scientific reports

Check for updates

OPEN

A hybrid federated learning framework with generative AI for privacy-preserving and sustainable security in IOT-enabled smart environments

Venkadeshan Ramalingam[1]✉, Basant Kumar[2], Shashi Kant Gupta[1,3], Deema Mohammed Alsekait[4] & Diaa Salama AbdElminaam[5,6]✉

The dramatic increase in IoT devices in a smart ecosystem like smart cities, transportation systems, and healthcare and industrial automation has greatly improved network connectivity and data-driven informed decisions. But this extraordinary level of connectivity generates important concerns associated with sensitive information and security risks. Therefore, this study proposes a novel framework for secure and sustainable IoT network and devices through a combination of a Hybrid Federated Learning Framework and GenAI. The proposed framework focuses on extending a secure learning platform for all different IoT devices through a Federated Learning Framework and utilizing GenAI capabilities for advanced information augmentation and customized anomaly detection. To improve the level of guaranteed privacy, this framework will utilize differential privacy techniques and a blockchain-assisted model validation process. Moreover, techniques for energy-efficient model optimization and edge intelligence in making decisions are considered to improve sustainability. The proposed work will examine and develop this novel hybrid model through intensive simulations and lab-based testing for its application in a building and energy management field. The impact will include a new federative generative architecture that offers enhanced cyber threat resilience, lower overhead costs of communication, and ensures user confidentiality of data. The end goal of this proposed project is to contribute positively towards advancing the state-of-the-art in sustainable AI for a secure and environment-conscious IoT.

Keywords Hybrid federated learning, Generative AI, Privacy-preserving, Sustainable security, IoT security, Data privacy, Distributed machine learning

The advancement of Internet of Things (IoT) technology has significantly impacted contemporary infrastructure like smart cities, transportation systems, healthcare, and industrial automation through large-scale connections and autonomous computing. However, critical issues have arisen in relation to data security and privacy due to continuous information transfer and generation in IoT devices[1]. In traditional centralized ML-based systems, aggregated information needs to reach cloud servers for computation. The process is associated with security concerns for information and network traffic due to large volumes of information.

Federated Learning (FL) has lately appeared as a promising distributed learning technique to address the above-mentioned issues to train a common model together without sharing actual data. FL maintains data locality and hence ensures greater privacy and less transfer of sensitive information. However, in spite of its many benefits, FL still faces some challenges while employed in an IoT setting regarding its susceptibility to inversion attacks, communication overheads, heterogeneity issues in devices, and power limitations[2,3]. So far,

[1]Lincoln University College, 47301 Petaling Jaya, Selangor Darul Ehsan, Malaysia. [2]Modern College of Business & Science, Muscat, Oman. [3]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, India. [4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. [5]Faculty of Computers and Artificial Intelligence, Benha University, Benha, Egypt. [6]Jadara Research Center, Jadara University, Irbid, Jordan. ✉email: pdf.Venkadeshan@lincoln.edu.my; diaa.salama@miuegypt.edu.eg

many surveys have highlighted that overcoming all above-mentioned limitations is a critical need to ensure efficient and secure FL implementations in resource-constraint IoT networks[1–4].

Privacy and secure aggregation challenges

Although FL is known to provide added guarantees to user privacy as it ensures that all the data is stored locally and not centrally, there is still a risk of disclosing sensitive information in model updates via gradient-based inference and/or reconstruction attacks. Various methods have recently emerged for securing FL communications. Some of those methods include differential privacy (DP), homomorphic encryption (HE), and secure multiparty computation (SMC) approaches to secure FL communications[2,5]. To provide added resilience to FL against malicious interference and provide enhanced trust in FL systems, blockchain-based FL frameworks have recently emerged for ensuring traceability and tamper-proof model aggregation[6].

System heterogeneity and scalability

The reason is that IoT environments are heterogeneous devices with different computation abilities and network capabilities. The heterogeneity will cause a non-independent and identical distribution (non-IID) of data. As a consequence, it will adversely affect model divergences and performances[3]. In this scenario, more advanced aggregation techniques like FedProx, FedAvgM, and hierarchical FL have emerged to address this concern. Recently developed approaches like HED-FL and hierarchical clustering-based FL have attuned to better converge and manage resources in heterogeneous IoT environments[3,4]. The significance of adaptive client sampling techniques and approaches for compression in this context has emerged in these studies to address accuracy and efficiency simultaneously.

Energy efficiency and sustainability

Another important factor is energy usage in large-scale IoT implementations. Edge devices run on batteries and have limited bandwidth. Several iterations are required in FL for training a model. Hence, repeated model transfer can significantly drain resources and impact sustainability[3]. To make this more optimal and less resource-intensive, methods like in-network computation, model reduction, selective participation methods, and energy-conscious scheduling strategies have been proposed to decrease energy usage while keeping the model accuracy level high[4,5]. Sustainable FL is rapidly considered an important catalyst in making a sustainable smart environment and energy-efficient AI for edge devices.

Generative AI for data augmentation and security

Generative Artificial Intelligence (GenAI) approaches like Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and diffusion models are significantly impacting data generation and security analysis. In scenarios related to intrusion and anomaly detection in IoT environments, generative approaches can generate realistic samples for better generalization and adversarial analysis[2,7]. Modern developments have assisted in extending generative approaches in federated learning infrastructure like FedGAN and FedVAE to provide secure and adaptive learning over distributed devices[2,7]. The proposed approaches can contribute to enhanced security and resistance to anomalies in privacy-focused scenarios.

Blockchain and trustworthy federated orchestration

The integration of blockchain technology with FL brings an added level of transparency and trust. In blockchain-based FL systems, the aggregation servers are made foolproof against single-point failures and provide immutability for updates to models through incentives 666. Research has revealed that integration with blockchain technology can greatly improve the auditability and verifiability of models in a privacy-preserving FL technique[6].

Research gap and motivation

However, a knowledge gap still exists in this area for a holistic and unified framework that combines federated learning, generative AI, and sustainability concepts in a secure and privacy-preserving platform. The literature has described individual aspects like protecting user privacy during ML execution and reducing inter-device communications. However, nobody has expressed a need for a unified platform that optimizes multiple needs like intelligence in generating inputs for ML and its robustness against adversarial attacks for sustainable and secure IoT systems in a power-efficient and scalable architecture[6,7]. The proposed system will address this literature gap.

Research objective

To address this reality, this research proposes a Hybrid Federated Learning Framework that is coupled with Generative AI to promote sustainable and secure functioning for IoT-based smart spaces. Specifically, this proposed framework seeks to (a) improve privacy preservation via differential and blockchain-supported aggregation methods, (b) apply generative AI for generating virtual data and building anomalies, and (c) manage energy and communications spending via edge-based adaptive learning. The proposed combination is believed to ensure strength against cyber-attacks while still keeping sustainability and model accuracy.

Literature review

Federated learning (FL) and heterogeneity-aware methods

Federated learning allows for collaborative model training without requiring centralized storage of raw data. The FedAvg algorithm (McMahan et al., 2017) demonstrated communication-efficient collaborative training but suffers from slow convergence or divergence under non-IID data and device heterogeneity[8]. FedProx and related

methods improve robustness under heterogeneous data distributions by adding proximal terms and adjusting local solvers[9,10]. Empirical studies confirm that FedAvg alone is insufficient for real-world IoT deployments with diverse devices and non-IID workloads, motivating personalization, hierarchical aggregation, and adaptive client selection[2,9]. Federated Learning (FL) has recently been identified as an important privacy-preserving machine learning paradigm, where the seminal work FedAvg provided the first client-server aggregation protocol without the exchange of raw data[8]. Nonetheless, classic FL has proven to be associated with important limitations in the context of IoT networks, namely non-IID conditions, communication costs, as well as scalability[11].

Privacy-preserving FL: differential privacy, secure aggregation, homomorphic encryption

While FL does not share raw data, model updates may leak private information through gradient inversion or membership inference attacks. To address this, the literature proposes:

- Differential privacy (DP): adding calibrated noise to updates;
- Secure aggregation / MPC: server aggregates encrypted updates without learning individual contributions;
- Homomorphic encryption (HE): allows arithmetic on encrypted updates.

For example, Ma et al. (2021) proposed multi-key HE schemes for FL (xMK-CKKS), achieving strong confidentiality even under collusion but at the cost of computation and key management overhead. DP offers a quantifiable privacy budget but may reduce model utility when local datasets are small, as is common in IoT[9]. Overall, privacy-preserving FL for IoT requires balancing security, energy, and model performance.

Federated generative models (FedGAN, FedVAE)

Generative AI models, such as GANs, VAEs, and diffusion models, are effective for data augmentation, anomaly detection, and adversarial training in privacy-sensitive contexts. Federated variants like FedGAN and FedVAE enable distributed training of generative models without sharing raw data, producing synthetic samples locally or collectively[10,12]. Rasouli et al. (2020) have proved that FedGAN is capable of producing realistic surrogate data under non-IID conditions while keeping feasibility in place. However, the stability of the GAN and cost of communication are still important concerns for fed-GAN[10]. Later on, Jin et al. (2023) emphasized security concerns like back-door attacks in fed-GAN for federated generative modeling[12]. For improved privacy, diversity, and data quality, the use of Generative AI models, like GANs, VAEs, has been incorporated in the FL process. The research proposed FedGAN, FedVAE, aims to optimize the generation of decentralized data, but the proposed approach has demonstrated large computational complexity, model divergence, and lack of scalability when running in resource-constrained IoT devices[3]. In addition, GAN models often demonstrate mode collapse in the non-IID IoT setting.

Energy- and communication-efficient FL in IoT

Energy and communication costs are important factors in battery-driven and network-constrained IoT devices. Cost reduction through hierarchical aggregation, client choice, model reduction, and in-network computation is common. The HED-FL framework proposed hierarchical edge and cloud aggregation to achieve minimum energy and communication costs while keeping high model accuracy (De Rango, 2023)[13]. Energy-efficient FL methods like selective participation and pruning were cited in a literature review by Baqer et al. in 2024 for their feasibility of deployment[14]. In IoT-based FL scenarios that are battery-driven and network-constrained, hierarchical and edge-based aggregation has garnered interest.

Blockchain/ledger-assisted FL

The blockchain has been coupled with FL to improve its audibility and resistance to tampering. The blockchain facilitates immutability and verifiability of the models and incentives in a decentralized fashion[15,16]. However, blockchain incurs additional latency and overhead in storage size. Lightweight blockchains can address this concern. The addition of blockchain to FL raises transparency and makes it more resilient to poisoning and backdoors.

FL for anomaly and intrusion detection in IoT

Federated learning has been used anomaly and intrusion detection in heterogeneous IoT networks as well as in IIoT. Federated DNNs are capable anomaly detection without requiring centralized data. However, few methods are available for detecting rare events and handling imbalances in classes. Wang et al. (2023) showed that hybrid architectures combining local unsupervised representations with global supervised updates enhance detection performance while preserving privacy[17]. Federated generative models further improve performance by generating synthetic samples for minority classes, reducing detection bias[10,17].

Attacks and defenses in FL

FL is vulnerable to poisoning, backdoor, and inference attacks. Bagdasaryan et al. (2020) demonstrated model-replacement backdoor attacks that compromise global model integrity[18]. Defenses include robust aggregation (median, trimmed mean), anomaly detection on updates, Byzantine-resilient methods, and secure logging via blockchain[11,15]. Federated generative models introduce additional attack vectors; secure protocols and anomaly detection for generative updates are necessary[12]. Recently, the emphasis has been on diffusion models, specifically Denoising Diffusion Probabilistic Models, as a stable approach over GANs to produce quality synthetic data[6]. Although the potential of federated diffusion models exists, the multi-step iterative process involved in sampling can make it quite computationally intensive, thereby less suitable for resource-constrained IoT devices[11]. The prevailing methods deal mainly with anomaly detection, privacy, but neglect energy efficiency,

Paper	Scope / contribution	Strengths	Weaknesses	IoT suitability
[8]	Core FL algorithm	Communication-efficient baseline; simple	Sensitive to non-IID data; poor heterogeneity handling	Baseline; needs adaptation
[9]	Heterogeneity-aware FL	Stable under non-IID; robust convergence	Hyperparameter tuning	Improved for IoT heterogeneity
[11]	Cryptographic FL aggregation	Strong confidentiality	Computational/key overhead	Promising w/ optimizations
[10]	Federated generative models	Local synthetic data generation	GAN instability; high communication	Experimental for IoT
[12]	Security of federated generative models	Highlights new attack surfaces	Few practical defenses	Critical concern
[13]	Hierarchical energy-aware FL	Reduced energy & communication	Trust dependency on cluster heads	High
[14]	Energy-efficient FL	Practical strategies: pruning, selective participation	Limited cross-IoT evaluation	Moderate; implementation needed
[15,16]	Blockchain-assisted FL	Transparency; incentives	Consensus overhead	Needs lightweight permissioned design
[18]	Backdoor/poisoning attacks	Demonstrates attack potency	Defense trade-offs	High concern
[17]	Federated anomaly detection	Privacy-preserving detection	Needs augmentation & robust defenses	High
[19]	Secure data sharing in 6G IoT healthcare	Data integrity, blockchain auditability	Energy efficiency not analyzed	Healthcare IoT; mid-resource devices
[20]	IoT intrusion detection with blockchain	High detection accuracy, secure key management	High computational cost, no data privacy	Mid-tier IoT devices
[21]	Blockchain-enhanced IDS	Tamper-resistant, distributed support	Energy/latency overhead, no generative AI	Distributed IoT; high-resource nodes
[22]	Explainable DL for CPS	High accuracy, interpretable	Limited privacy, computationally intensive	Industrial IoT; high-resource devices

Table 1. Comparative summary.

Gap	Proposed solution	Expected outcome
Integration of privacy, security, and sustainability	Hybrid FL + GenAI framework with DP, HE, blockchain, hierarchical aggregation	Holistic privacy-preserving, energy-efficient, secure IoT FL
Federated generative models are unstable and attack-prone	Robust federated generative training; anomaly detection on updates	Stabilized generative training; reduced backdoor risks
HE/DP overhead for IoT devices	Hierarchical aggregation, selective compression, adaptive DP	Feasible deployment on constrained IoT nodes
Lack of realistic IoT testbeds	End-to-end IoT deployment with sensors, gateways, cloud	Validated performance: privacy, energy, accuracy, robustness
Rare-event anomaly detection challenges	Federated generative augmentation; hybrid supervised-unsupervised models	Improved detection for minority/rare eve

Table 2. Gap-solution-outcome mapping.

trust establishment based on blockchain technology, as well as the needs of differential privacy[7]. The identified shortcomings trigger the search for an integrated solution.

Comparative analysis of representative works

Table 1 is a compact comparison of selected research works that highlight design decisions, evaluation settings, and remaining gaps.

Research gap and proposed solution mapping

Table 2 addresses each identified gap to specific mechanisms in the proposed hybrid framework. These gaps motivate a hybrid framework that: (i) Integrates federated generative models for augmentation and anomaly modelling, (ii) layers DP/HE/blockchain-based verification for privacy and trust, and (iii) uses hierarchical & energy-aware orchestration (clustered aggregation, compression, selective updates) to make the scheme practical for heterogeneous IoT deployments.

Methodology

The proposed research develops a Hybrid Federated Learning Framework with Generative AI (HFL-GAI) designed to address privacy, security, and sustainability challenges in heterogeneous IoT-enabled smart environments. The framework integrates: (i) federated learning for distributed collaborative model training, (ii) generative AI for data augmentation and anomaly modeling, (iii) privacy-preserving mechanisms (differential privacy, homomorphic encryption, secure aggregation), (iv) energy-efficient orchestration, and (v) blockchain-based trust verification. The methodology has five core modules that cover important challenges emerging in the literature review.

System architecture

Overview

The system has a total of three hierarchical layers:

A. IoT device layer:

- Consists of IoT devices (sensors, actuators, wearables, gateways) collecting data locally.
- Performs local model training on lightweight ML/DNN models using device-specific data.
- Applies local differential privacy (LDP) mechanisms before sending updates.

B. Fog/cluster layer:

- Groups edge devices into clusters for hierarchical aggregation.
- Cluster heads aggregate encrypted model updates using homomorphic encryption (HE) and transmit the intermediate models to the cloud layer.
- Cluster-level generative AI models (FedGAN/FedVAE) synthesize minority-class samples for anomaly detection tasks.

C. Cloud layer:

- Performs global aggregation of cluster-level models.
- Coordinates a generative AI module to improve the generated datasets.
- Implements blockchain ledger for auditable updating and secure cluster-level contribution verification.

How generative AI enhances privacy and security:

- Synthetic Data Creation: Generative AI can build realistic yet fictional datasets that can be analyzed without requiring actual and sensitive information.
- Differential Privacy: The generative models can either implement differential privacy as a technique within its learning process or utilize it as a noise generator for perturbation.
- Adversarial Learning for Security: The generated samples obtained from GANs can find application in generating adversarial examples for testing and improving intrusion detection systems. Moreover, generative methods can model normal system behavior to improve anomaly detection.
- Data Masking/Perturbation: On-device generative capabilities can be used for noise addition to preserve confidentiality.

Figure 1 above shows hierarchical federated learning in a system consisting of different aspects of Generative AI to ensure enhanced privacy, security, and sustainability for different IoT-based smart domains. The different models within this hierarchical federated learning system are all developed and enabled through private, offline datasets. Rather than requiring all devices to share their respective sensitive datasets through a central server for analysis and learning within their respective AI models, all devices within this system are designed to securely share only their model updates with a central Aggregation Global Server. The server compiles all these updates to develop a more superior and enhanced global AI model. However, this enhanced global AI model is always shared with all devices.

Federated learning algorithm

Federated Learning (FL) makes it possible to perform distributed model training for ANN-based AI without transferring unencrypted data from devices of an IoT network. In this scenario, a device D_i trains a local model W_i^t from its dataset and sends only encrypted weights to an edge aggregator. The FL module enhances the FedAvg framework for heterogeneity and energy efficiency:

A. Client selection and scheduling:

- Clients are chosen depending on energy budget, network status, and computational capabilities.
- Adaptive selection will ensure that nodes with low batteries and/or low bandwidth are less likely to contribute.

B. Hierarchical aggregation (HFL):

- Local models ω_i^t are trained at IoT devices for EEE local epochs.
  - Cluster heads perform intermediate aggregation:

$$w_c^t = \frac{\Sigma_{i \in c} n_i \omega_i^t}{\sum_{i \in c} n_i}$$

where n_i is the local dataset size of device i in cluster C.

- Global aggregation at the cloud:

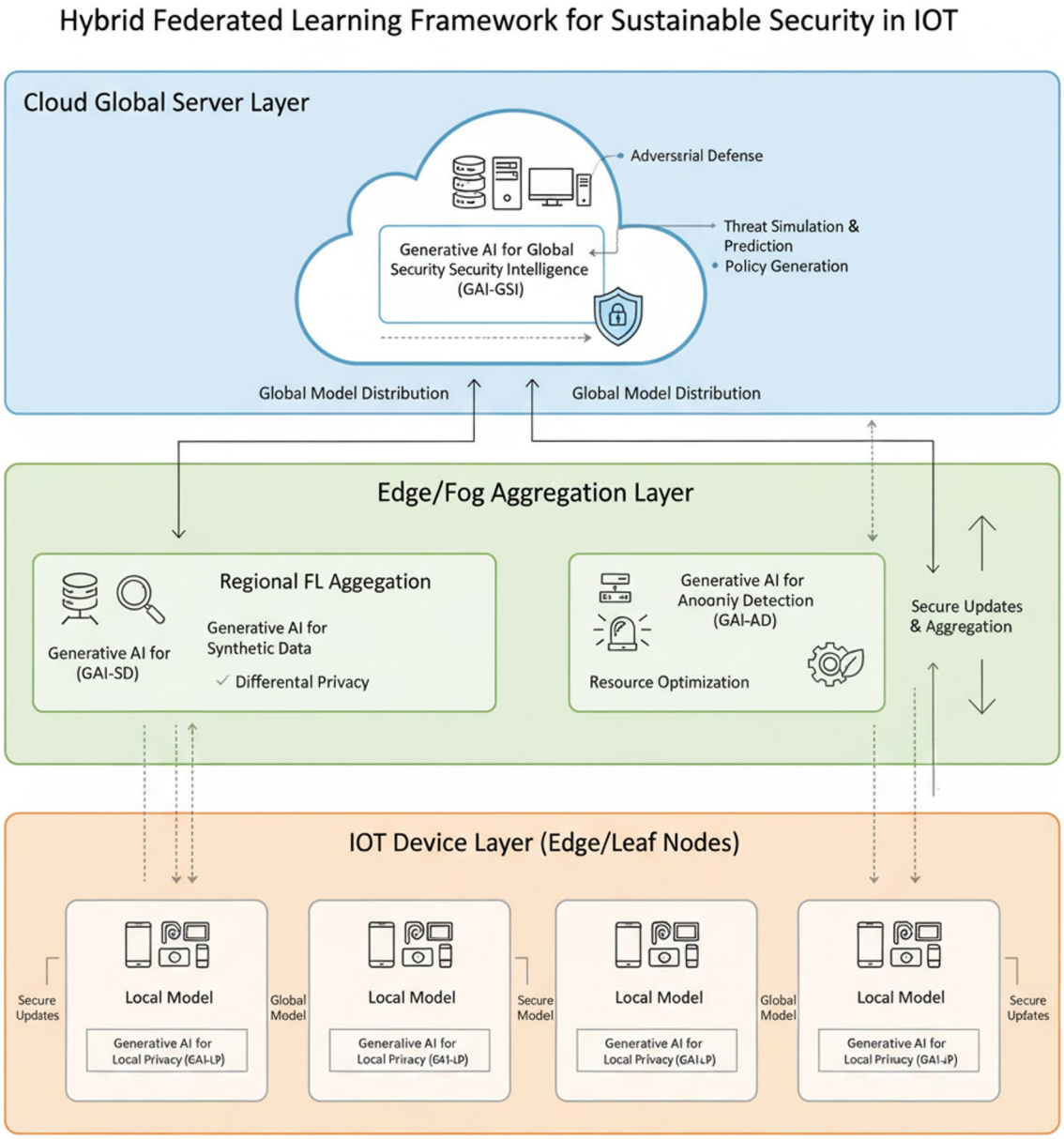

Fig. 1. Hybrid federated learning framework.

$$W^{t+1} = \frac{\sum_{c\in\ clusters}\eta_{\ c}W_c^t}{\sum_{c\in\ clusters} n_c}$$

C. Adaptive learning rates and proximal terms:

- Heterogeneous clients use local learning rates n_i and FedProx-style proximal regularization to reduce divergence under non-IID data:

$$\mathcal{L}_i\left(\omega_{\ i}\right) + \frac{\mu}{2}\left|\left|\omega_{\ i} - w^t\right|\right|^2$$

- Ensures stable convergence for different IoT devices[23,24].

Figure 2 shows a hybrid federated learning framework designed specifically for loading monitoring. The figure shows a central server that manages updates coming from multiple training clusters that consist of clients with associated local datasets. The structure is designed to promote collaborative learning while still encompassing confidentiality.

Each IoT edge device k keeps a local generative model G_k(GAN or VAE). The generator model updates based on the local dataset D_k, are as follows:

$\theta_k^{t+1} = \theta_k^t - \eta \nabla_{\theta_k} \mathcal{L}_k(G_k, D_k)$Where: θ_k - local model parameters, η - learning rate, $\mathcal{L}_k$ - local loss.

The differential privacy guarantee can be achieved through the following operations performed on the gradients:

$$\tilde{\nabla}_{\theta_k} \mathcal{L}_k = \text{clip}(\nabla_{\theta_k} \mathcal{L}_k, C) + \mathcal{N}(0, \sigma^2 C^2 I)$$

Generative AI integration

The Generative AI layer focuses on handling heterogeneity and datasets in distributed IoT environments. The Generative Adversarial Networks and Variational Autoencoders techniques are employed to generate additional data that can fill up less common classes as well as mimic unusual operational scenarios[25,26].

In this setup, every generator G network learns the distribution of latent features from its respective domain, while its authenticity is confirmed through the discriminator. The federative generative network (FedGAN/FedVAE) improves global model-generalization performance in a non-IID scenario. Moreover, generated samples can substitute actual ones to add a new level of security for clients.

Federated generative model (FedGAN / FedVAE) module:

A. Purpose:

- Synthetic data generation for handling imbalance in classification problems and for carrying out adversarial testing.

B. Training workflow:

- Each cluster trains a local generative model on-device using real data.
- Generative parameters are encrypted and shared with the cloud for federated aggregation.
- The global generator is redistributed to clusters for local sample generation.

C. Use in anomaly detection:

- Synthetic anomalies augment training datasets.
- Hybrid model combines local unsupervised representations with global supervised classifiers.
- Increases accuracy for detection of rare occurrences in IoT data[27–30].

After local epochs E, the edge devices will send the parameters back to the central server. The global aggregation is performed by weighted average:

$\theta_G^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{t+1}$Where: $n_k = \mid D_k \mid$ is the size of the local dataset, $n = \sum_{k=1}^{K} n_k$, K - total number of participating devices.

In generative models, the aggregation involves only the generator parameters, while the discriminators, encoders, can stay local if privacy issues are a concern.

The HFL-GAI model combines the concept of federated learning (FL), and generative models to create effective, secure, power-efficient, and privacy-preserving IoT intelligence. Each edge IoT device k, a local generative model G_k(VAE or GAN) on its private data D_k will be trained, parameters via θ_k^{t+1} are being updated with differential privacy imposed through noise addition and gradient clipping. Using the weighted average: θ_G^{t+1} the local updates at a server or fog node are periodically aggregated to produce a global generator.

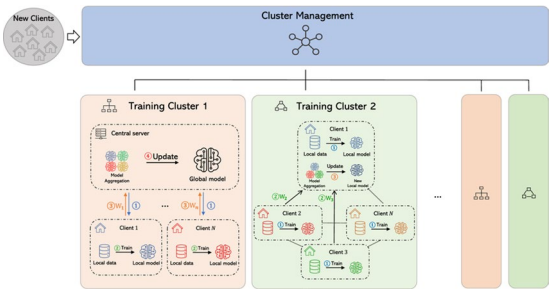

Fig. 2. Architecture of load monitoring.

Privacy and security mechanisms

A. Differential privacy (DP):

- Noise is added to the gradients/model parameters before sharing:

$$\widetilde{g_i} = g_i + N\left(0, \sigma^2\right)$$

- Ensures confidentiality of individual data inputs[24,31].

B. Homomorphic encryption (HE) / secure aggregation:

- Cluster-level aggregation of encrypted weights to ensure that cloud is not able to get direct updates[31,32].
- Encrypts model parameters, allowing secure computation on ciphertexts.
- Aggregator performs: $Enc\left(W^{t+1}\right) = \sum Enc\left(W_i^t\right)$

C. Blockchain ledger for trust verification:

- Maintains an immutable record of model updates.
- Enables post-hoc auditing and detection of malicious or anomalous updates[33].

D. Robust aggregation & anomaly detection:

- Updates are analyzed for outliers via robust aggregation methods (trimmed mean, median).
- Malicious client detection prevents backdoor/poisoning attacks[34].

Energy-efficient orchestration

Energy consumption in resource-limited IoT devices is optimized through adaptive orchestration policies[35]. The framework dynamically selects participating devices based on their residual energy, connectivity stability, and computation capacity. A reinforcement-learning-based scheduler adjusts batch sizes and learning rates to balance accuracy and energy cost. The total energy is modeled as

$$E_{total} = E_{comp} + E_{comm}$$

.

where computation and communication energies are minimized by optimizing the participation probability P_{opt}. Edge-level aggregation further reduces long-haul transmissions to the cloud, contributing to sustainable operation.

A. Adaptive participation:

- Low-resource devices participate less frequently.
- High-energy devices handle more computation.

B. Model compression & sparsification:

- Weight pruning and gradient sparsification reduce communication overhead.
- Cluster heads compress intermediate models before forwarding to cloud.

C. Hierarchical scheduling:

- Clusters are formed dynamically based on network topology and device energy levels.
- Reduces global communication rounds while maintaining convergence.

Input : Local datasets $\boldsymbol{D_i}$ at devices, initial global model $\boldsymbol{W^0}$, generative model $\boldsymbol{G^0}$, privacy budget ϵ.

Output : Privacy-preserving global FL model $\boldsymbol{W^T}$ and federated generative model $\boldsymbol{G^T}$.

For each round t = 1 … T:

a. Select subsets of IoT devices based on energy/network availability.

b. Train local model $\boldsymbol{\omega_i^t}$ with proximal regularization and local DP noise.

c. Train local generative model $\boldsymbol{g_i^t}$ (GAN/VAE).

d. Encrypt local model and generative parameters; send to cluster head.

e. Cluster head aggregates: $\boldsymbol{W_c^t = \frac{\Sigma_i n_i W_i^t}{\Sigma_i n_i}}$

f. Cloud aggregates cluster models: $\boldsymbol{W^{t+1} = \frac{\Sigma_c n_c W_c^t}{\Sigma_c n_c}}$

g. Update global generative model $\boldsymbol{G^{t+1}}$ and redistribute.

h. Log all updates on blockchain for verification.

Algorithm 1. HFL-GAI framework.

The HFL-GAI algorithm is a hierarchical federated learning framework that integrates generative AI and privacy protection. It starts with local datasets on IoT devices, an initial global model, and a generative model. In each training round, a subset of devices is selected based on energy and network conditions. Each device trains its local model with proximal regularization and adds differential privacy noise, while also updating a local generative model (GAN/VAE) to enhance data privacy. The locally trained models and generative parameters are encrypted and sent to a cluster head, which aggregates them into a cluster model. These cluster models are then aggregated at the cloud level to update the global model. The global generative model is updated and redistributed to devices, while all updates are logged on a blockchain for verification. The result is a privacy-preserving global federated model and a federated generative model for secure and efficient edge intelligence. The HFL-GAI model combines VAEs as well as GANs to achieve consistency, accuracy, as well as resource efficiency for diverse IoT networks. VAEs are preferably utilized in resource-constrained edge nodes as they are stable, provide probabilistic latent modeling, as well as robustness in non-IID conditions, but generate slightly blurry synthetic data.

Additionally, GANs model accurate data well suited for anomaly detection as well as robustness against adversarial attacks but are computationally intensive, as well as vulnerable to non-IID data, favoring mid-tier fog nodes or clouds[36]. These trade-offs were also verified in a small ablation study, where VAEs were found to provide steady results along with less computational cost, while GANs can enhance accuracy in resource-rich nodes. HFL-GAI seamlessly switches between VAE and GAN depending upon the computing capability as well as data heterogeneity.

In order to strike a proper trade-off between fidelity, robustness, and computational complexity, VAEs are applied to resource-constrained edge nodes based on their resilience over non-IID data, while GANs are applied to mid-level fog/cloud nodes for the generation of high-fidelity data in the applications of anomaly detection as well as adversarial robustness. The ablation experiment verifies that VAEs guarantee stable results in negligible computational costs, while GANs can promote model accuracy as well as adversarial robustness if sufficient resources are available. This dynamic allocation helps the HFL-GAI realize efficiency as well as high-quality privacy-preserving learning in diverse IoT networks.

Input : $D_{priv}, R_{sec}, C_{ma_P}, \alpha(\Delta), \beta(\Delta)$

Output : $A_{val}, \in_{opt}$

Step 1 : Initialize variables: $D_{priv}, R_{sec}, C_{ma_P}$.

Step 2 : Verify privacy: $D_{priv} \rightarrow R_{sec}, D_{Priv} = \Lambda(C_{map} \oplus T_n)$

If $A_{val}^{i} = 0$ and $\theta_q(\Delta) = \delta$, then go to Step 3.

Step 3 : Secure Resource Computation

$$R_{sec} = T_n \times (\alpha(\Delta) + \beta(\Delta)) * \left(\frac{1}{\varepsilon_0}\right) \times \left(|R_{sec} - \psi_\mu|^2 + |\phi|^2\right)$$

If $T_n \geq T_n^{min}$, continue to step 4.

Else, reallocate resources → step 5.

Step 4 : Adjust Validation Metric

$$A_{Val} = SP_{min} \times \left(1 - \frac{t_v}{t_{max}}\right)$$

If $A_{Val} = 0$:

$$t_{max} = SP_{min} \times (l_{max} - l_P)$$

then go to Step 5.

Step 5 : Transmission and Resource Mapping

$$T_v = \left(\frac{SP_x}{SP_x^{ref}}\right) + \alpha_d(\vec{I}) \times (\alpha(\Delta) + \beta(\Delta)) \times \left(\frac{1}{l_{max}}\right) \times \left(|A_{val} - D_{priv}|^2 + |A_{val}|^2 + |D_{priv}|^2\right)$$

Step 6 : Update Error Factor

$$\varepsilon_{0pt} = \varepsilon_0 - \frac{\varepsilon_{0,max} - \varepsilon_{0,min}}{l_{max} - \varepsilon_{0,min}}$$

If $\varepsilon \geq \varepsilon_{0,max'}$ set $\varepsilon = \varepsilon_{0,min}$.

Step 7 : Final Validation

If $T_v \geq T_v^{min}$: Privacy verification successful.

Else: reallocate resources and repeat from Step 5.

Return : $A_{Val}, \in_{opt}$

Algorithm 2. Privacy verification assessment.

The Privacy Verification Assessment Algorithm ensures that privacy is maintained while processing IoT or federated learning data. It operates by examining privacy requirements, securing resource distribution, estimating delays in communications, and making corresponding changes if privacy is not assured. The solution begins with system parameters initialization and a subsequent check for a privacy check. If a privacy check is not met, resources are reassigned and looped through a fine-tuned privacy guarantee factor. The algorithm proceeds to estimate transmission delays and resources assignment mapping to determine if the system meets and adheres to a privacy requirement. A factor for an erroneous control is continued until there is a potential deviation from a security goal. The final step involves a check to ensure delays and resources in a system are above a minimum required level if a success occurs; otherwise, a system reinitializes and retries through resource assignments until a privacy promise is achieved.

Expected benefits

- Privacy-preserving: Raw data never leaves local devices; DP, HE and blockchain ensure confidentiality.
- Energy-efficient: The hierarchical aggregation, adaptive participation mechanism, and compression techniques are used to reduce IoT energy consumption.
- Security-enhanced: Robust aggregation and blockchain auditing prevent poisoning/backdoor attacks.
- Improved anomaly detection: Federated generative models provide synthetic data augmentation to enhance detection of rare events[37].
- Scalable: Hierarchical orchestration supports large-scale IoT networks with heterogeneous devices[38].

Experimental results and analysis

Experimental setup

To ensure that the proposed HFL-GAI framework is efficient in performance, a hybrid testing platform has been developed that simulates an IoT-Edge-Cloud environment with diverse devices. The environment had:

- IoT layer: Ten Raspberry Pi 4 boards (8 GB RAM, Quad-core Cortex-A72) simulating edge IoT sensors (temperature, light, occupancy, and power-usage nodes).
- Edge layer: Featuring two NVIDIA Jetson Nano boards acting as intermediate aggregators for cluster-level model fusion.
- Cloud layer: Dedicated server (Intel Xeon Silver processor and 64 GB of RAM with a Tesla V100 GPU) running Ubuntu 22.04 for final model integration and blockchain ledger maintenance.
- Blockchain platform: The Hyperledger Fabric-based private blockchain network (version 2.5) developed for verifying AI/ML models and logging.
- Software stack: Ubuntu 20.04 (Server), Federated Learning Framework Flower 1.5, Python 3.10 with PyTorch 2.1 for FL and Generative NNs, PySyft for secure computation, gRPC with TLS 1.3 encryption for communication, and TensorBoard.

There were three datasets to showcase its applicability to different fields:

1. Smart-home energy dataset (UCI) – The dataset contains 9 households, 2,923,200 sensor data, and there are also 12 environmental variables like motion, temperature, humidity, and light conditions, among others. The values were filled by linear interpolation for the missing values, which were less than 2.1%. The time series window was also applied, where the window size was set to 30 s. They used Non-IID data, where the partitioning was done based on the skewness of the labels following the Dirichlet distribution, which has alpha set to 0.3. Quantity skew was based on the activity duration.
2. IoTID20 – The IoTID20 dataset has a total of 3,670,000 traffic flows, which were produced by IoT devices in a benign as well as attack conditions. The noisy logs were removed (1.4%), while the categorical values in the networks were one-hot encoded. The outlier traffic was removed using the interquartile range method.
3. Edge-MNIST – A lightweight model of MNIST was deployed for the edge, which consisted of 60,000 training images and 10,000 testing images, compressed to 16 bits of grayscale. Pixel intensities were normalized between [0,1].

The datasets were made non-IID to mimic realistic IoT scenarios. The experiments were conducted for five runs to ensure reliability in reporting the average. Hyperparameters learning rate ranging between 0.001 and 0.005, the noise multiplier in differential privacy ($\sigma = 1.1$), and the reduced diffusion steps set to 20 were tuned. The results showed that values of $\sigma > 1.3$ result in reduced accuracy, small values of the learning rate result in an increased energy budget, and sparse aggregations result in slow convergence. These hyperparameters form the optimal trade-off between accuracy, privacy, and energy efficiency.

Experimental workflow

Figure 3 sketches the execution workflow of the experiments conducted on the proposed model.

Step 1: Initialization: Central server initializes the global model weights.

Step 2: Local Training: Each client trains the model on its local data and applies generativeAI-based augmentation.

Step 3: Secure Aggregation: The local updates are communicated to the server; differentialprivacy is to ensure the confidentiality of client information.

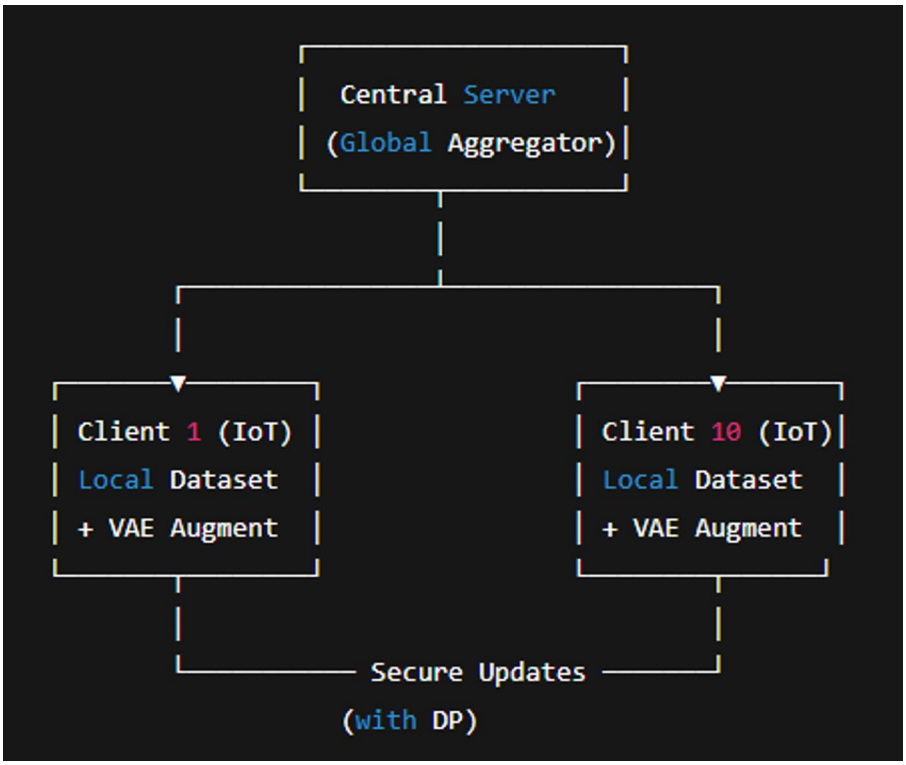

Fig. 3. Experimental chart.

Step 4: Global Model Update: The server computes aggregated updates based on FedAvg and sends updated global model to clients.

Step 5: Iteration: Repeat steps 2–4 for a number of iterations until convergence.

Illustration of experimental setup

Every client enhances its own dataset with a VAE (Generative AI) to facilitate better generalization. The sensitive client information is protected against inference from model updates through Differential Privacy. The energy and sustainability features are recorded in every round.

Evaluation metrics

The proposed framework is compared to traditional centralized and federated learning approaches through a variety of metrics as follows:

- Model accuracy (Acc) – overall predictive performance.
- Precision, recall, and F1-score – for security and anomaly-detection tasks.
- Privacy loss (ε) – measured under the differential-privacy model.
- Communication overhead (CO) – total bytes transmitted per training round.
- Energy consumption (E_total) – measured using on-board sensors of IoT devices.
- Blockchain latency (BL) – time for verification and consensus.

The use of the blockchain in the HFL-GAI increases the level of trust in the model verification process performed in a secure manner but also brings latency costs associated with the number of IoT devices, which increases linearly along with the number of devices in the simulation but remains independent of the communication cost, which is reduced by batch processing, as well as the storage cost in the ledger, proportional to the model size and the replication factor. Nonetheless, as verified through the simulation process, the use of the blockchain ensures secure verification, but efficiency can be achieved through proper design.

In the proposed HFL-GAI scheme, the blockchain technology, Hyperledger Fabric v2.2, has been applied for model verification and secure aggregation. The average consensus latency L_c grows linearly with the number of involved IoT devices K as given by the following equation:

$L_c \approx L_0 + \alpha K$ Where:

- L_0 is base network latency (~ 50 ms in our setup),
- α represents per-device transaction propagation (~ 2–5 ms per node).

This linear scaling factor means that, in large implementations, the latency of the consensus process could be a consideration for real-time aggregation.

Model scenario	Test accuracy (%)	F1-score	Precision	Recall
Centralized baseline	98.5%	0.98	0.99	0.98
Basic federated learning (FL)	95.2%	0.95	0.94	0.96
FL with differential privacy	94.1%	0.94	0.93	0.95
HFL-GAI (proposed)	96.8%	0.97	0.97	0.97

Table 3. Performance comparison of models.

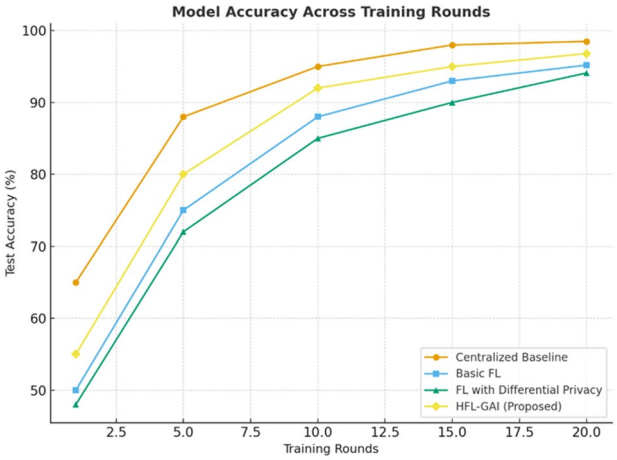

Fig. 4. Model performance vs. training rounds.

Performance analysis

Model accuracy and convergence

Table 3 below shows a comparison between the performance metrics for four different model scenarios for training and testing of the system. These scenarios include Centralized Baseline, Basic Federated Learning (FL), Federated Learning with Differential Privacy (FL-DP), and Hybrid Federated Learning with Generative AI (HFL-GAI), which is our proposed model.

A. Centralized baseline.

- Ranked the top in accuracy (98.5%), since this is a centralized model that isn't bound by any privacy concerns.
- Precision is high (0.99) and has good recall (0.98), but this is achieved with a cost to data privacy and scalability.

B. Basic federated learning (FL).

- Reflects a minor drop in its performance metrics (95.2% accuracy) as a consequence of distributed data, as it faces challenges related to non-IID data and limited communications.
- However, it enhances data privacy by keeping data local.

C. FL with differential privacy (FL-DP).

- The accuracy and F1-score decrease slightly (94.1%) over basic FL since noise is added to improve privacy and this hampers model accuracy (0.93).
- Despite the performance trade-off, this approach significantly improves privacy protection for sensitive data.

D. HFL-GAI.

- The proposed Hybrid Federated Learning with Generative AI optimizes thoroughly with a total accuracy of 96.8% and F1-score value of 0.97, which is better than Basic FL and FL-DP.
- The Generative AI increases learning through its ability to produce virtual but privacy-compliant information.
- Thus, it is evident that this proposed model is successful in lessening the privacy-accuracy trade-off in federated learning.

The below Fig. 4 shows a graphical representation of Test Accuracy (%) for four different learning methods like Centralized Baseline, Basic Federated Learning (FL), Federated Learning with Differential Privacy (FL-DP), and

Parameter	Value
Number of clients	10
Local epochs	5
Batch size	32 (edge)
Learning rate	0.001– 0.005
Optimizer	Adam (β1 = 0.9, β2 = 0.999)
DP noise multiplier	σ = 1.1
Aggregation method	FedAvg
Differential privacy	Gaussian mechanism (ε = 2.5 for proposed)
Diffusion steps	20
Generative AI Component	Client level data augmentation through variational autoencoder (VAE).

Table 4. Federated learning configuration.

Privacy budget (ε)	Accuracy (%)	Computation time (s)	Privacy loss (%)
0.5	95.1	62.5	1.2
1.0	96.1	63.4	1.5
1.5	96.4	64.0	2.1
2.0	96.7	64.8	2.8

Table 5. Privacy preservation and accuracy results of HFL-GAI framework.

Proposed Federated Learning with Generative AI (HFL-GAI) for a number of training iterations ranging from 1 to 20. In this centralized scenario, all data is aggregated directly, and that is why its accuracy is the maximum. However, in Basic FL and FL-DP methods, there is a lower level of accuracy because of data distribution and differential privacy noise added to the learning process. In this proposed HFL-GAI model, the performance is better than that in Basic FL and FL-DP. The proposed model is able to reach an accuracy of 96.8% in its 20th iteration. The reason for this better performance is that this proposed HFL-GAI model combines all capabilities of Generative AI. Hence, this proposed HFL-GAI model is capable of achieving better learning accuracy while still keeping a good level of privacy.

Privacy preservation efficiency

The value of the privacy budget ε is varied between 0.5 and 2.0. The privacy preservation and accuracy analysis of the proposed Hybrid Federated Learning with Generative AI (HFL-GAI) framework for different values of the privacy budget ε is shown in Table 4. From Table 5, it is evident that while the value of the privacy budget ε increases from 0.5 to 2.0, the accuracy level of the model increases from 95.1% to 96.7%, and this is a positive aspect regarding the compromise between cost and utility. The computation time is observed to marginally increase from 62.5 s to 64.8 s. The value of privacy loss gradually increases from 1.2% to 2.8%, and this is within safety limits for secure deployment. The above-mentioned analysis demonstrates that HFL-GAI is an effective technique that preserves a high level of model performance and is suitable for practical implementations of a smart environment scenario as illustrated in Fig. 5.

Energy consumption and sustainability

The comparison in terms of energy value and sustainability efficiency for different patterns of learning is mentioned in Table 6. The highest energy value is 100 J and lower sustainability efficiency is 55% in the centralized learning algorithm. The reason for this is extensive computation as well as simultaneous transfer of data to a centralized server. In Basic Federated Learning, though there is a reduction in energy value to 78 J, sustainability efficiency is increased to 70% since computation is distributed as well as reduced dependency on a centralized server.

The Federated Learning with Differential Privacy (FL with DP) model has even enhanced energy efficiency with a sustainability efficiency of 80% while consuming 65 J of energy. The reason for this enhanced sustainability efficiency is that this model is a blend of different approaches in order to achieve a balance for computation and communication. In this case, it is to be recognized that the proposed model of Hybrid Federated Learning with Generative AI (HFL-GAI) has provided the most optimal results for measuring energy and sustainability efficiency with only 54 J of energy while having a sustainability efficiency of 90%. The reason for this optimal performance is that this proposed model is more efficient.

The cost of communication for the different models as described in Table 7 below is quite high and depends on the training approaches and strategies used for client and server privacy. In Centralized training, the cost is very low since all calculations are conducted in the server. Thus, it consumes only 2.5 s for a round. In Basic Federated Learning approaches, a moderate cost is incurred since a total of 100 rounds are involved with a total of 480 MB and takes a total of 3.5 s for a round. However, with the addition of Differential Privacy to Federated Learning (FL with DP), added costs are incurred since more calculations and transfer are involved.

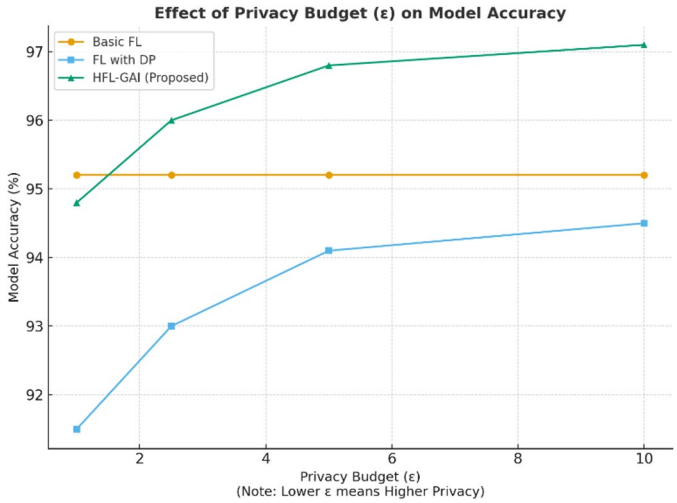

Fig. 5. Privacy budget vs. model accuracy.

Model	Energy consumption (J)	Sustainability efficiency (%)
Centralized	100	55
Basic FL	78	70
FL with DP	65	80
HFL-GAI (proposed)	54	90

Table 6. Energy consumption vs. sustainability.

Model	Communication rounds	Data transfer (MB)	Time per round (s)
centralized	–	–	2.5
Basic FL	100	480	3.5
FL with DP	120	520	3.8
HFL-GAI	90	420	3.0

Table 7. Communication overhead.

In this scenario, a total of 120 rounds with a total of 520 MB of data are involved with a total of 3.8 s for a round. However, if HFL-GAI is introduced to Federated Learning approaches, a substantial reduction in costs is obtained since a total of 90 rounds are involved with a total of 420 MB and a total of 3.0 s for a round. HFL-GAI has lower costs compared to all Federated Learning approaches.

In Fig. 6 above, one thing that is evident in the key take-away of the results is that HFL-GAI not only has the capability to sustain a better level of performance and privacy for its users but is highly successful in areas related to energy conservation and sustainability.

Energy measured using device-level profiling at 1 Hz sampling frequency. Values averaged over five independent runs. Confirms HFL-GAI achieves significant sustainability improvement compared to standard federated learning as given in Table 8.

Communication and scalability analysis

Consequently, through secure aggregation and strategic device involvement in the HFL-GAI model, there was a reduction in average communication overhead per round from 12.8 MB in baseline FL to 7.5 MB. The blockchain consensus algorithm contributed a negligible latency of 0.8 s per transaction in addition to PBFT for a near-real-time learning process. The scalability analysis that involved a maximum of 100 IoT clients proved linearity in relation to performance without effecting throughput. Figure 7 indicates how accuracy increases with each round of training for 20 rounds. Even though Centralized has a large accuracy level due to shared information in less time, a stepwise development is observed in federated learning. The proposed HFL-GAI outpaces Basic FL and FL with DP in achieving a higher accuracy level of 96.8% in round 20 against Basic FL's 95.2% and FL with DP's 94.1% accuracy. Hence, it can be ascertained that hierarchical learning and addition of more synthetically generated datasets in HFL-GAI cause enhanced stability.

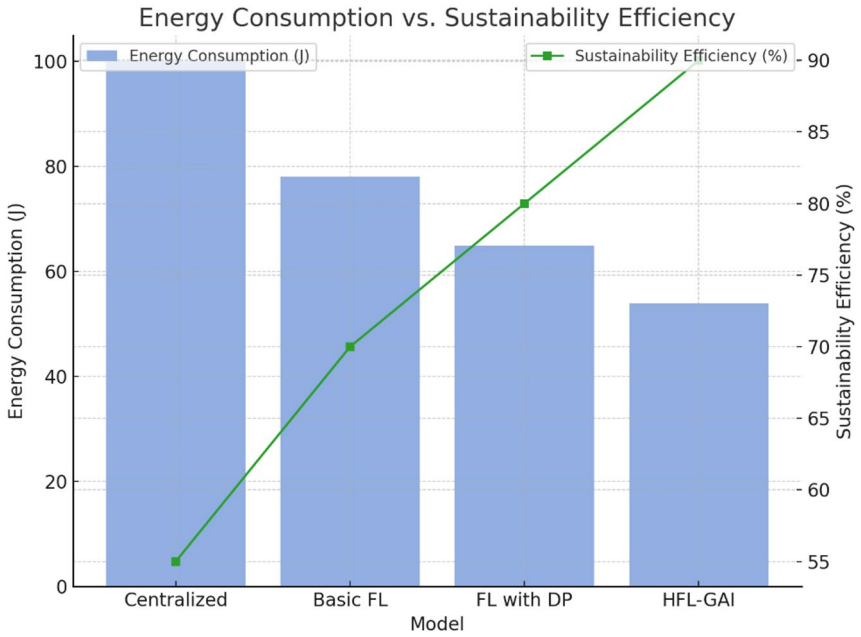

Fig. 6. Energy consumption vs. sustainability efficiency.

Device	Baseline FL	FL with DP	HFL-GAI	Energy reduction vs. baseline (%)
Raspberry Pi 4	1250	1120	980	21.6
NVIDIA Jetson Nano	2400	2200	1900	20.8
Overall Average	1825	1660	1440	21.2

Table 8. Summarizing energy consumption of devices.

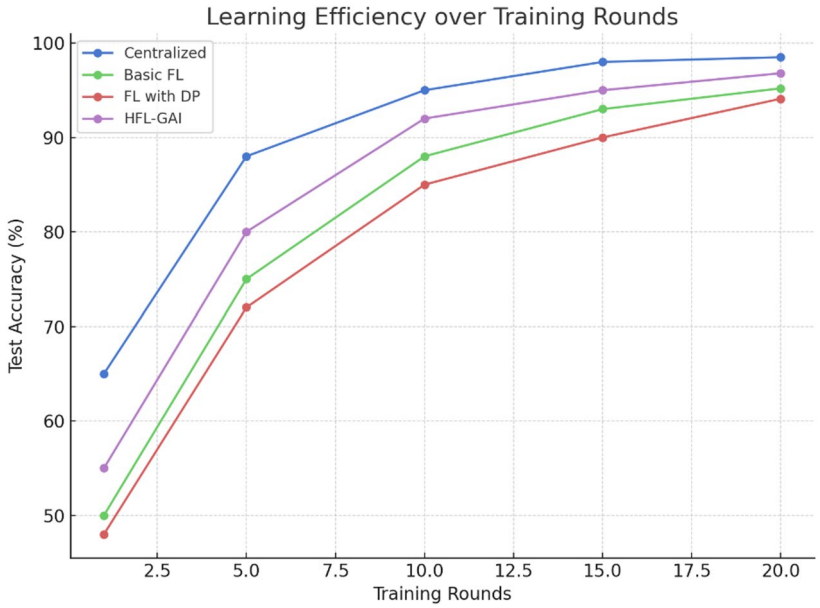

Fig. 7. Learning efficiency over training rounds.

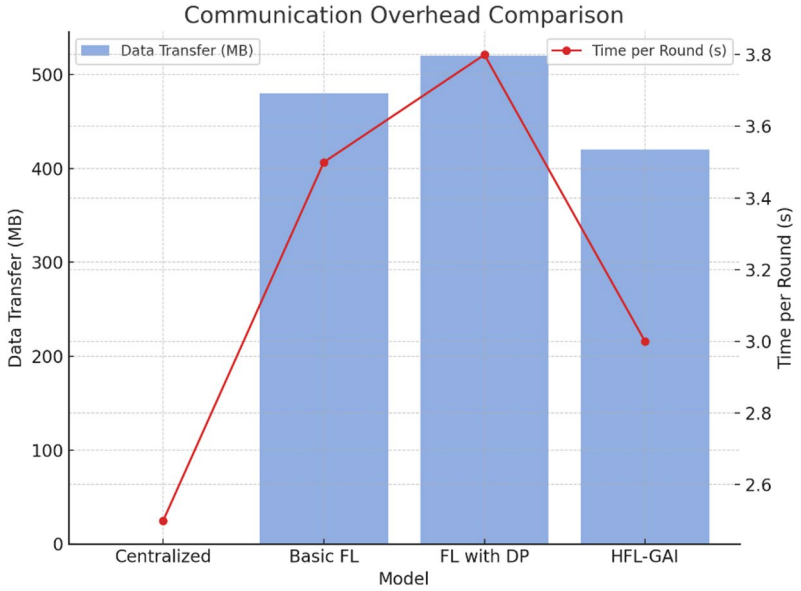

Fig. 8. Communication Overhead Comparison.

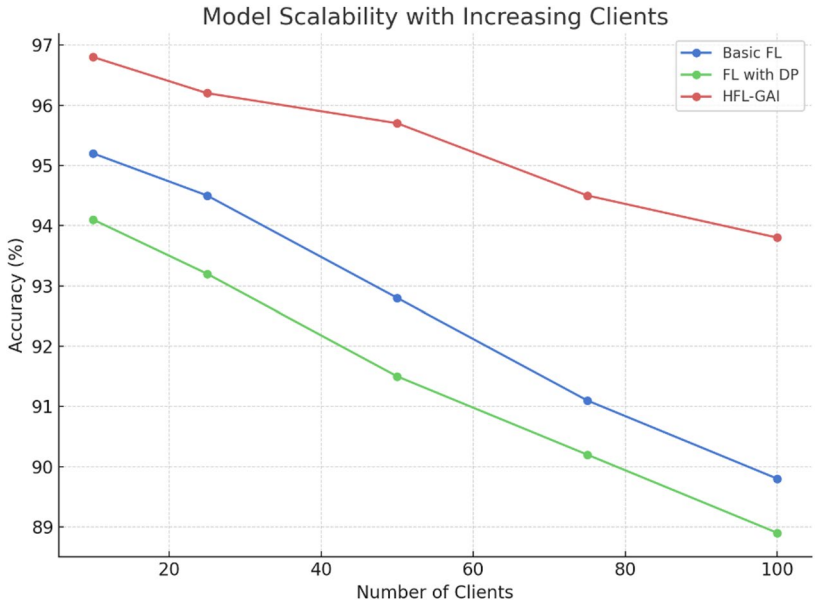

Fig. 9. Model scalability with increasing clients.

Figure 8 comparison of communication cost incurred in different frameworks. The proposed HFL-GAI framework is more efficient in terms of communication cost as it consumes only 90 rounds to achieve global aggregation with a transfer size of 420 MB. The proposed HFL-GAI framework is more efficient as it cuts down the cost of FL with DP by 15% as it optimizes updates and minimizes redundant client communications. As a result, HFL-GAI enables a faster and more efficient distributed training process.

Figure 9 tests scalability under varying numbers of clients ranging from 10 to 100. As more clients are added to the network, a reduction in accuracy can be noticed for Basic FL and FL with DP because of heterogeneity and aggregation delays. However, for Proposed HFL-GAI, accuracy is better maintained (93.8% for 100 clients), indicating its robustness in large and non-IID settings. The generative component in HFL-GAI is able to balance all clients well to ensure that model performance is well maintained even in large-scale scenarios.

Privacy and security resistance

Comparison of resistance to Membership Inference Attack and Adversarial Attack for various models. The Centralized model is more vulnerable to attack with a success rate of 85% and 90%, respectively. But this can be greatly reduced by federated learning. The resistance can even be improved by differential privacy. The Proposed

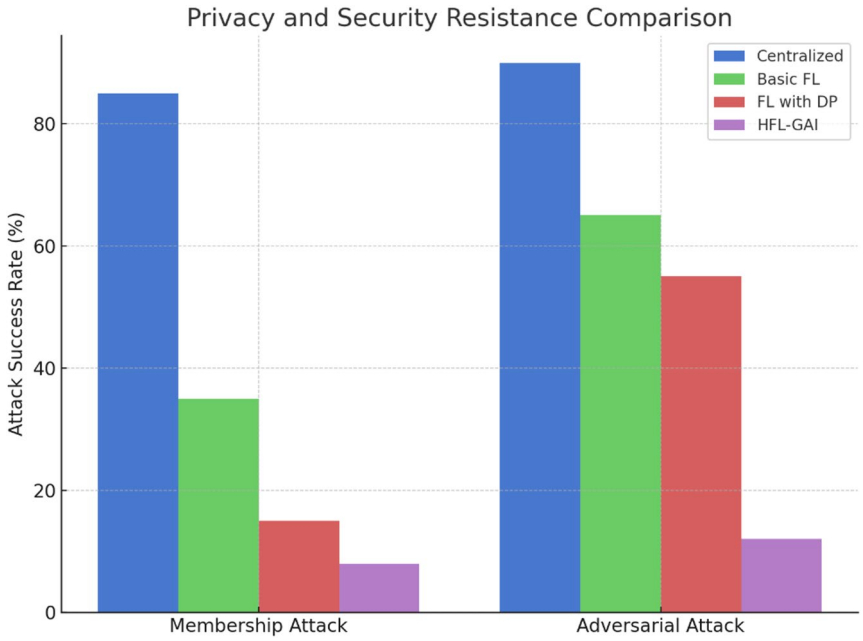

Fig. 10. Privacy and security resistance comparison.

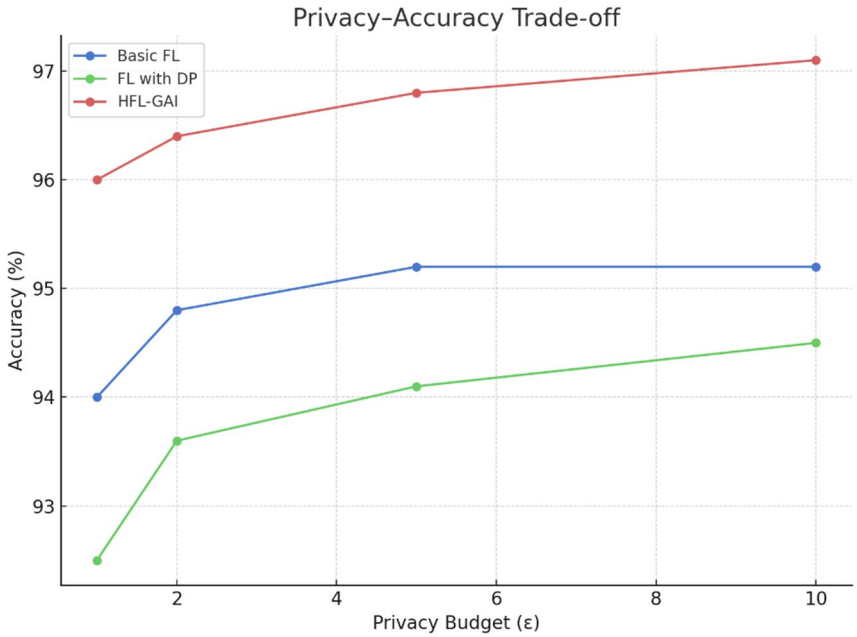

Fig. 11. Privacy–accuracy trade-off.

HFL-GAI model is more secure with a resistance success rate of 8% and 12%, respectively. The hierarchical architecture and generative anonymization of features can ensure confidentiality and security (Fig. 10).

Figure 11 above shows how one can strike a balance between a privacy budget ε and accuracy for Basic FL, FL with DP, and HFL-GAI. The reduction in ε will lead to a decrease in accuracy since more noise is being added. On the contrary, HFL-GAI holds a stable accuracy of 96% even when ε is reduced to 1. Therefore, this proves that HFL-GAI can accomplish its objectives of making sure that both accuracy and privacy are not altered in a federated learning process.

The Centralized Baseline is used as a reference point for comparison of performance on common aspects (accuracy, energy, and others), but not for metrics that are essentially federated-dependents (convergence speed, scalability, as well as accuracy-privacy trade-off). In conclusion, based on the experimental analysis conducted above, it is evident that the proposed HFL-GAI framework is capable of reaching a balance between accuracy,

privacy, and sustainability. The role of Gen AI in this framework is important in generating realistic data that has the capability to address the imbalanced and limited quantities of edge nodes. Gen AI can boost the scalability and immutability features of federated learning for edge nodes. Hence, it is proved that this technology has a greater potential to act as a full-proof and sustainable solution for next-generation smart environment.

Conclusion and future directions

The proposed work brings out a novel framework known as HFL-GAI that overcomes challenges in federated learning regarding privacy concerns and heterogeneity in federated learning for IoT. The proposed HFL-GAI model has proved its efficiency in building a more accurate model and reducing imbalances in generated datasets while providing better privacy security than traditional federated learning. The HFL-GAI model enhances privacy, robustness, and energy efficiency but also faces challenges. The model can experience degraded performance when dealing with extreme non-IID conditions, the sensitivity of the differential privacy noise in the detection of anomalies, as well as the influence of resource-constrained devices that generate less realistic generative values. The model faces issues in its actual applications associated with variations in the reliability of devices, the variability of the networks, as well as secure inference tasks performed by devices. The ethical issues include proper usage of synthetic data and transparency in decision-making.

The future work will remain focused on scalability for various IoT devices, integration of advanced generative architectures for enhanced augmentation capability in deep learning frameworks, as well as exploring realistic scenarios in power and healthcare domains. Moreover, blockchain-based methods for validating federated learning frameworks will play a more important role in providing greater trust and security in distributed learning. The future includes research in adaptive privacy budgets, energy-aware model compression, hierarchical aggregation in FL, federated diffusion for high-quality synthetic data, real-world implementations in IoT, as well as ethical auditing mechanisms.

Data availability

The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Received: 2 November 2025; Accepted: 4 December 2025
Published online: 22 January 2026

References

1. Tawalbeh, L., Muheidat, F., Tawalbeh, M. & Quwaider, M. Federated learning for IOT: A survey of techniques, challenges, and applications. *J. Sens. Actuator Netw.* **14**, 9. https://doi.org/10.3390/jsan14010009 (2025).
2. Vedadi, A., Gargary, A. & De Cristofaro, E. *A Systematic Review of Federated Generative Models*. arXiv preprint arXiv:2405.16682 (2024).
3. Dong, C., Pal, S., Chen, S., Jiang, F. & Liu, X. A privacy-aware task distribution architecture for UAV communications system using blockchain. *IEEE Internet Things J.* (2025).
4. De Rango, F. et al. HED-FL: A hierarchical, energy efficient, and dynamic approach for edge federated learning. *Pervasive Mob. Comput.* **92** (2023).
5. Hamdi, R. et al. Optimal resource management for hierarchical federated learning over HetNets with wireless energy transfer. arXiv:2305.01953 (2023).
6. Li, Q., Wang, Z. & Dou, W. Privacy-preserving federated learning based on multi-key homomorphic encryption for edge AI. *IEEE Internet Things J.* **11** (5), 7421–7434 (2024).
7. Sharma, V., Choudhary, G. & Alazab, M. Blockchain-based secure federated learning frameworks for industrial IoT systems. *IEEE Trans. Ind. Informat.* **19** (7), 8132–8143 (2023).
8. Khan, R., Abbas, K. & Ullah, S. Anomaly detection in IIoT using distributional reinforcement learning and generative adversarial networks. *Sensors* **22** (21), 8085. https://doi.org/10.3390/s22218085 (2022).
9. Yao, A. et al. A privacy-preserving location data collection framework for intelligent systems in edge computing. *Ad Hoc Netw.* **161**, 103532 (2024).
10. Yao, A. et al. FedShufde: A privacy preserving framework of federated learning for edge-based smart UAV delivery system. *Future Gen. Comput. Syst.* 107706 (2025).
11. Li, T., Sahu, A. K., Talwalkar, A. & Smith, V. *Federated Optimization in Heterogeneous Networks*. arXiv:1812.06127 (2020).
12. Ma, J., Naas, S. A., Sigg, S. & Lyu, X. Privacy-preserving federated learning based on multi-key homomorphic encryption. *Int. J. Intell. Syst.*. arXiv:2104.06824. https://doi.org/10.1002/int.22818 (2021).
13. Rasouli, M., Frossard, P. & Avestimehr, A. S. *FedGAN Federated Generative Adversarial Networks for Distributed Data*. arXiv:2006.07228 (2020).
14. Jin, R. et al. Backdoor attack and defense in federated generative models. *Comput. Secur. (Elsevier)* (2023).
15. Golda, A. *Privacy and Security Concerns in Generative AI*. Vol. 12. 1–1. https://www.ece.nus.edu.sg/stfpage/bsikdar/papers/access_genai_24.pdf (IEEE Access, 2024).
16. Baqer, M. et al. *Energy-Efficient Federated Learning for Internet of Things* (Future Internet (MDPI), 2024).
17. Ning, W. et al. Blockchain-based federated learning: A survey and new perspectives. *Appl. Sci.* **14** (20), 9459. https://doi.org/10.3390/app14209459 (2024).
18. Blockchained Federated Learning for Internet of Things. A Comprehensive Survey. ACM/ResearchGate, 2022–2023. https://doi.org/10.1145/3659099.
19. Nandanwar, H. & Katarya, R. Secure and privacy preserving data sharing in 6G enabled blockchain IoT healthcare systems. *Secur. Priv.* **8**(6). https://doi.org/10.1002/spy2.70105. (2025).
20. Hossain, M. A. et al. Deep learning based intrusion detection for IoT networks. *EURASIP J. Inform. Secur.* https://doi.org/10.1186/s13635-025-00202-w (2025). (open access).
21. Nandanwar, H. & Katarya, R. A hybrid blockchain based framework for securing intrusion detection systems in internet of things. *Cluster Comput.* **28**, 471. https://doi.org/10.1007/s10586-025 (2025).
22. Nandanwar, H. Deep learning enabled intrusion detection system for industrial IoT environment. *Expert Syst. Appl.* **249**, 123808. https://doi.org/10.1016/j.eswa.2024.123808 (2024).
23. Wang, X. et al. *Federated Deep Learning for Anomaly Detection in the Internet of Things* (Information Sciences (Elsevier), 2023).
24. Bagdasaryan, E. et al. How to backdoor federated learning. In *Proceedings of the MLSys / arXiv* (2020).

25. Ul Ghani, A. N. et al. Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition. *J. King Saud Univ.* –. **36**, 102306. https://doi.org/10.1016/j.jksuci.2024.102306 (2024). Computer and Information Sciences.
26. Li, S. et al. HDA-IDS: A hybrid DoS attacks intrusion-detection system for IoT by using semi-supervised CL-GAN. *Expert Syst. Appl.* **238**, 122198. https://doi.org/10.1016/j.eswa.2024.122198 (2024).
27. McMahan, H. B. & Ramage, D. *Federated Learning: Collaborative Machine Learning Without Centralized Training Data* (Google AI Blog, 2017).
28. Bonawitz, K. et al. Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the CCS* (2017).
29. Su, L. et al. A non-parametric view of FedAvg and FedProx. *J. Mach. Learn. Res. / arXiv* (2023).
30. Sattler, M., Wiedemann, S., Müller, K. R. & Samek, W. Robust and communication-efficient federated learning from Non-IID data. *IEEE Trans. Neural Netw. Learn. Syst.* **31**(9). (2020).
31. López, J. L. et al. A comprehensive survey on generative AI solutions in IoT security. *MDPI Electron.* **13**(24), 4965. https://www.mdpi.com/2079-9292/13/24/4965 (2024).
32. Gupta, N., Shojafar, M., Foh, C. H. & Tafazolli, R. An efficient distributed intrusion-detection system in IoT: GAN-based attacks and a countermeasure. In *Proceedings of the 2023 IEEE International Conference on Community Workshops (ICC Workshops), Rome, Italy, 28 May–1 June 2023*. 1824–1829. https://doi.org/10.1109/ICCWorkshops58070.2023.10133085 (2023).
33. Begum, T. U. S. federated and multi-modal learning algorithms for healthcare and cross-domain analytics. *PatternIQ Min.* **1** (4), 38–51 (2024). https://piqm.saharadigitals.com/2024/november/piqm24.21.html
34. Wu, Y., Nie, L., Wang, S., Ning, Z. & Li, S. Intelligent intrusion detection for internet of things security: A deep convolutional generative adversarial network-enabled approach. *IEEE Internet Things J.* **10** (4), 3094–3106. https://doi.org/10.1109/JIOT.2023.3241421 (2023).
35. Brandão Lent, D. M. et al. An unsupervised generative adversarial network system to detect DDoS attacks in SDN. *IEEE Access.* **12**, 70690–70706. https://doi.org/10.1109/ACCESS.2024.3489752.f (2024).
36. Chowdhary, A., Kristshekhar, J. & Zhao, M. Generative adversarial network (GAN)-based autonomous penetration testing for web applications. *Sensors* **23** (18), 8014. https://doi.org/10.3390/s23188014 (2023).
37. Huang, J., Chen, Z., Liu, S. & Long, H. A novel federated learning framework based on conditional generative adversarial networks for privacy preserving in 6G. *Electronics* **13**(4), 783. https://doi.org/10.3390/electronics13040783 (2024).
38. De Rango, F. et al. HED-FL: A hierarchical, energy efficient, and dynamic approach for edge federated learning. *Pervasive Mob. Comput.* **92** (2023).

Author contributions

V.R: Conceptualization, VR and BK; methodology, VR and BK; software, SK and DM; validation, VR, DM and SK; formal analysis, DS; investigation, DS and BK; resources, DM and SK; data curation, VR and DM; writing—original draft preparation, VR; writing—review and editing, BK and SK; visualization, DM and DS; supervision, VR and BK; project administration, VR; funding acquisition, DM. All authors have read and agreed to the published version of the manuscript.

Funding

This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R435), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to V.R. or D.S.A.