IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 October 2023, accepted 9 November 2023, date of publication 20 November 2023,
date of current version 8 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3335245

SURVEY

FL_GIoT: Federated Learning Enabled Edge-Based Green Internet of Things System: A Comprehensive Survey

JOSEPH BAMIDELE AWOTUNDE[1], SAMARENDRA NATH SUR[2], (Senior Member, IEEE), RASHEED GBENGA JIMOH[1], (Senior Member, IEEE), DAYO REUBEN AREMU[1], DINH-THUAN DO[3], (Senior Member, IEEE), AND BYUNG MOO LEE[4], (Senior Member, IEEE)

[1]Department of Computer Science, Faculty of Information and Communication Sciences, University of Ilorin, Ilorin 240003, Nigeria
[2]Department of Electronics and Communication Engineering, Sikkim Manipal Institute of Technology, Sikkim Manipal University, Majitar, Rangpo, Sikkim 737136, India
[3]School of Engineering, University of Mount Union, Alliance, OH 44601, USA
[4]Department of Intelligent Mechatronics Engineering and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, South Korea

Corresponding author: Byung Moo Lee (blee@sejong.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by Korea government (MSIT) under Grant NRF-2023R1A2C1002656, was supported by the MSIT (Ministry of Science and ICT), Korea under Grant IITP-2023 RS-2022-00156345 (ICT Challenge and Advanced Network of HRD Program), and was supported by the faculty research fund of Sejong University in 2023.

ABSTRACT In today's world, the importance of the Green Internet of Things (GIoT) in the transformed sustainable smart cities cannot be overstated. For a variety of applications, the GIoT may make use of advanced machine learning (ML) methodologies. However, owing to high processing costs and privacy issues, centralized ML-based models are not a feasible option for the large data kept at a single cloud server and created by multiple devices. In such circumstances, edge-based computing may be used to increase the privacy of GIoT networks by bringing them closer to users and decentralizing them without requiring a central authority. Nonetheless, enormous amounts of data are stored in a distribution mechanism, and managing them for application purposes remains a difficulty. Hence, federated learning (FL) is one of the most promising solutions for bringing learning to end devices through edge computing without sharing private data with a central server. Therefore, the paper proposes a federated learning-enabled edge-based GIoT system, which seeks to improve the communication strategy while lowering liability in terms of energy management and data security for data transmission. The proposed model uses FL to produce feature values for data routing, which could aid in sensor training for identifying the best routes to edge servers. Furthermore, combining FL-enabled edge-based techniques simplifies security solutions while also allowing for a more efficient computing system. The experimental results show an improved performance against existing models in terms of network overhead, route interruption, energy consumption, and end-to-end delay, route interruption.

INDEX TERMS Federated learning, network overhead, energy consumption, edge computing, green Internet of Things, security and privacy, end-to-end delay, route interruption.

I. INTRODUCTION

The Internet of Things (IoT) is a term used to represent a collection of technologies and fields of study that enable global communication among physical things all over the world. The IoT in recent years is equipped with various cutting-edge computing and detecting proficiencies with innovations in Deep Learning (DL) models [1], [2]. This emergence has opened various opportunities in several fields for significant applications like the Green Internet of Things (GIoT) for sustainable smart cities, healthcare systems, and vehicular networks [3]. The IoT connects physical things to

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

generate a substantial amount of data using various sensors and forward data intelligently. Due to the fact that the IoT-based system consists of huge parts and entities, the total energy consumption of the network may be lowered with minimal reduction in the energy consumption of each network device. Furthermore, because vast data created by IoT-based devices is stored on servers, it is vital to design an energy-efficient network. As a result, developing and cost-effective energy management inside the IoT system is critical. Green wireless communication is also vital in developing an energy-efficient IoT because IoT elements often connect over wireless channels [4].

Therefore, GIoT research focuses on reducing energy consumption in IoT-based systems, aligning with sustainable cities. Researchers propose algorithms to solve energy-related problems, improving the acceptability of IoT-based systems internationally. Research focuses on reducing energy consumption in GIoT design and development to enhance the acceptability of IoT-based systems internationally, with a major emphasis on reducing greenhouse gas emissions [5]. GIoT applications are created in industries like healthcare, manufacturing, engineering, and smart cities to increase productivity and cost-effective performance. Edge computing is a distributed computing method that employs a number of edge servers to improve response time while minimizing latency. The combination of edge computing with GIoT improves internet backbone efficiency in terms of processing and data storage, but security concerns, low-powered sensors with battery capacity difficulties, and transmission range remain. As a result, adopting a new paradigm to provide energy services with secure data transmission for sustainable cities utilizing GIoT-based systems is critical.

Edge computing is a cloud storage solution for data sources outside the cloud, utilizing end devices to bring training models closer to data production [6], [7]. The edge-cloud computing network consists of a cloud server, end devices, and edge nodes [8], [9], [10]. However, it incurs high transmission costs and requires ongoing training [11], [12]. Edge computing can deter privacy-conscious consumers from participating in model training, leading to stricter privacy rules [13], [14]. To address this, Federated Learning (FL) is used to facilitate collaborative learning of complex model training data within users' devices [15], [16]. This approach can enhance GIoT performance by allowing local data to train within a cloud server, reducing the need for data concentration in a cloud server. The combination of FL enabled edge-based will significantly increase the performance of the GIoT network. Because the traditional cloud-based ML-based approach requires data to be centered or concentrated in a cloud server. Hence, this study proposes an FL-enabled edge-based collaboration for GIoT. The followings are the key contributions of the paper:

- The applicability of FL-enabled Edge-based servers in the GIoT paradigm was presented. The FL-based model was used to intelligently model the data in real-time and thereby increase the GIoT communications and reduce the energy consumption of the GIoT-based systems.
- In GIoT-enabled distributed networks, the combination of the FL model and edge-based delivers optimum energy consumption with the least routing overhead and a healthy efficiency toward sustained development.
- The implementation of a FL enabled edge-based system guarantees a safe GIoT system for sustainable cities against hostile acts, because the data will not be processed outside the GIoT cloud, and the FL approach will be utilized to train the data.
- It keeps track of situations involving total data secrecy to categorize the GIoT sensors involved in data transmission.

The remainder of this paper is as follows. Section II represents the application of GIoT. It is followed by the extensive review on the existing works in section III. Section IV consists of mathematical model and methodology followed in this paper. Section V contains detailed analysis of the results corresponding to the proposed system. Section VI contains the study limitations and future work followed by the conclusion in section VII.

II. PROMISING APPLICATIONS OF GREEN INTERNET OF THINGS

The GIoT paradigm aims to reduce energy usage by connecting everything, anytime, and anywhere. It consists of intelligent, self-contained systems that share data and access other sources [1], [2]. Energy-efficient devices and sensors are used to collect data. However, building a green intelligent network still presents challenges. Integrating energy efficiency in IoT-based layers will make green technology a reality. Advanced Internet applications and gadgets are crucial for environmental preservation and cleaner air. Green renewable energy proficiency is essential for energy savings. Optimizing IoT operations and reducing energy consumption is essential for mineral wealth preservation and habitat restoration. Energy-efficient strategies are needed in production, operation, and disposal departments.

The data collected by devices and sensors are interpreted in the processing systems since most GIoT outdoor applications operate similarly, and wireless channels are used to transfer the required information. Hence, the three main purposes of using GIoT energy are: (i) data capturing using sensors, (ii) processing, and (iii) data transmission. The real-time operating systems and periodic wake-up mechanism energy usage are insignificant. Therefore, analyzing the energy usage of a GIoT-based system for energy efficiency and minimizing the number of these processes as much as feasible becomes crucial [17]. Apart from reducing energy use, ways of creating energy from alternative sources such as solar, wind, and geothermal should be researched. Temperature, wind speed, and daylight hours all have an impact on these power generating source. The GIoT's four dimensions are illustrated in Figure 1.

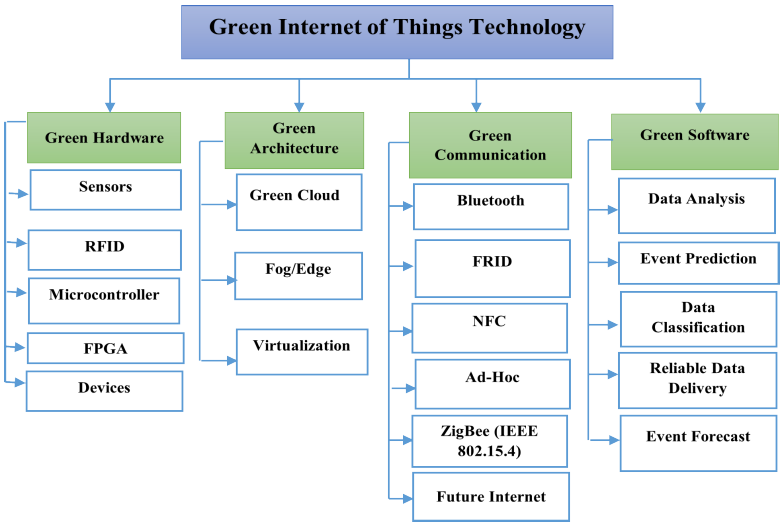

FIGURE 1. The green internet of things general components.

A. APPLICATION ASPECTS OF GIOT SYSTEM

There are numerous applications and services available for GIoT technology, as demonstrated in Figure 2. Among the components are smart cities, smart energy and smart grid systems, crystallized intelligence, industrial automation, intelligent health systems, and smart logistics. GIoT can be employed in several scenarios due to its low energy utilization and excellent flexibility to the environment.

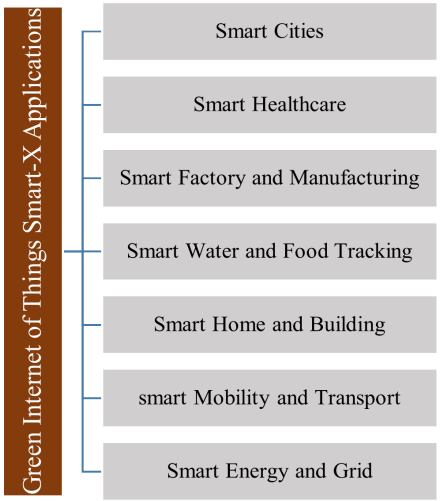

FIGURE 2. Application of green internet of things in Smart-X.

1) GIOT FOR SMART CITIES

In smart cities, the application of GIoT can aid in providing real-time answers to emerging challenges and enhance urban flow management. In recent years, smart cities have sparked increased interest in a variety of issues, including population aging, climate change, technology advancements, economic and environmental changes, and so on. Smart parking, traffic management, and evaluating the strength of buildings, bridges, and monuments have all benefited from IoT-based solutions. In recent years, GIoT has been seen in different sustainable smart cities, such as smart traffic, light, transit, and smart bridges [18], [19]. As a result, becoming green is a must to reduce overall electricity usage and reduce environmental damage.

2) GIOT FOR SMART HOMES

In 2002, the European Union (EU) parliament passed a rule requiring European countries to implement specified practices to improve energy efficiency in households and offices [20]. In this regard, several research initiatives have been initiated to improve the energy efficiency of the GIoT systems, such systems including AIM, DEHEMS, SEEMPubs, IntUBE, and DIMMER, [21]. The GIoT reduction of energy waste in smart homes has been governed by the EU Directive for the management of smart systems [17]. When individuals who reside in a smart house depart, the GIoT automatically turns off lights. Furthermore, GIoT-based cooling systems can manage the house temperature according to interior activities while using the least amount of energy. As a consequence, by monitoring and recording energy-related metrics, GIoT can reduce building energy use and associated expenditures, improving the quality of life by making cities green [22].

3) GIOT FOR THE SMARTER ENVIRONMENT AND IMPROVE INDUSTRIAL CONTROL

The GIoT technology has been used to detect forest fires in the field of smart ecosystems, monitor drinking water, evaluate air and saltwater pollution, govern the surrounding region, establish a smart grid, and detect forest fires. Furthermore, the IoT may be utilized in sensitive applications such as recalling fluid identification for server farms, predicting erosion and radiation at thermal energy stations to generate spill notifications, and monitoring fragile constructions to prevent disintegration. Being eco-friendly means that no significant harm is done to the environment in situations where this innovation is directly linked to the climate.

4) AGRICULTURE AND ANIMAL HUSBANDRY IN THE GIOT SYSTEM

GIoT technology has the potential to boost crop longevity and quantity in the agriculture and livestock industries. GIoT systems can be more beneficial in tracking and monitoring farm animals, monitoring soil moisture and tree pests, setting up smart meteorological stations, and caring for newborn animals, among other things [23]. Green guidelines must be followed at all phases of the growth of healthy crops and animal products for people.

5) GIOT FOR E-HEALTH

As technology gadgets have improved human well-being in healthcare systems, GIoT techniques have been developed to improve medical systems. Medical refrigerators can be monitored, athletes can be cared for, elderly patients can be watched more easily, and UV radiation can be accessed via the IoT. To monitor various physiological aspects of the human body, many GIoT-based medical sensors and gadgets with limited battery life have been developed. If an object in these programs does not need to be active at a specified moment, its status is changed to power-saving mode to save energy. Furthermore, if no processing tasks are assigned, the CPU speed is lowered. Given that GIoT is so close to humans in many applications, it must be environmentally friendly to demonstrate that it is not dangerous. It's also worth mentioning that one of the GIoT's goals is to reduce the number of sensors required to monitor physiological signals [24]. Delivering a green brain-to-machine interface is also crucial in brain-controlled GIoT applications [25].

III. RELATED WORK

This study conducted a Comprehensive Literature Review (CLR) on GIoT-enabled enabled with various technology, with a focus on incorporating various concepts related to security and privacy of IoT-based systems like FL, Edge computing, and AI, DL, and ML-based models and their utilization in GIoT technology. Rapid, dependable, low-latency IoT communication links are becoming increasingly necessary, and GIoT has evolved as an innovative technology to meet this demand. Nevertheless, there are many technological and tactical challenges in GIoT adoption. Understanding the current stage of the investigation is crucial to identifying the key challenges and opportunities in order to build and execute GIoT in interactions with diverse technologies in a sustainable and effective manner. In order to provide a thorough understanding of the current research being done in this section of study conducts CLR on GIoT-enabled models using FL, Edge computing, ML, DL, and AI.

Equipment and software aspects should be considered for GIoT technology with hardware solutions producing devices that consume less energy without sacrificing performance. Software solutions, on the other hand, enable current systems to utilize less energy by maximizing resource use. Electricity-saving virtual machine techniques should also be introduced. The FL model protects the participants' privacy by disclosing parameters from the trained model rather than real data, which is the model's primary aim. However, several recent studies have discovered that when FL players or FL servers are unethical, security and privacy concerns might arise. FL's objective is hindered since the global model's influence might be tainted, and users' privacy can be threatened during model training. In order to get a better understanding of this study well, a comprehensive review was carry out.

A. EDGE COMPUTING, NETWORK THROUGHPUT, AND LATENCY

Through a variety of edge servers, edge computing enhances reaction time while minimizing latency in a distributed fashion. Low-powered sensors have limitations with regard to battery life, transmission range, and security, even though the combination of edge computing and GIoT greatly enhances network performance in terms of processing and data storage.

In [26], the authors analyze the placement of edge computing resources on an Internet-wide scale, revealing that these strategies can improve cloud access latency by up to 30%. They propose an edge-cloud collaborative computing system (ECCS) based on open-source EdgeX and Huawei openLooKeng, which is low-latency, low-power, and intelligent, making it suitable for real-time IoT applications. However, it does not specifically mention network throughput or the term GIoTs System.

In [27], the authors proposed an edge computing architecture for the IoT, which brings down storage, computation, and communication services from the cloud server to the network edge, resulting in low latency and high availability. Edge computing brings down storage, computation, and communication services from the cloud server to the network edge. ScalEdge addresses the challenges of scalability in edge computing by providing a scalable architecture that can handle a large number of IoT devices and data streams. The study incorporates techniques such as data partitioning, load balancing, and resource management to efficiently distribute the workload across edge devices, and includes mechanisms for fault tolerance and reliability to ensure the continuous operation of the system. The study does not mention network throughput or the term GIoTs System.

The authors in [28] presented a comprehensive survey to analyze how edge computing can improve the performance of IoT networks and classify edge calculations into different groups based on the architecture and study their performance by comparing network latency, bandwidth usage, power consumption, and overhead. The study established that edge computing migrates data calculations or storage to the edge of the network near the end-user, and educes latency and improves performance of IoT networks. The study failed to mention network throughput or the term GIoTs System.

The authors in [29] presented a comprehensive survey, analyzing how edge computing improves the performance of IoT networks and considers security issues in edge computing,

evaluating the availability, integrity, and the confidentiality of security strategies of each group, and proposing a framework for security evaluation of IoT Networks with edge computing. The study maintained that edge computing reduces latency and improves performance in IoT networks, and analyzed diverse edge computing architectures and their performance. The paper did not discuss on both GIoT system and network throughput.

In [30], the authors proposed a personalized FL framework for intelligent IoT applications, addressing heterogeneity issues and achieving fast-processing capacity and low latency. It presents a case study of IoT-based human activity recognition to demonstrate its effectiveness. Authors in [31] proposed a Local Data Reduction framework to address latency and cost constraints in IoT data processing. It uses the Markovian birth-death process and outperforms the WLDR model, demonstrating its effectiveness in meeting QoS requirements for real-time IoT systems.

B. FEDERATED LEARNING, ARTIFICIAL INTELLIGENCE, AND DEEP LEARNING ENABLED WITH IOT, AND GIOT-BASED SYSTEMS

A key component of implementing AI at the edge of the GIoT scenario is FL, which allows numerous devices to cooperatively train a common ML model while maintaining the privacy of all local data. The single point of failure and scalability problems of centralized FL can be resolved by distributed FL (DFL) based on Device-to-Device (D2D) communications, although D2D links' communication resource limitations apply. Therefore, it is essential to lower the FL models' data communication volume between devices.

One of the first studies to show the viability of utilizing a trained model to extract information from deep or machine learning models is reference in [32]. The authors show that throughout the training phase, the proposed correlations in the training data are collected into the trained model. As a result, publishing the trained model might result in an unauthorized exposure to hackers that was not intended. For example, a trained adversary's speech recognition system can deduce a user's race or gender. The authors of [33] propose a model- reversal approach for separating data from choice tree-based or facial acknowledgment prepared models. The goal of this method is to compare the objective element vector to every possible value and then produce a weighted likelihood evaluation of the correct value. The findings of the investigation suggest that the adversary may perfectly replicate an image of the casualty's face using this approach. On the other hand, the authors of [34] propose a neural network-based method for estimating the local models of FL players who are left out during training. The base station assigns resource blocks to users whose models have the largest impact on the global FL model first in the system model. One user in specific is selected to be permanently connected to the base station. These estimated values are used as input by the feedforward NN to forecast the model parameters of users who were left out of the training iteration. Base stations can now incorporate more locally trained FL model parameters into each iteration of global aggregation, leading to faster FL convergence.

Federated Learning is used in a dynamic and uncertain portable edge network environment with varying constraints, such as distant organization and energy circumstances. Deep Q-Learning (DQL) may be utilized to simplify asset distribution for model preparation, as stated in [35]. Members of the framework model, like as mobile phones, collaborate to create DNN models that a FL server need. Cell phones require a lot of energy, a lot of CPU, and a lot of distant data transfer capability. To diminish energy utilization and preparing time, the server should distinguish the proper measures of information, energy, and CPU assets that the cell phones will burn through for preparing. The server is an expert in a stochastic improvement problem in which the state space contains the CPU and energy conditions of the phones, and the activity space contains the quantity of information units and energy units collected from the phones. The reward is determined by the amount of data collected, the amount of energy consumed, and the amount of time it takes to train. To overcome the server's problem, the authors in [36] proposed a Double Deep Q-Network (DDQN). The proposed scheme reduces the energy usage by roughly 31% when compared to the greedy algorithm, and the training delay by up to 55% when compared to the random scheme, according to the simulation data. As an extension to [35], the authors of [37] propose a resource allocation technique based on DRL, with the extra risk that FL members are mobile and may leave the network coverage zone. Even without previous knowledge of the mobile network, the FL server can optimize resource allocation amongst players, such as channel selection and device energy use.

To identify device failures in Industrial Internet of Things (IIoT), the authors in [38] presented an FL approach based on blockchain. The FL system's platform architecture is built on blockchain and supports the verified integrity of client data. Each client generates a Merkle tree regularly, with each leaf node representing a client data record and the root being recorded on the blockchain. Furthermore, to address data heterogeneity, a new centroid distance weighted federated averaging (CDW FedAvg) algorithm is proposed, which takes into account the distance between positive and negative classes in each client dataset. The empirical research results of FL-based production line fault prediction were presented by the authors in [39]. For Horizontal Federated Learning (HFL) and Vertical Federated Learning (VFL), federated support vector machine (SVM) and federated random forest (RF) algorithms are developed. An experimental technique is proposed to evaluate the efficacy of FL and centralized learning algorithms. In [40], the authors devised a FL technique for DL-based machinery fault detection. The model aggregation method is altered adaptively utilizing a dynamic verification approach based on the FL framework, which overlooks some customers' low-quality data. In addition, a self-supervised

learning technique for learning structural information from little training data is proposed. This approach offers both data augmentation and multitasks learning effects. Experiments on two rotating equipment datasets suggest that this method can be used to diagnose faults in rotating machinery.

The proposed method and the typical centralized training method on the Non-IID, however, still have a large gap. Edge device failures have a significant impact on IIoT industrial product manufacturing. The authors in [41] developed a new communication-efficient on-device FL-based deep anomaly detection framework for sensing time-series data in IIoT to overcome this challenge. It allows distributed edge devices to work together to increase the generalization ability of an anomaly detection model. To accurately detect abnormalities and an attention mechanism-based Convolutional Neural Network- Long Short-Term Memory (CNN-LSTM) model is presented. To avoid memory loss and gradient dispersion, it employs a CNN module based on an attention method to collect key fine-grained characteristics. To increase the efficiency of communication and fulfill the urgency of manufacturing anomaly detection, a gradient compression technique based on Top-k selection is developed.

The contribution of devices to the worldwide aggregation of FL was quantified by [42]. The learning model's accuracy and reliability have been increased. An adaptive calibration approach of global aggregation frequency is suggested based on a deep Q network (DQN), which minimizes the loss function of FL under a certain resource budget. In a time-varying communication environment, it realizes the dynamic trade- off between computing energy and communication energy. To detect network threats in industrial cyber-physical systems, the authors in [43]developed DeepFed, an FL-based intrusion detection model using CNN and GNU. Multiple industrial cyber-physical systems can use the specified FL framework to create a comprehensive intrusion detection model for privacy protection. To maintain the secrecy and privacy of model parameters during the training process, a secure communication protocol based on the Paillier cryptosystem was created. The model is highly effective in detecting various sorts of network threats in industrial cyber-physical systems, according to tesing on a data set from a real industrial cyber-physical system. Many smart city applications have been developed to assist the public in utilizing proactive and adaptive solutions [44], [45]. On the other hand, most Green IoT devices are utilized to collect a big amount of smart data and are required to achieve a reliable and energy-efficient solution. In order to manage diverse routing processes in sustainable cities, GIoT-assisted applications have been discovered. The most difficult objectives, however, are data latency and resource management efficiency. Edge computing is also being combined with GIoT to improve compute and storage resources. Nonetheless, the research community is still grappling with intelligent and optimized energy systems.

Furthermore, due to the large amount of data collected in GIoT systems, many re-transmissions may occur, as well as network dis-connectivity, thus, transmission fees and over- heads are incurred. By extending the extent of energy gaps, such solutions increase the unpredictability of IoT systems in green communications [46], [47]. Malicious nodes can also affect communication networks and disturb the monitoring environment of green urbanization. In an unmanaged environment, GIoT devices are more exposed to security risks. These limitations have a big influence on GIoT data and put transmission privacy in jeopardy. Therefore, the combination of FL-enabled edge-based computing will help in the integration of security solutions in GIoT sustainable cities given protection to the energy-oriented route and network threats.

In [48], the authors proposed an energy-efficient integration of joint edge intelligence nodes, focusing on bandwidth allocation, CPU frequency, transmission power optimization, and learning accuracy. The study optimizes computation frequency allocation and reduces energy consumption in IoT devices. The Alternative Direction Algorithm (ADA) is proposed to reduce complexity and energy consumption at each iteration of FL time. At the expense of a slight increase in FL time from IoT devices to edge intelligence nodes, the suggested Alternative Direction Algorithm can modify the frequency of the central processor unit and power transmission regulation to lower energy usage. The authors in [49] proposed framework uses a blockchain network for secure model aggregation, with each node hosting an SGX-enabled processor. This ensures model authenticity, integrity, and tamper-proof storage. Experiments were conducted with various CNN models and datasets to evaluate its performance.

C. FEDERATED LEARNING, AGGREGATION ALGORITHM, LOCAL MODEL TRANSPORTATION, AND CENTRALIZED FL FOR IOT, AND GIOT-BASED SYSTEMS.

The authors in [50] explored the use of Async-HFL for converging speed under system heterogeneities and stragglers. It designates device selection and device-gateway association at the gateway and cloud levels, demonstrating its faster convergence and cost savings compared to state-of-the-art asynchronous FL algorithms. Authors in [51] presented a secure, reliable FL algorithm that integrates hybrid differential privacy, categorizes users based on privacy needs, and proposes an adaptive gradient clip scheme and improved composition method for improved performance. In [52], the authors explored the integration of edge computing and FL in medicine, focusing on the potential of intelligent processing of clinical visual data, enabling remote healthcare centers to securely benefit from multi-modal data.

Similarly, authors in [53] proposed a DRL-based joint secure aggregation and resource orchestration scheme for hierarchical FL assisted by untrusted mobile-edge computing (MEC) servers. The scheme aims to maximize

long-term social welfare while minimizing data size, payment, and resource orchestration. The hierarchical reward function-based DRL algorithm (MATD3) is proposed, achieving superior performance over comparison algorithms. The authors in [54] introduced a mobile crowdsensing-based geospatial physical distance monitoring model for efficient pandemic management. It analyzes human mobility information to identify hot-spot regions and monitors physical distance mandates. The model also includes an Android application called SocialSense for effective pandemic management. Experimental results show improved accuracy in hot-spot identification and physical distance monitoring compared to existing approaches

In [55], the authors proposed a SemiPFL framework that supports edge users with limited labeled data sets and unlabeled data. It involves edge users collaborating to train a Hyper-network, generating personalized autoencoders. The framework outperforms state-of-the-art federated learning frameworks in various application scenarios, including wearable health and IoT. It also performs well for users without labeled data sets and increases performance with increased labeled data and users. The authors in [56] proposed a novel adaptive mechanism for CSFL motivates organizations to contribute data resources in dynamic training environments, using multi-agent reinforcement learning to optimize strategies without private information or precise accuracy. In [57], the authors presented a privacy-preserved FL approach for cyber-attack detection in edge-based IoT ecosystems. The lightweight convolutional Transformer network is designed to identify attacks by learning attack patterns from local edge devices. The approach outperforms traditional FL in detection accuracy and is effective in handling non-stationary data.

The authors in [58] presented an algorithm that improves the privacy of terminated raw data by enhancing differential privacy before transmission to the edge server, thereby ensuring privacy for gradient attacks on FedGAN. In [59], the authors presented an edge learning-based green content distribution scheme for IC-IoT, enhancing speed and recovery capability through intelligent path selection and distributed coding. The scheme's effectiveness and performance have been verified through simulation experiments. The authors in [60] discussed the design of FL at the network edge, models the incentive interaction between a global server and devices, presents open research challenges, and offers future research perspectives.

Similarly, authors in [61] employed deep reinforcement learning (DRL) agents on edge nodes to indicate IoT device decisions, while federated learning (FL) is used to train agents distributedly, demonstrating the effectiveness of these methods in dynamic IoT systems. The authors in [62] proposed a Deep Reinforcement Learning (DRL)-based green resource allocation mechanism for mobile users, aiming for energy efficiency and user satisfaction, with its effectiveness validated through simulation results. Furthermore, authors in [63] proposed a secure, efficient AIoT scheme for private energy data sharing in smart grids. It introduces an edge-cloud-assisted federated learning framework, local data evaluation mechanism, optimization problems for Energy Distributors (EDOs) and energy service providers, and a two-layer deep reinforcement-learning-based incentive algorithm for EDO participation.

The existing work have been so far conducted mostly on IoT-based network, and some on IIoT, Mobile, and IoMT-based applications. To the best of our knowledge this will the first study on the use of FL enabled with Edge computing on GIoT-based system. In order to improve the performance of the GIoT networks, this article proposes a FL enabled with edge computing for security and privacy concerns associated to GIoT networks in order to find potential solutions to mitigate these risks. Additionally, we provide some privacy preservation measures to increase network security. We use distributed FL for privacy because the FL algorithm is also sensitive to privacy concerns. Table 1 shows the comparison of the model analysis with existing studies.

IV. METHODS AND MATERIALS

A. FEDERATED LEARNING-ENABLED EDGE-BASED DESIGN

When comparing the FL model's implementation to traditional cloud-centric training methodologies, the model training on edge-enabled networks offers the following benefits: (i) As the amount of data that needs to be sent to the cloud is minimized, the network bandwidth cab be used very efficiently. In other words, aggregated and updated hyper-parameters can be communicated rather than communicating raw data for processing. As a result, data transmission costs are minimized dramatically, and backup infrastructures are relieved of their pressure. (ii) The FL model ensures proper privacy, especially when it uses edge computing in the GIoT platform since users' raw data does not need to be sent to the cloud-based on the preceding statement. This improves user privacy and minimizes the likelihood of eavesdropping to some levels, assuming that FL players and servers are not malevolent. Indeed, with improved privacy, more users will be ready to participate in shared model training, allowing for the development of better prediction frameworks. (iii) The FLS offers low latency as most ML models utilized at the edge nodes can be regularly trained and updated using FL. Similarly, major decisions, such as real-time processing can be made locally at the edge nodes or end devices in the Multi-access edge computing (MEC) architecture [65]. As a result, the latency is significantly reduced compared to when choices are taken in the cloud before being sent to end devices. This is crucial for time-sensitive operations like real-time processing in emergence for decision making in GIoT systems, where even the smallest delays can be fatal [30], [66], [67].

FL allows users to train a shared model cooperatively while maintaining their details on their devices, reducing privacy issues. As a result, FL can be used to train machine learning models in mobile edge networks. There are mainly two main

TABLE 1. Comparison of the proposed model with existing FL-based model.

Model Reference	Application	Effective use of resources	Edge	Network Throughput	Latency	Energy consumption	Security	Privacy Preservation (PP)	Local model transportation (LMT)	Centralized FL (CFL)	Aggregation algorithm (AA)
[50]	IoT	✓	×	✓	✓	✓	✓	×	×	✓	×
[64]	IoT	✓	✓	✓	✓	✓	×	×	×	×	×
[49]	IIoT	✓	×	×	×	✓	✓	✓	×	×	✓
[51]	IoT	✓	×	×	×	✓	×	✓	✓	×	×
[52]	IoMT	✓	✓	×	×	✓	✓	✓	×	×	✓
[53]	Mobile	✓	✓	×	×	✓	✓	×	×	✓	✓
[54]	Mobile	×	×	×	✓	✓	×	×	✓	✓	✓
[55]	IoT	✓	✓	×	×	✓	×	×	✓	✓	×
[56]	IIoT	✓	×	×	×	×	✓	✓	×	✓	×
[57]	IoT	✓	✓	×	×	×	✓	✓	×	✓	×
[58]	IoT	✓	✓	×	×	×	✓	✓	×	✓	×
Proposed Work	GIoT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

✓:Implemented ×: Not Implemented

entities in the FL model: (i) the participants (data owners), and the FL server (model owner). Let the set of N data owners be represented by $N = 1, \ldots, N$, each with a private dataset $D_{i\epsilon}N$. By using its dataset D_i, each data owner i to train a local model w_i and send the local model parameter only to the FL server. The $w = U_{i\epsilon}Nw_i$ are aggregated by all collected local models to generate a global model w_G. The local model is different from the traditional centralized that uses $D = U_{i\epsilon}ND_i$ to train a model w_T, the model training takes place centrally before the data from each source is aggregated.

B. PROPOSED MODEL

The proposed system adopts the same method for the radio model in [68] to compute the energy consumption. $E_{Tr}(l, d)$ is the energy consumed in transferring data bits of size l over a distance of d, as shown in Eq. 1.

$$E_{Tr}(l, d) = \begin{cases} l(E_e + E_{fs} * d^2), & if\ d \leq d_t \\ l(E_e + E_{amp} * d^4), & if\ d \leq d_t \end{cases} \quad (1)$$

where E_e denotes the energy transferred at a point of size l, E_{fs} denotes the energy supplied and E_{amp} represents for either the quantity of electrons passing across the wire or the rate at which current is flowing through the circuit.

The receiving node, on the other hand, dissipates the quantity of energy consumption $E_{Rx}(l)$, is given by Eq. 2.

$$E_{Rx}(l) = E_c * l. \quad (2)$$

where E_c is the energy consumption at E_{fs} supply. The study adopts a three-layer network in GIoT, consisting of green devices, servers, and edge nodes for GIoT devices. Wireless communication networks connect devices with limited communication and computational resources to servers. Models that map the physical status of devices and update in real-time are edge-based nodes. The server to which a device belongs establishes its edge node, where the device's history and current behavior are moving close to an edge node form by collecting and processing the device's existing key physical state. The edge of the training node $i\, edge_i(t)$ within time t can be represented as

$$edge_i(T) = \left\{F(w_i^t), f_i(t), E_i(t)\right\}, \quad (3)$$

where the currently trained parameter w_i^t of node i, $F(w_i^t)$ is the current training state of the node i, the energy consumption is represented by $E_i(t)$, and the current computational capability is $f_i(t)$ of node i.

It has worth noting that the mapped value of an edge differs from the actual value. The CPU frequency deviation $f_i'(t)$ is used to represent the difference between the device's real value and its edge translating estimate. As a result, following normalization, the edge model may be stated as follows:

$$edge_i'(T) = \left\{F(w_i^t), f_i'(t), E_i(t)\right\}. \quad (4)$$

This model may accept the device's physical state data and self-calibrate derived from the empirical divergence values while maintaining device consistency and giving back information in real-time, dynamic optimization of the physical environment is achieved.

The curator transmits the job and the populated global model w_0 in the first step of federated learning task initialization. The training node i then utilizes its data D_i to update the local model parameters w_i^t to determine the best parameter that minimizes the loss function after receiving w_0. Equation 5 gives the formula to minimizes the loss function for the best parameter is as follow:

$$F(w_i^t) = \frac{1}{D_i} \sum_{x_j, y_j \epsilon D_i} f(w_i^t, x_j, y_j), \quad (5)$$

where $F(w_i^t)$ are the true values for instances quantifying the difference between estimated running data, D_i, t representing the current local iteration index, and the samples of training data is x_j, y_j.

For the proposed model to count for malicious updates, we introduce learning quality and interaction records to

weaken the threat of malevolent data. The curator j's belief for the node i in the time slot t can be stated as follows using the subjective logic model:

$$b_{i\to j}^{t} = \frac{(1-u_{i\to j}^{t})q_{i\to j}^{t}}{f_{l}'(t)} \cdot \frac{\alpha_{i}^{t}}{\beta_{i}^{t}} \tag{6}$$

where the edge deviation of the curator j is $f_l'(t)$ to the node i, the number of positive interactions is α_i^t, and the number of malicious actions is β_i^t such as uploading indolent data, the quality of learning based is $q_{i\to j}^{t} = \frac{w_i^t - \tilde{w}}{\sum_{i=1}^{n} w_i^t - \tilde{w}}$ based on the trustworthiness of most training devices.

The mismatch between the attributes supplied by a node and the predicted value of the attributes uploaded by all nodes has a substantial impact on a client's learning performance. Eq. 6 shows that the higher the reputation value, the higher the client's learning quality in response. In addition, the curator will choose the node with the greatest trust value to improve training accuracy and prevent malicious assaults. In non-IID FL models, the curator utilizes the *FoolsGold* technique to identify untrustworthy nodes based on the steepest adjustment variety of indigenous model updates. The curator i's trust worth for the node j is stated as

$$T_{i\to j} = \sum_{t=1}^{T} b_{i\to j}^{t} + iu_{i\to j}^{t}, \tag{7}$$

where the coefficient indicating the degree of uncertainty is $i\epsilon[0, 1]$ affecting the reputation and the failure probability is $u_{i\to j}^{t}$ of the packet transmission. The curator retrieves in the global aggregation the updated status values and integrates the relevant nodes' local models w_i^t into a balanced learning algorithm. This is represented as

$$w_k = \frac{\sum_{i=1}^{N_d}\sum_{t=1}^{T} T_{i\to j} w_i^t}{\sum_{i=1}^{N_d} T_{i\to j}}. \tag{8}$$

N_d is the number of training devices, and w_k is the global parameter after thek^{th}global aggregate.

The IoT devices and local model layer, the edge computing and aggregation server layer, and the smart IoT application layer are the three levels that make up the FL-based architecture for IoT data. Each layer has an impact on the network quality of service as well as the model dependability. According to this scenario, the GIoTs environment has edge servers that are placed along the applications partway, including wireless base stations and devices equipment. The local models from the GIoT applications are combined into a global model based on their local data using the edge computing server. The GIoT applications only share their local models, rather than their local data, in order to protect their privacy. However, FL is the underlying principle of the system, which involves GIoTs environment completing learning tasks in a distributed manner.

As shown in Figure 3, in order to deliver their cloud service to end customers, cloud providers must combine sparsely distributed user traffic through a carrier's access gateway

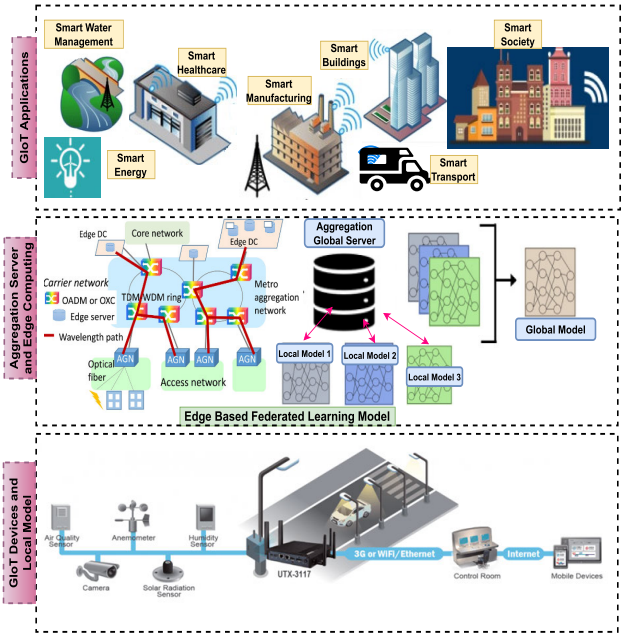

FIGURE 3. The general overview of the federated learning architecture for GIoT networks.

nodes (AGNs) and send it to datacenters. They must build a virtualized aggregation network to link AGNs with their datacenters in order to achieve this. Network services can now be moved from dedicated hardware to distributed pools of commodity servers thanks to network functions virtualization (NFV) [68], [69]. Network edge functions can be moved from dedicated hardware to dispersed pools of commodity servers thanks to network functions virtualization. Transport between access gateway nodes and such servers hosting virtual network functions (VNFs) is provided via metro aggregation networks.

Cloud providers can build their own virtualized metro aggregation networks by including NFV onto those networks. By effectively using network resources for cloud access, this raises the quality of service (QoS) of their cloud services. In order to connect datacenters with carrier's AGNs, cloud providers must use less physical network infrastructure due to intense competition and an increase in data traffic. The solution to this problem rests in how a cloud provider's virtual network is mapped onto a carrier's physical network infrastructure.

C. PROBLEM FORMULATION FOR EXPERIMENTS

Table 2 shows the network parameters that were utilized to evaluate the proposed model. With probability sampling, the number of sensor nodes in the sensing area of 100m2 is set to 200 and will remain stable. The initial energy of the sensor nodes is set to 5j, the transmitted signal is set to 20m, and the maximum size of the data packet is set to 64 bits. The trace file is created after 1000 seconds of simulation, and the statistics obtained are used to examine the results. NS-3 simulator tool and a well-known simulator have been used in conducting the experiments. The tool has been

TABLE 2. Simulation setup parameters.

Parameters	Characteristics
Sensor Nodes	200 [70]
Edge Servers	3-35
Network Attackers	5-35
Initial Energy	5j [70]
Payload size	256 bytes
Control Message	25bits
Simulation Time	1000ms
Simulation areas	100m x 100m
Sensors Deployment	Random
Max transmission	20m
Packet Size	64bits

widely used by several authors to evaluate the packet level and node behavior for realistic network state and unpredictable behavior. To get the attention of the node, the attackers flood the network with fake packets, causing communication links to become congested and sensor data to be lost. Both the source and destination sensor nodes are not assumed to be attackers in the proposed approach. Due to long-term resource budget constraints, solving the sensor node may be problematic. If the current aggregation's energy consumption is too high, there will be an energy scarcity in the future. Furthermore, because this is a nonlinear programming issue, the complexity climbs exponentially as the number of FL rounds increases. As a result, the sensor node and long-term resource budget constraints will need to be simplified.

V. RESULTS AND DISCUSSION

The proposed model scheme performance is compared with other existing works like ISEC [71], kROp [72], Diversity aware approach [73], and SWSNM [74] routing protocols, using various benchmark schemes like network overhead, energy consumption, end-to-end delay, network throughput, and route interruption. The Transistor-Transistor Logic Circuit (TTL) values ranged from 100 to 300 minutes, the number of nodes ranged from 65 to 200, and the message creation interval ranged from 15 to 35 secs to 65-75 seconds. The results in Fig. 4 and Fig. 5 show the performance evaluation for energy consumption. Under various scenarios, the results of the energy consumption show that the proposed model improves the energy consumption by 35% and 15% when compared with the existing model using several attackers and edge nodes. The energy consumption under various scenarios increases due to the transmitting of excessive control messages accordingly to the ISEC model. The proposed model still performed better than the ISEC model due to the introduction of the FL model enabled edge server. The FL model reduces the energy consumption resources and shows network stability since the data processing is done using the FL model enabled edge computing that brings processing closer to the end-users. The FL model includes a multimetric training node that obtains optimal routing decisions better than that of existing models.

The experimental result and improvement, unlike existing models that next-hop without consideration of regular link measurement, thus resulting in an additional energy cost of

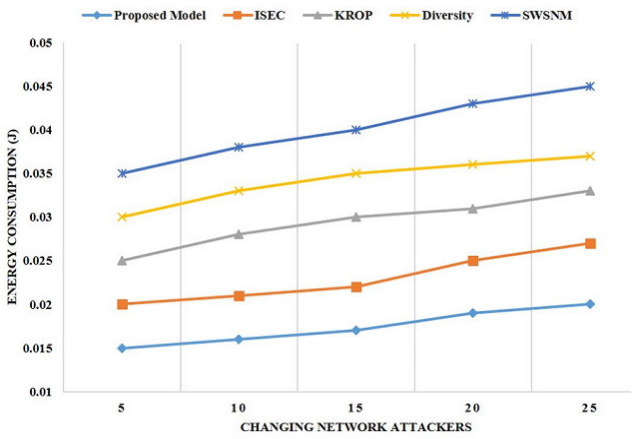

FIGURE 4. The energy consumption changing network attacker.

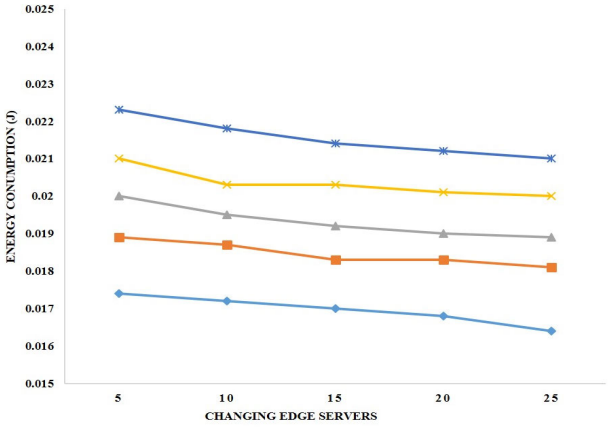

FIGURE 5. The energy consumption with changing edge servers.

reconstruction of routing paths. Although ISEC models will consider this, the performance of the model is not as that of the proposed model due to the introduction of the FL model enabling edge server in the GIoT environment. The proposed system with the consideration of nodes attributes selects the most secure routes intelligently even when compared with the ISEC model. Hence, the proposed model incorporates link asymmetry distance requirements along with the energy reduction since the processing can be done in the edge nodes with the help of the FL model enabled, reducing the energy consumption of the GIoT system sensors.

For the changing of an attacker and edge server, the proposed model performed better compared with the ISEC model with the numerical value of 3% and 1%, respectively, but when compared with another existing model, the numerical performance is 21% and 12% respectively in the case of network throughput results. Fig. 6, Fig. 7 show the results of the network throughput, this improvement was due to the introduction of the FL model enabled edge for GIoT that seriously improve energy-efficient, secure GIoT with the least network overhead and link-aware of the model. Furthermore, the proposed model was able to

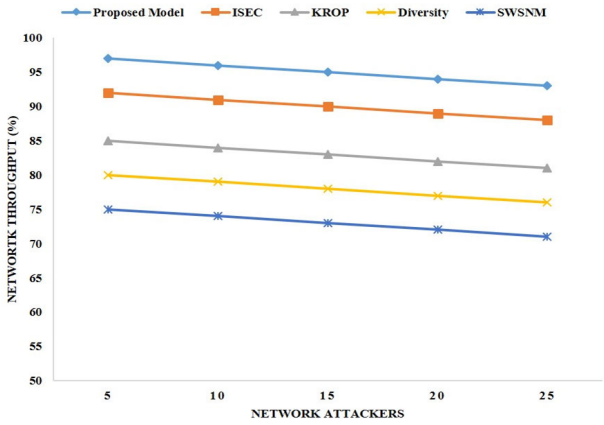

FIGURE 6. The network throughput with changing network attackers.

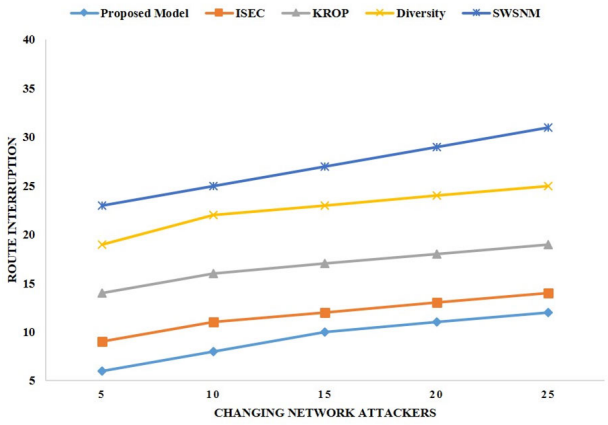

FIGURE 8. The route interruption with changing network attackers.

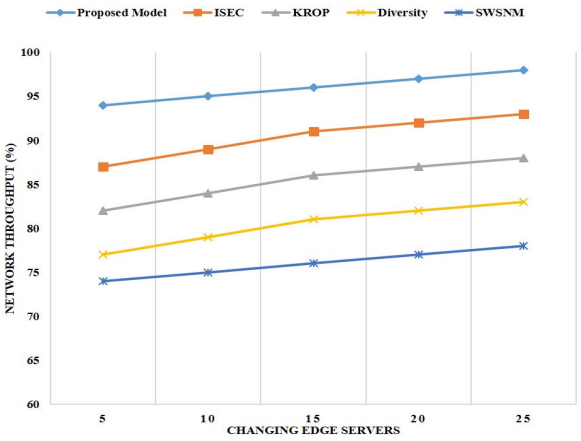

FIGURE 7. The network throughput with changing edge servers.

FIGURE 9. The route interruption with changing edge servers.

prevent the attackers from redirecting the sensors' data to other routes for high throughput, and the FL model can be used for processing network maintenance with it-enabled edge computing. The FL system will continuously be monitoring the linking routine to prevent attackers from gaining access to any penetrating data of the client in the GIoT system.

The proposed model performed better in terms of route interruption when compared with existing models with varying edge servers and attackers. This was so because the proposed model using the FL method secures communication channels within data forwarders and is very reliable. The FL model was able to secure the GIoT system by preventing attackers from gaining access to the edge nodes. The proposed model secures the constructed routes better than existing models since the FL enabled edge can be used to move data closer to the device network processing and prevent attackers from manipulating the confidentially of the system, and reduce packet drop ratio. Fig. 8 displays the changing attackers and Fig. 9 shows the edge server route interruption performance in comparison with existing models.

A. THE EFFECTS OF ENCOUNTER THRESHOLD (ET) IN NETWORK SYSTEMS ON THE PROPOSED MODEL

Encounter Threshold (ET) is a parameter in wireless communication networks, especially in protocols related to opportunistic networking or Delay Tolerant Networks (DTN) [75]. It determines the minimum level of signal strength required for two devices to establish communication or to exchange data. In networks where continuous connectivity isn't guaranteed, such as in environments with intermittent connectivity or sparse network coverage, ET becomes a crucial factor [76]. This parameter helps in optimizing communication and resource utilization in scenarios where nodes may only sporadically encounter each other due to mobility or other factors.

The ET concept is often associated with protocols like the Bundle Protocol (BP) in DTNs, where nodes communicate opportunistically by passing data when they come into close proximity or "encounter" each other [77]. ET in such protocols determines when nodes should engage in data exchange based on signal strength or other criteria. ET in network systems refers to the minimum signal strength or criteria that must be met for two network devices to establish

TABLE 3. Effect of varying encounter threshold (ET) on the network parameters.

Encounter threshold	Delivery probability	Average hop count	Overhead ratio	Dropped messages	Average latency
55%	0.902	2.245	4.934	342	**1854**
65%	0.895	2.249	4.781	321	3457
75%	0.925	2.102	4.453	301	3412
85%	**0.876**	**1.708**	4.571	**206**	4623
95%	0.919	1.723	**3.729**	228	3261

a connection or communication [78]. Varying the ET can have several effects on network parameters:

1) CONNECTIVITY AND COVERAGE

Adjusting the ET affects how devices connect and interact within the network. Lowering the threshold might result in more frequent connections among devices, potentially expanding the coverage area. Conversely, a higher ET could limit connections to stronger signals, reducing coverage but potentially improving network stability and reliability within a smaller area.

2) NETWORK DENSITY

Lowering the ET can increase network density by allowing devices with weaker signals to join the network. This could lead to more congested communication channels and increased interference. On the other hand, a higher ET might decrease network density by allowing only stronger signals, reducing potential interference and congestion.

3) POWER CONSUMPTION

Lower ET values might require devices to constantly search for and attempt connections with weaker signals, consuming more power. Conversely, a higher ET might reduce power consumption as devices spend less energy attempting to connect to signals below the set threshold.

4) LATENCY AND THROUGHPUT

Lowering the ET could potentially increase latency due to increased competition for network resources among a higher number of devices. This competition for resources might decrease overall throughput as more devices contend for access. Conversely, a higher ET might reduce latency and improve throughput by limiting the number of devices competing for network resources.

5) NETWORK STABILITY AND RELIABILITY

A higher ET could result in a more stable and reliable network as it filters out weaker and potentially unstable connections. However, this might also limit the network's adaptability and flexibility in dynamic environments. Lowering the ET might make the network more adaptable but could introduce instability due to weaker connections.

6) SECURITY

A higher ET might enhance security by allowing only stronger, authenticated devices to connect, reducing the risk of unauthorized access. Conversely, a lower ET could make the network more vulnerable to unauthorized access from weaker or less secure devices.

Based on the various effects of ET in network system for two network devices to establish a connection or communication. The proposed model varying the default setup to see how the network system will response generally. Using various values of ET with the default setup, the simulation was run severally. Table 3 shows the effect of changing the encounter threshold (ET) on the network parameters and increasing the ET. The results show a better performance of 0.876 at 85% ET on delivery probability, 1.708 at 85% ET on average hop count, 3.729 at 95% ET on overhead ratio, and 206 at 85% ET on dropped messages. This shows the great effect of the FL model-enabled edge computing on the simulation parameters. The ET was greatly improved when compared with existing models. The model performed best when the parameter was with a VALUE of 85%. At this tread hold, the dropped messages and hop count decrease as the ET increases to 85%, thus, the delivery probability increases marginally. This was so because the FL enabled edge allowed the nodes to gain more context information in the network, and more context information was the best for routing to make decisions using the proposed model.

When adjusting the ET in a network, it's crucial to consider the specific requirements of the network environment, such as coverage area, the density of devices, power constraints, and the desired balance between connectivity, stability, and security. Fine-tuning the ET involves finding a balance that optimizes network performance based on these requirements. Testing and monitoring the network's behavior after adjusting the ET can provide insights into its impact on various network parameters, allowing for further optimization if needed.

VI. THE STUDY LIMITATIONS AND FUTURE WORK

By using the least amount of energy for a large number of GIoT devices and huge data sets to train the local models, the proposed model outperformed all other methods. According to the findings, there is little variation in the suggested model energy-saving effectiveness when the number of nodes is increased from 25 to 150. The suggested model demonstrates how to balance the aforementioned elements by optimizing each GIoT device transmission power, scheduling them, and adjusting the transmission rate. The FL enabled Edge-Based GIoT systems present numerous benefits, but they also come with limitations and areas for potential future work. Here are some of these aspects:

A. THE LIMITATIONS

1) COMMUNICATION OVERHEAD

FL involves frequent communication between edge devices and the central server, leading to increased communication overhead. This could result in higher energy consumption and latency, especially in resource-constrained environments.

2) PRIVACY CONCERNS

While FL aims to preserve data privacy by keeping data on local devices, there can still be privacy risks associated with model updates transmitted during the learning process. Ensuring robust privacy measures is crucial.

3) HETEROGENEITY OF DEVICES

Edge devices in GIoT systems vary significantly in terms of computational power, storage capacity, and communication capabilities. This heterogeneity poses challenges in maintaining uniformity and efficiency in the learning process. Security Risks: Edge devices in GIoT systems may be more vulnerable to security threats compared to centralized systems. FL models can be susceptible to poisoning attacks or model inversion attacks, requiring robust security measures.

B. THE FUTURE WORK

1) OPTIMIZATION TECHNIQUES

Developing more efficient communication protocols and algorithms to reduce the communication overhead and optimize the learning process on resource-constrained edge devices.

2) PRIVACY-PRESERVING TECHNIQUES

Advancing encryption methods, differential privacy, and other techniques to enhance privacy protections during FL, ensuring that sensitive information remains secure.

3) ADAPTIVE LEARNING MODELS

Creating adaptive and dynamic learning models that can adjust to the diversity and heterogeneity of edge devices, allowing for more efficient and personalized learning.

4) ROBUST SECURITY MEASURES

Strengthening security protocols to mitigate potential vulnerabilities and threats, including exploring robust methods against adversarial attacks on FL systems.

5) ENERGY-EFFICIENT SOLUTIONS

Designing energy-efficient algorithms and hardware solutions to minimize energy consumption on edge devices, thereby contributing to a more sustainable GIoT infrastructure.

6) STANDARDIZATION AND INTEROPERABILITY

Developing standardized frameworks and protocols to enhance interoperability among different GIoT devices, ensuring seamless integration and communication in federated learning setups.

7) REAL-TIME ADAPTATION

Enabling real-time adaptation and optimization of models based on dynamic changes in edge device conditions, improving the system's responsiveness and adaptability.

Addressing these limitations and pursuing future work in these areas will contribute to the advancement and widespread adoption of FL enabled Edge-based GIoT systems, making them more efficient, secure, and privacy-preserving.

VII. CONCLUSION

Edge computing is a promising solution for managing millions of sensors and devices in GIoT. It migrates data computation and storage to the edge of the network, reducing traffic flows, bandwidth requirements, transmission latency, and extending the lifetime of nodes with limited battery resources. This approach offers a more efficient and cost-effective solution for GIoT applications. In the study, there is a comprehensive survey, analyzing how FL, edge, AI, DL, and ML based models can improve the performance of GIoT networks. The review is categorizing into different groups based on the technologies used in GIoT systems, and compare network latency, bandwidth usage, energy consumption, and overhead to evaluate how well they function. The study also examines security concerns in GIoT applications, evaluating their security strategy, availability, integrity, and confidentiality. Hence, proposed a framework for GIoT networks with FL enabled with edge-based GIoT system. FL is proposed to address computational complexity by localizing a model on GIoT devices and sharing parameters in edge nodes. This edge intelligence-aided GIoT network aims to reduce latency and energy consumption without affecting global model convergence. Finally, study compare the performance of proposed model with some of the existing work. In future works, there will be a focus on developing reliable and effective AI, DL, and ML-based algorithms to offer intelligent scheduling of packet transmission in the context of the development of channel state information over time in GIoT networks. Future research will examine more complicated scenarios, compare the suggested model with models based on algorithms, and consider channel power allocation.

REFERENCES

[1] J. B. Awotunde, R. G. Jimoh, M. AbdulRaheem, I. D. Oladipo, S. O. Folorunso, and G. J. Ajamu, "IoT-based wearable body sensor network for COVID-19 pandemic," in *Studies in Systems, Decision and Control*. Cham, Switzerland: Springer, Jul. 2021, pp. 253–275.

[2] J. B. Awotunde, S. O. Folorunso, A. K. Bhoi, P. O. Adebayo, and M. F. Ijaz, "Disease diagnosis system for IoT-based wearable body sensors with machine learning algorithm," in *Hybrid Artificial Intelligence and IoT in Healthcare*. Singapore: Springer, 2021, pp. 201–222.

[3] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

[4] X. Liu and N. Ansari, "Toward green IoT: Energy solutions and key challenges," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 104–110, Mar. 2019.

[5] C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.

[6] J. B. Awotunde, R. G. Jimoh, O. E. Matiluko, B. Gbadamosi, and G. J. Ajamu, "Artificial intelligence and an edge-IoMT-based system for combating COVID-19 pandemic," in *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*. Springer Singapore, Nov. 2021, pp. 191–214.

[7] J. B. Awotunde, A. K. Bhoi, and P. Barsocchi, "Hybrid cloud/fog environment for healthcare: An exploratory study, opportunities, challenges, and future prospects," in *Hybrid Artificial Intelligence and IoT in Healthcare*. Singapore: Springer, 2021, pp. 1–20.

[8] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[9] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[10] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 869–904, 2nd Quart., 2020.

[11] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2795–2808, Oct. 2016.

[12] M. K. Abiodun, E. A. Adeniyi, J. B. Awotunde, A. K. Bhoi, M. AbdulRaheem, and I. D. Oladipo, "A framework for the actualization of green cloud-based design for smart cities," in *IoT and IoE Driven Smart Cities*. Cham, Switzerland: Springer, Dec. 2021, pp. 163–182.

[13] J. Zhang, J. Wang, Y. Zhao, and B. Chen, "An efficient federated learning scheme with differential privacy in mobile edge computing," in *Machine Learning and Intelligent Communications*. Cham, Switzerland: Springer, 2019, pp. 538–550.

[14] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021.

[15] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, "Privacy preservation in federated learning: An insightful survey from the GDPR perspective," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102402.

[16] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen, and S. Bakas, "Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data," *Sci. Rep.*, vol. 10, no. 1, p. 12598, Jul. 2020.

[17] A. E. Varjovi and S. Babaie, "Green Internet of Things (GIoT): Vision, applications and research challenges," *Sustain. Comput., Informat. Syst.*, vol. 28, Dec. 2020, Art. no. 100448.

[18] M. Gheisari, G. Wang, and S. Chen, "An edge computing-enhanced Internet of Things framework for privacy-preserving in smart city," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106504.

[19] O. C. Abikoye, A. O. Bajeh, J. B. Awotunde, A. O. Ameen, H. A. Mojeed, M. Abdulraheem, I. D. Oladipo, and S. A. Salihu, "Application of Internet of Thing and cyber physical system in industry 4.0 smart manufacturing," in *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics* (Advances in Science, Technology & Innovation). Cham, Switzerland: Springer, 2021, pp. 203–217.

[20] P. S. Mallaburn and N. Eyre, "Lessons from energy efficiency policy and programmesin the U.K. from 1973 to 2013," *Energy Efficiency*, vol. 7, no. 1, pp. 23–41, Feb. 2013.

[21] I. D. Oladipo, M. AbdulRaheem, J. B. Awotunde, A. K. Bhoi, E. A. Adeniyi, and M. K. Abiodun, "Machine learning and deep learning algorithms for smart cities: A start-of-the-art review," in *IoT and IoE Driven Smart Cities*. Cham, Switzerland: Springer, Dec. 2021, pp. 143–162.

[22] V. A. Orfanos, S. D. Kaminaris, P. Papageorgas, D. Piromalis, and D. Kandris, "A comprehensive review of IoT networking technologies for smart home automation applications," *J. Sensor Actuator Netw.*, vol. 12, no. 2, p. 30, Apr. 2023.

[23] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[24] M. A. Albreem, A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M. N. M. Yasin, "Green Internet of Things (GIoT): Applications, practices, awareness, and challenges," *IEEE Access*, vol. 9, pp. 38833–38858, 2021.

[25] D. Zhang, S. Liu, J. Zhang, G. Li, D. Suo, T. Liu, J. Luo, Z. Ming, J. Wu, and T. Yan, "Brain-controlled 2D navigation robot based on a spatial gradient controller and predictive environmental coordinator," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 12, pp. 6138–6149, Dec. 2022.

[26] L. Corneo, N. Mohan, A. Zavodovski, W. Wong, C. Rohner, P. Gunningberg, and J. Kangasharju, "(How Much) can edge computing change network latency?" in *Proc. IFIP Netw. Conf. (IFIP Networking)*, Jun. 2021, pp. 1–9.

[27] M. Babar and M. Sohail Khan, "ScalEdge: A framework for scalable edge computing in Internet of Things–based smart systems," *Int. J. Distrib. Sensor Netw.*, vol. 17, no. 7, pp. 1–11, Jul. 2021.

[28] S. Wang, "Edge computing: Applications, state-of-the-art and challenges," *Adv. Netw.*, vol. 7, no. 1, p. 8, 2019.

[29] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[30] J. B. Awotunde, R. O. Ogundokun, and S. Misra, "Cloud and IoMT-based big data analytics system during COVID-19 pandemic," in *Efficient Data Handling for Massive Internet of Medical Things* (Internet of Things). Cham, Switzerland: Springer, 2021, pp. 181–201.

[31] S. Bebortta, D. Senapati, C. R. Panigrahi, and B. Pati, "An adaptive modeling and performance evaluation framework for edge-enabled green IoT systems," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 836–844, Jun. 2022.

[32] G. Ateniese, L. V. Mancini, A. Spognardi, A. Villani, D. Vitali, and G. Felici, "Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers," *Int. J. Secur. Netw.*, vol. 10, no. 3, p. 137, 2015.

[33] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 1322–1333.

[34] M. Chen, H. V. Poor, W. Saad, and S. Cui, "Convergence time optimization for federated learning over wireless networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2457–2471, Apr. 2021.

[35] T. T. Anh, N. C. Luong, D. Niyato, D. I. Kim, and L.-C. Wang, "Efficient training management for mobile crowd-machine learning: A deep reinforcement learning approach," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1345–1348, Oct. 2019.

[36] F. Li, B. Shen, J. Guo, K.-Y. Lam, G. Wei, and L. Wang, "Dynamic spectrum access for Internet-of-Things based on federated deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7952–7956, Jul. 2022.

[37] H. Chen, S. Deng, H. Zhu, H. Zhao, R. Jiang, S. Dustdar, and A. Y. Zomaya, "Mobility-aware offloading and resource allocation for distributed services collaboration," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 10, pp. 2428–2443, Oct. 2022.

[38] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5926–5937, Apr. 2021.

[39] N. Ge, G. Li, L. Zhang, and Y. Liu, "Failure prediction in production line based on federated learning: An empirical study," *J. Intell. Manuf.*, vol. 33, no. 8, pp. 2277–2294, May 2021.

[40] Y. Li, Y. Chen, K. Zhu, C. Bai, and J. Zhang, "An effective federated learning verification strategy and its applications for fault diagnosis in industrial IoT systems," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16835–16849, Sep. 2022.

[41] Y. Liu, S. Garg, J. Nie, Y. Zhang, Z. Xiong, J. Kang, and M. S. Hossain, "Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6348–6358, Apr. 2021.

[42] Q. Song, S. Lei, W. Sun, and Y. Zhang, "Adaptive federated learning for digital twin driven industrial Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6.

[43] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.

[44] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in industrial Internet of Things network-based on deep learning model with rule-based feature selection," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–17, Sep. 2021.

[45] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and security concerns in IoT-based healthcare systems," in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care* (Internet of Things). Cham, Switzerland: Springer, 2021, pp. 105–134.

[46] M. AbdulRaheem, G. B. Balogun, M. K. Abiodun, F. A. Taofeek-Ibrahim, A. R. Tomori, I. D. Oladipo, and J. B. Awotunde, "An enhanced lightweight speck system for cloud-based smart healthcare," in *Proc. Int. Conf. Appl. Inform.* (Communications in Computer and Information Science). Cham, Switzerland: Springer, 2021, pp. 363–376.

[47] R. O. Ogundokun, J. B. Awotunde, E. A. Adeniyi, and F. E. Ayo, "Crypto-stegno based model for securing medical information on IOMT platform," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 31705–31727, Jul. 2021.

[48] A. Salh, R. Ngah, L. Audah, K. S. Kim, Q. Abdullah, Y. M. Al-Moliki, K. A. Aljaloud, and H. N. Talib, "Energy-efficient federated learning with resource allocation for green IoT edge intelligence in B5G," *IEEE Access*, vol. 11, pp. 16353–16367, 2023.

[49] A. P. Kalapaaking, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and M. Almashor, "Blockchain-based federated learning with secure aggregation in trusted execution environment for Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1703–1714, Feb. 2023.

[50] X. Yu, L. Cherkasova, H. Vardhan, Q. Zhao, E. Ekaireb, X. Zhang, A. Mazumdar, and T. Rosing, "Async-HFL: Efficient and robust asynchronous federated learning in hierarchical IoT networks," in *Proc. 8th ACM/IEEE Conf. Internet Things Design Implement.*, May 2023, pp. 236–248.

[51] W. Liu, J. Cheng, X. Wang, X. Lu, and J. Yin, "Hybrid differential privacy based federated learning for Internet of Things," *J. Syst. Archit.*, vol. 124, Mar. 2022, Art. no. 102418.

[52] G. Srivastava, R. K. Dasaradharami, Y. Supriya, G. Yenduri, P. Hegde, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Federated learning enabled edge computing security for Internet of Medical Things: Concepts, challenges and open issues," in *Security and Risk Analysis for Intelligent Edge Computing*. Cham, Switzerland: Springer, 2023, pp. 67–89.

[53] T. Zhao, F. Li, and L. He, "DRL-based secure aggregation and resource orchestration in MEC-enabled hierarchical federated learning," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 17865–17880, Oct. 2023.

[54] D. De, S. Ghosh, and A. Mukherjee, "SocialSense: Mobile crowd sensing-based physical distance monitoring model leveraging federated learning for pandemic," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100872.

[55] A. Tashakori, W. Zhang, Z. Jane Wang, and P. Servati, "SemiPFL: Personalized semi-supervised federated learning framework for edge intelligence," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 9161–9176, May 2023.

[56] S. Yuan, B. Dong, H. Lvy, H. Liu, H. Chen, C. Wu, S. Guo, Y. Ding, and J. Li, "Adaptive incentivize for cross-silo federated learning in IIoT: A multi-agent reinforcement learning approach," *IEEE Internet Things J.*, early access, Sep. 20, 2023, doi: 10.1109/JIOT.2023.3315770.

[57] L. Osman, O. Taiwo, A. Elashry, and A. E. Ezugwu, "Intelligent edge computing for IoT: Enhancing security and privacy," *J. Intell. Syst. Internet Things*, vol. 8, no. 1, pp. 55–65, 2023.

[58] Q. Zeng, L. Zhou, Z. Lian, H. Huang, and J. Y. Kim, "Privacy-enhanced federated generative adversarial networks for Internet of Things," *Comput. J.*, vol. 65, no. 11, pp. 2860–2869, May 2022.

[59] Q. Shen, J. Wu, and J. Li, "Edge learning based green content distribution for information-centric Internet of Things," in *Proc. 42nd Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2019, pp. 67–70.

[60] L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. H. Nguyen, and C. S. Hong, "Federated learning for edge networks: Resource optimization and incentive mechanism," *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 88–93, Oct. 2020.

[61] Y. Han, D. Li, H. Qi, J. Ren, and X. Wang, "Federated learning-based computation offloading optimization in edge computing-supported Internet of Things," in *Proc. ACM Turing Celebration Conf.*, China, May 2019, pp. 1–5.

[62] M. Yang, P. Yu, Y. Wang, X. Huang, W. Miu, P. Yu, W. Li, R. Yang, M. Tao, and L. Shi, "Deep reinforcement learning based green resource allocation mechanism in edge computing driven power Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 388–393.

[63] Z. Su, Y. Wang, T. H. Luan, N. Zhang, F. Li, T. Chen, and H. Cao, "Secure and efficient federated learning for smart grid with edge-cloud collaboration," *IEEE Trans. Ind. Informat.*, vol. 18, no. 2, pp. 1333–1344, Feb. 2022.

[64] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 35–44, 2020.

[65] D. Borsatti, G. Davoli, W. Cerroni, and C. Raffaelli, "Enabling industrial IoT as a service with multi-access edge computing," *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 21–27, Aug. 2021.

[66] L. A. Saketkoo et al., "A comprehensive framework for navigating patient care in systemic sclerosis: A global response to the need for improving the practice of diagnostic and preventive strategies in SSc," *Best Pract. Res. Clin. Rheumatology*, vol. 35, no. 3, Sep. 2021, Art. no. 101707.

[67] M. Liyanage, P. Porambage, A. Y. Ding, and A. Kalla, "Driving forces for multi-access edge computing (MEC) IoT integration in 5G," *ICT Exp.*, vol. 7, no. 2, pp. 127–137, Jun. 2021.

[68] H. U. Adoga and D. P. Pezaros, "Network function virtualization and service function chaining frameworks: A comprehensive review of requirements, objectives, implementations, and open research challenges," *Future Internet*, vol. 14, no. 2, p. 59, Feb. 2022.

[69] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[70] T. Saba, A. Rehman, K. Haseeb, T. Alam, and G. Jeon, "Cloud-edge load balancing distributed protocol for IoE services using swarm intelligence," *Cluster Comput.*, vol. 26, no. 5, pp. 2921–2931, Jan. 2023.

[71] K. Haseeb, I. Ud Din, A. Almogren, I. Ahmed, and M. Guizani, "Intelligent and secure edge-enabled computing model for sustainable cities using green Internet of Things," *Sustain. Cities Soc.*, vol. 68, May 2021, Art. no. 102779.

[72] D. K. Sharma, S. K. Dhurandher, D. Agarwal, and K. Arora, "KROp: K-means clustering based routing protocol for opportunistic networks," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 4, pp. 1289–1306, Feb. 2018.

[73] Z. Zhao, G. Min, W. Gao, Y. Wu, H. Duan, and Q. Ni, "Deploying edge computing nodes for large-scale IoT: A diversity aware approach," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3606–3614, Oct. 2018.

[74] R. A. Alshinina and K. M. Elleithy, "A highly accurate deep learning based approach for developing wireless sensor network middleware," *IEEE Access*, vol. 6, pp. 29885–29898, 2018.

[75] A. P. Silva, K. Obraczka, S. Burleigh, J. M. S. Nogueira, and C. M. Hirata, "A congestion control framework for delay- and disruption tolerant networks," *Ad Hoc Netw.*, vol. 91, Aug. 2019, Art. no. 101880.

[76] R. Dhall and S. Dhongdi, "Review of protocol stack development of flying ad-hoc networks for disaster monitoring applications," *Arch. Comput. Methods Eng.*, vol. 30, no. 1, pp. 37–68, Jul. 2022.

[77] W. Khalid, N. Ahmad, S. Khan, N. U. Saquib, M. Arshad, and D. Shahwar, "FAPMIC: Fake packet and selective packet drops attacks mitigation by Merkle hash tree in intermittently connected networks," *IEEE Access*, vol. 11, pp. 4549–4573, 2023.

[78] S. S. Sefati and S. Halunga, "Ultra-reliability and low-latency communications on the Internet of Things based on 5G network: Literature review, classification, and future research view," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 6, p. e4770, Apr. 2023.

JOSEPH BAMIDELE AWOTUNDE is currently a Lecturer with the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria. He was a part of the team that won the Artificial Intelligence for Females in Science Technology, Engineering and Mathematics (AI4FS) Grant sponsored by the Royal Academy of Engineering (Higher Education Partnerships in Sub-Saharan Africa (HEP SSA) 22/24). He has to credit more than 150 publications in reputable outlets, such as Elsevier, Springer, and Hindawi among others covering journals, edited conference proceedings, and chapters in books. His research interests include artificial intelligence, the Internet of Things, cybersecurity, information security, social computing, bioinformatics, and biometrics. He is a member of many professional bodies within and outside Nigeria, such as the International Association of Engineers and Computer Scientists (MIAENG), the Computer Professional Registration Council of Nigeria (MCPN), and the Nigeria Computer Society (MNCS).

SAMARENDRA NATH SUR (Senior Member, IEEE) received the M.Tech. degree in digital electronics and advanced communication from Sikkim Manipal University, in 2012, and the Ph.D. degree in MIMO signal processing from the National Institute of Technology (NIT) Durgapur, in 2019. He is currently an Assistant Professor (SG) with the Department of Electronics and Communication Engineering, Sikkim Manipal Institute of Technology, Sikkim Manipal University. He has published several SCI/Scopus-indexed international journal and conference papers. His current research interests include broadband wireless communication (MIMO and spread spectrum technology), advanced digital signal processing, remote sensing, and radar image/signal processing (soft computing). He is a member of the IEEE Internet of Things Technical Community, the IEEE Signal Processing Society, and the Institution of Engineers (IEI), India. He is also a regular reviewer of reputed journals, namely IEEE, Springer, Elsevier, Taylor and Francis, IET, and Wiley. He is currently editing several books with Springer Nature, Elsevier, Routledge, and CRC Press. He is serving as an Associate Editor for *International Journal on Smart Sensing and Intelligent Systems* (SCOPUS) and a guest editor for topical collection/special issues of the journal, such as Springer Nature and MDPI.

RASHEED GBENGA JIMOH (Senior Member, IEEE) was the Head of the Department, the Deputy Director of the Ilorin Business School, and the Dean of the Faculty. He is currently a Professor with the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, with almost two decades of university teaching, research, and administrative experience. He has to credit more than 100 publications in reputable outlets covering journals, edited conference proceedings, and chapters in books. He has successfully supervised more than 40 master's dissertations and 16 Ph.D. theses. He has equally won a number of research grants. His research interests include cybersecurity, information systems, human–computer interactions, and soft computing. He is a member of many professional bodies within and outside Nigeria.

DAYO REUBEN AREMU was the Head of the Department of Computer Science, University of Ilorin. He is currently an Associate Professor with the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, with more than two decades of university teaching, research, and administrative experience. His research interests include software engineering, grid computing, big data analytics, information security, and artificial intelligence. He has to credit a number of publications in reputable outlets covering journals, edited conference proceedings, and chapters in books. He has successfully supervised several master's dissertations and Ph.D. theses. He is a member of the Nigeria Computer Society (NCS) and the Computer Professional of Nigeria (CPN).

DINH-THUAN DO (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical engineering from Vietnam National University Ho Chi Minh City (VNU-HCM), in 2007 and 2012, respectively. Prior to joining academia, he was a Senior Engineer in the telecommunications industry with VinaPhone Mobile Network (the biggest cellular network provider in Vietnam) (2003–2009). Prior to joining the University of Mount Union, he was a Research Scientist with the University of Colorado Denver, in 2022, and The University of Texas at Austin, in 2021. His publications include more than 120 SCIE/SCI-indexed journal articles, seven edited books (IET, CRC, and Springer), and more than 50 international conference papers. He was a recipient of the 2015 Golden Globe Award by the Vietnamese Ministry of Science and Technology (top 10 outstanding scientists nationwide). He also received the Medal of Creative Young Talents, in 2015. Recently, he was rewarded as the Best Editor of *ICT Express* (Elsevier), in July 2023. He serves as an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and *Computer Communications* (Elsevier). He has also served as a Lead Guest Editor/Guest Editor in more than 20 special issues of journals, such as *Physical Communications* (Elsevier) and *Annals of Telecommunications* (Elsevier).

BYUNG MOO LEE (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of California at Irvine, Irvine, CA, USA, in 2006.

He is currently an Associate Professor with the Department of Intelligent Mechatronics Engineering, Sejong University, Seoul, South Korea. Prior to joining Sejong University, he had ten years of industry experience, including research positions with the Samsung Electronics Seoul Research and Development Center, Samsung Advanced Institute of Technology (SAIT), and the Korea Telecom (KT) Research and Development Center. During industry experience, he participated in IEEE 802.16/11, Wi-Fi Alliance, and 3GPP LTE standardizations. He also participated in Mobile VCE and Green Touch Research Consortiums, where he made numerous contributions and filed a number of related patents. His research interests include wireless communications, signal processing, and machine learning applications. He was the Vice Chairperson of the Wi-Fi Alliance Display MTG, from 2015 to 2016.