International Journal of Wireless Information Networks (2022) 29:36–57
https://doi.org/10.1007/s10776-021-00549-0

A Survey on Next Generation IoT Networks from Green IoT Perspective

Annu Malik[1] · Rashmi Kushwah[1]

Received: 4 November 2020 / Revised: 7 October 2021 / Accepted: 24 December 2021 / Published online: 4 January 2022

Abstract

Internet of Things (IoT) is a collection of a huge number of heterogeneous devices, which can communicate, collect, and share data through the prevailing web. In the current world scenario, the dependence on technologies and the Internet is increasing very rapidly. The IoT came with many applications in the real world in the form of a smart city, home monitoring system, environmental condition monitoring, and social networking. With these IoT applications, there are many restrictions, such as insufficient resources, limited capacity, and processing capabilities. The Green IoT has emerged with new advantages, which is an energy-efficient and environment-friendly procedure that reduces emission, pollution, and minimizes operational costs and power consumption. Over the last few years, a plethora of Green IoT solutions has played a critical role in the IoT paradigm. A detailed study on several prevalent and innovative IoT solutions in terms of Green IoT is performed in this paper. More specifically, the assessment and comparison of these Green IoT solutions are carried out based on their characteristics, technology used, outcomes, usability, and their limitations. This survey is envisioned to assist as a guideline and a conceptual framework for Green IoT development and research. It also offers an organized assessment of existing Green IoT techniques and highlights several potentially substantial research directions and developments towards Green IoT.

Keywords Internet of Things · Green IoT · Wireless sensor network · IoT challenges · IPv6 · M2M · Smart connectivity

1 Introduction

The evolution of technologies repeatedly has assured the Internet of Things (IoT) to take up opportunities in the field of information and communication technology. IoT governed the infinite number of devices over the network to deliver outstanding smart services to the users. IoT provides us with plenty of resources to contribute to our daily life needs. IoT uses smart sensors and actuators which operate collectively to detect, collect and transmit appropriate data over the web from the environment. The transmission of this large number of information requires a tremendous amount of energy, high cost, and a lot of security [1].

The IoT has six key components and they are: identification, sensing, communication, computation, services, and semantics [2]. The main components of IoT that contribute to its overall functionality are shown in Fig. 1. These components are described as follows:

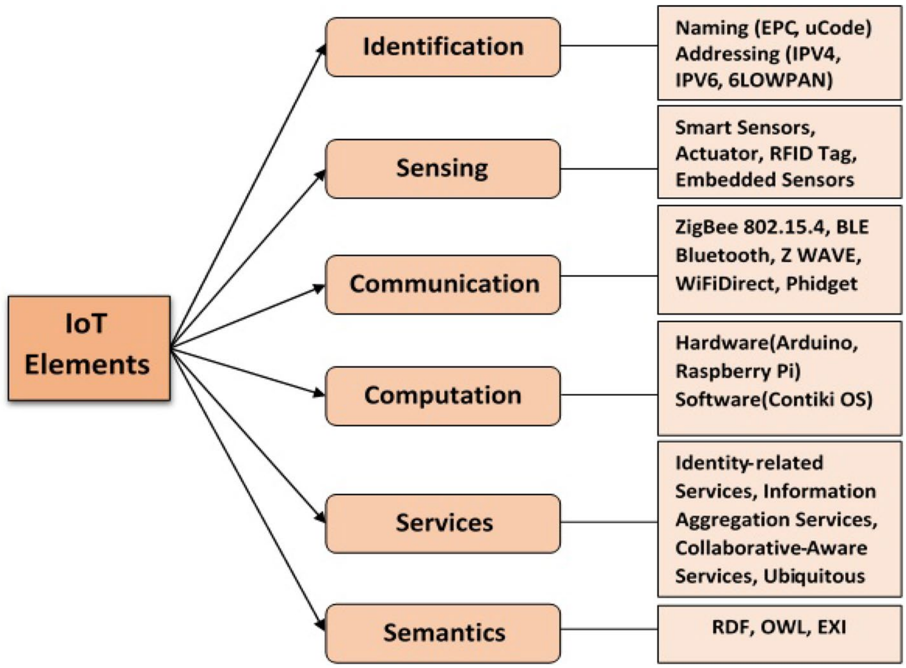
- *Identification* Identification method such as the radio frequency identification (RFID) tag provides the detection of an object within the network using a common chip or sticker attached to it. Addressing methods of IoT objects over the networks use IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) that provide a compression mechanism over IPv6 for low power wireless networks [2].
- *Sensing* The IoT sensors that can be smart wearable sensing devices are used to gather different tangible information. Multiple onboard sensors are fitted with the sensor nodes in the networks that can take surrounding readings such as temperature, moisture level, acceleration, traffic, and house surveillance [3].
- *Communication* There are many communication protocols used for the IoT. Some of the important protocols are constrained restful environments (CoRE), constrained application protocol (CoAP), and message queue telemetry transport (MQTT) [4].

✉ Annu Malik
annu.knit@gmail.com

Rashmi Kushwah
rashmi.31130@gmail.com

[1] Jaypee Institute of Information Technology, Noida, India

Fig. 1 IoT elements



- *Computation* Computation is used to provide data processing hardware and software specifications. Computation is carried out by various embedded devices, processors, application-specific integrated arrays, and various applications.
- *Services* Identity-related services, information aggregation services, collaborative aware services, and pervasive services are the IoT services. Services related to identification are used to evaluate entities. Information aggregation services collect all data and prepare reports after processing. The collaborative aware services based on acquired data decide further activities. Ubiquitous services recommend the use of collaborative-aware services as per the requirements of the system [4, 5].
- *Semantics* Semantics in the IoT is related to the capability to properly collect data from devices to provide the types of assistance required. Semantics can also be noticed as the ability to abstract information effectively by different strategies to convey fundamental services. Semantics technologies such as resource description framework and web ontology language are generally used [4].

All sensor devices can be connected to the Internet through the low power wide area (LPWA) technology to restrain energy consumption. LPWA offers effective energy resource usage at a low price to a wide variety of users over the networks. LPWA highlights features such as the ability to provide low-power access. The Narrow-Band Internet of Things (NBIoT) is a recently developed radio technology that helps to ensure an energy-efficient, cost-effective, sustainable, and low-power framework [6].

The next generation of IoT is defined as the use of smart technologies at the core of IoT devices that require strong communication, reliable interface, and real-time processing and information analysis [7]. This development is based on the incorporation of several primary information communication technologies including modern communication protocols, cloud technologies, machine intelligence, and cryptography. Many modern technologies in the Green IoT field are encouraged like 5G technology, edge computing, smart storage, and smart healthcare [8]. The number of network-connected devices is going to increase in the future. Therefore, Green IoT architecture has to adapt it. However, energy usage and problem-solving are all seen as barriers to efficient IoT implementation. The 5G-enabled IoT includes higher data rates, higher coverage, and maximum throughput, which provide a solution for future IoT. Due to many heterogeneous nodes involved in the 5G-IoT network, the standardization problem occurs. Several edge computing technologies have emerged from various backgrounds to reduce latency, enhance spectral performance, and help the massive communication form of the machine [9]. It provides a cheaper, quicker, and more efficient approach to data handling by storing data locally.

In earlier studies, many review works have been done on Green IoT in which the basic requirement of Green IoT is explained in four levels like hardware, software, communication and architecture [10–12]. In the proposed work, the procedure for Green IoT has been explained about these levels. Various key enabling technologies of green IoT have been discussed and compared with the existing techniques based on their characteristics, technology used, outcomes, usability, and their limitations. The challenges, applications, and research motivation for Green IoT and benefits to switch from IoT to Green IoT are discussed. We have categorized techniques of green IoT in energy efficiency, cost-effectiveness, security and privacy, delay constraints, and traffic offloading with their merits in the reference of Green IoT. Different criteria for Green IoT attainment and identification of research gaps and limitations to support future research are discussed. Various issues to achieve Green IoT have also been discussed to assist researchers while finding open research problems in the field of Green IoT. All the previous review papers focused on energy efficiency and security in Green IoT [13, 14]. Besides that our work has considered multiple factors from the perspective of Green IoT including cost, delay-constraint, and traffic offloading.

In this work first, we have discussed enabling technologies and applications of Green IoT, thereafter various challenges and research motivation for Green IoT have been discussed. Next, the complete review section is divided into five review categories such as energy efficiency based techniques, security and privacy based techniques, cost efficiency based techniques, delay-constrained based techniques and traffic offloading based techniques. All the review categories are focused on various parameters such as proposal/algorithm, characteristics, technology used, outcome of work, and usability/ application. Finally, a summary of various issues/limitations and research gaps found in the literature for Green IoT are discussed in Tables 6 and 7 respectively.

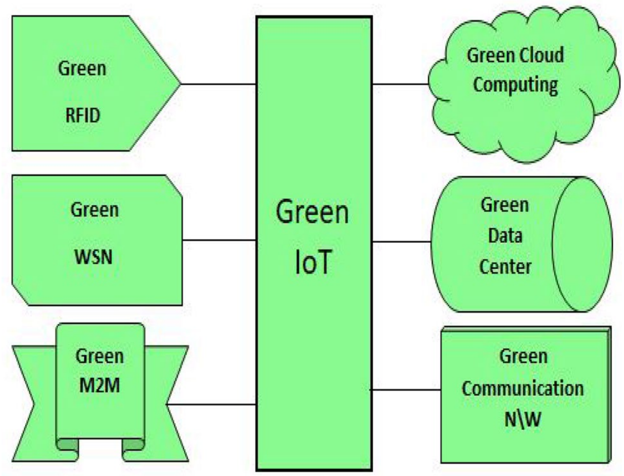


Fig. 2 Green IoT technologies

1.1 Enabling Technologies for Green IoT

There is an urge for Green computing to minimize energy consumption, lower cost, and high security. The Green IoT is the revolution in the IoT sector. To produce IoT as Green, some characteristics need to be appraised. The main characteristic is to make devices more energy efficient with improved communication protocols and network architecture. Other characteristics are to reduce network size, to produce a cost-effective and secure system with minimal environmental emissions and pollution. The Green IoT has six main enabling technologies such as Green RFID, Green wireless sensor networks, Green machine to machine communication, Green cloud computing, Green data centre, and Green Internet and communication technology [15] that is shown in Fig. 2. The enabling technologies for Green IoT are described as follows:

- *Green RFID* The RFID tag is a unique identifier for any object, which is used to store information about that object. The transmission is carried out by RFID. These tags are generally active and passive. Active tags use batteries for powering the signal transmissions hence increases the range of transmission while the passive tags do not use their batteries though follow the induction method for garnering energy [5].
- *Green wireless sensor networks (GWSN)* GWSN is a combination of sensor nodes and a base station. Sensor nodes sense the data from their surroundings and transfer the sensory data to the base station. To make WSN Green, the sensor nodes and base station must follow the following energy-saving methods [5, 16]: (i) sensor nodes should use specific sensing or peer-powering sensors. (ii) Sleep scheduling and compressed sensing should follow such methods of effective communication route forwarding between sensors and cloud systems under record at the base station. (iii) An efficient algorithm for the gateway nodes for load balancing. (iv) Computation of the resource allocator factor.
- *Green machine to machine (GM2M)* The machine to machine communication consumes more energy therefore, for efficient use of energy the methods to be followed are as: intelligently adjust the transmission power, design efficient communication protocols, activity scheduling, joint energy-saving mechanisms and employ energy harvesting (EH) [5].
- *Green cloud computing (GCC)* In GCC for reducing the power consumption, the selection of hardware and software should be made based on their energy requirements.
- *Green data centre (GDC)* GDC swallows a large amount of power and emits more carbon dioxide with the high operational cost that can be restrained by using renewable and Green energy resources.
- *Green Internet and communication technology (GICT)* For GICT some points to be followed are [5]: (i) send only data that are needed. (ii) Minimize the length of the wireless data path. (iii) Renewable Green power sources.

Integration of the cloud and IoT has emerged as a prominent concept in recent times. In contrast to rising demands for intensive evaluation of sensor-generated data, the primary goal is to use the limited computational power of IoT. Edge computing can be used as a supplement to cloud-based solutions, which has become the leading technology [7]. 5G develops a system that provides good bandwidth, supports essential services, and satisfies the need for the IoT. For the 5G network implementation, a combination of lower-band (under 1 GHz), a middle band (1 GHz to 6 GHz), and higher-band bandwidth is used to enable high data speeds, decreased delay, and improve spectrum usage [17]. A smart city uses modern information and communication technologies to deliver basic and essential facilities such as governance, schooling, medical, community security, housing, infrastructure, and household services. Smart electricity metres in houses that take full advantage of IoT have evolved and are available in various designs and sizes. As a result, the development of cheaper, reduced power, and customer-friendly smart metres that aids in saving energy could be significant in Green IoT [18]. It is vital to optimise IoT performance and minimize energy usage as much as possible to save and clean up the ecological environment. An energy-efficient strategy should be used to diminish the power consumption of all Green IoT devices. For industrial and agricultural applications, rechargeable batteries and usage of renewable energy from solar and wind power are viable possibilities. To save energy, energy management scheme (EMS) works on a technique that compromises the capacity of data to be transmitted over the internet [15]. Renewable energy from solar and wind power is essential because it allows saving more resources and costs. The development of the Green IoT is possible using renewable energy resources which produce an acceptable CO_2 footprint. Adaptive Energy-Aware Computation Offloading technique uses solar power and grid power supply to improve energy efficiency [19]. An accurate weather prediction feature using artificial intelligence could be included in this offloading technique to develop a reliable network infrastructure in Green IoT.

Green IoT presents a hierarchical framework for placing objects/things in IoT. It prolongs the network lifetime by allowing direct communications among relay nodes and not allowing communications among sensing nodes. The framework can migrate the traffic load from sensing nodes to relay nodes [6]. Green IoT uses resource-constrained devices, such as RFID, sensor nodes, and high-end data servers. It is important to find a way to provide security among heterogeneous devices in the Green IoT paradigm.

1.2 Applications of Green IoT

Using recyclable material in the production of IoT devices will help in making environmental friendly networks. E-waste is a reason for environmental damage therefore, Green IoT can be achieved by managing e-waste. The analysis gives a solution by printing both sides of the paper at the organizational level [5]. Various applications of IoT and Green IoT in the field of smart industry, smart transport, smart city, data centre, smart healthcare, smart agriculture, and smart building are shown in Fig. 3. Some applications of IoT and Green IoT in our daily life are described as follows [1, 5]:

- *Smart industry* Smart industries are adopting robotics technology into production and manufacturing processes. Robotics is used to detect the fault and analyze data during production for increasing productivity.
- *Smart transport* Intelligent traffic system is the usual example of smart transport that monitors the traffic and report accordingly to diminish the probability and cause of an accident.
- *Smart city* In a smart city many more facilitated applications like automated traffic monitoring, smart parking, smart garbage management, and smart home services came into existence.
- *Data centre* Data centre is a repository that is used for storage, management, and distribution of information. The automation of the data centre makes it more dynamic and flexible. The routine tasks of data centre such as patching, monitoring, updating, scheduling, and configuration are all managed automatically by IoT devices.
- *Smart healthcare* The facilities in hospitals for monitoring and tracking patients improved drastically with the help of embedded sensors and actuators.
- *Smart agriculture* The revolution in agriculture is raised by introducing a smart irrigation system and sensor technology. It has improved farm monitoring by using sensors in the crop field.
- *Smart building* Some automatic equipment is used in smart buildings such as lighting systems, shading system, window opening system, elevators, and air quality control system.

A virtualized sensor network as a service may be envisioned in Green information and communications technologies for improving energy efficiency [5]. For managing power consumption solar power and grid power are used as primary and secondary energy supply respectively. To enhance the efficiency of weather prediction features an intelligence techniques can be included [19]. To prohibit energy consumption during the idle state of sensor nodes, gateway scheduling and wake-up and sleep scheduling techniques can be used [20]. Data centers driven by solar power sources can substantially reduce energy, cost and carbon emissions [21]. Three types of EH techniques such as solar-based, moving vehicle-based

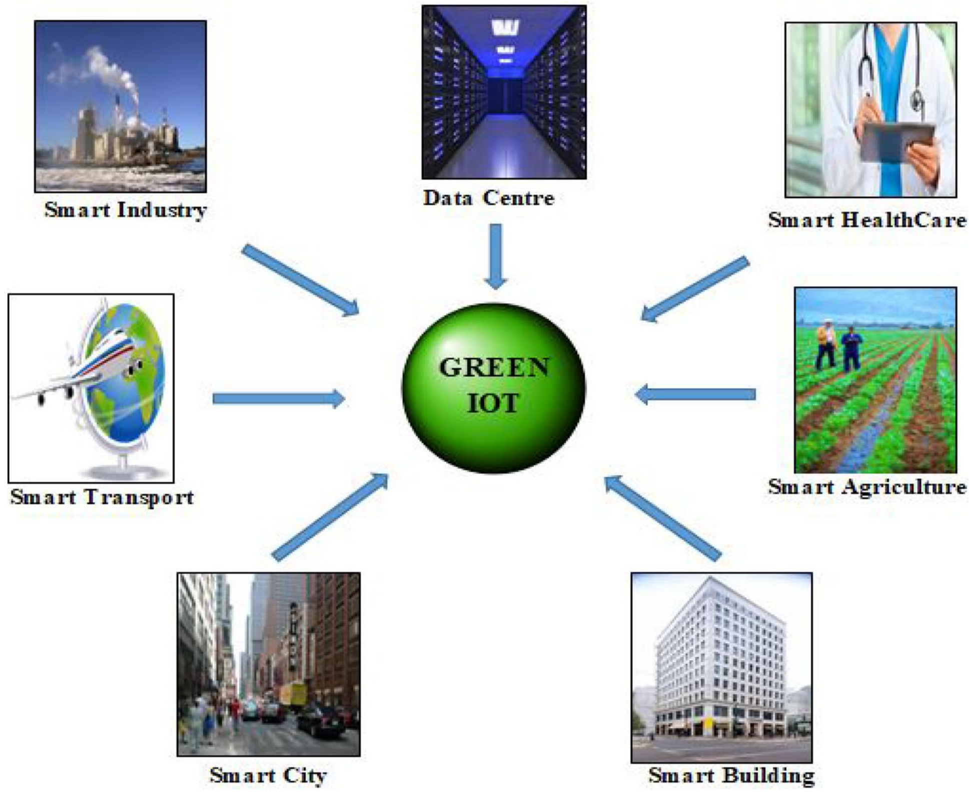


Fig. 3 Applications of green IoT

and radio frequency-based can be used to recharge their batteries from renewable sources [22]. Lightweight protocol along with triple data encryption standards can be included for improving security in the field of Green IoT [23]. By applying artificial intelligence in edge computing, only useful data will be filtered and sent to the cloud. This approach can eliminate the expenses in terms of bandwidth and data transfer costs [9, 24]. In the differentiated services based data routing (DSDR) scheme, data routing can be performed statically for different areas to resolve delay and energy efficiency problems [25]. To allocate communication resources according to the requirement of data traffic, an energy-efficient multiple slots frame scheduling scheme can be applied to more complex network scenarios [26]. By adding a systematic deployment of devices in rendezvous-based routing protocol more security threats can be eliminated [27]. Congestion problems in resource-aware and reliable strategy can be resolved by adding varying sized channel slots in objective function computation [28].

The succeeding sections are as follows: Sect. 2 briefly discusses the challenges and research motivation for Green IoT. Section 3 addresses the review of various techniques to achieve Green IoT. Section 4 presents various issues found in the Green IoT literature. In Sect. 5, a review of the research gaps found in Green IoT literature is presented. Finally, the concluding remarks and recommendations are given in Sect. 6 for future study.

2 Challenges and Research Motivation for Green IoT

Green IoT necessitates the adoption of processes that reduce power consumption and pollution while not degrading system performance. The most important challenge for the Green environment is conserving energy and lowering CO_2 emissions. All IoT devices are battery-operated and to extend the network's operational period energy saving is necessary during the data communication. Many studies are focusing on developing Green communication in which bandwidth usage is optimized, harmful emissions are minimized and power usage is optimally decreased [29]. Besides the infrastructure facilities, the primary concern in the implementation of Green IoT is ensuring both security and privacy. With the adoption of Green IoT, an intruder may discover new ways to breach the system causing new security and privacy concerns and requiring more secure communications [14, 30, 31]. Security methods implementation places an additional load on IoT devices resulting in excessive energy and power consumption. Including security, we must discover mechanisms that take into account both energy usage and the expected quality requirements [32]. Moreover, securing IoT devices is a challenge as system requirements, power usage and budget constraints will increase in opposite directions. While reconfiguring Green computing in an IoT framework these constraints including security, quality, energy and cost must be considered [33]. The total cost of a service can be reduced by optimizing product quality, communication network and performance [34].

Energy harvesting emerges as a viable technique for extending battery life by delivering adequate power in Green computing. To improve the energy efficiency of delay-sensitive applications the computational latency should be considered. In Edge Computing, mobile edge computing (MEC) server reduces overall computational latency and power consumption for delay-sensitive IoT devices [35]. The computational latency can be achieved at the expense of energy efficiency. Although, to make a Green system while reducing energy requirements, delay and traffic offloading need to be satisfied. In MEC servers, a combined optimization of energy consumption and latency is accomplished using the Latency-Aware Green (LAG) computing method to balance this trade-off [36]. Therefore, to ensure Green computing in any Internet framework along with high energy efficiency and reduced pollution we have considered security, cost, delay, and traffic constraints.

The energy efficiency of Wi-Fi tethering devices has been improved by utilising power conservation mode in the power saving mode (PSM) strategy. The primary idea behind this strategy is to optimise the number of idle intervals to save energy. The energy requirement can be reduced by optimizing the number of sleep intervals, although it compromises the delay requirement. Similarly, the energy savings are primarily dependent on the precision of network traffic forecasting [37]. A hierarchical framework is proposed to increase the network lifetime by permitting direct communications between relay nodes instead of sensor nodes. The framework is capable of traffic offloading from the sensor to relay nodes [6]. When Green IoT is concerned, security and safety are the top priorities. Together with privacy, we must consider some technologies that consider both power consumption and the required QoS. Green IoT research has recently centred on Green IoT technologies like Green RFID, GWSN, GM2M, GDC, GCC and GICT [5, 16]. As the usage and availability of personal devices rise, it is becoming essential to fulfil both Green and low-cost computing requirements. When it is about the selection of hardware, the main objective is to find something that would be low-cost, easy to handle with more stability [17]. Some applications like recognition software, virtual reality, and online video games demand high computational power and minimal network delay. MEC is considered as a solution to the excessive latency in job offloading. MEC gathers data from end-users or IoT devices and evaluates it at the network's edge. Offloading computationally heavy tasks to the MEC will result in energy savings for short-latency devices and applications [38]. A detailed study is required to develop the procedure for raising awareness about how effectively applies IoT technologies in greening the network. Several constraints like delay, traffic, cost and security should be considered while achieving more generic energy efficient results in Green IoT.

Implementing a Green IoT system leads to miscellaneous challenges. To handle such challenges there are requirements of durable battery, cost-effective robust and flexible connectivity, interoperability of heterogeneous hardware, and various security mechanisms [15]. Although, the main restriction on implementation is because of limited resources available for IoT devices such as limited energy, limited computation, and limited processing proficiency. Therefore, we can categories the following constraints in the deployment of Green IoT.

- Energy efficiency
- Cost-effectiveness
- Security and privacy
- Delay constraints
- Traffic offloading
- Emission and pollution in the environment

In the current world scenario as the dependence on technologies and the Internet is increasing very rapidly, therefore, the IoT came with many applications in the real world. However, it becomes more challenging as IoT devices have many constraints such as energy efficiency, cost-effectiveness, security and privacy, delay constraints, traffic offloading, and carbon emissions in the environment. Hence, the proposal of energy-efficient, cost-effective, secure, and low carbon emission plays a vital role in Green IoT.

In general, Green IoT can be viewed as the combination of four main elements, that is, Green hardware, Green software, Green architecture, and Green communication. Green hardware consists of sensors, RFID, and a microcontroller. Green software can be defined as data analytics, prediction, classification, and reliable delivery of data. Green communication can be specified as the technology used for information exchange over the network for example Bluetooth, Zigbee, network field communication, RFID and, Ad hoc. The Green architecture can be seen as GCC, Green edge computing, fog computing, and all kind of virtual computing [10]. Two important Green IoT elements are described as follows:

- *Green RFID* One of the newest short-range wireless technologies similar to RFID systems is near-field communication. With a working range of up to 20 cm, NFC works on the 13.56 MHz radio frequency band. Within RFID technologies, near-field communication is more user-oriented. RFID plays an important role towards a green and sustainable environment by reducing air pollution, tracking ecosystem functioning, saving power consumption, and optimizing waste management. Therefore, the biodegradable RFID tag is an initiative concerning Green IoT [13].
- *GCC* The main purpose of GCC is to limit the use of harmful substances, minimize energy usage as well as improving the recovery and recycling of obsolete products and garbage. GCC provides eco sustainable and energy-efficient technologies while offering excellent power management in the cloud. The goal of GCC is to create high-end computing systems such as data centres and clouds that satisfies the quality-of-service expectations. GDCs transfer virtual computers to other machines and hibernate idle machines to conserve a considerable amount of energy. GCC refers to a variety of methods for conserving energy such as reduced CPU power dissipation, Green energy supplies, efficient energy storage facilities, reduced cooling requirements and enhanced clock gating [29, 39]. Cloudlet is proposed in [9], which is located at the edge of the internet and a medium-sized and efficient cloud data store. The primary objective of the cloudlet is to enable resource-intensive and integrated mobile applications by offering low latency mobile technologies with efficient computing resources.

Green IoT systems help in the reduction of waste products, the protection and monitoring of the environment, and the minimization of operating costs and energy. To have very little effect on the environment, the complete production process of Green IoT should concentrate on Green architecture, Green building, Green consumption, and finally Green recycling. Now a day's many operators of data centres and servers are investing in environmentally friendly projects. The service providers are inspired to accelerate the transition to renewable energy. There are some challenges and benefits to switch from IoT to Green IoT such as software-based, hardware-based, routing algorithm-based, and policy recycling-based to save energy and cost. An effective energy-harvesting-aware routing algorithm (EHARA) [22] is proposed for Green Internet to predict the arrival of harvested energy at the nodes. Three EH techniques which are solar-based, moving vehicle-based and radio frequency-based are discussed in EHARA. These EH techniques are used by IoT devices to get energy and recharge their batteries from renewable sources. A green Internet-based energy harvested wireless sensor network (EH-WSN) [40] architecture allows the WSN node to be powered by a thermoelectric generator to reduce the cost of hardware and improve energy efficiency. Sleep scheduling and wake up protocol are used to prohibit direct communication between two sensor nodes. The EH-WSN architecture saves energy and increase the life span of the system.

Green IoT has several advantages over IoT, some of which are listed below:

- Environmental friendly Green IoT minimizes the adverse environmental impacts of computer hardware development and demolition while ensuring long-term environmental protection [41].
- In Green IoT, all the devices, communication networks, sensor systems, clouds and the webs work together to improve energy efficiency [29].
- Green IoT provides better use of resources while ensuring high performance. The GDCs require computer peripherals to evaluate the gathered data and the devices which are used to design and produce computer parts should be recyclable [22, 41].
- Green IoT ensures low latency and cost-effectiveness. The MEC allows for resource distribution that is economic and faster in reference to energy utilization and response time respectively. It also extends the device's lifetime while ensuring low cost [42].
- Green computing improves the adherence and compliance of organizations in fulfilling business requirements laid by their interested parties along with their reputation [41].
- Green IoT provides sustainability by using renewable energy resources. EH is essential for energy balancing and supporting Green communication. Around the world, there is a large production of energy from renewable sources. As of November 27, 2020, renewable energy accounted for 38% of India's installed electricity generation capacity [32].

In this paper with an effort towards Green IoT, a survey on various energy-efficient, cost-effective, and secure techniques is performed with a detailed focus on delay constraints and traffic offloading. This paper will be beneficial for researchers, who want to get the deepest knowledge about Green IoT and various ways to implement it efficiently. This paper contributes to various factors that should be considered while implementing a Green framework in various IoT techniques.

3 Review of Various Techniques to Achieve Green IoT

This section studies the work that contributed to achieving the Green IoT. Many researchers have demonstrated the effective use of various schemes toward achieving a Green IoT perspective; however, it still needs to be well addressed in terms of energy efficiency, cost efficiency, security, delay constraint analysis, and traffic offloading. The contributions by various researchers for achieving Green IoT have been broadly classified into the following techniques:

(1) Energy efficiency based techniques
(2) Security and privacy based techniques
(3) Cost efficiency based techniques
(4) Delay-constrained based techniques
(5) Traffic offloading based techniques

3.1 Review of Energy Efficiency Based Techniques for Green IoT

Many energy-efficient techniques can focus on IoT but classification and design of processes and components used in an IoT system in the reference of Green IoT can aid in the development of a Green network. In this section, various Green IoT schemes such as collaborative location-based sleep scheduling (CLSS) and time and priority-based sleep scheduling (TPSS) mechanisms [5], cross-interface gateway scheduling scheme and green IoT gateway (GIG) scheme [37] are discussed while focusing on various Green networking parameters in terms of hardware usages, software applications and various scheduling algorithms. Various EH and management techniques such as an effective EHARA [22], light energy-harvesting, radio frequency energy-harvesting and vibration energy-harvesting [43] are discussed. Energy efficiency based techniques define a way of utilizing less energy to implement a process. Various schemes to achieve energy efficiency are discussed with their applications in the field of Green IoT. Table 1 provides the outline of work discussed in the energy-efficient based techniques. The following are the contributions under energy efficiency based techniques:

- *Software-based, hardware-based, policy-based, and awareness based Green IoT techniques* [1] are used to provide selective sensing and intelligent tradeoffs.
- *CLSS and TPSS* mechanisms [5] focused on Green Information and Communications Technologies (ICTs) such as Green RFID, Green WSN, GCC, GM2M, and GDC. These Green ICTs enhance the WSN lifetime, security, quality of service, and decrease the WSN energy consumption.
- *Zonal thermal pattern analysis (ZTPA) and energy efficient adaptive health monitoring System* [6] enhanced indoor coverage. These methods reduce power consumption, provide latency insensitivity, and massive connection support towards Narrow Band IoT (NBIoT).
- *EMS* [15] for scheduling of the processes of energy-based nodes for IoT perform data minimization by using data prioritization, compression, and fitting. EMS provides fault tolerance, tests energy consumption and the number of failure nodes for WSN, RFID, and Mobile Ad hoc Network (MANET) in the IoT environment.
- *Lyapunov optimization on time and energy cost (LOTEC)* [19] algorithm balances the data processing time and cost while handling energy consumption in two modes of power supply. LOTEC algorithm uses solar power as the primary energy supply and grid power as the backup supply.
- *An effective EHARA* [22] is proposed to predict the arrival of harvested energy at the nodes. Three EH techniques are solar-based, moving vehicle-based, and radio frequency-based. These EH techniques are used by IoT devices to get energy and recharge their batteries from renewable sources.
- *Cross-interface gateway scheduling scheme and GIG scheme* [37] are used to minimize the energy consumption of high-power WiFi radios and low-power ZigBee. This GIG scheme dynamically schedules for both WiFi and ZigBee data transmission to maximize the energy efficiency of the gateway with bounded delay.
- *Light EH, radio frequency EH, and vibration EH schemes* [43] minimize the power consumption of the batteries. The power management integrated chip is used to increases the life of the system and uses 6LowPAN, Wi-Fi, and ZigBee for communication.
- *Sleep scheduling and wake up protocol* [20] are used to prohibit direct communication between two sensor nodes. The preferred architecture may save energy and increase the life span of the system.
- *Energy conservation with the assistance of resourceful mules (ECARM)* [44] is used for resourceful mules (RM) selection, information exchange, cycling coordination, and fast recovery. ECARM provides energy conservation with the assistance of RM, which saves energy for WSN.

3.2 Review of Security and Privacy Based Techniques for Green IoT

The implementation of security and privacy techniques can lead to excessive energy consumption and performance

Table 1 Summary of energy efficiency based techniques

Author	Proposal/algorithm	Characteristics	Technology used	Outcome of work	Usability/application
Rushan et al. [1]	Green IoT techniques	Reduce network size, provide intelligent tradeoffs	Selective sensing, hybrid architecture, policy making	Recycling of IoT devices	Activity tracking at home, industry, transportation
Chunsheng et al. [5]	CLSS and TPSS mechanisms	Green RFID, Green WSN	Sensor-cloud as traditional WSN	Enhance WSN lifetime, security, QoS	Industry automation, health monitoring system
Sakshi et al. [6]	ZTPA, energy efficient adaptive health monitoring system	Enhanced indoor coverage, low power consumption, massive connection support	LPWA technologies like LoRa, SigFox	Cost-effective, reliable, low power consumption	Utility-meter, industry automation, environmental monitoring
Omar et al. [15]	EMS for scheduling	Minimized data transmission, high fault tolerance	Data prioritization, compression, fitting	Low energy consumption, small number of failed nodes	Power retaintion for a long time
Yucen et al. [19]	LOTEC algorithm	Solar power and grid power supply	Lyapunov optimization technique	Green energy production without increasing response time	Delay sensitive IoT applications
Thien et al. [22]	An effective EHARA	Improve energy efficiency, QoS, network lifetime	Solar-based, moving vehicle-based, RF-based EH Techniques	Manage variations of traffic load, more energy availability	In design of routing protocols for EH WSN
Hua et al. [37]	Cross-interface gateway scheduling	Minimize energy consumption	Dynamic scheduling	Energy efficient device for gateway communications	Lighting, heating, ventilation, air condition appliances
Afghan et al. [43]	Light EH, radio frequency EH, and vibration EH schemes	Provide energy management	6LowPAN, Wi-Fi, ZigBee with EH schemes	Increase lifetime, minimize power consumption	Smart parking system, surveillance, environmental monitoring
Kun et al. [20]	Sleep scheduling, wake up protocol	Save energy, balance traffic loads	Three-layer architecture	Increase life time	Protection of industry plants via control and surveillance
Yi et al. [44]	ECARM technique	Save energy for WSN	Wake-up/sleep cycling, and duty cycling	Cycling coordination, and fast recovery	Intelligent transportation, environment surveillance

Table 2 Summary of security and privacy based techniques

Author	Proposal/algorithm	Characteristics	Technology used	Outcome of work	Usability/application
Sarmadullah et al. [48]	Mutual authentication key establishment protocol	Reduce memory size, encryption latency	On-line symmetric key method	Automated validation of Internet security protocols	Automatic health monitoring, controlling
Feng et al. [49]	Authentication, credential update schemes	Authentication, access control	Four-way handshakes, root password security method	System access as administrator, privileged, regular users	Storm-water runoff challenges
Mithileysh et al. [50]	SVSS	Low cost, extensible, flexible wireless system	Wireless communication, cloud networking, fuzzy algorithm	Detect, monitor device remotely	Fleet management, tracking vehicles
Ishaq et al. [45]	ECDH technique	ZWave, thread protocols for authorization	Z-Wave follows TDES method	Authorizes an exchange of temporary keys	Security applications
Ted H. Szymanski [46]	Centralized SDN scheme	Enhance security, privacy, performance, energy efficiency	Deterministic virtual networks, lightweight encryption	Detect unauthorized packets, improve security	Smart power grid, smart healthcare
Bhawna et al. [51]	AEE approach	Solution for jointly global-optimal attacking mode	Theoretical solution for physical layer security	AEE using joint optimization	Smart home, smart city
Reem et al. [23]	Lightweight, secure multi-factor device authentication protocol	Robustness, low complexity, minimum computations cost	Bit-wise XOR operation, one-way hash function	Mutual authentication, data confidentiality, message integrity	Distributed real-time IoT applications
Pallavi et al. [47]	ABE algorithm	Security algorithms in middleware	ABE as security algorithm	Control all communications with security	Heterogeneous networking environments
Ishtiaque et al. [42]	MEC technique	Caching, cooperative task offloading, security service assignments	Non-linear program optimization	Reduced energy consumption, security-breach cost	Autonomous vehicles, virtual reality, interactive gaming
Peter Aufner [52]	STRIDE, CORAS, LINDDUN frameworks	Study of various threat modeling frameworks	Security, privacy threat modeling	Gap identification in threat modeling frameworks and IoT	Research area related to security in IoT

degradation. Therefore, including the security we must discover mechanisms that take into account both energy usage and the expected quality assurance [32]. In this section, various Green IoT techniques such as elliptic curve Diffie-Hellman (ECDH) technique [45], centralized software defined networking (SDN) [46] and attribute-based encryption (ABE) algorithm [47] are discussed to enhance security, privacy, performance and energy efficiency in the Green IoT. Security and privacy are very crucial in networking, communication and information exchange over the network. Various techniques to achieve more security and privacy in the Green IoT are discussed. Table 2 provides the outline of work discussed in the security and privacy based techniques. Some contributions under security and privacy based techniques are as follows:

- *Scalable mutual authentication and key establishment protocol* [48] check the reliability of authentication and cryptographic material creation and management. For the large-scale Internet security-sensitive protocols and applications, it uses an industrial-strength automated analysis tool. This scheme occupies little memory and consumes low energy during the authentication and key generation processes with low encryption latency.
- *The authentication and credential update schemes* [49] provide authentication and access control. The authentication process includes four-way handshakes and the credential of a system administrator to an IoT node is its root password. The proposed authentication and credential update schemes give access to the system depending on permission levels as administrator, privileged or regular users.
- *Smart vehicle security system (SVSS)* [50] employs the integration of RFID, global positioning system (GPS), Global System for Mobile communication (GSM), wireless communication, cloud networking, and fuzzy algorithm. This system provides double security and helps one to locate the device on a map with remote control.
- *ECDH technique* [45] authorizes an exchange of temporary keys for secure communication. Z wave and thread are used with datagram transport layer security (DTLS) or transport layer security (TLS) for secure communication. ZWave is based on propriety design, and the thread is completely based on standards.
- *Centralized software defined networking (SDN)* [46] scheme enhanced security, privacy, performance, and energy efficiency in the IoT. The combination of a centralized software-defined networking and deterministic virtual network with long key encryption lowers the capital and energy costs. SDN detects unauthorized packets quickly and achieves exceptional security, privacy, performance, and energy efficiency in the IoT.
- *Attacker energy efficiency (AEE) approach* [51] is an energy-aware attacking strategy for hybrid attacks. AEE uses theoretical analysis of physical layer security in the secure IoT to reduces the secrecy rate.
- *Lightweight and secure multi-factor device authentication protocol* [23] uses two schemes. TLS and secure sockets layer (SSL) protocols for dynamic key generation, data confidentiality, and message integrity. Configurable physical unclonable functions (PUF) and channel-based parameters support TLS and SSL protocols.
- *Attribute based encryption (ABE) algorithm* [47] provides more security than other security algorithms. The security is enforced within the middleware by utilizing many security algorithms such as digital signature algorithm (DSA), Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), data encryption standard (DES), and triple data encryption standard (3DES). Middleware also handles all the communications between a client and the target applications.
- *MEC technique* [42] uses caching, task offloading, and security service allotment for IoT networks. MEC offloads IoT tasks to the edge servers without disputed delay requirements. The offloaded tasks are encrypted and decrypted at the user devices and MEC servers. The MEC technique is prepared as a constrained non-linear program (NLP) optimization.
- *STRIDE, CORAS, and LINDDUN frameworks* [52] are used for threat modeling. STRIDE (an acronym that stands for six categories of security risks: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges), CORAS (a method for security risk analysis) and LINDDUN (an acronym for seven privacy threat categories: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance) threat modeling frameworks are discussed which deal with security and privacy threats.

3.3 Review of Cost Efficiency Based Techniques for Green IoT

Many cost-effective techniques are used to reduce the cost by optimizing product quality, communication network and performance. Some schemes are discussed that balance the trade-off between energy and cost such as minimal energy consumption algorithm (MECA) [2] and centralized and distributed user association algorithm [53]. These schemes are used to reduce the cost based on estimated energy consumption. An EH-WSN [40] scheme uses EH to keep low cost and utilizes renewable resources for efficient power usage. Remote system management unit (RSMU) [54] provides a

Table 3 Summary of cost efficiency based techniques

Author	Proposal/algorithm	Characteristics	Technology used	Outcome of work	Usability/application
Jun at al. [2]	MECA algorithm	Minimize operational costs power consumption	A three-layer system framework	Long network lifetime	Smart home, smart city, transport
Bang at al. [53]	Centralized and distributed user association algorithm	Reduced energy cost	Green energy allocation/real-location user association algorithm	Reduce operational complexity	Smart cities environment monitoring
Hamid et al. [55]	Fog-based data analytics scheme	Optimize resource allocation, minimize response time	Data consumer association, virtual machine placement using MINLP formulation	High computing performance, cost-efficient resource allocation	Pipeline monitoring, smart traffic light systems
Michal et al. [40]	EH-WSN architecture	Hardware cost reduction, more energy efficient	Ultra-low-power microcontroller units	Overcharging protection threshold	Industrial, wearable applications
Emran et al. [56]	Ultra low cost and compact chipless RFID sensor scheme	Cost reduction of identification sensor	RFID humidity sensor, ELC sensor based on frequency shifts	cost reduction by flexible printing substrates	Low-cost tagging, sensing, automated, robust applications
Alexander et al. [57]	Distributed wireless MAC protocol	Eco friendly, cost-effective, low power technique	Energy efficient, power minimization approach	Improved SINR with minimized transmitting power	Computing and automation applications
Lavanya et al. [59]	Low-cost fertilizer intimation system	A low cost, accurate, intelligent farming technique	CoAP and IPV6 for low power WAN	useful in the agriculture sector for huge production	To analyze soil nutrients in agricultural farms
S.Din et al. [34]	Clustering algorithm with mobility management	High data rate with lower usage of bandwidth	Clustering with mobility management	Green IoT and location address for 5G communication	Healthcare data communication
Marufa Y et al. [54]	RSMU with GUI	Low cost, energy-efficient,, sustainable environment for driving system	RSMU to evaluate energy management, maintenance	Minimize cost of Green energy based system	Smart city, remote highway lighting system
Felisberto et al. [58]	Cost and energy-efficient IoT edge device scheme	Cost-effective, energy-efficient building occupancy estimation	LoRaWAN, MQTT	Collect and transmit the networking and environmental parameters	Smart homes, building management

driving system of low cost, low power and a sustainable environment. In this subsection, various schemes to achieve cost efficiency are discussed with their applications in the field of Green IoT. Table 3 provides the outline of work discussed in the cost efficiency based techniques. Some cost-efficiency based techniques are as follows:

- *MECA* [2] grasps the clustering principle and uses the Steiner tree algorithm to solve the optimization problem. MECA uses hierarchical deployment and confers a three-layer system framework for large-scale IoT deployment. The relays in the proposed framework are connected in a mesh mode to achieve a long network lifetime by arranging network objects cost-effectively to form a Green IoT.
- *A centralized and distributed user association algorithm* [53] allocates the Green energy in the time domain for each base station. The algorithm reduces the energy cost based on estimated energy consumption scenarios. The user association algorithm is also used to perform spatial resource allocation.
- *Fog-based data analytics scheme* [55] optimizes resource allocation and reduces response time. All the tasks such as data consumer association, task distribution, and virtual machine placement are performed at a lower cost. Mixed-integer nonlinear programming (MINLP) is applied to the minimum cost problem.
- *An EH-WSN* [40] architecture allows the WSN node to be powered by a thermoelectric generator to reduce the cost of hardware and improve energy efficiency. EH is performed with temperature difference and uses a rechargeable battery which keeps the charge much longer.
- *An ultra-low cost and compact chipless RFID sensor scheme* [56] reduces the cost of the sensor by flexible printing substrates. The Electric Inductive-Capacitive (ELC) sensor gives an efficient frequency shift for effective sensing.
- *Distributed wireless Medium Access Control (MAC) protocol* [57] is used to improve the Signal-to-Interference plus Noise Ratio (SINR) without increasing the transmitter power. It is an environment friendly, cost-effective, and low power technique. Physical-MAC provides both the energy-saving and cost-saving.
- *The clustering algorithm* [34] with mobility management reduces energy consumption and provides a high data rate. The used algorithm consumes low bandwidth and arranges all mobile devices into a separate cluster.
- *RSMU* [54] with a Graphical User Interface (GUI) is used in a Green highway lighting system. RSMU provides a safe and smooth driving system of low cost, low power, and a sustainable environment.
- *A cost and energy-efficient IoT edge device scheme* [58] is used for effective building occupancy estimation. This scheme collects and transmits networking and environmental parameters to the cloud. The messages sent by the edge devices are then collected by the long range wide area network (LoRaWAN) gateways. These messages are forwarded using MQTT which uses secure IP connection, specific web services made available by a representational state transfer (RESTful) application programming interface (API).

3.4 Review of Delay-Constrained Based Techniques for Green IoT

Delay requirements can be assured at the expense of energy efficiency. To ensure Green computing in IoT while reducing energy consumption delay constraints should be focused. Some techniques are discussed such as Delay Based Workload Allocation (DBWA) [60] that gives minimal energy consumption and guarantees delay. Utility-based Adaptive Duty Cycle (UADC) [61] routing algorithm is discussed to ensure reliability, low energy consumption and desired delay. A balanced energy-delay solution [62] and a delay DSDR scheme [63] are discussed to reduce transmission delay and enhance energy efficiency in Green IoT. Many IoT applications are vulnerable to delay constraints and the performance of the system can be severely affected by the long delay. Table 4 provides the outline of work discussed in the delay-constrained based techniques. To guarantees delay for delay-sensitive applications in the field of Green IoT, various techniques have been summarized as follows.

- *Accelerated gradient algorithm* [64] is implemented for optimal offloading decisions and overcome the energy minimization problem. The algorithm is applied to fog nodes for fog computation offloading under expected time latency. The algorithm achieves an optimal offloading ratio at a fast speed.
- *Delay Based Workload Allocation (DBWA)* [60] algorithm is based on the Lyapunov drift-plus penalty theory. The algorithm provides the optimal workload allocations among local edge servers, neighbor edge servers, and the remote cloud. DBWA gives minimal energy consumption towards the IoT-edge-cloud system and guarantees delay.
- *UADC* [61] routing algorithm uses a performance evaluation function to evaluate the relevance of choosing different relay nodes. It selects the node based on the utility of the system to perform data relay. The utility function combines comprehensive indexes such as the reliability, energy consumption, and delay of the node.

Table 4 Summary of delay constraints based techniques

Author	Proposal/algorithm	Characteristics	Technology used	Outcome of work	Usability/application
Siguang et al. [64]	Accelerated gradient algorithm	Minimize energy consumption, guarantee delay	Accelerated gradient algorithm	Optimal offloading decision at fast convergence speed	Time-sensitive, industrial applications
Mian et al. [60]	DBWA algorithm	Reduce energy consumption and delay	Lyapunov drift-plus penalty theory	Evade queuing delay, queuing workloads for jobs offloading	Augmented reality, delay-sensitive applications
Jiaze et al. [61]	UADC routing algorithm	Improve energy efficiency with reduced transmission delay	UADC with performance evaluation function	High energy utilization rate with lower delay	Transportation, healthcare, power grid
Adila et al. [62]	A balanced energy-delay solution based on the evolutionary approach	Balance energy-delay	Evolutionary Algorithm approach	Improves energy consumption and delay	Real-time, low latency IoT applications
Ashkan et al. [65]	AFP and LFP modes	Evaluate and model service delay	AFP and LFP modes for processing	AFP has minimum service delay as compare to LFP	Real-time IoT applications
Amitav Mukherjee [66]	URLLC system	Provide trade-offs between delay and energy efficiency	Low-rate error correction coding	Improve delay, energy efficiency	Augmented reality, remote surgery
Mingfeng et al. [63]	DSDR scheme	Reduce transmission delay	Direct forwarding, wait forwarding methods	Reduce transmission delay of delay-sensitive, delay-tolerant data	Fire monitoring, weather monitoring systems
Wassim et al [67]	Fog-to-fog communication algorithm	Minimize end to end dela	Resource selection algorithm	Fog-to-cloud communication with lower delay	Smart health care, smart environmental monitoring
Yiqin et al. [24]	DPCOEM algorithm	Low maintenance cost, minimum response time	Lyapunov optimization to acquire the parallel offloading strategy	Energy stability, sustainability	Biomedical applications
Gaofeng et al [38]	JUAOD-ORA scheme	Reduce latency, save energy	Lagrange multiplier method with DRL	Low complexity in dynamic environments	Traffic, space information system

- *A balanced energy-delay solution* [62] is based on the evolutionary algorithms approach. In this approach, each object is assigned to only one fog instance and the total execution time remains below acceptable delay. Hence, the number of objects increases which maximizes fog utilization and the average latency with a linear slope.
- *All Fog Processing (AFP) and Light Fog Processing (LFP) modes* [65] are used to reduce the service delay by sharing the load. In used modes, fog layer lies between IoT devices and the cloud. It could handle the majority of IoT service requests to reduce the overall service delay.
- *Ultra-Reliable Low Latency Communications (URLLC) system* [66] can be created by allocating a large bandwidth for the data and using an Orthogonal Frequency-Division Multiplexing (OFDM). Total handover delay can be reduced effectively by using low-rate error correction coding with multi-antenna beamforming.
- *A delay DSDR scheme* [63] is proposed to reduce transmission delay by establishing energy-efficient routing paths. In this scheme, routing is dynamically selected according to the delay requirements of data. Two different strategies are used as, direct-forwarding for delay-sensitive data to minimize end-to-end delay and a wait-forwarding method for delay-tolerant data to perform data fusion for reducing energy consumption.
- *Fog-to-Fog (F2F) communication algorithm* [67] is proposed which approves fogs to communicate with each other to process job requests and minimize the overall end-to-end latency. The algorithm improves the traditional Fog-to-Cloud (F2C) communication and increases the probability for a job to meet its delay related requirements.
- *Dynamic Parallel Computing Offloading and Energy Management (DPCOEM) algorithm* [24] adopts the parallel offloading strategy in MEC to solve the problem based on the Lyapunov optimization technology. The algorithm achieves approximately optimal performance, provide energy stability, and sustainability.
- *A Joint User Association and Offloading Decision with Optimal Resource Allocation (JUAOD-ORA) scheme* [38] is applied to obtain the optimal solution which uses the Lagrange multiplier method and Deep Reinforcement Learning (DRL). The JUAOD-ORA algorithm performs better with low complexity to reduce the latency and energy cost-effectively.

3.5 Review of Traffic Offloading Based Techniques for Green IoT

To deploy Green IoT while reducing energy requirement delay and traffic offloading need to be satisfied. In this section, some techniques to achieve traffic offloading in Green IoT are discussed. The reinforcement learning technique with the Dyna-Q scheme [35] and radio resource management (RRM) algorithm [69] are used to save energy by reducing the load of the regular network. Clustering algorithm with the device-to-device collaboration [25] allows faster communication and reduces energy consumption by the collaborative device-to-device communications. A Two-stage Energy-Aware Traffic Offloading (TEATO) scheme [73] is used to minimize half of the power consumption for daily traffic with a renewable power source. In this section, various techniques to perform traffic offloading on multiple communication systems are discussed. Table 5 provides the outline of work discussed in the traffic offloading based techniques.

- *The reinforcement learning technique with the Dyna-Q scheme* [35] is an extension of Q-learning which incorporates both EH and MEC. This scheme offloads the computation task through the selection of an optimal offloading rate. The remaining task is computed in a very less time with low complexity.
- *Conditional traffic offloading scheme* [68] eliminates interference and traffic congestion possibility by using efficient traffic offloading technique. This technique selects the proper operation mode of small cells and fulfills the macro user application's quality of service requirements. The scheme is generally applied to heterogeneous network setup.
- *RRM algorithm* [69] is used for intelligent dynamic traffic distribution among femto and WiFi networks. It is used to shift most of the traffic from the core network to the WiFi, therefore it saves energy by reducing the load of the regular network and minimize congestion.
- *Genetic algorithm-based adaptive offloading (GA-OA) scheme* [70] can be used to achieve low complexity, low delay, and processing time with improved request success ratio and effective traffic handling. The process of traffic handling and request processing is carried out in both the infrastructure and gateway part of the architecture.
- *A low-complexity energy-aware and adaptive traffic offloading strategy (EATO)* [71] reduces the average on-grid energy consumption. EATO strategy adopts harvested renewable energy and traffic offloading to improve system performance and minimize energy consumption.
- *Clustering algorithm with device to device collaboration* [25] allows faster communication and reduces energy consumption by collaborative device to device communications. The use of heterogeneous macrocell and small cell base stations (SBS) contributed to allowing traffic offloading on two levels: offloading of macrocell traffic by SBS and offloading of macro and small cell traffic by

Table 5 Summary of traffic offloading based techniques

Author	Proposal/algorithm	Characteristics	Technology used	Outcome of work	Usability/application
Pankaj et al. [35]	Reinforcement learning technique with Dyna-Q scheme	Reduce convergence rate, offloading rate, energy consumption	Reinforcement learning for selection of MEC server	Offload computation task through selection of a minimal offloading rate	Smart healthcare, environmental monitoring
I. AlQerm and B. Shihada [68]	Conditional traffic offloading scheme	Eliminate interference, traffic congestion	Online reinforcement learning methodology	Maintain QoS, improve offloading decision quality	Industrial applications
Yiqin et al. [24]	DPCOEM algorithm	Green and Sustainable MEC framework	Lyapunov optimization technology	Energy stability, sustainability	Biomedical application
Adrian et al. [69]	RRM algorithm	Traffic management, energy saving by integrated WiFi network	Intelligent dynamic traffic distribution	Reduce traffic, congestion	Residential buildings, enterprise premises, metro stations
Azham et al. [70]	GA-OA scheme	Low complexity and less processing time	Effective traffic handling, request processing	Low processing time, delay, complexity	Delay minimization for IoT fog cloud applications
Lin et al. [71]	Low-complexity EATO strategy	Lower energy consumption by adopting renewable energy, traffic offloading	Online adaptive traffic offloading, bandwidth allocation strategy	On-grid energy consumption minimization	Agriculture, industrial, smart cities
Elias et al. [25]	Clustering algorithm with device to device collaboration	Energy saving, QoS improvement	Clustering algorithm	Reduce energy consumption, increase data rates	Live streaming based applications
Ankan et al. [72]	FAR, HSM and UBS schemes	Predict future data transfer with reduced latency	High-level petri nets with content dissemination schemes	Reduce message drop, improve performance	Data and traffic-intensive applications
Shan et al. [73]	A Two-stage TEATO scheme	Minimize on-grid network power consumption	Multiple SBS with the renewable power sources	Traffic offloading with minimized power	Smart environmental monitoring
Minghui et al. [26]	Traffic-aware multiple slot frames scheduling algorithm	High reliability, energy efficiency, low duty cycle	Time Synchronized Channel Hopping (TSCH)	Efficient resources allocation	Industrial IoT

Table 6 Summary of various issue/limitation found in the literature

S. no.	Author names	Optimization techniques used to provide green IoT framework	Various issues/limitations	Category
1.	Omar et al. [15]	Data prioritization, compression and fitting	Send limited size data only	Energy efficiency based technique
2.	Yucen et al. [19]	Solar power and grid power supply	Otimization is possible in presence of solar energy	Energy efficiency based technique
3.	Kun et al. [20]	Sleep scheduling and wake up protocol	Compromised scalability	Energy efficiency based technique
4.	Yi et al. [44]	Energy conservation with the assistance of RM	Weak data security	Energy efficiency based technique
5.	Mithileysh et al. [50]	Green RFID	More risk of forgery and hacking	Security and privacy based technique
6.	Reem et al. [23]	Lightweight protocol	A malware can compromise the entire security	Security and privacy based technique
7.	Pallavi et al. [47]	Middleware handles all the communications	Security breach in direct data transfer to cloud	Security and privacy based technique
8.	Michal et al. [40]	Thermoelectric generator	A fault can cause permanent destruction of the battery	Cost efficiency based technique
9.	Felisberto et al. [58]	LoRaWAN and MQTT	Long evaluation time	Cost efficiency based technique
10.	Amitav Mukherjee [66]	Low-rate error correction coding	Need connection re-establishment at each radio link failure	Delay constraints based technique
11.	Mingfeng et al. [63]	Wait forwarding method	Complex Data routing	Delay constraints based technique
12.	Elias et al. [25]	Collaborative device to device communications	The proximity between MTs required for faster communication	Traffic offloading based technique
13.	Shan et al. [73]	Renewable power sources	Traffic offloading not considered for overlapped SBSs	Traffic offloading based technique
14.	Rakesh et al. [27]	Rendezvous-based routing protocol	Random deployment of devices promotes more security threats	Security and privacy based technique
15.	Xiang et al. [74]	On-demand scheduling	Unsatisfied delay requirements	Energy efficient and delay constraints based technique
16.	Ranji et al. [75]	Energy-efficient and delay-aware offloading scheme	Devices within specific range never collaborate on offloading	Energy efficient and delay constraints based technique
17.	Bhandari et al. [28]	Resource aware and reliable objective function	Congestion problem, resource-constrained network	Energy efficiency based technique

the device to device communications, hence it increases the data rates of mobile terminals.

- *Forecast and relay scheme (FAR)* [72] is a hybrid scheme for message replication (HSM). With HSM a Utility-Based Scheme (UBS) is also used in which a new symbolic model verifier has been employed for the verification of the content dissemination in the dynamic and delay-tolerant data environments. UBS avoids message loops, lowers the message drop rate, and improves performance.
- *A two-stage energy aware traffic offloading (TEATO) scheme* [73] is used to decide traffic offloading for the multiple SBS. Using energy arrival and traffic load information, it can minimize half of the power consumption for daily traffic with renewable power sources.
- *Traffic-aware multiple slotframes scheduling algorithm* [26] computes available slot sets and allocates communication resources according to the requirement of data traffic to fulfill the end-to-end real-time communication. The algorithm is based on the Time Synchronized Channel Hopping (TSCH), which can be used in both single-hop and multi-hop wireless industrial network scenarios on a star topology and tree topology.

4 Various Issues/Limitations Found in the Literature for Green IoT

A list of issues in accomplishing Green IoT is given in Table 6. These issues are relevant from the Green IoT viewpoint concerning different strategies on energy efficiency, cost efficiency, security, delay, and traffic offloading techniques. The various issues to achieve Green IoT have been identified in the literature and some of them are as follows: To save energy, EMS [15] worked on the technique of decreasing the capacity of data to be transmitted over the internet. LOTEC [19] system uses dual-energy resources, solar power, and grid power supply to improve energy efficiency. To enhance the network efficiency by utilizing a solar supply, a more accurate weather prediction feature should be included. In [20], three-layer architecture is used for IoT deployment which compromised scalability for energy-efficient system. The use of ECARM [44] may weaken data security and in duty-cycled WSN it does not perform efficiently. In [50] the information sent and obtained from the current security system is prone to forgery and hacking. A malware embedded in any of the communication devices or the presence of an opponent on the same subnet can compromise the device security [23]. The system requires a longer evaluation time to compare gathered information with efficient employee occupancy [58]. In [66] to manage energy efficiency and delay in case of the radio link failure, it requires to re-establish the connection. DSDR [63] scheme solves the problem of delay and energy efficiency but it is not effective for improving network lifetime. Data routing is chosen dynamically for different areas which are complex tasks. The proximity between MTs is required for faster communication [25]. In [27] a rendezvous-based routing protocol is proposed in which the random deployments of devices promote more security threats. To reduce the energy usage on-demand scheduling is used which is not able to satisfy all time delay requirements [74]. In Energy-efficient and delay-aware offloading scheme (EEDOS) [75], devices within a specific range are not willing to collaborate on offloading which is an issue in the device to device communication. Resource Aware and reliable objective function (RAROF) [28] is used to enhance the energy efficiency and lifetime of the network which uses multi-queuing based traffic.

5 Research Gaps Found in the Literature for Green IoT

In this paper, a detailed study is performed to find the research gaps related to the real-time implementation of Green IoT. Some of the identified gaps are as follows: In [2] to achieve a more energy-efficient IoT system compressed sensing techniques can be applied in the hierarchical framework. In [19] to enhance the network efficiency, a new feature should be included for more precise and accurate weather prediction. In cross interface scheduling [37] the interference problem of Zigbee and Wifi can be solved by using Z-Wave protocol as it works on the different frequency band. Effective gateway scheduling can be used to improve ZigBee link quality. The green roof monitoring system proposed in [49] emphasized authentication and credential techniques. The other security features such as confidentiality and integrity should be included in the IoT system. In [53] to minimize energy consumption cost, the concept of on-grid and solar energy is used. The on-grid energy of a centralized algorithm without borrowing can be improved. More cost optimization can be achieved in [55] by adding a selective sensing module to the fog layer and considering privacy-preserving data analytics and the mobility of data generators. In [40] to make the power management process independent of the user application, an embedded real-time operating system with a pre-emptive scheduler should be integrated. To minimize delay in IoT systems through fog computing the delay-cost trade-off should be considered [65]. Data integrity can be considered with delay constraint to guarantee transmission latency [63]. To predict future jobs the task processing history can be utilized in each fog and node [67]. In [26] multiple slots frame scheduling schemes can be applied to more complex network scenarios such as mesh topology. The complexity of the sensing framework [27] should be reduced with real-time implementation. In [65] on-demand scheduling is used while to satisfy delay requirement proactive method should be introduced. EEDOS [74] is more vulnerable against attack because of their limited computation power, security should be considered. In RAROF [28] to resolve the congestion problem, an efficient message scheduling technique should be introduced. Some important research gaps are identified and addressed in Table 7.

6 Conclusion and Future Work

In this paper, various techniques for achieving Green IoT based on different constraints such as energy efficiency, security, cost efficiency, delay constraints analysis, and traffic offloading have been categorized and discussed. A detailed review of various techniques related to each category to achieve Green IoT has been provided in this paper. Some issues to achieve Green IoT have also been discussed with some identified research gaps to assist researchers while finding open research problems in the field of Green IoT. Focusing on the energy-saving for Green IoT, the renewable energy resource and EH should be adopted. To accomplish a more secure Green IoT system with discussed techniques some modifications for a more secure encryption algorithm will be considered as a future endeavour. To improve the

Table 7 Summary of various research gaps found in the literature

S. no.	Author names	Optimization techniques used to provide green IoT framework	Research gap identified	Category
1.	Jun at al. [2]	Hierarchical deployment in a three-layer system framework	Compressed sensing techniques	Cost efficiency based technique
2.	Chunsheng et al. [5]	Green information and communications technologies	A virtualized sensor as a service	Energy efficiency based technique
3.	Yucen et al. [19]	Solar and grid power supply.	Intelligent weather prediction feature required	Energy efficiency based technique
4.	Thien et al. [22]	EH techniques	EHARA algorithm with IEEE 802.15.4 CSMA/CD	Energy efficiency based technique
5.	Hua et al. [37]	Cross-interface WiFi and ZigBee data transmission	Interference problem of Zigbee and Wifi	Energy efficiency based technique
6.	Sarmadullah et al. [48]	Automated Internet security protocols	IPsec/IKE cyber security protocols	Security and privacy based technique
7.	Feng et al. [49]	Restricted user access	Lack of confidentiality and integrity	Security and privacy based technique
8.	Reem et al. [23]	Lightweight protocol	Triple Data Encryption Standard in the same scheme	Security and privacy based technique
9.	Bang at al. [53]	Green energy resources	On-grid energy of a centralized algorithm without borrowing	Cost efficiency based technique
10.	Hamid et al. [55]	Optimize resource allocation and reduce response time	Lack of privacy-preserving data analytics	Cost efficiency based technique
11.	Michal et al. [40]	Thermoelectric generator	Preemptive scheduling	Cost efficiency based technique
12.	Ashkan et al. [65]	AFP and LFP modes	Delay-cost trade-off in fog computing	Delay constraints based technique
13.	Mingfeng et al. [63]	Wait forwarding method	Data integrity with delay constraint and transmission latency	Delay constraints based technique
14.	Wassim et al. [67]	Resource selection algorithm	Future jobs prediction	Delay constraints based technique
15.	Minghui et al. [26]	Resources allocation according to the traffic requirement	Multiple slots frame scheduling is required	Traffic offloading based technique
16.	Rakesh et al. [27]	Rendezvous-based routing protocol	Complexity reduction with real-time implementation	Security and privacy based technique
17.	Xiang et al. [74]	On-demand scheduling	Proactive method for delay requirement and on-demand allocation	Energy efficient and delay constraints based technique
18.	Ranji et al. [75]	Energy-efficient and delay-aware offloading scheme	Computation power, security	Energy efficient and delay constraints based technique
19.	Bhandari et al. [28]	Resource aware and reliable objective	Efficient message scheduling technique	Energy efficiency based technique

delay and traffic offloading schemes the delay-cost trade-off, task processing history, and various intelligent scheduling from the Green IoT perspective should be considered. Furthermore, the actual impact of Green IoT on the environment and economy would be of importance; therefore, more research to achieve Green IoT is required. IoT will change the path of emerging technologies in the future if focused and determined work is carried out.

References

1. R. Arshad, S. Zahoor, M. A. Shah, A. Wahid, and H. Yu, Green IoT: an investigation on energy saving practices for 2020 and beyond, *IEEE Access*, Vol. 5, pp. 15667–15681, 2017.
2. J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, A novel deployment scheme for green Internet of Things, *IEEE Internet of Things Journal*, Vol. 1, No. 2, pp. 196–205, 2014.
3. A. Gapchup, A. Wani, A. Wadghule, and S. Jadhav, Emerging trends of green IoT for smart world, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 5, No. 2, pp. 2139–2148, 2017.
4. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, Internet of Things: a survey on enabling technologies, protocols, and applications, *IEEE Communications Surveys and Tutorials*, Vol. 17, No. 4, pp. 2347–2376, 2015.
5. C. Zhu, V.C. Leung, L. Shu, E.C.-H. Ngai, Green Internet of Things for the smart world, *IEEE Access*, Vol. 3, pp. 2151–2162, 2015.
6. S. Popli, R. Kumar, and S. Jain, A survey on energy efficient narrowband Internet of Things (Nbiot): architecture, application, and challenges, *IEEE Access* Vol. 7, pp. 16739–16776, 2018.

7. G. Neagu, M. Ianculescu, A. Alexandru, V. Florian, and C. Z. Radulescu, Next generation IoT and its influence on decision-making: an illustrative case study. In *7th International Conference on Information Technology and Quantitative Management (ITQM 2019), Procedia Computer Science*, Vol. 162, pp. 555–561, 2019.
8. K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, Internet of Things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios, *IEEE Access*, Vol. 8, pp. 23022–23040, 2020.
9. Y. Ai, M. Peng, and K. Zhang, Edge computing technologies for Internet of Things: a primer, *Digital Communications and Networks*, Vol. 4, No. 02, pp. 77–86, 2018.
10. E. Varjovi, and S. Babaie, Green Internet of Things (GIoT): vision, applications and research challenges, *Sustainable Computing: Informatics and Systems*, Vol. 28, pp. 100448, 2020.
11. R. Ahmed, M. Asim, S. Z. Khan, and B. Singh, Green IoT: issues and challenges. In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, pp. 378–382, 2019.
12. A. Bashar, Review on sustainable green Internet of Things and its application, *IRO Journal on Sustainable Wireless Systems*, Vol. 01, No. 04, pp. 256–264, 2019.
13. F. K. Shaikh, S. Zeadally, and E. Exposito, Enabling technologies for green Internet of Things, *IEEE Systems Journal*, Vol. 11, No. 2, pp. 983–994, 2017.
14. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, Security and privacy for green IoT based agriculture: review, blockchain solutions, and challenges, *IEEE Access*, Vol. 8, pp. 32031–32053, 2020.
15. O. Said, Z. Al-Makhadmeh, and A. Tolba, EMS: an energy management scheme for green IoT environment, *IEEE Access*, Vol. 8, pp. 44983–44998, 2020.
16. V. Tahiliani, and M. Digalwa, Green IoT systems: an energy-efficient perspective. In *Proceedings of 2018 Eleventh International Conference on Contemporary Computing (IC3)*, pp. 1–6, 2018.
17. M. A. Albreem, A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M. N. Mohd Yasin, Green Internet of Things (GIoT): applications, practices, awareness, and challenges. *IEEE Access*, Vol. 9, pp. 38833–38858, 2021.
18. M. Aboelmaged, Y. Abdelghani, and M. A. Abd El Ghany, Wireless IoT based metering system for energy efficient smart cites. In *29th International Conference on Microelectronics (ICM)*, pp. 1–4, 2017.
19. Y. Nan, W. Li, W. Bao, F. C. Delicato, P. F. Pires, Y. Dou, and A. Y. Zomaya, Adaptive energy-aware computation offloading for cloud of things systems, *IEEE Access*, Vol. 5, pp. 23947–23957, 2017.
20. K. Wang, Y. Wang, Y. Sun, S. Guo, and J. Wu, Green industrial Internet of Things architecture: an energy-efficient perspective, *IEEE Communications Magazine*, Vol. 54, No. 12, pp. 48– 54, 2016.
21. E. Baccour, S. Foufou, R. Hamila, and A. Erbad, Green data center networks: a holistic survey and design guidelines. In *2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1108–1114, 2019.
22. T. D. Nguyen, J. Y. Khan, and D. T. Ngo, A distributed energy-harvesting-aware routing algorithm for heterogeneous IoT networks, *IEEE Transactions on Green Communications and Networking*, Vol. 2, No. 4, pp. 1115–1127, 2018.
23. R. Melki, H. N. Noura, and A. Chehab (2019) Lightweight multi-factor mutual authentication protocol for IoT devices. *International Journal of Information Security*. https://doi.org/10.1007/s10207-019-00484-5
24. Y. Deng, Z. Chen, X. Yao, S. Hassan, and A. M. A. Ibrahim, Parallel offloading in green and sustainable mobile edge computing for delay-constrained IoT system, *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 12, pp. 12202–12214, 2019.
25. E. Yaacoub, H. Ghazzai, M. S. Alouini, and A. Abu-Dayya, On the impact of D2D traffic offloading on energy efficiency in Green LTE-A HetNets, *Wireless Communication Mobile Computing*, Vol. 15, pp. 1089–1105, 2015.
26. M. Min, Z. Yang, Y. Zhang, Y. Wang, and Z. Li, Traffi-aware multiple slotframes scheduling algorithm in industrial IoT applications using IEEE802.15.4e TSCH. In *IEEE 16th International Conference on Communication Technology (ICCT)*, Hangzhou, pp. 608–614, 2015.
27. R. K. Lenka, A. K. Rath, and S. Sharma, Building reliable routing infrastructure for green IoT network, IEEE Access, Vol. 7, pp. 129892–129909, 2019.
28. K. S. Bhandari, and G. H. Cho, An energy efficient routing approach for cloud-assisted green industrial IoT networks, *Integration of Green ICTs and Industry into Green Governance for a Sustainable Ecosystem*, Vol. 12, No. 18, p. 7358, 2020.
29. S. H. Alsamhi, Ou Ma, M. S. Ansari, and Q. Meng, Greening Internet of Things for smart everythings with a green-environment life: a survey and future prospects, 2018.
30. A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, H. Karimipour, and S. R. Karizno, SLPoW: secure and low latency proof of work protocol for blockchain in green IoT networks. In *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, 2020.
31. G. M. W. Al Sadoon, H. A. Makki, and A. R. Saleh, Green computing system, health and secure environment management system. In *4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, pp. 1–6, 2017.
32. N. Khan, A. A. B. Sajak, M. Alam, and M. S Mazliham, Analysis of green IoT. In *Journal of Physics: Conference Series*, p. 0120122, 2021.
33. D. Oliveira, T. Gomes, and S. Pinto, Towards a green and secure architecture for reconfigurable IoT end-devices. In *ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS),* pp. 335–336, 2018.
34. S. Din, A. Ahmad, A. Paul, and S. Rho, MGR: Multi-parameter green reliable communication for Internet of Things in 5G network. *Journal of Parallel Distributed Computing*, 2018. https://doi.org/10.1016/j.jpdc.2017.12.012
35. P. K. Kashyap, S. Kumar, and A. Jaiswal, Deep learning-based offloading scheme for IoT networks towards green computing. In *IEEE International Conference on Industrial Internet (ICII)*, Orlando, USA, pp. 22–27, 2019.
36. N. Dao, T. Nguyen, M. Luong, T. Nguyen-Thanh, W. Na, and S. Cho, Self-calibrated edge computation for unmodeled time-sensitive IoT offloading traffic, *IEEE Access*, Vol. 8, pp. 110316–110323, 2020.
37. H. Qin, B. Cao, J. He, X. Xiao, W. Chen, and Y. Peng, Cross-interface scheduling towards energy efficient device-to-gateway communications in IoT, *IEEE Internet of Things Journal*, Vol. 7, No. 3, pp. 2247–2262, 2019.
38. G. Cui, X. Li, L. Xu, and W. Wang, Latency and energy optimization for MEC enhanced SAT-IoT networks, *IEEE Access*, Vol. 8, pp. 55915–55926, 2020.
39. J. M. T. I. Jayalath, E. J. A. P. C. Chathumali, K. R. M. Kothalawala, and N. Kuruwitaarachchi, Green cloud computing: a review on adoption of green-computing attributes and vendor specific implementations. In *International Research Conference on Smart Computing and Systems Engineering (SCSE)*, pp. 158–164, 2019.
40. M. Markiewicz, P. Dziurdzia, T. Konieczny, M. Skomorowski, L. Kowalczyk, T. Skotnicki and P. Urard, Software controlled low cost thermoelectric energy harvester for ultra-low power wireless sensor nodes, *IEEE Access*, Vol. 8, pp. 38920–38930, 2020.

41. M. Muniswamaiah, T. Agerwala, and C. C. Tappert, Green computing for Internet of Things. In *7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 182–185, 2020.
42. M. Ishtiaque, A. Zahed, I. Ahmad, D. Habibi, and Q. V. Phung, Green and secure computation offloading for cache-enabled IoT networks, *IEEE Access*, Vol. 8, pp. 63840–63855 (2020).
43. A. S. Adila, A. Husama, and G. Husi, Towards the self-powered Internet of Things (IoT) by energy harvesting: trends and technologies for green IoT. In *2nd International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS)*, Cavan, pp. 1–5, 2018
44. Y. Qu, K. Xu, J. Liu, and W. Chen, Toward a practical energy conservation mechanism with assistance of resourceful mules, *IEEE Internet of Things Journal*, Vol. 2, No. 2, pp. 145–158, 2015.
45. I. Unwala, Z. Taqvi, and J. Lu, IoT security: ZWave and thread. In *2018 IEEE Green Technologies Conference*, pp. 176–182, 2018
46. T. H. Szymanski, Security and privacy for a green Internet of Things, *IEEE Computer Society*, Vol. 19, No. 5, pp. 34–41 (2017).
47. K. N. Pallavi, R. V. Kumar, and P. Kulal, Study of security algorithms to secure IOT data in middleware. In *Second International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 305–308, 2018
48. S. Khan, A. I. Alzahrani, O. Alfarraj, N. A. Ali, H. Al-Bayatti, Resource efficient authentication and session key establishment procedure for low-resource IoT devices, *IEEE Access*, Vol. 7, pp. 170615–170628, 2019.
49. F. Ye, Y. Sun, and A. Rettig, Authentication and access control for an IoT green roof monitoring system. In *IEEE 15th International Conference on Dependable, Autonomic and Secure Computing*, pp. 251–256, 2017.
50. M. Sathiyanarayanan, S. Mahendra, and R. Babu Vasu, Smart security system for vehicles using Internet of Things (IoT). In *Second International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 430–435, 2019.
51. B. Ahuja, D.Mishra, and R. Bose, Optimal green hybrid attacks in secure IoT, *IEEE Wireless Communications Letters*, Vol. 9, No. 4, pp. 457–460, 2020.
52. P. Aufner, The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, 2019. https://doi.org/10.1007/s10207-019-00445-y
53. B. Wang, Q. Yang, L. T. Yang, and C. Zhu, On minimizing energy consumption cost in green heterogeneous wireless networks, *Computer Networks*, Vol. 129, No. 2, pp. 522–535, 2017.
54. M. Y. Mukta, M. A. Rahman, A. T. Asyhari, and M. Z. A. Bhuiyan, IoT for energy-efficient green highway lighting systems: challenges and issue. *Journal of Network and Computer Applications*, 2020. https://doi.org/10.1016/j.jnca.2020.102575.
55. H. R. Arkian, A. Diyanat, and A. Pourkhalili, MIST: Fog-based data analytics scheme with cost-efficient resource provisioning for IoT crowdsensing applications, *Journal of Network and Computer Applications*, Vol. 82, pp. 152–165, 2017.
56. E. M. Amin, M. S. Bhuiyan, N. C. Karmakar and B. W. Jensen, Development of a low-cost printable chipless RFID humidity sensor, *IEEE Sensors Journal*, Vol. 14, No. 1, pp. 140–149, 2014.
57. A. Markhasin, V. Belenky, V. Drozdova, A. Loshkarev, and I. Svinarev, Cost-effective ubiquitous IoT/M2M/H2H 5G communications for rural and remote areas. In *International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–8, 2016.
58. F. Pereira, S. I. Lopes, and N. B. Carvalho, Design of a cost-effective multimodal IoT edge device for building occupancy estimation. In *5th IEEE International Smart Cities Conference (ISC2)*, pp. 122–128, 2019.
59. G. Lavanya, C. Rani, and P. Ganeshkumar, An automated low-cost IoT based Fertilizer Intimation System for smart agriculture. *Sustainable Computing: Informatics and Systems*, 2018. https://doi.org/10.1016/j.suscom.2019.01.002
60. M. Guo, L. Li, and Q. Guan, Energy-efficient and delay-guaranteed workload allocation in IoT-edge-cloud computing systems, *IEEE Access*, Vol. 7, pp. 78685–78697, 2019.
61. J. Wang, C. Hu, and A. Liu, Comprehensive optimization of energy consumption and delay performance for green communication in the Internet of Things. *Hindawi Mobile Information Systems*, 2017. https://doi.org/10.1155/2017/3206160
62. A. Mebrek, L. M. Boulahia, and M. Esseghir, Efficient Green solution for balanced energy consumption and delay in the IoT-Fog-Cloud computing. In *IEEE 16th International Symposium on Network Computing and Applications (NCA)*, Cambridge, pp. 1–4, 2017.
63. M. Huang, A. Liu, T. Wang, and C. Huang, Green data gathering under delay differentiated services constraint for the Internet of Things, *Wireless Communications and Mobile Computing*, 2018. https://doi.org/10.1155/2018/9715428.
64. S. Chen, Y. Zheng, K. Wang, and W. Lu, Delay guaranteed energy-efficient computation offloading for industrial IoT in fog computing. In *IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.
65. A. Yousefpour, G. Ishigaki, and J. P. Jue, Fog computing: towards minimizing delay in the Internet of Things. In *IEEE International Conference on Edge Computing (EDGE)*, Honolulu, pp. 17–24, 2017.
66. Amitav Mukherjee, Energy efficiency and delay in 5G ultra-reliable low-latency communications system architectures, *IEEE Network* 32(2), 55–61, 2018.
67. W. Masri, I. A. Ridhawi, N. Mostafa, and P. Pourghomi, Minimizing delay in IoT systems through collaborative fog-to-fog (F2F) communication. In *Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, Milan, pp. 1005–1010, 2017.
68. I. AlQerm, and B. Shihada, Energy efficient traffic offloading in multi-tier heterogeneous 5G networks using intuitive online reinforcement learning, *IEEE Transactions on Green Communications and Networking*, Vol. 3, No. 3, pp. 691–702, 2019.
69. A.Kliks, N. Dimitriou, A. Zalonis, and O. Holland, WiFi traffic offloading for energy saving. In *ICT*, Casablanca, pp. 1–5, 2013.
70. A. Hussain, S. Manikanthan, T. Padmapriya, and M. Nagalingam, Genetic algorithm-based adaptive offloading for improving IoT device communication efficiency, *Wireless Networks*, 2019. https://doi.org/10.1007/s11276-019-02121-4.
71. L. Wang, X. Zhang, S. Wang, and J. Yang, An online strategy of adaptive traffic offloading and bandwidth allocation for green M2M communications, *IEEE Access*, Vol. 5, pp. 6444–6453, 2017.
72. A. Ghosh, O. Khalid, R. N. B. Rais, A. Rehman, S. U. R. Malik, and I. A. Khan, Data offloading in IoT environments: modeling, analysis, and verification, *EURASIP Journal on Wireless Communications and Networking*, 2019. https://doi.org/10.1186/s13638-019-1358-8.
73. S. Zhang, N. Zhang, S. Zhou, J. Gong, Z. Niu, and X. Shen, Energy-aware traffic offloading for green heterogeneous networks, *IEEE Journal on Selected Areas in Communications*, Vol. 34, No. 5, pp. 1116–1129, 2016.
74. X. Xiang, W. Liu, and T. Wang, Delay and energy-efficient data collection scheme-based matrix filling theory for dynamic traffic IoT, *Wireless Communication Network*, Vol. 168, pp. 1–25, 2019
75. R. Ranji, A. M. Mansoor, and A. A. Sani, EEDOS: an energy-efficient and delay-aware offloading scheme based on device to device collaboration in mobile edge computing, *Telecommunication System*, Vol. 73, pp. 171–182, 2020.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Annu Malik received the B.Tech degree in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow, in 2009 and the M.Tech degree in Computer Science and Engineering from Uttarakhand technical University, Dehradun in 2015. She is currently pursuing her Ph.D. in Computer Science and Engineering at Jaypee Institute of Information Technology, Noida, India. Her primary research areas of interest are Compute Networks, Internet of things and image processing.

Rashmi Kushwah received the B.E. degree in Computer Science and Engineering from UIT Barkatullah University, Bhopal, in 2006 and the M.Tech. degree in Software Engineering from Maharshi Dayanand University, Rohtak in 2009. She has completed her Ph.D. in Information Technology at ABV-Indian Institute of Information Technology and Management, Gwalior, India in 2018. Her research interests include performance of mobile adhoc network, heterogeneous networks and Internet of Things.