591583.
54. S. Sridhar and G. Manimaran, “Data integrity attack and its impacts on voltage control loop in power grid,” in *2011 IEEE Power and Energy Society General Meeting*, Jul. 2011, pp. 1–6. doi: 10.1109/PES.2011.6039809.
55. T. O. Olowu, S. Dharmasena, A. Hernandez, and A. Sarwat, “Impact Analysis of Cyber Attacks on Smart Grid: A Review and Case Study,” in *New Research Directions in Solar Energy Technologies*, H. Tyagi, P. R. Chakraborty, S. Powar, and A. K. Agarwal, Eds. Singapore: Springer, 2021, pp. 31–51. doi: 10.1007/978-981-16-0594-9_3.

56. M. Mohammadpourfard, Y. Weng, I. Genc, and T. Kim, “An Accurate False Data Injection Attack (FDIA) Detection in Renewable-Rich Power Grids,” in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, May 2022, pp. 1–5. doi: 10.1109/MSCPES55116.2022.9770151.
57. Y. Isozaki *et al.*, “Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids With PVs,” *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016, doi: 10.1109/TSG.2015.2427380.
58. R. Mohammadi, “A comprehensive Blockchain-oriented secure framework for SDN/Fog-based IoUT,” *International Journal of Information Security*, Mar. 2023, doi: 10.1007/s10207-023-00683-1.
59. W. Luo, W. Ma, and Q. Gao, “A dynamic trust management system for wireless sensor networks,” *Security and Communication Networks*, vol. 9, no. 7, pp. 613–621, 2016, doi: 10.1002/sec.1384.
60. M. Mohammadpourfard, A. Sami, and Y. Weng, “Identification of False Data Injection Attacks With Considering the Impact of Wind Generation and Topology Reconfigurations,” *IEEE Transactions on Sustainable Energy*, vol. 9, no. 3, pp. 1349–1364, Jul. 2018, doi: 10.1109/TSTE.2017.2782090.
61. P. Wlazlo *et al.*, “Man-in-the-middle attacks and defence in a power system cyber-physical testbed,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021, doi: 10.1049/cps2.12014.
62. Y. Yang *et al.*, “Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems,” pp. 138–138, Jan. 2012, doi: 10.1049/cp.2012.1831.
63. L. Hadjidemetriou *et al.*, “Demonstration of Man in the Middle Attack on a Feeder Power Factor Correction Unit,” in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, Oct. 2020, pp. 126–130. doi: 10.1109/ISGT-Europe47291.2020.9248779.
64. G. Tertytchny *et al.*, “Demonstration of Man in the Middle Attack on a Commercial Photovoltaic Inverter Providing Ancillary Services,” in *2020 IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–7. doi: 10.1109/CyberPELS49534.2020.9311531.
65. T. A. Youssef, M. El Hariri, N. Bugay, and O. A. Mohammed, “IEC 61850: Technology standards and cyber-threats,” in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Jun. 2016, pp. 1–6. doi: 10.1109/EEEIC.2016.7555647.
66. M. S. Wara and Q. Yu, “New Replay Attacks on ZigBee Devices for Internet-of-Things (IoT) Applications,” in *2020 IEEE International Conference on Embedded Software and Systems (ICESS)*, Dec. 2020, pp. 1–6. doi: 10.1109/ICESS49830.2020.9301593.
67. L. Pavithra and D. Rekha, “Prevention of Replay Attack for Isolated Smart Grid,” in *Next Generation Information Processing System*, Singapore, 2021, pp. 251–258. doi: 10.1007/978-981-15-4851-2_27.
68. J.-C. Yeom, Q. Zhou, I.-A. Song, Y.-S. Lee, and I. Ra, “Authentication Mechanism for IoT Device in Micro Grid Environments,” in *Computational Intelligence and Intelligent Systems*, Singapore, 2019, pp. 281–291. doi: 10.1007/978-981-13-6473-0_25.
69. “Resilient Control Design Based on a Sampled-Data Model for a Class of Networked Control Systems Under Denial-of-Service Attacks | IEEE Journals & Magazine | IEEE Xplore.”

https://ieeexplore.ieee.org/abstract/document/8933052 (accessed Feb. 04, 2023).

70. L. Liang, K. Zheng, Q. Sheng, W. Wang, R. Fu, and X. Huang, “A Denial of Service Attack Method for IoT System in Photovoltaic Energy System,” in *Network and System Security*, Cham, 2017, pp. 613–622. doi: 10.1007/978-3-319-64701-2_48.
71. D. Ding, M. Savi, F. Pederzolli, M. Campanella, and D. Siracusa, “In-Network Volumetric DDoS Victim Identification Using Programmable Commodity Switches,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1191–1202, Jun. 2021, doi: 10.1109/TNSM.2021.3073597.
72. M. Dimolianis, A. Pavlidis, and V. Maglaris, “SYN Flood Attack Detection and Mitigation using Machine Learning Traffic Classification and Programmable Data Plane Filtering,” in *2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, Mar. 2021, pp. 126–133. doi: 10.1109/ICIN51074.2021.9385540.
73. K. S. Bhosale, M. Nenova, and G. Iliev, “The distributed denial of service attacks (DDoS) prevention mechanisms on application layer,” in *2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (SIKS)*, Oct. 2017, pp. 136–139. doi: 10.1109/SKS.2017.8246247.
74. X. Zhong, I. Jayawardene, G. K. Venayagamoorthy, and R. Brooks, “Denial of Service Attack on Tie-Line Bias Control in a Power System With PV Plant,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 5, pp. 375–390, Oct. 2017, doi: 10.1109/TETCI.2017.2739838.
75. B. Kang *et al.*, “Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations,” in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Sep. 2015, pp. 1–8. doi: 10.1109/ETFA.2015.7301457.
76. R. Fu, X. Huang, J. Sun, Z. Zhou, D. Chen, and Y. Wu, “Stability Analysis of the Cyber Physical Microgrid System under the Intermittent DoS Attacks,” *Energies*, vol. 10, no. 5, Art. no. 5, May 2017, doi: 10.3390/en10050680.
77. Y. Wang, M. Zhang, K. Song, T. Li, and N. Zhang, “An Optimal DoS Attack Strategy Disturbing the Distributed Economic Dispatch of Microgrid,” *Complexity*, vol. 2021, p. e5539829, Apr. 2021, doi: 10.1155/2021/5539829.
78. J. Liu, X. Lu, and J. Wang, “Resilience Analysis of DC Microgrids Under Denial of Service Threats,” *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3199–3208, Jul. 2019, doi: 10.1109/TPWRS.2019.2897499.
79. A. Chavez *et al.*, “Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems,” in *2019 IEEE CyberPELS (CyberPELS)*, Apr. 2019, pp. 1–6. doi: 10.1109/CyberPELS.2019.8925064.
80. S. N. Islam, Z. Baig, and S. Zeadally, “Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019, doi: 10.1109/TII.2019.2931436.
81. J. E. Sullivan and D. Kamensky, “How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid,” *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, Apr. 2017, doi:

10.1016/j.tej.2017.02.006.

82. I.-C. Alert, “Cyber-attack against ukrainian critical infrastructure,” *Cybersecurity Infrastruct. Secur. Agency, Washington, DC, USA, Tech. Rep. ICS Alert (IR-ALERT-H-16-056-01)*, 2016.
83. K. Zetter and others, “Inside the cunning, unprecedented hack of Ukraine’s power grid,” *Wired*, vol. 9, pp. 1–5, 2016.
84. “Ukraine power cut ‘was cyber-attack,’” *BBC News*, Jan. 11, 2017. Accessed: Feb. 04, 2023. [Online]. Available: https://www.bbc.com/news/technology-38573074
85. “CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids | Dragos,” Jun. 12, 2017. https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/ (accessed Feb. 04, 2023).
86. L. Learned, “Risks posed by firewall firmware vulnerabilities,” Tech. rep. North American Electric Reliability Corporation, 2019.
87. “Satellite cyber attack paralyzes 11GW of German wind turbines,” *pv magazine International*, Mar. 01, 2022. https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/ (accessed Feb. 04, 2023).
88. “Cyber attack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435),” *cert.gov.ua*. https://cert.gov.ua/ (accessed Feb. 04, 2023).
89. “Industroyer2 malware targeting Ukrainian energy company.” https://www.ironnet.com/blog/industroyer2-malware-targeting-ukrainian-energy-company (accessed Feb. 04, 2023).
90. “IT malfunction at enercity.” https://www.enercity.de/presse/betrieb-und-baustellen/2022/it-stoerung (accessed Feb. 04, 2023).
91. S. M. 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, Sep. 2020, doi: 10.1109/TII.2019.2956734.
92. T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, “A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard,” *IEEE Access*, vol. 7, pp. 156044–156053, 2019, doi: 10.1109/ACCESS.2019.2948117.
93. D. Ishchenko and R. Nuqui, “Secure Communication of Intelligent Electronic Devices in Digital Substations,” in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Apr. 2018, pp. 1–5. doi: 10.1109/TDC.2018.8440438.
94. J. Johnson, “Roadmap for photovoltaic cyber security,” SAND2017-13262, 1782667, 668568, Dec. 2017. doi: 10.2172/1782667.
95. P. J. Hueros-Barrios, Fco. J. Rodríguez, P. Martín, M. Gayo, and I. Fernández, “Addressing cybersecurity threats in prosumer-based nanogrids with MQTT communication,” in *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Jul. 2022, pp. 1–6. doi: 10.1109/ICECET55527.2022.9872918.

96. H. Zeghida, M. Boulaiche, and R. Chikh, “Securing MQTT protocol for IoT environment using IDS based on ensemble learning,” *International Journal of Information Security*, Mar. 2023, doi: 10.1007/s10207-023-00681-3.
97. M. Chlela, G. Joos, and M. Kassouf, “Impact of cyber-attacks on islanded microgrid operation,” in *Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems*, New York, NY, USA, Jun. 2016, pp. 1–5. doi: 10.1145/2939940.2939943.
98. “DOE Releases Plan for Improving Cybersecurity in Renewable Energy, Manufacturing, Buildings, and Transportation Research and Development,” *Energy.gov*. https://www.energy.gov/eere/articles/doe-releases-plan-improving-cybersecurity-renewable-energy-manufacturing-buildings (accessed Feb. 04, 2023).
99. J. Engel, “Renewables lag in cyber safeguards: Here’s how the sector plans to catch up,” *Renewable Energy World*, Mar. 24, 2022. https://www.renewableenergyworld.com/om/renewables-lag-in-cyber-safeguards-heres-how-the-sector-plans-to-catch-up/ (accessed Feb. 04, 2023).
100. O. A. Omitaomu and H. Niu, “Artificial Intelligence Techniques in Smart Grid: A Survey,” *Smart Cities*, vol. 4, no. 2, Art. no. 2, Jun. 2021, doi: 10.3390/smartcities4020029.

Figures

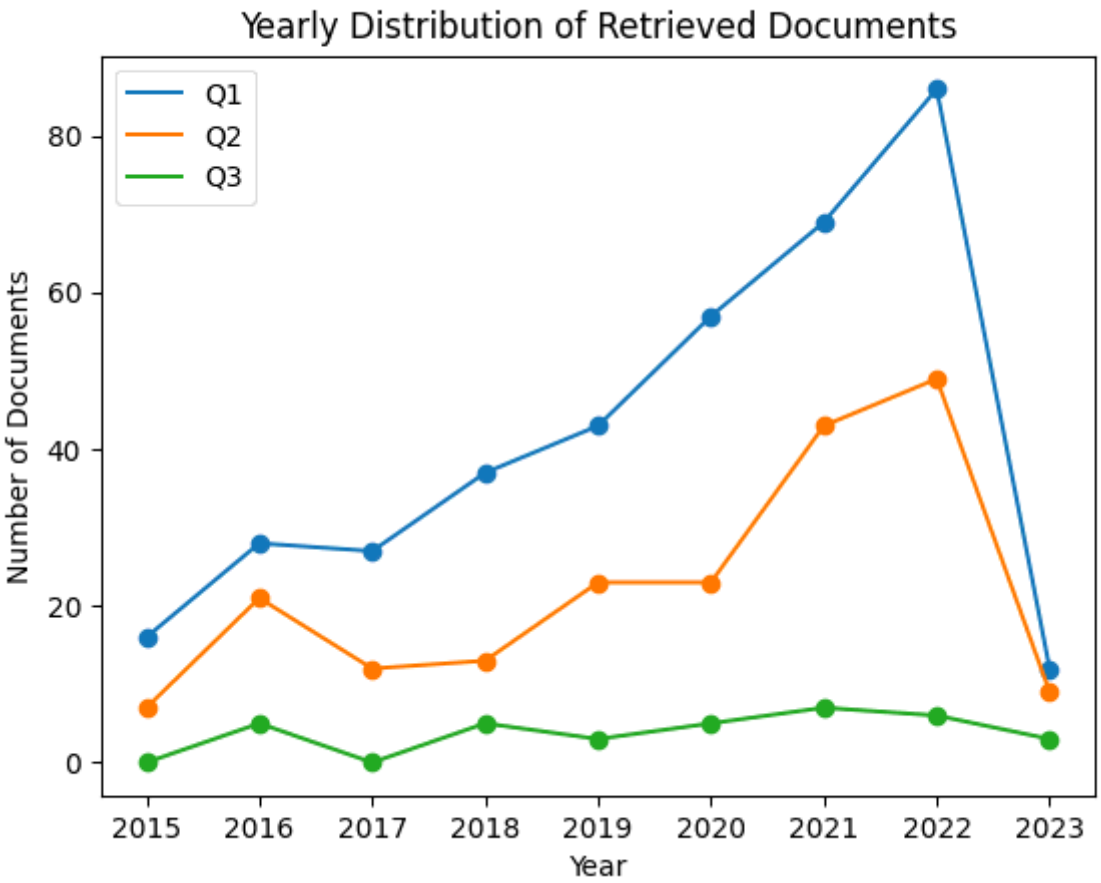

Figure 1

Yearly Distribution of retrieved documents

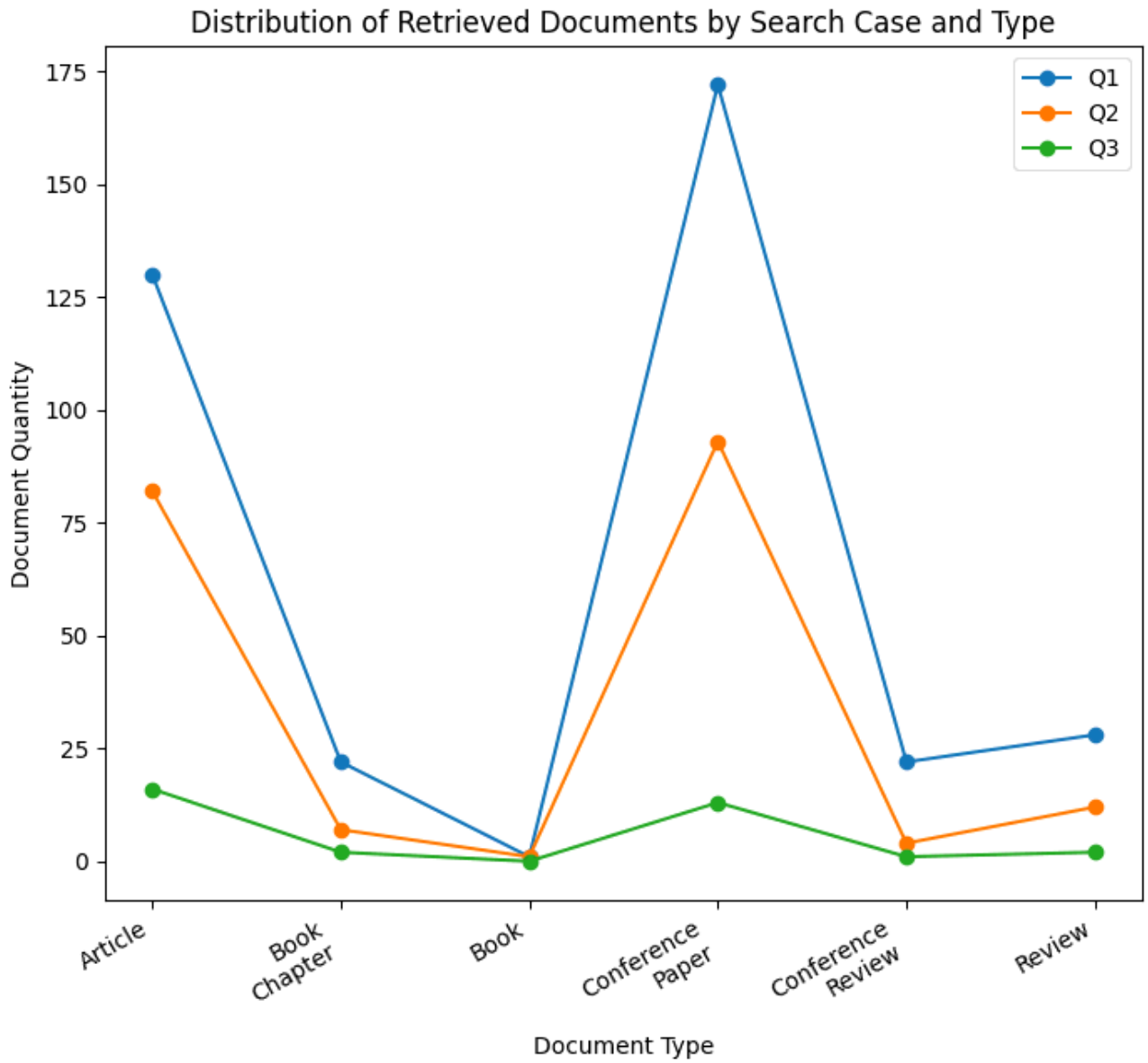

Figure 2

Distribution of documents by search case and Type

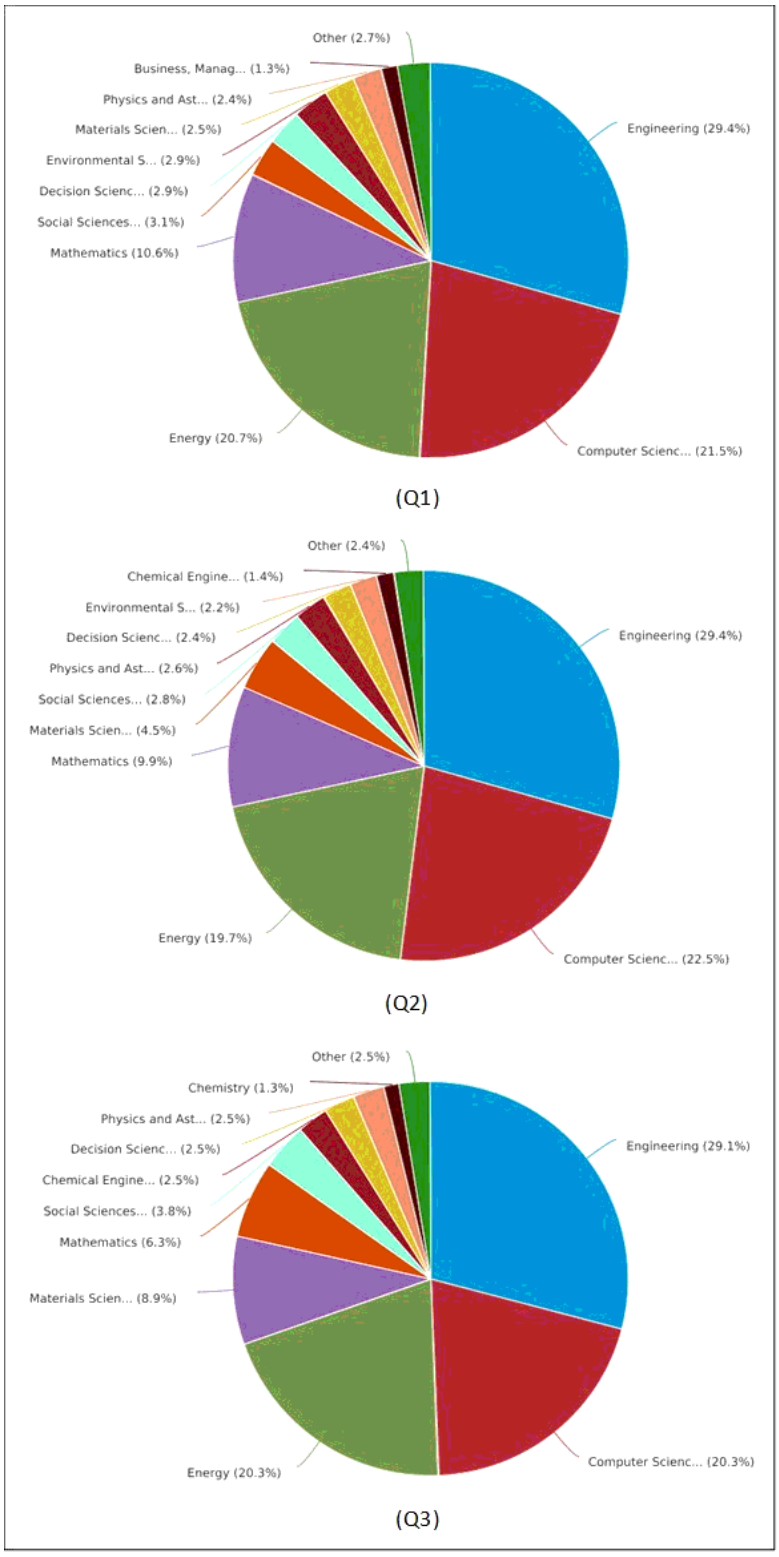

Figure 3

Distribution of the research documents by subject area

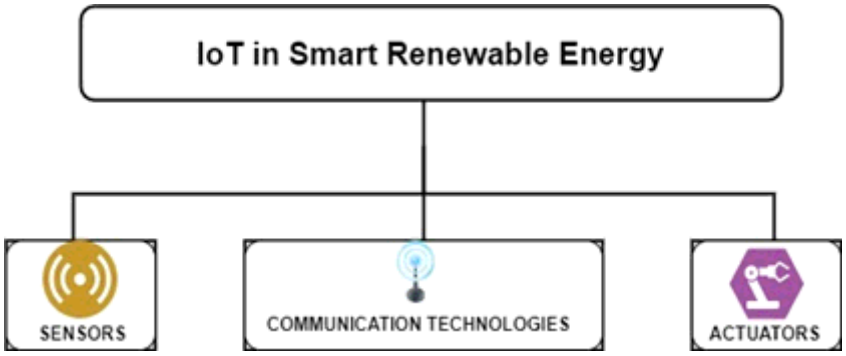

Figure 4

IoT in smart Renewable Energy

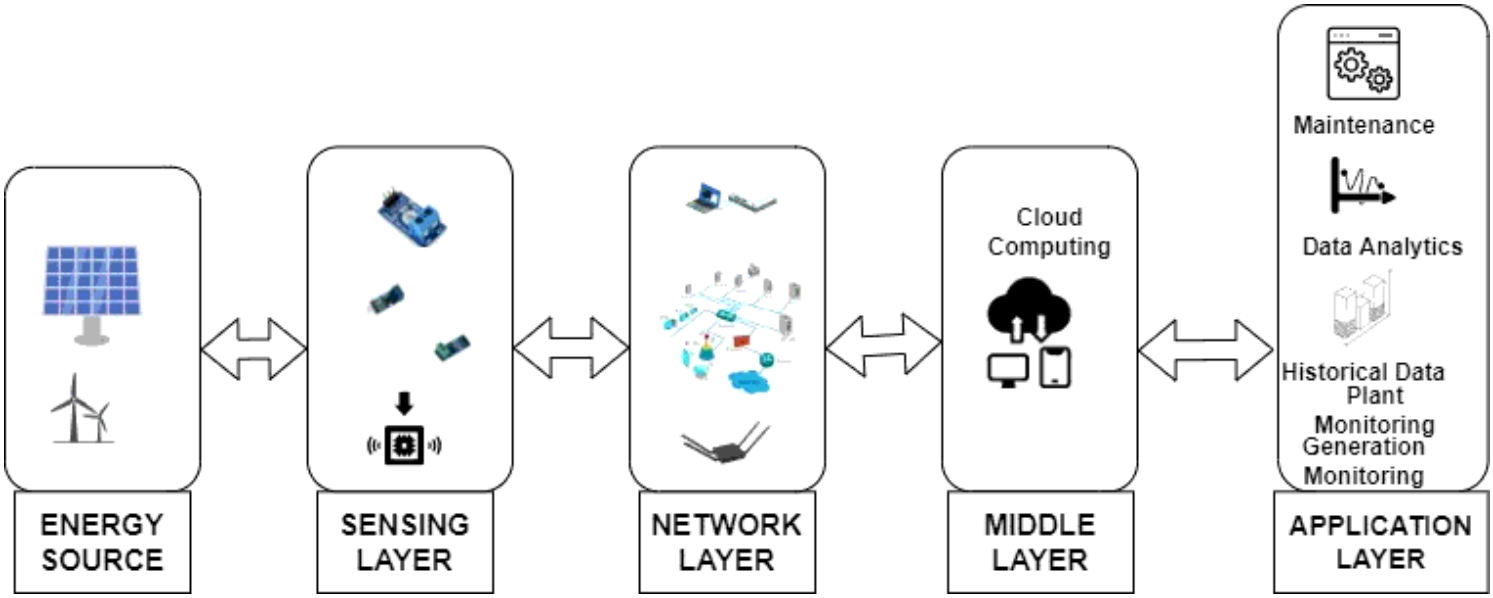

Figure 5

IoT architecture in Smart Renewable Energy [29]