Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

An energy-efficient and reliable data gathering infrastructure using the internet of things and smart grids

T. Vinothkumar, S.S. Sivaraju, Anuradha Thangavelu & S. Srithar

To cite this article: T. Vinothkumar, S.S. Sivaraju, Anuradha Thangavelu & S. Srithar (2023) An energy-efficient and reliable data gathering infrastructure using the internet of things and smart grids, Automatika, 64:4, 720-732, DOI: 10.1080/00051144.2023.2205724

To link to this article: https://doi.org/10.1080/00051144.2023.2205724

Published online: 24 May 2023.

AUTOMATIKA
2023, VOL. 64, NO. 4, 720–732
https://doi.org/10.1080/00051144.2023.2205724

REGULAR PAPER

OPEN ACCESS Check for updates

An energy-efficient and reliable data gathering infrastructure using the internet of things and smart grids

T. Vinothkumar[a], S.S. Sivaraju [a], Anuradha Thangavelu[b] and S. Srithar[c]

[a]Department of Electrical and Electronics Engineering, RVS College of Engineering and Technology, Coimbatore, Tamilnadu, India; [b]Department of Electrical and Electronics Engineering, KCG College of Technology, Chennai, India; [c]Department of Computer science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

ABSTRACT

Introduction: The Internet of Things (IoT) and Smart Grids (SGs) growth results from the advancement of computer hardware and ubiquitous computation for energy-efficient and reliable data gathering.

Background: The limitations of the present cloud computing framework in energy systems remain unresolved, such as fully recognizing the requisites of high data usage with low latency which is discussed for a cloud computing scheme in IoT-based smart power stations.

Problem Statement: IoT growth results from the advancement of computer hardware and ubiquitous computation. Among the various IoT solutions, SGs stand out because they combine several embedded smart techniques to increase the security and dependability of electricity grids.

Methodology: A Particle Swarm Optimization based energy efficient integration of Smart Grid (PSO-SG) is designed using IoT. Modern technology establishes a novel hardware and software architecture and integrates cloud services into the cloud-based electricity network.

Findings: As a result, a sizable amount of data produced by the electricity network will be examined, handled, and saved at the network. IoT-based power systems will enable the interconnection and administration of large endpoint devices, offer real-time evaluation and treatment of vast data, and promote the modernization of the power grid with the help of the cloud computing model.

ARTICLE HISTORY
Received 13 February 2023
Accepted 17 April 2023

KEYWORDS
Internet of things; smart-grids; cloud computing; energy optimization

1. Introduction to smart grid optimisation

The Internet of Things (IoT) was created as a result of the expansion of computer devices and pervasive computing [1]. This technology covers a number of devices with varying functionality that may be integrated into the same surroundings or in other contexts. Industry 4.0, logistics, and smart cities are some examples of common IoT uses. This article focuses on Smart Grids (SGs), which are further classified into traffic, sewage, agricultural, surveillance systems, and microgrids [2,3].

Conventional power grids are facilities whose main purpose is to transfer and distribute energy from distant plants to end customers [4]. In contrast, SGs make extensive use of communication technology inside the electricity network to facilitate the flow of status data between various grid elements. This characteristic enables more efficient implementation of process operations and control techniques than standard alternatives. What defines an SG as "intelligent" is its capacity for communication links, sensors, management options, and the usage of protocols that enable data interchange [5]. Therefore, all players in the energy sector, from production to commercial or residential consumers, must collaborate to ensure the continual creation and use of SG-generated information. As a result of its creation being aimed at different ends, the connection between the various protocols of the IoT and SG is the most difficult.

In microgrids, there are several kinds of power connectors and detectors, such as sensing devices, temperature monitoring, immersion detectors, motion detectors, current leakage detectors, and smart surveillance sensors, which may enable IoT-based smart energy systems. In this example situation, in which IoT technologies are used to power energy systems, essential characteristics of microgrids, such as data visualization, predictive modelling, failure detection, and self-healing

CONTACT S.S. Sivaraju sssivaraju@gmail.com, sssivaraju@ieee.org Department of Electrical and Electronics Engineering, RVS College of Engineering and Technology, Coimbatore 641 402, Tamil Nadu, India

[6]. For IoT adoption in microgrids, there are a number of technological issues that have yet to be thoroughly investigated.

1.1. Challenges or limitations proposed system

1) The transition from conventional electricity networks to smart grids will face several technological obstacles. Therefore, data standardization and data fusion are required for the digitalization of power grids to occur.
2) According to Chinese Electrical Council data, imbalances between electrical supply and energy sales occur often in energy systems, and electrical transmission losses are substantial [7]. According to data on the power demand of the whole community, the electricity usage of different sectors varies substantially, notably between the main industry and heavy manufacturing. Therefore, current power systems cannot be implemented in real-time to meet the electrical needs of consumers [8].
3) With the proliferation of new smart transmission and distribution connections, it is critical to establish device plug-and-play and compatibility [9]. Despite the recent publication of and discussing the connection between big data and environmental sustainability-related problems, the interaction between big data analytics and cyber-physical systems (or IoT) has remained an unresolved issue in the energy sector.

Challenges of the Proposed System to Be Addressed in the Following Manner: By creating a new programme and equipment design, PSO-SG primarily integrates edge computing with existing cloud-based power grids in order to address above issues is designed a new system. It implements a model for edge devices and smart grids, which comprises control, health monitoring, data collection, and implementation scenarios for IoT-based microgrids. The proposed work IoT-based microgrids named Particle Swarm Optimization based energy efficient integration of Smart Grid (PSO-SG) to increase the security and dependability of electricity grids. PSO is a technique for work balancing that is a self-adaption and learning method. The two most significant elements of PSO methods are the populace, also called the swarm, and the answers often called the components. The realization of parallelization and analysis of information from numerous gathering stations, connected devices, and end-users of microgrids at the network's corner, dispersed quick response services and advanced analysis, including forecasting, personal privacy, and allocation of resources enhancement.

The Remainder of the Article is Organized in the Following Manner: Section 2 illustrates the background of the smart grid and IoT integration models. The proposed Particle Swarm Optimization based energy efficient integration of Smart Grid (PSO-SG) is designed and theoretically analysed in section 3. The simulation outcomes and the findings of the designed model are listed in section 4. Section 5 indicates the findings of the proposed system and its conclusions.

2. Background to the integration of IoT and smart grids

This section begins with a review of previous work on IoT-based microgrids, followed by an explanation of edge devices.

To achieve the application of a smart grid, it is necessary to overcome a number of difficulties. Protecting the smart grid is a very difficult and urgent undertaking. Using Machine Learning (ML), this study proposes a secured Demand-Side Management (DSM) engine for the IoT-enabled infrastructure [10]. The suggested DSM engine is accountable for preserving the efficient consumption of energy in accordance with predetermined priorities. A unique resilient paradigm is being developed to control intrusions into the power grid. Using the ML classification, the resistant agent anticipates fraudulent entities. It is suggested that intelligent power administration and connection managing agents analyse energy data to maximize energy use.

This article advocates an approved stage for a safe service delivery machine using machine learning for the Internet of Things [11]. The proposed management system safeguards the efficient use of energy depending on user preferences. To regulate intrusions into the smart grid, an example of unique flexibility was suggested. When an inelastic agent predicts fraudulent businesses, ML classifications are applied. To improve energy utilization, recommend power efficiency and intermediary control firms for analysing power data. To evaluate the effectiveness of the suggested programme, a simulation of the proposed model efficacy is performed.

The data acquired from the users of SMs is private and confidential, the blockchain to be private in the research [12]. The comprehensive security analysis utilizing the random oracle concept, nonmathematical detection techniques, and software-based standard security validation demonstrated that a system is resilient to several threats. By using widely-used multiprecision integers and an irrational mathematics cryptographic package, it conducts the research observations necessary for comparative comparison. A comparison analysis demonstrates that the system offers more operational aspects and offers superior safety, in addition to its cheap computing and communication expenses, when compared to previously suggested schemes that are comparable.

The architecture of smart energy administration technology is designed to substitute for a total power outage in an area with regulated partial load dropping based on the desire of the customer [13]. A presentation of experiments is conducted under the assumption of a load management occurrence while also taking into account the peak load limitation in various circumstances and altering the priority allocated to equipment. Smart energy management combines cost-optimization methods based on usage time and convenience with sensory memory elements.

The Wireless Sensor Network (WSN) based on the Internet of Things is a new technology that involves integration. This paper proposes and demonstrates a method for the development and deployment of WSN-based communications networks that involve the integration and automated management of the power grid [14]. This study enables the enhancement of grid share for energy quality maintenance. The dynamic regulator has regulated the energy quality issue and voltage increase. The effectiveness of smart grid surveillance control systems has been proven and studied using the appropriate arrangements and actuators.

Current encryption techniques typically involve techniques for the smart grid context that demand more capacity and more processing time. This study presents a lightweight certificate-based transfer of documents with a proxy re-encryption system for intelligent grid-based Internet of Things gadgets in an effort to reduce computing and social communication expenses [15]. For the safety and effectiveness of the suggested method, it used a position curve cryptographic algorithm with 80-bit keys and modest variables. Also, it compared the proposed system with the current surrogate encryption with re-encryption techniques. The results show that the new approach provides strong security with minimal costs for computing and networking.

This system presents a novel privacy-preserving data-gathering technique for IoT-enabled microgrids that allows for rapid data source verification and integrity checking, as well as the safe user joins and departures [16]. Unlike previous methods, the suggested system is resistant to hostile data-gathering attacks by internal or external hackers and can achieve full data secrecy not only from malicious aggregators but also from a curious control centre for an authorized user. The comprehensive safety and performance study demonstrates that the suggested PDAM satisfies a number of well-known safety features and the effectiveness requirements of an intelligent grid system.

This research, dubbed IoT-SG [17], the research proposes a novel anonymous signature-based authorized key exchange mechanism for IoT-enabled microgrid environments. After the initial rollout, IoT-SG also allows for the phase of dynamic intelligent metre insertion. The security of IoT-SG has been thoroughly evaluated using official security testing using the widely accepted basic arbitrary Oracle prototype Real-Or-Random (ROR) instrument, comprehensive security testing using the widely used advanced confirmation of Internet safety procedures and systems instrument, and unofficial safety testing.

The Wind-Driven Bacterium-Feeding Engine (WBFE) [18] is a mix of Wind-Driven Optimization (WDO) and Bacteria-Feeding Optimization (BFO) methods. Furthermore, it established a technique based on the suggested WBFE to methodically regulate the power consumption of IoT-enabled domestic intelligent devices by planning to reduce Peak-to-Average Ratios (PAR), decrease energy costs, and enhance comfort conditions. This improves energy efficiency, hence enhancing the durability of cellular residential structures in green infrastructure. The WBFA-based technique instantly reacts to price-based programmes to overcome the primary issue of programmes, which is the inability of customers to react to signals due to a lack of awareness. To validate the efficiency and efficacy of the suggested WBFA-based method, extensive simulations are conducted.

Sort-Tile-Recursive (STR) [19] tree for adopt mobile edge computing to support sensory data gathering. Edge nodes in edge networks gather sensory data from their subordinating social robots in a periodic manner. Design an edge network division method by constructing an improved STR tree, which can cluster the edge nodes and decrease unnecessary energy consumption. Experimental results show that technique is more efficient than traditional ones in decreasing energy consumption.

Energy-efficient sensory data gathering mechanism, where the category of sensory data is processed by adopting the compressed sensing algorithm [20]. The sensory data are forecasted through a data prediction model in the cloud, and sensory data of an IoT node is necessary to be routed to the cloud for the synchronization purpose, only when the category provided by this IoT node is different from the category of the forecasted one in the cloud. Experiments are conducted and evaluation results demonstrate that approach performs better than state-of-the-art techniques, in terms of the network traffic and energy consumption.

Artificial Bee Colony (ABC) for data gathering [21]. Propose a reliable spanning tree construction algorithm, which is called reliable spanning tree construction in IoT (RST-IoT). Proposed algorithm utilizes the ABC algorithm to generate proper trees. In this method, hop count distances of the devices from the base station, residual energies of the devices, and their mobility probabilities are considered to measure the appropriateness of the trees. Moreover, the proposed algorithm generates a number of trees instead of a single one. These trees are arranged according to their preferences and used for data gathering in succession.

Each tree is employed for data gathering upon splitting the preceding one. The simulation results show that RST-IoT improves the reliability of data gathering in emergency applications compared to the previous approaches.

The IoT supports the technology and communication required to make "smart grids" smart.

In the context of the smart grid, IoT has concrete applications for monitoring electricity generation, gauging intelligent power consumption, managing energy efficiency, and much more.

Consequently, IoT devices might be extensively used in smart buildings, connected cars, universal healthcare, advanced factories, and smart homes. Issues involving advanced technologies connected to edge networks, load management, and energy-efficient transmission have sparked intense debates in academia and industry. As there are several power biosensors in IoT-based microgrids, these gadgets must analyse datasets at the network's edge to fulfil real-world needs such as local electric distribution, transfer, and accident warnings. With edge devices, edge data does not need to be sent to a distant cloud network for analysis, eliminating the potential for postponed answers. In this instance, an open framework for connectivity, processing, storing, and deployment are required at the network's edge, near the device or information source, in order to offer smart edge solutions for the energy sensors' data. Realizing that information is no longer required to be transferred through remote networks, the service's safety and stability are now more manageable.

3. Proposed particle swarm optimization based energy efficient integration of smart grid

This section describes the system of microgrids based on IoT. The research will initiate the specialized services of IoT-based distributed generation backed by edge devices that are implemented in the three main situations, namely power delivery with increased vigilance of IoT smart power systems, micro-grid processes of IoT distributed generation, and developed metering structures of IoT distributed generation.

3.1. Fog computing for smart grid architecture

Consider an IoT-enabled SG design in which a large-scale, globally disparate microgrid (such as a wind farm) is filled with hundreds to millions of actuators and sensing devices. This system may also have a multitude of largely autonomous elements or components (turbines). Each subsystem is a somewhat sophisticated system with several current controls. Formal organizational principles of larger networks (such as safety) dictate that each subsystem be capable of semi-autonomous but coordinated operation.

A network of controllers with wide perspectives may be used for this purpose. The controller group uses the components to produce an overall image, establishes a method, and implements the method for each component. The method is universal yet tailored to each subsystem based on its specific status (locations, wind incidences, and cases of the turbines). The constant supervisory function of the universal controller (collecting data, constructing the distributed system, and setting the method) necessitates a fast response time, which is attainable locally in the edge-centred installation, also called the fog. Such a system creates vast quantities of data, the majority of which are usable in real time. It is also used to rework the procurement conditions with the International Standard Organization (ISO) if required. Much beyond real-time network implementations, the data is used for longer-term (months or years) and broader scenario-based analytics. The cloud is the ideal environment for running such batch analyses. SG necessitates storage and processing architecture with an effective communications system between the components, the systems, and the network in general (the cloud).

The system architecture of the proposed model is shown in Figure 1. The system has three layers and the functions of the wind farm, distribution and consumption are shown. The concept underpinning fuzzy controller is the spread of storage, communication, and computing resources from the cloud server. The fog designs are totally distributed, predominantly centralized, or a hybrid of the two. Specific hardware and software components are used to build fog technologies. A tailored cloud service will allow particular programmes to operate everywhere, eliminating the requirement for cloud-, endpoint-, and edge-device-specific apps. It allows apps from many suppliers to operate on the same physical computer without interfering with each other. In addition, the Fog Cluster (FC) provides a standard lifecycle administration architecture for all programmes, with the ability to compose, configure, dispatch, activate and deactivate, add and remove, and update apps. In addition, it creates a safe runtime platform for fog programmes and operations.

The system depicts a multi-tiered fog-depended cloud computing system in which a large amount of SM management and computing duties are hybridized with Fuzzy Controller Networks (FCN) in addition to the information centre-based computation assistance. The purpose of hybridization is to counteract the dispersion created by the infiltration of services into smart grid systems, which necessitates the active expansion of management, storage, communication, and computing resources across diverse edges or terminals. The framework enables the entire implementation of Internet of Things solutions in a cloud environment by facilitating

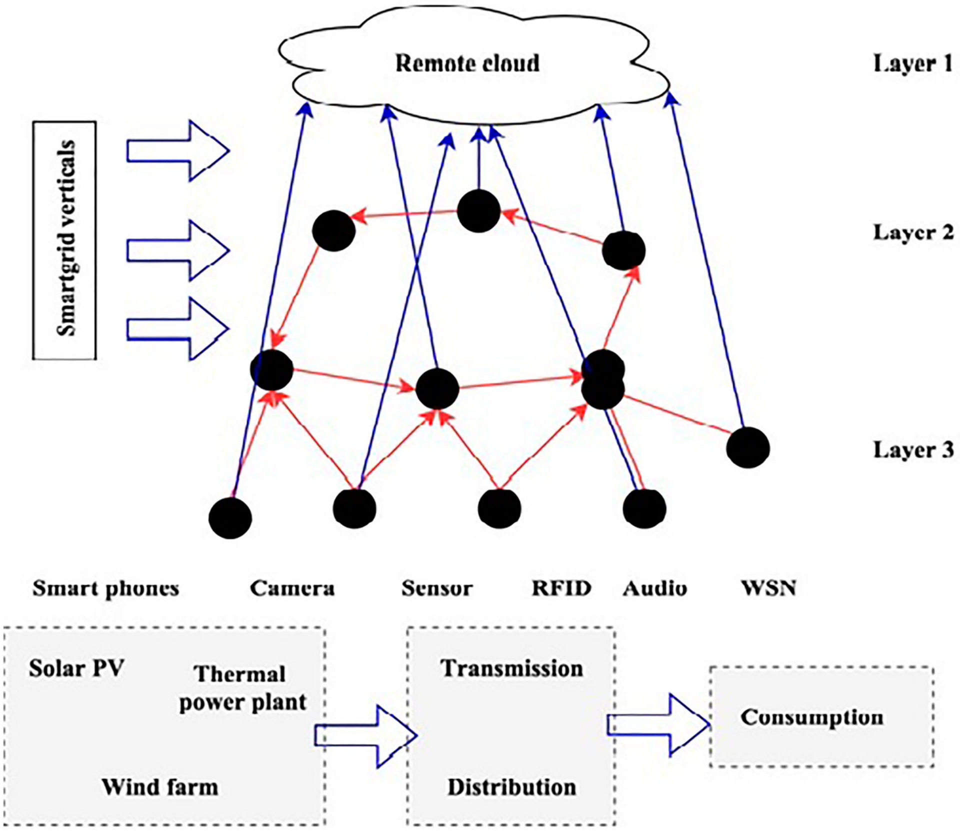

Figure 1. System Architecture of the Proposed Model.

an analytical model on sensor information and ensuring efficient supply allocation.

3.1.1. Layer 1

The lowest tier comprises IoT devices filled by smart grid infrastructure facilities, which are further interconnected by transparent, highly scored, and lower-cost sensing nodes distributed throughout the smart grid horizontal lines, i.e. production, transfer, and consumption. As a result, the architectural components of this tier include Radio Frequency Identity (RFID), gadgets, webcams, Infrared (IR) sensors, laser scanning, Global Positioning System (GPS) units, and other data collection entities.

3.1.2. Layer 2

The subsequent tier, often known as the FC tier, is the primary component in a conventional FC model. Despite the fact that Cisco and Bonomi primarily developed the concept of FCN, the distributing, computing, and storage capacities. Their interplay and their installation as a service scheme have not been precisely classified. It is intended that the FCNs would assess the datasets depending on the non-functional needs of organizations today, such as latencies, QoS, stability, etc. Moreover, the vast amount of digital sensing data produced by these geographically dispersed sensors must be analysed as a unified entity.

The FC layer incorporates intermediary computing capabilities into many sublayers. The lowest level, nearest to the higher layers, is composed of several low-power and high-performance computer nodes or end devices, such as specialized gateways, mobile network ground stations, and so on. Each edge device encompasses a set of sensors inside its area in order to conduct local and immediate analysis. The network edge results can be completely integrated into the SG apps or sent to the top tier for further processing. The latter may include reports of completed tasks or precompiled information that is prepared for analysis at a higher level. For instance, the instantaneous output is utilized to give a real-time control method to infrastructural development, such as notifying law enforcement of any localized and minor risks to a monitoring electric vehicle network.

The end-to-end layered architecture of the suggested PSO-SG system is shown in Figure 2. The three layers namely the cloud layers, fog layers and end-user layers are shown in the figure. The smart grid, cloud server and the user. Clusters are efficiently integrated with energy constraints. The higher sublayer has computer nodes called FCN, which are either connected to edge nodes from lower levels or to Internet data centres in the top layer through reliable communication lines.

To accomplish tasks, FCNs at the same level are often mirrored to networks below them in the structure. The fuzzy controller constructs sub-trees of fuzzy networks,

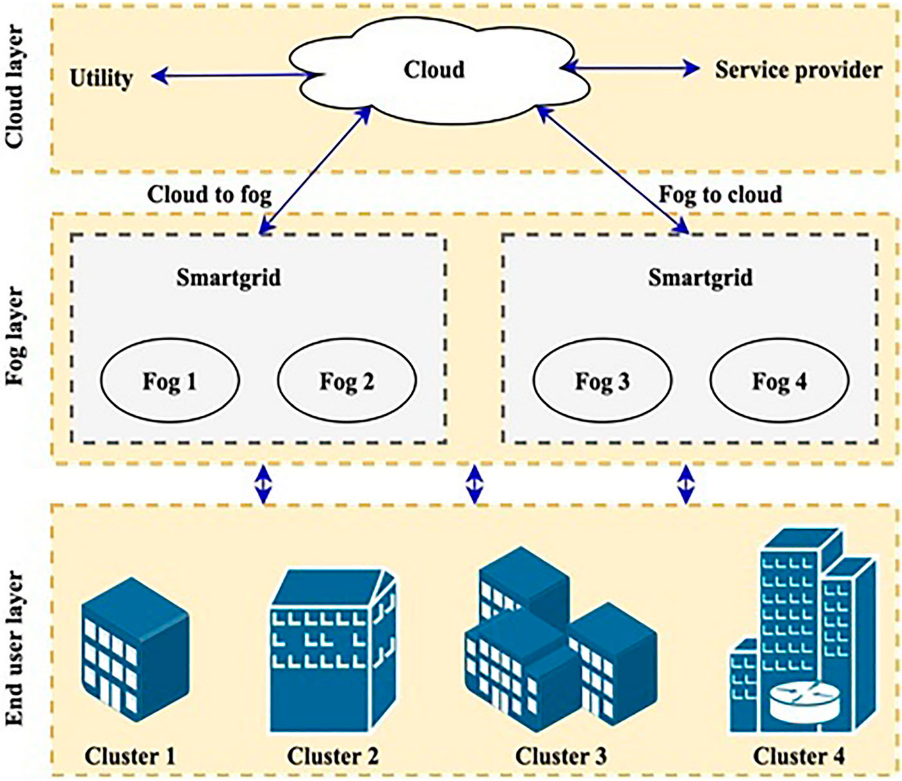

Figure 2. The End-to-End Layered Design of the Proposed PSO-SG.

with each component at a deeper level of the tree being handled by the ones at a shallower level, according to the master-slave model. In the FC layer, a typical connection of such structures is presented. Consider, for example, an SG electricity distribution scenario in which FCNs are allocated temporal and geographical data to detect possible hazardous occurrences in power lines, such as power robberies, network infiltration, etc. In such cases, these computer processing endpoints will turn off the electricity source from the substations, and the results of the analysis will be fed back and noted to the top layer (from the village power station to Supervisory Control And Data Acquisition, to city-wide energy dispersion centres or production authorities) for complicated, cultural, and larger-scale behavioural assessment and situation tracking. The dispersed analyses from multiple-layer fog networks (aggregate analytics in real-time scenarios) done at the fuzzy controller serve as localized “reflex” actions to prevent possible occurrences. In the meantime, a substantial portion of IoT data created by applications for smart grids does not need to be sent to distant clouds; hence, reaction delay and capacity utilization issues might be readily resolved.

3.1.3. Layer 3

The cloud technology or data centre, which provides universal or centralized surveillance and management, is at the highest level. Using high-efficiency dispersed computing and storage components, data centres can conduct grid-wide behavioural analyses. To enable flexible decision-making, the outcomes of cloud-layer analysis may include event identification, pattern identification, and connection modelling. One of the primary goals of cloud-layer analysis is to make that infrastructure and service providers can do operations that require greater responsiveness and are prepared to handle brownouts and outages.

3.2. System architecture

In constructing an IoT-based system, wireless sensor networks and Generalized Packet Radio Services (GPRS) might be considered. A Wireless sensor network is a wireless network comprised of several IoT devices, each of which is outfitted with sensors for monitoring physical problems [22]. GPRS is a Global System for Mobile communication (GSM) based wireless transmission packet system that offers point-to-point Internet Protocol connections across long distances. GPRS is a processing system that permits multiple data transfers, a large signal range, quick deployment, and minimal maintenance expenses.

GPRS equipment seems obsolete when compared to 3G and 4G technologies. Nevertheless, it remains a dependable and effective choice for data handling and transmission. In addition, some transmitting and distributing systems are situated in distant regions where 3G and 4G coverage is unavailable. The system depicts the usual system design of the IoT for the monitoring of electricity delivery and distribution. One may install sensor nodes that measure actual occurrences.

Using either single hopping or multiple hops, the data recorded by sensing devices is gathered and consolidated before being communicated across the network connection to a server for assessment, decision-making, and implementation of relevant conditions.

The server component of the cloud-based function is what stores the information and provides access to it. The method employs a mix of GPRS technologies and wireless modules to send sensor data. In this system, two-layer wireless communication may be implemented for more freedom and versatility. The initial level employs IEEE 802.15.4 wirelessly, which is low expense, consumes little power, and has a transmission distance of 100–1,000 metres per node. Regarding Zigbee communication capacity, this system provides a mesh network. The primary advantage of the mesh architecture is that each node may interact directly with every other node inside the coverage region. In addition, it improves network stability and maintains wireless connectivity if one of the nodes fails, loses signal, or is deactivated. The second floor employs the GPRS modules to aid the network in data transmission or relaying. In addition to enhancing network speed for actual statistics, GPRS architecture is more economical and resilient. The GPRS module also allows Transmission Control Protocol (TCP) or Internet Protocol (IP) communication, allowing data to be sent directly to the servers using the domain of a specific node. Using two-layer wireless sensing networks increases the reliability of data collection and transmission to the server or cloud control layer.

3.2.1. Transmission hardware design

The system has four components: wireless sensor networks, data transmission, a server (cloud administration), and a desktop. The wireless sensor network is capable of monitoring the physical environment in power lines, including temperatures, moisture, conductivity heat, tension gauge, wind speed, and power dissipation, among other variables. Sensors gather sensing information and transmit it through information transmitters from node to node or base station to client. The combined data is then delivered through GPRS to achieve data transfer between the wireless sensor networks and the servers. The server gathers, processes, analyses, and saves all sensor data via the GPRS connection module. The cloud administration system is linked to the network and has designated internet locations in order to collect and transmit information to the desktop. The desktop is a surveillance station that analyses the WSN's broadcast parameters. The fact that it is linked to the internet permits remote connection by operational employees.

3.2.2. Distribution hardware design

The system has the equipment installed for the IoT-based distribution network. Similarities exist between the WSN device, schematic diagram, transmission architecture, data analysis, and the communications network. Therefore, sub-station status management is the distributing system's primary priority. Power stations should be fitted with a detector and smart metre in order to monitor essential parameters such as power and supply profiling, transformer temperatures, oil levels, loading condition, defects, and outages [23]. Surveillance on generation and dispersion systems based on the Internet of Things is a potent instrument for increasing system resilience, as it enables early warning and surveillance through cloud-based data analysis. The dissemination and distribution network status may be presented graphically on a desktop computer, laptop, or mobile device.

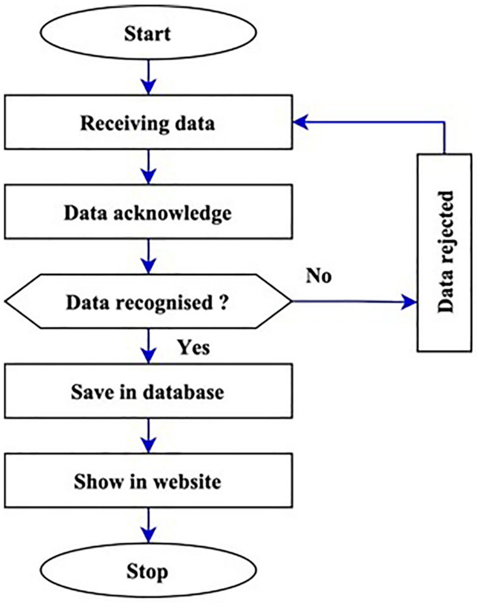

Figure 3. The Software Workflow of the Proposed PSO-SG.

3.2.3. Software engineering

In general, this platform's software consists of WSN technology and IoT technology. Both are custom-built programmes that are deployed on the sensor network, coordinator endpoints, integrated system software, apps, and servers. The computer's flowcharts are shown in Figure 3.

The wireless sensor network software is primarily accountable for device startup, sensor data gathering, and analogue-to-digital data analysis. The information is then transmitted to the server via wireless connections or GPRS. IoT technology is a software solution that is linked to the network and has an Internet address. This programme handles data validation, receiving, interpretation, and storage. Sensor information is saved in databases and is accessed via a web application.

3.3. Problem definition

The proposed system has three levels. The cloud system is the highest and most superficial tier. The third and last tier is the user level. These levels interact with one another to meet the requirements of the customers. The proposed system model consists of six geographically distinct regions. Through the power system, the consumer initiates queries to the fog for calculations and other necessary operations. The Fog serves the needs of its customers by making efficient use of its capabilities. The work set TS can be written in Equation (1).

$$TS = TS_1, +TS_2, \cdots, TS_m \tag{1}$$

The work set is denoted $TS_x; where\ x = 1, 2, \cdots, n$. One may specify the number of virtual computers in a fog using Equation (2).

$$VM = VM_1 + VM_2 + \cdots + VM_v \tag{2}$$

The virtual machine is denoted $VM_x; where\ x = 1, 2, \cdots, v$. The aim function is to reduce the operating and reaction time, which is formally expressed in Equation (3).

$$K_{min} = \sum_{y=1}^{m} \sum_{x=1}^{n} RT \times P_{xy} \times D \tag{3}$$

The reaction time is denoted RT, the probability is denoted P_{xy}, and the delay is denoted D. The Fitness function is calculated using Equation (4).

$$F = \max\{E_{VM_1}(F_1), E_{VM_2}(F_2), \cdots, E_{VM_m}(F_m)\} \tag{4}$$

Here, $E_{VM_1}(F_1)$represents the time required to execute the set of activities on fog F_1 on VM_1. F_1 is the collection of user groupings, hence $F_1 = \{C_1, C_2, \cdots, C_n\}$,where x is the number of customers in F_1. In addition, n is the number of virtual machines and m is the number of clouds.

3.3.1. Processing period

The processing period is dependent on the virtual machine's capability and the size of the workload. The calculation is expressed in Equation (5).

$$PT = \sum_{x=1}^{N} \sum_{y=1}^{M} P_{xy} \times A_x \tag{5}$$

The probability is denoted P_{xy}, and the size is denoted A_x.

3.3.2. Response time

The response time is determined as the delay between when the task performance began and when the customer made a request to be produced using Equation (6).

$$RT = D_t + F_t - A_t \tag{6}$$

The delay time, finish time and arrival time are expressed $D_t, F_t and A_t$.

3.3.3. Cost

Price is another crucial aspect of cloud and fog. The two price-determining factors are the cost of information transport and the cost of virtual machines. U is a common factor and β is the transmission price per gigabyte. The cost factor with the given time is denoted in Equation (7).

$$C_T = C_{DT} + C_{MG} + C_{VM} \tag{7}$$

The cost function of distribution transmission, microgrid and the virtual machine are expressed $C_{DT}, C_{MG}, and C_{VM}$. The cost function of the virtual function is denoted in Equation (8).

$$C_{VM} = \sum_{x=1}^{N} (VM_{F_t} - VM_{I_t})U \tag{8}$$

The finish time of the virtual machine and the initial time of the virtual machine are denoted as $VM_{F_t} and VM_{I_t}$. The constant factor is denoted U.The cost function of the delay time is expressed in Equation (9).

$$C_{DT} = \frac{T_T}{D_{used}\beta} \tag{9}$$

The total time is denoted T_T, the user data is denoted D_{used}, and the transfer cost is denoted β.

Equation (10) shows the overall period needed by the virtual machine to find the result.

$$T_T = F_T - S_T \tag{10}$$

The finish time and the start time are expressed $F_T\ and\ S_T$.

3.4. Proposed approach

Particle Swarm Optimization (PSO) is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. It solves a problem by having a populace of candidate solutions, here dubbed particles, and moving these particles around in the search-space according to simple mathematical formulae over the particle's position and velocity. Each particle's movement is influenced by its local best known position, but is also guided toward the best known positions in the search-space, which are updated as better positions are found by other particles. This is expected to move the swarm toward the best solutions. PSO is a successful and valued global search technique. The principal space is the search space through which a subset of principal components or principal features were explored and selected via PSO. PSO, the particles represent candidate solutions in the search space particles and form a populace which is also known as a swarm.

PSO is a technique for work balancing that is a self-adaption and learning method. The two most significant elements of PSO methods are the populace, also called the swarm, and the answers often called the components. The efficiency of the method is affected by the best location ($\hat{p}_x$) and the universal best location ($\hat{g}$). The fitness value produces a finite result, termed the fitness valuation, for each particle. Every particle's goal features are established and confirmed over the period. The procedure additionally yields the particle's speed (v_x) and position (p_x). This technique defines a particle as a dimensional area. Each component has a maximum and minimum value that it can accept. Alternately, every component of the speed vector may have data in the interval [0, 1], and each element of the PSO's location vector can have a number of either 0 or 1.

Equations (11)–(15), G is the gravitational value, c_1 and c_2 are intellectual and social factors that are generally 2, and r_1 and r_2 are randomized numbers, depicting the PSO operating in a domain. R_a is a deterministic number between 0 and x_R. m_R and x_R are the minimum and maximum transmitting limits, correspondingly. The speed of the xth element of the particle p is changed using Equations (11)–(13), while its location is changed using Equations (14) and (15):

$$v_x = wv_1 + c_1 r_1(\hat{p}_x - p_x) + c_2 r_2(\hat{g} - p_x) \tag{11}$$

$$\delta = \frac{x_R - m_R}{2} \tag{12}$$

$$v_x = \begin{cases} m_R & if\, v_x < \delta \\ \delta & else \end{cases} \tag{13}$$

$$p_x = R_a + v_x \tag{14}$$

$$v_x = \begin{cases} m_R & if\, p_x < m_R \\ x_R & if\, p_x > x_R \\ p_x & if\, m_R < p_x < x_R \end{cases} \tag{15}$$

Rather than producing a continuous output, the particle swarm optimization formulas are changed to provide an output of 0 or 1. Changing the m_R and x_R limits to 0 and 1, and Equation (16) will result in speeds in the range [0,1]. Furthermore, the location matrix is refreshed using more complex formulas than the continuous PSO, as shown in Equations (17) and (18), where R_a is a randomized binary and $s(p_x)$ is the value of the particle's nonlinear functions, i.e. Euler's number. In the solution, the sigmoidal operator was used to boost the result such that it remained in the interval [0, 1]:

$$v_x = \begin{cases} m_R & \text{if } v_x < m_R \\ x_R & \text{if} v_x > x_R \\ v_x & \text{if} m_R < p_x < x_R \end{cases} \tag{16}$$

$$s(p_x) = \frac{1}{1 + \exp(-p_x)} \tag{17}$$

$$p_x = \begin{cases} m_R & \text{if } s(p_x) < R_a \\ x_R & else \end{cases} \tag{18}$$

The most essential variable in Equation (11) is w, which determines the dimension of the searching area. The dimensionality must neither be so large that it is practically rare nor must it be small that many repetitions are required to find the optimal solution. Typically, the omega falls in 0.8 and 0.2. In terms of shifting the equilibrium among the particle's local and worldwide searching ability, the Resource Intensity Weights (RIW) method presented surpasses the others. RIW employs Linear Decreasing Inertia Weight (LDIW) in conjunction with a SA process to enhance the likelihood of reaching a solution with fewer repetitions and in a shorter period. LDIW still has disadvantages, mostly owing to the restricted search engine capability at the beginning of the PSO cycles. The weighted vector of the component is denoted in Equation (19).

$$w^s_{it} = \frac{w_{max} - w_{min}}{it_{max}}(it_{max} - it) \tag{19}$$

w^s_{it} is the weight vector of component x in repetition number it, w_{max} is a specified highest allowable weighting value, w_{min} is a present absolute minimum w value, and it_{max} is a predetermined maximal number of repeats. The maximum in the investigation, it_{max} was set at 500. The entire optimization of a binary optimization technique is detailed in Algorithm 1.

```
#binary optimization algorithm
Compute computational period
Set the swarm ($n_F$)
Initialise universal best
For x $=$ 0 to $n_F$ do
  For y $=$ 0 to $n_F$ do
    Compute inertia
    Compute new speed
    Compute new locations
Evaluate solutions
    Upgrade particle capacity
    Upgrade universal best
  End
End
```

Even if a PSO element begins its journey at the universal optimum, it will rapidly depart. Conversely, if a PSO element does not locate an optimum answer and is trapped in space, its general searching ability decreases as a result of the linear decrease, decreasing the likelihood of discovering an ideal option. As a consequence, the capability of the repetition front end to locate the nearest optimal solution increases. In conjunction with the LDIW, a Selection Approach (SA) was used to resolve the LDIW difficulties.

As previously stated, the primary goal of RIW is to counteract the detrimental effects of LDIW on both local and universal searching capabilities. RIW takes previous speed and the subatomic PSO element efficiency into account, determining the historical influence by picking inertia values, and then adapts to the optimal solution. To benefit from previous speeds and an ideal state, employed an annealing technique using a cooling heat value. In order to enhance the likelihood of modifying the speed of a component, the mean optimum functions of each component and the highest fitness obtained for every electron are factored into an equation. The iteration time is expressed in Equation (20).

$$T_{it} = \frac{F^{it}_{mean}}{F_{best}} - 1 \tag{20}$$

In this formula, T_{it}denotes the annealed heat value for the present incarnation, F^{it}_{mean}denotes the mean of all documented fitness values up to the meaning of the current repetition, and F_{best} is the particle's highest documented measured value. The austenitizing likelihood of the suggested protocol will be calculated, p_F is the particle's existing fitness in the iterative process it is an iterative function, and F_{it} is the preceding particle's wellness in the iterative process it-k; k is a repaired number, $\propto$ is Euler's amount, and T_{it}denotes the refrigerating heat. The inertia weight is denoted w^x_{it}, and the binary random number is denoted R_a. The Euler's amount, particle data and the weight of the particle are expressed in Equations (21) to (23).

$$\propto = \frac{F_{it-k} - F_{it}}{T_{it}} \tag{21}$$

$$p^{it}_x = \begin{cases} 1 & F_{it-k} < F_{it} \\ exp(\propto) & else \end{cases} \tag{22}$$

$$w^x_{it} = \begin{cases} q + \frac{R_a}{2} & \propto > R_a \\ \frac{R_a}{2} & else \end{cases} \tag{23}$$

The final weights are adjusted to better integrate the smart grid into the IoT devices. The system is optimized using the PSO method and the simulation outcomes are verified in the next section.

4. Experimental outcomes and the findings

To test the viability of the aforementioned hypothesis, the research did computer modelling on prediction models, privacy preservation, and bandwidth usage utilizing edge computation and cloud computing architectures. Using theoretical data sets, the research models urban power pricing. The urban power pricing dataset is collected form kaggle machine learning repository. To verify the impact of simulation analysis, the research generates the changing trend of the data set over time. PSO-SG method used set the number of hidden layers to 10, the information gain to 0.00005, the trained data set to 3800, the testing data set to 2000, and the optimum solution repetition times to 30 in the simulations. This system can produce precise forecasts. As the years pass, the findings of the prediction curve become more congruent with the actual values. The computation's precision has been proven. The simulation parameters are efficiency, end-to-end delay, price, error in terms of: Mean Squared Error (MSE), Mean Absolute Error (MAE), Precision and accuracy.

The efficiency analysis of the proposed PSO-SG system is shown in Figure 4. The efficiency of the integration of the smart grid with the IoT systems is analyzed, and the results are measured with respect to the number of device variations. As the IoT device count increases, the efficiency of the system also increases. The efficiency is increased using the PSO method, and energy is saved using both the IoT-based WSN and optimization methods for various densities of nodes.

The end-to-end delay analysis of the proposed PSO-SG system is measured with respect to the device count, and the results are plotted in Figure 5. The devices are varied from 10 to 100, with a step count of 10 devices for the experimental analysis. As the device count increases, the respective delay increases, which may be due to the multiple hops between the IoT devices and energy-efficient optimization models. The proposed PSO-SG enhances the power generation in the smart grid, and the respective power is distributed using the PSO model.

The price of the power analysis using the proposed PSO-SG is measured, and the results are plotted in Figure 6. The cost of the power generated by the smart grid is calculated per minute, and the variation is due to different environmental factors. The predicted and actual costs of electricity are compared. The proposed PSO-SG shows a lesser deviation from the actual value to the predicted value because of the smart integration of particle swarm optimization. The results ensure the highest accuracy in determining the results.

The error analysis of the suggested PSO-SG system is measured in terms of mean squared error (MSE) and mean absolute error (MAE), and the comparisons of the results are plotted in Figure 7. The experimental results show the efficiency of the PSO-SG system with a lesser or negligible error. The particle swarm optimization algorithm improves energy efficiency, particularly in smart grids for power generation and distribution to users. The results are further enhanced using IoT devices.

The simulation results in terms of precision and accuracy are computed, and the overall results are plotted in Figure 8. The proposed PSO-SG system results are compared with those of existing models like Support Vector Machine (SVM), Convolutional Neural Network (CNN), Principal Component Analysis (PCA), and Fuzzy Classifier Algorithm (FCA). The findings show the efficiency and accuracy of the proposed PSO-SG system over the existing models. The simulated results primarily include four points:

- As the number of devices increases, the standard cloud-based grid requires more bandwidth efficiency than IoT-based microgrids.

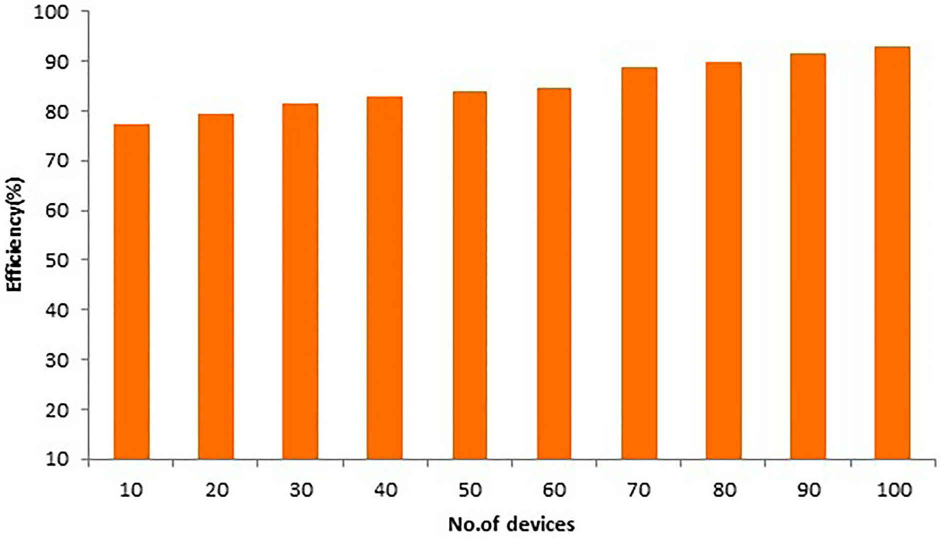

Figure 4. Efficiency Analysis of the Proposed PSO-SG.

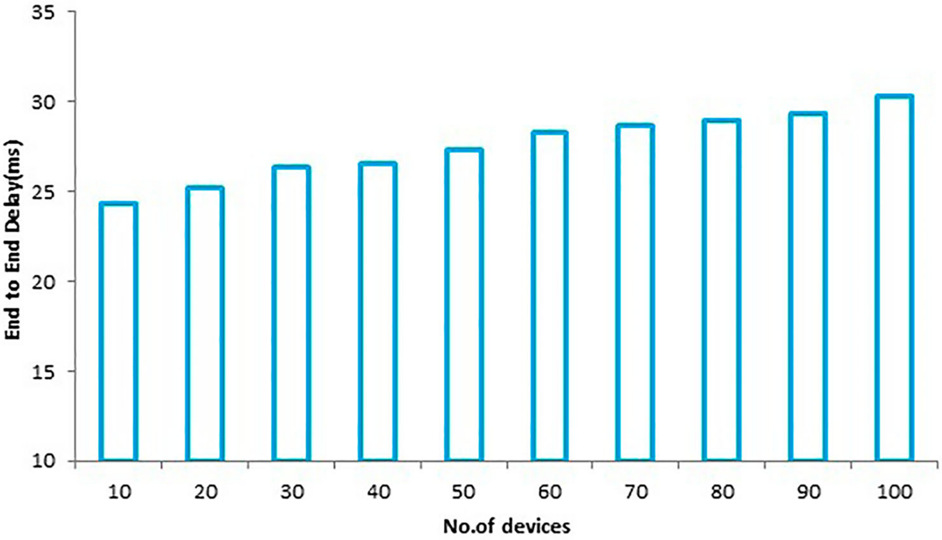

Figure 5. End-to-End Delay Analysis of the PSO-SG.

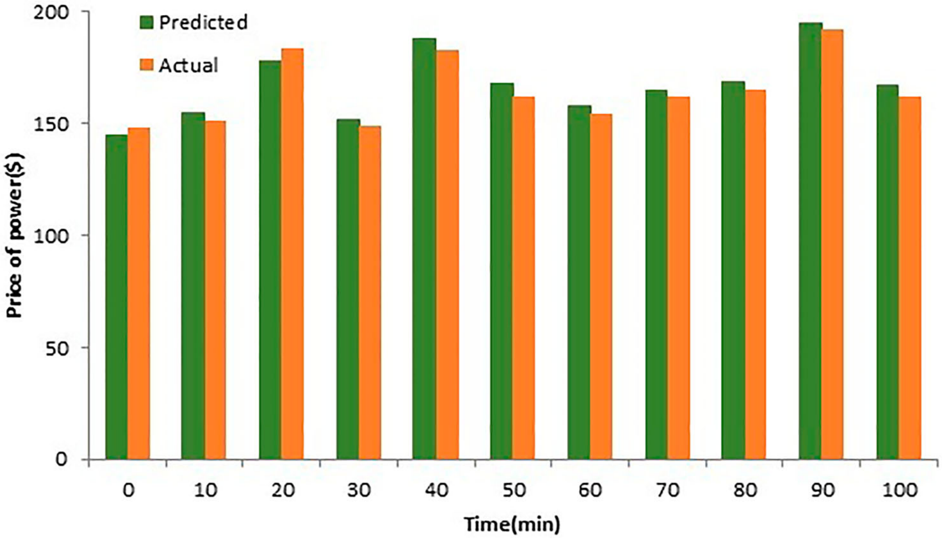

Figure 6. Price of the Power Analysis.

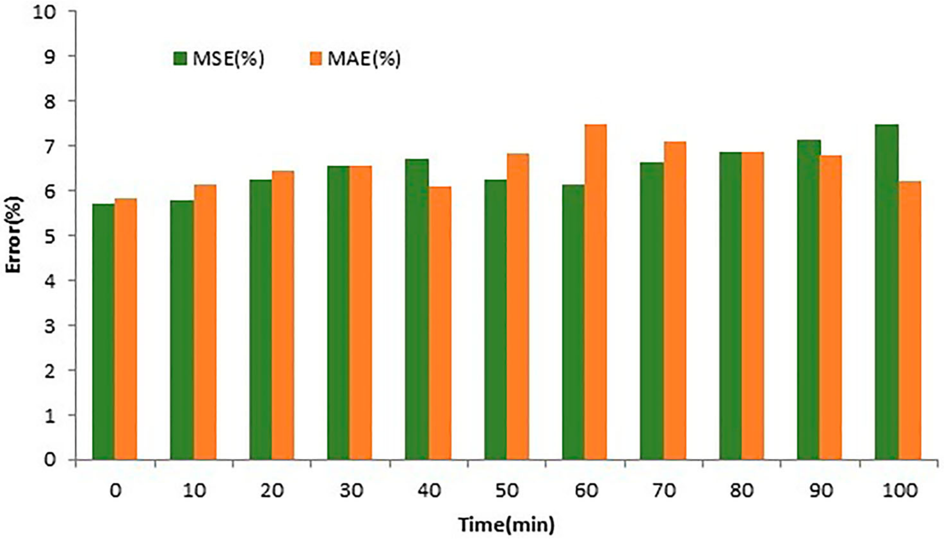

Figure 7. Error Analysis of the Proposed PSO-SG System.

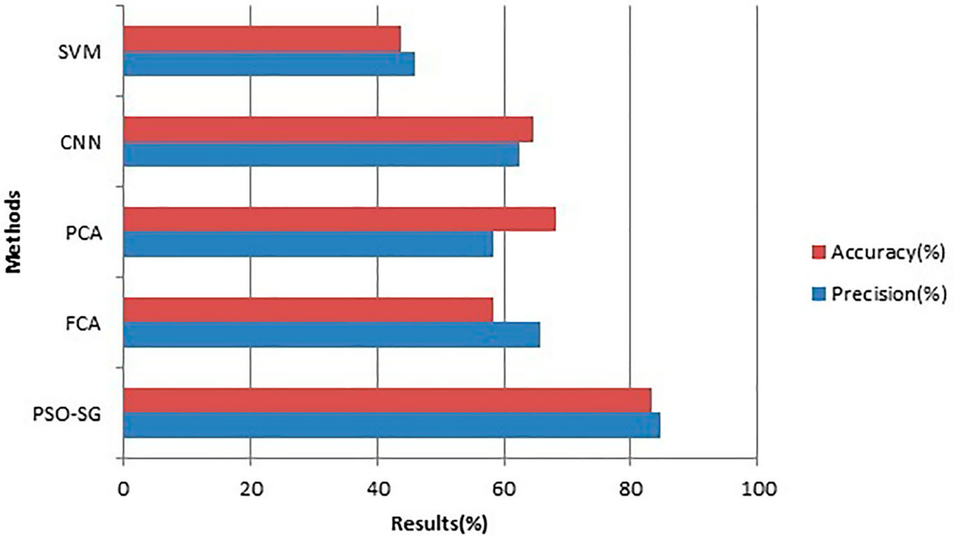

Figure 8. Simulation Results Analysis.

- The communication bandwidth requirements of a system with edge devices are always lower than those of the cloud.
- It is demonstrated that an electric grid with an edge computer design slows data transfer speed.
- Latency and capacity are measures of quality service. Based on simulations of bandwidth and latency, it is clear that the network edge design's Quality of Service (QoS) efficiency outperforms that of cloud-centric distributed generation.

5. Conclusion and the findings

This work has concentrated primarily on resolving issues generated by IoT-based distributed generation, including quick reactions to user requirements, intelligent planning, intelligent servicing, intelligent comments to customers, and rapid market reactions. This paper presents an architecture that introduces edge computing to IoT-based microgrids. In addition, power distribution, micro-grids, sophisticated metering technologies, and the use of edge devices are heavily covered in the three primary power system concepts. Compared to typical cloud-based energy systems, both real-time response and edge computing-based services demonstrate the system's benefits in full.

New efforts will include integrating edge computing into electricity grids to enable real applications. In particular, the commercial benefit of edge computing applied to power networks will be shown, and the practicability of the approach will be examined. Notably, while the method employed maps packets straight to the packet, other methodologies for protocol assimilation result in data transmitting into the sky and require the construction of the system or perhaps even the use of a graphical user interface, which inhibits its use on platforms with restricted storage and handling assets. The research has determined, based on numerical findings, that the suggested technique may successfully secure online privacy in the network and provide new options for the implementation of IoT-based microgrids. Future research will include (1) implementing the system on a physical testing ground to assess the integrated gateway while connecting a cellphone with a pretty intelligent device inside an SG system. (2) combining the IoT and the Smart Grid**:** Some of these challenges need to be addressed in future research endeavours. Need to factor in the scenarios where IoT devices work under extreme conditions and in diverse environments. These could be extreme temperatures, exposure to electromagnetic waves, or high voltages. Irrespective of the external conditions, reliability, compatibility, and performance cannot be compromised.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

S.S. Sivaraju http://orcid.org/0000-0003-1686-4703

References

[1] Hassan WH. Current research on Internet of Things (IoT) security: a survey. Comput Netw. 2019;148:283–294.

[2] Dileep G. A survey on smart grid technologies and applications. Renewable Energy. 2020;146:2589–2625.

[3] Tightiz L, Yang H. A comprehensive review on IoT protocols' features in smart grid communication. Energies. 2020;13(11):2762–24.

[4] Mirhosseini M, Keynia F. Asset management and maintenance programming for power distribution systems: a review. IET Gener Transm Distrib. 2021;15(16):2287–2297.

[5] Ghasempour A. Internet of things in smart grid: architecture, applications, services, key technologies, and challenges. Inventions. 2019;4(1):22–12.

[6] Bhardwaj KK, Khanna A, Sharma DK, et al. Designing energy-efficient IoT-based intelligent transport system: need, architecture, characteristics, challenges, and applications. Energy Conservation for IoT Devices: Concepts, Paradigms and Solutions. 2019;206:209–233.

[7] Liu S, Zhao Y, Lin Z, et al. Data-driven event detection of power systems based on unequal-interval reduction of PMU data and local outlier factor. IEEE Trans Smart Grid. 2020;11(2):1630–1643.

[8] Gheisarnejad M, Khooban MH. IoT-based DC/DC deep learning power converter control: real-time implementation. IEEE Trans Power Electron. 2020;35(12):13621–13630.

[9] Agarwal P, Alam M. Investigating IoT middleware platforms for smart application development. In Smart Cities—Opportunities and Challenges: Select Proceedings of ICSC 2019. Singapore: Springer ; 2020; p. 231– .

[10] Babar M, Tariq MU, Jan MA. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. Sustainable Cities Soc. 2020;62:102370–20.

[11] Dharmadhikari SC, Gampala V, Rao CM, et al. A smart grid incorporated with ML and IoT for a secure management system. Microprocess Microsyst. 2021;83:103954–8.

[12] Bera B, Saha S, Das AK, et al. Designing blockchain-based access control protocol in iot-enabled smart-grid system. IEEE Internet Things J. 2020;8(7):5744–5761.

[13] Pawar P. Design and development of advanced smart energy management system integrated with IoT framework in smart grid environment. J Energy Storage. 2019;25:100846–13.

[14] Bagdadee AH, Hoque MZ, Zhang L. IoT based wireless sensor network for power quality control in smart grid. Procedia Comput Sci. 2020;167:1148–1160.

[15] Hussain S, Ullah I, Khattak H, et al. A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for internet of things enabled smart grid. IEEE Access. 2020;8:93230–93248.

[16] Wang J, Wu L, Zeadally S, et al. Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid. ACM Trans Sens Netw (TOSN). 2021;17(3):1–25.

[17] Srinivas J, Das AK, Li X, et al. Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems. IEEE Trans Ind Inf. 2021;17(7):4425–4436.

[18] Hafeez G, Wadud Z, Khan IU, et al. Efficient energy management of IoT-enabled smart homes under price-based demand response program in smart grid. Sensors. 2020;20(11):3155–41.

[19] Ren D, Li X, Zhou Z. Energy-efficient sensory data gathering in IoT networks with mobile edge computing. Peer-to-Peer Networking Appl. 2021;14:3959–3970.

[20] Du X, Zhou Z, Zhang Y, et al. Energy-efficient sensory data gathering based on compressed sensing in IoT networks. J Cloud Comput. 2020;9:1–16.

[21] Najjar-Ghabel S, Yousefi S, Farzinvash L. Reliable data gathering in the internet of things using artificial bee colony. Turk J Electr Eng Comput Sci. 2018;26(4):1710–1723.

[22] Faheem M, Butt RA, Raza B, et al. Bio-inspired routing protocol for WSN-based smart grid applications in the context of industry 4.0. Trans Emerging Telecommun Technol. 2019;30(8):e3503.

[23] Fernandez JH, Omri A, Di Pietro R. Power grid surveillance: topology change detection system using power line communications. Int J Electr Power Energy Syst. 2023;145:1–11.