INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 18, Issue: 6, Month: December, Year: 2023
Article Number: 5890, https://doi.org/10.15837/ijccc.2023.6.5890

CCC Publications

AGORA UNIVERSITY PRESS

# Optimizing Heterogeneity in IoT Infra Using Federated Learning and Blockchain-based Security Strategies

V. Muthukumaran, R. Sivakami, V. K. Venkatesan, J. Balajee., T. R. Mahesh, E. Mohan, B. Swapna

**Venkatesan Muthukumaran**
Department of Mathematics,
College of Engineering and Technology,
SRM Institute of Science and Technology,
Kattankulathur, India muthu.v2404@gmail.com

**R. Sivakami**
Department of Computer Science and Engineering,
Sona College of Technology, Salem, India
shivasona07@gmail.com

**Vinoth Kumar Venkatesan**
School of Computer Science Engineering and Information Systems,
Vellore Institute of Technology, Vellore, India
vvinothkumar@ieee.org

**J. Balajee**
Department of Computer Science,
Mother Theresa Institute of Engineering and Technology,
Andhra Pradesh
jbbala@gmail.com

**T. R. Mahesh**
Department of Computer Science and Engineering
JAIN (Deemed-to-be University),
Bengaluru, India
*Corresponding author: t.mahesh@jainuniversity.ac.in

**E. Mohan**
Department of Electronics and Communication Engineering,
Saveetha School of Engineering,
SIMATS, Chennai, Tamilnadu, India.
emohan1971@gmail.com

**B. Swapna**
Department of Electronics and Communication Engineering
Dr. MGR Educational and Research Institute, Chennai, India.
swapna.eee@drmgrdu.ac.in

**Abstract**

The Internet of Things (IoT) and associated capabilities are becoming indispensable in the planning, operation, and administration of intricate systems of all sizes. High-end learning solutions that go beyond the boundaries of the problem are necessary for addressing the variety of communication concerns (compatibility, secure communication, etc.) in IoT settings. Building machine learning (ML) networks from disparate data sources is a cutting-edge practice known as Federated Learning (FL). In this article, we implement FL between edge-based servers and devices in a sparsely populated cloud to facilitate cohesive learning and the storage of critical information in smart IoT systems. FL enables collaborative training from a common model by aggregating smaller unit models via regulated edge network participants. Further, all the susceptible device's information and sensitive message transactions are addressed via blockchain technology. Thus, a blockchain-based security mechanism is integrated to secure user privacy and facilitate widespread practical adoption. Finally, a comparison is made between the proposed model and the three best free, open-source Federated Learning models already in use (FedPD, FedProx, and FedAvg). In terms of statistical, and data heterogeneity (>70% SDI, >97% accuracy), the experimental findings suggest that the proposed model performs better than the existing techniques.

**Keywords:** Security, Heterogeneity, Success Rate, Vulnerability, Federated Learning, performance, A-GAN, Accuracy.

# 1 Introduction

All the information needed to execute an ML/DL model must be maintained in one repository. A centralized system maintains a shared database to build and evaluate ML techniques. Since the vast majority of data processing time is spent in the cloud, all customer information is kept there, where it is subject to all of the data security concerns associated with cloud computing infrastructure. For example, cloud service providers may intentionally release the information for financial gain, or cyber-criminals or investment firms' rivals may compromise it. All ML/DL approaches follow the same rationale: the more knowledge they are fed during training, the more accurate they will become. In addition, the information is spread among several competitive firms, which is a critical challenge in the real-world. To that end, businesses with more customer information are in a better position to facilitate adaptation than those with less.

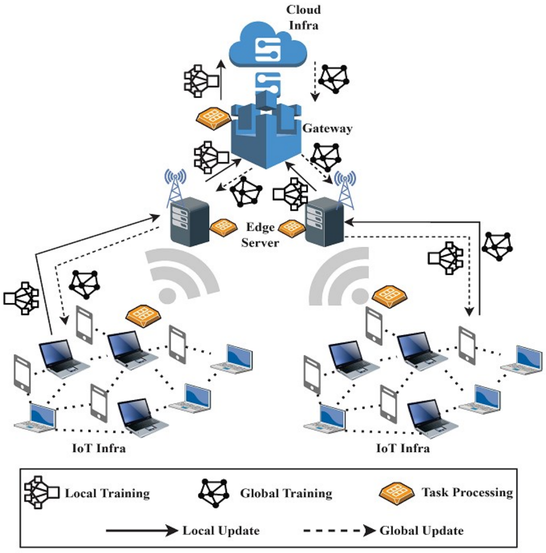

Figure 1: Generalized framework of FL

Therefore, FL was created as a solution to the problems associated with ML/DL. McMahan et al. [15] suggested the notion of FL. Sometimes the concept of FL goes by the name "collaborative learning strategies." It's a method of ML in which there is no central repository for the accumulated knowledge, but instead, several copies spread out throughout the network. Each distributed node will have its own copy of that information and will employ such data to train its own ML/DL model. Using these paradigms, users can share/update the final resultants; thus, they may avoid sending the entire dataset to the cloud environment. The generalized framework for the FL concept is shown in Figure 1.

Parallel to the transition from centralized ML/DL to decentralized FL, the traditional, centralized system framework is also moving towards a more decentralized form. Once thought to be the advent of the virtual digital world, cloud computing now facilitates the synchronization of records from many endpoints. Thus, it improves connected technologies like the IoT by offering storage space, compliance, and rapid computational power [1].

## 1.1 TO WHAT END DOES FL SERVE IOT?

Potential benefits for IoT systems that result from FL's decentralized, interactive, and confidentiality features are outlined in figure 2.

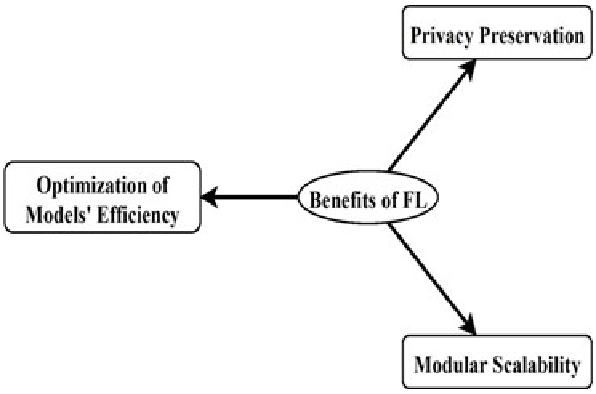

Figure 2: Benefits of FL for IoT Infra

*Safeguarding Users' Confidential Information:* In an ideal FL scenario, each IoT component would only absorb the knowledge required to perform its assigned function. As a result, the FT process reduces the potential for information leaks by keeping the original information on the deployed units locally and only transmitting pattern/gradient updates to the global model (if applicable).

*Optimizing Model Efficiency:* Due to data limitations, a solitary IoT device may not be smart enough to learn from an elevated prototype on its own. To train an elevated prototype, all connected devices in the IoT infrastructure must work within the paradigms of the FL framework, which further enables each member of the unit to gain access to and benefit from the accumulated data (considering all heterogeneous data) without compromising the privacy of those individuals' information. Furthermore, as the FL may regularly update the target domain, the edge node could also perform time-varying updates to its global model. Therefore, FL is a valuable technique for improving system performance in ways that cannot be done by any one component acting alone.

*Modular Scalability:* Due to its decentralized virtue, FL can efficiently and concurrently use the limited computational reserves present in a range of IoT endpoints distributed across various network regions. The data volume of the deployed networks is growing exponentially as the device capabilities at the edge layer improve, and storing all of this information on a single server will devastate computing resources as well as place an undue burden on the wireless channels, restricting their degree of adaptability. FL improves the resilience of IoT systems by enticing all the existing and new units to adopt the framework. Due to its collaborative and distributed processing features, it does so without placing any additional load on a single repository. The FL approach also eliminates the requirement for the massive transfer of processed accumulated data from IoT units, which reduces network overhead and enables greater adaptability, notably for limited bandwidth.

## 1.2 CHALLENGES AND OPPORTUNITIES

For FL to maximize its capabilities in a wide variety of applications, researchers must overcome a few obstacles that prevent FL from being enabled on potentially hundreds of millions of connected devices in the IoT [2].

1. This difficulty stems from factors such as individual IoT nodes' constrained capabilities and edge networks' restricted capacity.

2. Real-world contexts were notorious for their sporadic connections and accessibility.

3. A lack of community-wide standards and network design tools;

4. The temporal variation after implementations; how to prevent against adversary attacks and combine user data securely; and

5. The variety of IoT units in terms of their accessible capabilities.

Here, we lay out these difficulties and then provide several prospects that show great promise for resolving them.

Standard FL taxonomies include CFL, DFL, FTL, VFL, and HFL. When it comes to selecting the ML algorithm and organizing the local units, the central management unit in a centralized FL model takes on these roles. The procedure for centralized FL is as follows: The central hub organizes the list of nodes in a given region. Every client receives the model's instructions from the central hub, which is responsible for deciding the ML method. All local units use the same distributed ML-based model. Guidelines for the model are sent to the edge devices, which then begin training the model using the available data. The outcomes are released at the regional site, while consolidated results are available at the centralized hub.

Since EC could handle data everywhere from the source of information to the cloud services center, this improved client-server communication and significantly reduced interaction latency, both of which are essential for real-time, resource-intensive implementations. Furthermore, upstream EC can distribute the heavy workloads of cloud service centers, providing a practical, viable alternative to the issues faced in training [3-6].

However, in complicated IoT use cases, it is not feasible for all endpoints to concur on a single training phase, as is the case with classical FL. Performing customization on the unit, information, and design stages is one practical strategy to address these heterogeneous difficulties and arrive at a high-quality, tailored version for every system. As a result, in this research, we provide a multi-tasking FL technique for addressing the many forms of heterogeneity that arise in advanced IoT settings. Additionally, blockchain technology [7,8] offers top-tier protection for private data at both the edge as well as cloud levels.

## 1.3 MOTIVATION AND OBJECTIVE

Heterogeneity is an inherent property of IoT networks. FL is implemented across an IoT infrastructure where training datasets, data structures, and unit characteristics all vary. Therefore, heterogeneity is demonstrable and affects the efficiency of a federated network. Statistical and data-oriented heterogeneity are sorted out and briefly discussed in the following section.

Clients may build and train their ML model regionally using the FL process, which subsequently creates a global model by pooling the local models' standard gradients. Heterogeneity in hardware and software must be maximized. Computation, storage, and transmission capabilities vary from machine to machine, while statistical heterogeneity is reflected in the dissimilarity of collected data (distribution skew).

If adequately implemented, blockchain technology has the potential to improve the safety and confidentiality of federated training significantly. Several fundamental characteristics of blockchain technology are significant in the FL arena. These blockchain system features can improve FL's security, confidentiality, and trustworthiness, resulting in safer transactions, improved accessibility, and much more lavish rewards for stakeholders who share critical knowledge and models. It is crucial to provide a normalizing procedure in addition to the FL framework to enhance the effectiveness of FL approaches in heterogeneous circumstances. This study examines how to improve information preprocessing methods and FL approaches in heterogeneous networks [7-10].

The main objectives of optimizing heterogeneity and employing blockchain technology in federated learning are:

1. Improved security and privacy: Optimizing heterogeneity and using blockchain technology in federated learning helps to enhance the security and privacy of the data and models used in federated learning. This is particularly important when dealing with sensitive data or models that are critical to a business or organization.

2. Better data utilization: Optimizing heterogeneity can help to ensure that all participants in a federated learning network can effectively contribute to the training of a shared model, regardless of their data distribution or hardware capabilities.

3. Improved trust and transparency: The use of blockchain technology in federated learning can provide a secure, transparent, and tamper-proof record of the data and models used in federated learning, enabling better trust and transparency among participants.

4. Better data governance: Optimizing heterogeneity and using blockchain technology in federated learning can help to enforce data governance and regulatory compliance, ensuring that data and models are used ethically and responsibly.

These objectives aim to enhance the performance and robustness of federated learning while ensuring the security, privacy, and trust of the data and models used in federated learning.
The entire article is structured as follows: Section 1 presents the fundamental paradigms of FL along with the required security aspects; Section 2 signifies some of the most effective FL methods that are relevant criteria with the proposed characteristics; Section 3 specifies the inclusion of essential datasets and methodology to optimize the heterogeneity context that is common in IoT infrastructure; Section 4 includes the blockchain-based security strategy; Section 5 delineates the core analysis work of the research; and Section 6 concludes the groundwork of the study with some vital points and exposes the future plan of research extensions.

## 2 Related work

We mainly focus on algorithms that claim to incorporate heterogeneity in their design and comprehensively evaluate and compare them in terms of training time and model performance. Below we briefly summarize few relevant FL algorithms and their characteristics for future evaluations.
The FedAvg method for FL via endpoints was introduced as a safe, private, and effective communicator [11]. Zhou et al. concluded how recurrent pattern averaging might be used in practice to calculate the FL. FedAvg eliminates inactive users based on their average response time, assuming that all users would participate at the same rate. Despite its widespread use, FedAvg still has a number of shortcomings when it comes to dealing with heterogeneity's challenges [12].
The researchers proposed a new approach called "SCAFFOLD"that gets usage management variables (diversity minimization) to reduce the negative impact of heterogeneity. SCAFFOLD exploits the difference between the estimated update orientation of the server system and every end-user/client to do a localized correction of the newer version (update). As a result, it is said that the algorithm can resolve diversity and concur with far less interaction than competing approaches [13].
FedProx solves the heterogeneity issue in federal networks by assigning a different quantity of tasks to every deployed device. Also, it promises a steadier and accurate convergence behavior by using limited information from lagging nodes and adding a remote factor to account for differences in how the nodes are connected [14, 15].
Minimizing agglomeration loss on a vast infrastructure in a naïve way might have unintended consequences for the model's efficiency. A new optimization goal, motivated by the need for equitable

distribution of wireless communication resources, was presented in reference [16]. The algorithm's goal is to make the federalized network highly consistent in its correctness. As a result, the cumulative re-weighted risk minimizes by giving more weight to equipment exhibiting significant losses. The algorithm is said to be reliable, effective, and satisfactory.

Intending to maximize statistical effectiveness, the researchers in treated the volatility of FL parameters as a Byzantine loss. They provided decentralized optimization techniques called "FedMed" that are resistant to this kind of loss. Coordinate-wise averaging is used to combine approaches in this single-round communication technique. The method is guaranteed to be resilient towards Byzantine breakdown and is said to be effective while reaching optimal analytical solutions [17].

Zhang et al. suggested a fresh approach to the algorithm created based on the principles of primal-dual minimization. It presents a conceptual algorithm entitled FedPD that aims to optimize for interaction overhead and cope with the generic non-convex goal. The following table provides a comparative analysis of all the available algorithms that have been described in the sense of their capability to deal with various types of statistical and data heterogeneity [18].

Lu et al. [28] presented Digital Twin Edge Networks (DITENs), an emerging technology that could unite analog and virtual edge systems. To improve interaction reliability and data confidentiality assurance inside DITENs, it presents a revolutionary strategy that blends digital twins with edge networks and adds blockchain-enabled federated learning. The study also offers asynchronous consolidation and electronic twin-powered learning through reinforcement for efficient allocation of mediating users and utilisation of broad-spectrum resources. There are substantial gains in transmission efficiency as well as information protection, especially for IoT applications, as shown by research and computational results that support the efficacy of this strategy .

Mallah et al. [29] suggested a novel strategy for improving the performance and dependability of FL prototypes in IoT networks by using blockchain technology. In particular, the article strives to improve model updates by including data from only reliable IoT devices. To do this, researchers framed the issue as an optimization problem and tried to find the best number of "monitoring miners" for the blockchain. The top priorities are Reduced network latency, resource utilization, and power consumption. According to the findings, this study presents an optimized monitoring system that may significantly cut the overall training delay encountered by IoT equipment by 75%, providing a potentially game-changing approach for more robust and effective IoT-FL unification.

Waheed et al. [30] presented a revolutionary hybrid method for IoT-based medical apps that prioritizes security and privacy by combining FL with blockchain technology. This method leverages an encryption system with public keys to safeguard local model changes, while blockchain technology ensures the updates' integrity and enforces controls over who has access to them. Using FL makes it possible to safely aggregate models without compromising private patient information. Employing the EMNIST datasets, we show that the framework protects sensitive data while keeping computations as efficient as possible. The findings point to the hybrid approach's potential for enhancing safe and privacy-preserving IoT-enabled medical services, providing a worthwhile avenue for further study in this area.

# 3 Methodology

## 3.1 Problem Statement

The increasing adoption of federated learning in various industries poses challenges in security, privacy, data utilization, trust, and governance. Traditional federated learning architectures often struggle to account for heterogeneous data and computational capabilities across participating nodes, leading to suboptimal model training and potential misuse of sensitive data. Additionally, the lack of transparent and secure mechanisms for tracking and verifying the training process hampers trust among participants. Therefore, the problem is to design a FL system that leverages blockchain technology and optimization techniques for heterogeneity to not only enhance security and privacy but also to maximize data utilization, improve trust and transparency, and enforce robust data governance and compliance mechanisms.

| Algorithm | Communication Efficiency | Aggregation Method | Overhead | Performance on Non-IID Data | Heterogeneity Handling | Suitable for Non-IID Data | Suitable for Heterogeneous Data |
|---|---|---|---|---|---|---|---|
| FedAvg | Low | Weighted average | Low | Poor | Weighted average, assumes all clients have similar data | Poor | Poor |
| FedPD | High | Weighted average with data partitioning | Low | Good | Weighted average with data partitioning, can handle non-IID data | Good | Good |
| FedMed | Low | Median | Low | Good | Median, can handle non-IID data | Good | Good |
| Q-FedAvg | High | Quantized weighted average | Low | Poor (may introduce quantization noise) | Quantized weighted average, can handle non-IID data | Poor (may introduce quantization noise) | Good |
| FedProx | Low | Weighted average with proximal term | High | Good | Weighted average with proximal term, can handle non-IID data | Good | Good |
| SCAFFOLD | High | Adapts model architecture to data distribution | High | Good | Adapts model architecture to data distribution, can handle non-IID data | Good | Good |

Table 1: Comparison of Existing Models in terms of Heterogeneity

### 3.2 EMPIRICAL CONSIDERATIONS

This study investigates how data heterogeneity optimization might improve data security in a healthcare scenario [19]. While maintaining patient confidentiality, FL is utilized to create ML models employing medical record information gathered from various sources like MIMIC-III and MHEALTH [20]. FL allows for the training of better accurate models and mitigates the potential of overfitting, especially for small data samples, by combining information from a variety of domains. Better confidentiality, safety, transferability of ML frameworks, and more individualized treatment suggestions are among the distinct advantages of FL in the healthcare arena. The subsequent empirical tests were conducted in Matlab 2022b integrated with PyCharm-2018.3.7 framework, in support of a Core-TM i5-3470 @3.20GHz, and NVIDIA GeForce 910M hardware.

MIMIC-III is a comprehensive, single-centre repository that includes data on individuals diagnosed with the intensive care of primary and tertiary-care healthcare. Information collected might comprise but is not confined to the following: medicines, patient's vitals, diagnostic measures, service remarks and findings, adequate fluid, treatment protocols, diagnostic guidelines, visualization studies, length of hospitalization, survivorship statistics, and plenty more. In addition, the database supports studies in academia and industry, procedures, and practical training at the university level [20].

Ten interns representing a wide range of demographics and ages were recorded while participating in a range of different practices to create the MHEALTH from the UCI ML dataset. Magnetosphere polarity, acceleration, and rotational velocity measurements are taken via sensors strapped to the patient's sternum, left foot, and right forearm. In addition, the chest-mounted sensor data includes numerous ECG readings, which may be helpful for essential heart surveillance, detecting irregular heartbeats, or studying how physical activity affects the heart's electrical activity.

### 3.3 PREVALENCE OF HETEROGENEITY

It is usual for healthcare datasets to face the difficulty of having heterogeneous facts, which occur when the data originate from a range of resources and are collected from a variety of populations and might have varying features and patterns. Since this is the case, it can be challenging to create ML models that are both accurate as well as widely applicable across varied inputs. Here are a few instances of healthcare information heterogeneity:

1. Inter-subject unevenness: Data obtained from various subjects, even those with a similar diagnosis or medical problems, might have distinct distributions. Because of this, it may be challenging to evolve diverse models that are reliable in all instances.

2. Intra-subject unevenness: The status of a subject might evolve, which can lead to discrepancies in the data distribution obtained from multiple healthcare professionals. This may hamper efforts to create long-lasting models.

3. Information Standardness: Integrating information from many resources can be challenging because of information quality, precision, and consistency disparities.

4. Data Type: Patient records, subjects of research, and clinical materials are just a few examples of data storage formats that provide their own unique issues for interpretation and processing.

5. Demographic Disparities: Differences in multidimensional data across demographics with different characteristics, like gender, age, or ethnicity, make it hard to generalize observations from one group to another.

A diverse medical dataset refers to a dataset that includes a wide range of patient demographics, medical conditions, treatments, and outcomes. A diverse medical dataset is important because it helps to ensure that machine learning models developed using this data are generalizable to a wide range of patients and populations.A healthcare dataset must contain information on a large variety of patients with different characteristics, diagnoses, and treatment and result profiles to be considered diversified. Therefore, the ability of ML models trained on healthcare records to be applied to a wide variety of patients and communities depends on the dataset's diversity.

1. (a) **A-GAN TRAINING AND FL LEARNING**

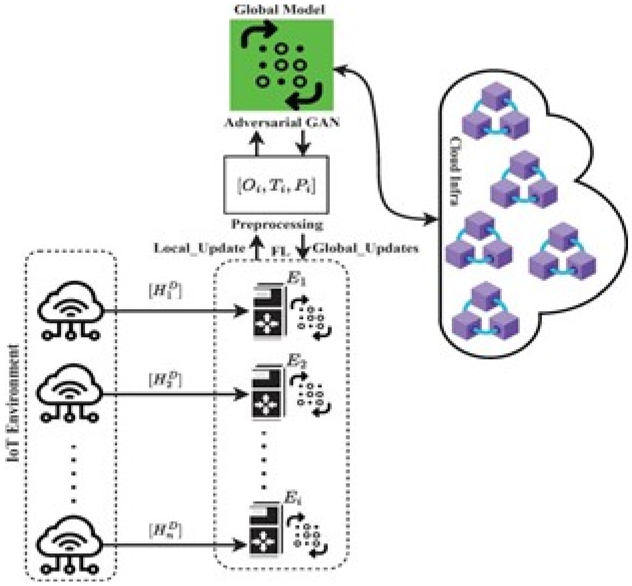

Figure 3: Architecture of Proposed Model

**Figure 3.**

Figure 3 represents the schematic depiction of the FL system [21-25]to optimize the data heterogeneity in IoT infra. The networking models can be trained using FL with A-GANs, which is useful when the data being used is dispersed throughout a network of devices. With the help of A-GANs, FL strategies can safely and effectively deal with data heterogeneity and privacy protection [24-27].

A generator subsystem in A-GAN is trained to produce synthetic information that is identical to the actual data maintained on every unit. With an adversarial loss function, the generator subsystem learns to create recombinant information that is distinct from the actual subject, while the discriminator subsystem attempts to identify the two apart.

The model can be trained using synthetic information instead of the actual data to protect security and confidentiality. To deal with data heterogeneity, FL with A-GANs is employed by retraining the generator subsystem to produce synthetic information that is comparable to the actual data at each edge device. While data from multiple devices seems to have high variability, training the model on samples that are comparable to the exact figures on each unit helps enhance the model's generalization capability.

## 3.4 WORKING OF A-GAN FOR FL

From figure 4, it is picturized that within the framework of FL, A-GANs can be utilized to protect the confidentiality of training records. Stakeholders (e.g., devices or users) in FL each maintain all training data private while training a pooled model with that data. An overall model is constructed by combining the locally learned models.

In A-GANs for FL, each edge server connected with several edge devices trains a local generator and discriminator subsystems on their data and then uses the generator to produce a generative model comprising synthetic data that can be distributed to other edge servers without disclosing any confidential details. Then, the synthesized data are used to train the global discriminator, which can be accessed by all edge servers and their connected devices.

There are several positive outcomes associated with using A-GANs for FL. For instance, FL enables the A-GAN to train a global model without exposing sensitive information. Furthermore, it is more difficult for any attacker to obtain private data from the information employed for training, which is why the utilization of synthetic information may assist in increasing privacy and security. Lastly, an adversarial loss can be employed during training to boost the model's quality since it encourages the

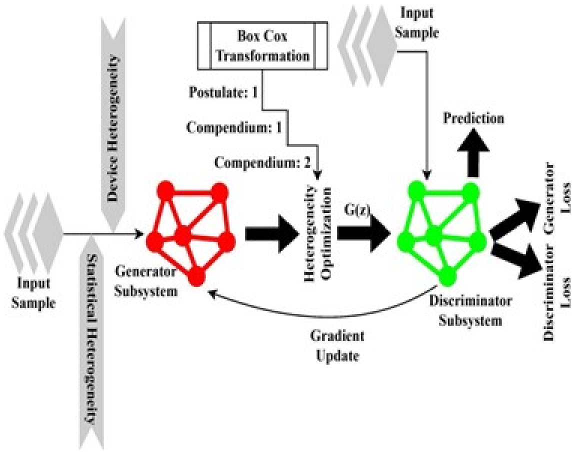

Figure 4: Working Process of A-GAN

generator to create synthetic information indistinguishable from actual data and the discriminator to categorize the actual and false data accurately.

### 3.5 HETEROGENEITY OPTIMIZATION

This investigation focuses on optimizing heterogeneous members and applying stable security to the optimized data in IoT networks infra [25]. To do the core process, defining the nature of heterogeneity in IoT-based networking systems is essential. Thus, with a proven definition, the subsequent compendium supports the facts of upcoming empirical observations.
POSTULATE 1: *A heterogeneity-oriented networking system includes a group of diverse nodes and connection establishments,* $\xi = \{\eta, \varepsilon, \upsilon, \delta, \tau\}$*, where* $\eta$ *and* $\varepsilon$ *represent the group of diverse nodes and their interconnection establishments, respectively. Moreover, they are also coupled with the mapping routinize functions for any node type* ($\upsilon$)*,* $[\tau\ \eta \rightarrow \upsilon]$ *and for any connection types* ($\delta$)*,* $[\tau\!: \varepsilon \rightarrow \delta]$*. In condition to these facts,* $(|\upsilon| + |\delta| \geq 2)$ *is considered.*
Learning a mapping routinize function to shift every node,$n \in \eta$, to a low-dimensional vector $\hat{L}^m$, where $m << \eta$, is the first step in optimizing heterogeneity among different data types. When representing nodes in the low-dimensional space, it is important that they retain not just the network's structure but also its robust interpretations. Such a heterogeneity network is trained using A-GAN with covariate shifting technique. Beside the processing facts, we incorporate Box-Cox transformation technique to optimize generated heterogeneity inputs feeds based on data heterogeneities, and device heterogeneities.
The equation $u = \left(v^{(\lambda)} - 1\right)/\lambda, \lambda \neq 0$ is part of the Box-Cox transformation, a statistical method for transforming data and devices that are skewed or have a skewed distribution. The Box-Cox transformation aims to make the data more suitable for analysis by transforming it into a distribution closer to normal. The equation represents a power transformation where the parameter $\lambda$ determines the type of transformation to be applied.
The equation can be derived as follows:Start with the equation for a power transformation

$$u{=}v^{\lambda} \tag{1}$$

Subtract '1' from both sides:

$$u{-}1{=}v^{\lambda}{-}1 \tag{2}$$

Divide both sides by (λ):

$$u{-}1/\lambda{=}v^{\lambda}{-}1/\lambda \tag{3}$$

The resulting equation $u = \left(v^{(\lambda)} - 1\right)/\lambda,\ \lambda \neq 0$ represents the Box-Cox transformation for lambda values that are not equal to zero. When lambda ($\lambda$) is equal to zero, the equation becomes the natural logarithm transformation, which is represented by the equation

$$v = \ln(u) \tag{4}$$

COMPENDIUM 1: *In statistical heterogeneity, $\forall u$, $v$, if $u \neq v$, then optimize (heterogeneity) by embracing diversity and promoting inclusion, leading to unlocking the full potential of collective knowledge and data.* Input considerations: *Re(u)* is the real part of $\mathbb{Z}log(v)$ is the natural logarithm to normalize/scale the heterogeneity factors, set of integers $W_k(\mathbb{Z})$ is the analytical continuation of the product log function. *Derivative 1:*

$$\operatorname{Re}(u) < 0,\ v = 0, \lambda = -\left(\frac{1}{u}\right) \tag{5}$$

*Derivative 2:*

$$\lambda \neq 0, u = 0, v = 1 \tag{6}$$

*Derivative 3:*

$$v \neq 0;\ \ v - 1 \neq 0;\ \ \log(v)\ \neq 0;\ \ u = 0;\ \ \lambda = 2i\pi n/\log(v)\ ;\ \ n \neq 0;\ n = \mathbb{Z} \tag{7}$$

*Derivative 4:*

$$v \neq 0;\ \ uW_n\left[-v^{-1/u}\log(v)\ /u\right] + \log(v)\ \ 0;\quad \log(v) \neq 0 \tag{8}$$

*Derivative 5:*

$$u\sqrt[u]{v} \neq 0;\ \ \lambda = -uW_n\left[-v^{-1/u}\log(v)\ /u\right] - \log(v\ )/u\log(v)\ ; n \in \mathbb{Z} \tag{9}$$

COMPENDIUM 2: For device heterogeneity, let D = (e, c) be a social graph, where e is a set of deployed edge devices and c is a set of established connections/edges that represent relationships between devices. Let M = (f, ℝ) be a feature graph, where f is a set of features and ℝ is a set of edges that represent co-occurrence or similarity between features. Let F be a function that maps each device d in e to a subset of f that represents the features associated with d. Let H be a function that maps each feature φ in f to an objective function that measures the value of φ in achieving a specific goal. To optimize heterogeneity in D with respect to H, it is essential to: Embrace diversity: For each pair of individuals *(d1, d2)* in e such that *d1* $\neq$ *d2*, maximize the dissimilarity between the feature sets ℝ*(d1)* and ℝ*(d2)* by minimizing a distance function *dist(*ℝ*(d1),* ℝ*(d2))* that takes into account the pair-wise co-occurrence or similarity between features in ℝ. Promote inclusion: For each feature $\varphi$ in *f,* maximize its contribution to the overall objective function *H(*ℝ*(d))* of the individuals *d* in *e* that possess $\varphi$ as a feature, by minimizing a cost function $\beta(\varphi)$ that penalizes the rarity or complexity of $\varphi$. Unlock the full potential of collective knowledge and data: Maximize the weighted sum of the individual objective functions *H(*ℝ*(d))* over all *d* in *e*, where the weight of each function is proportional to the degree of connectivity of *d* in *D*, subject to constraints that ensure fairness, privacy, and other ethical considerations. In formal notation, we can delineate the axiom as follows: $\forall$*D, M,* ℝ*, H, dist,* $\beta$*, maximize* $\sum$*(d*$\in$*e) deg_D(d) R((d)) subject to:* $\forall$*(d1, d2)*$\in$*e, d1* $\neq$ *d2, dist(*ℝ*(d1),* ℝ*(d2))* $\leq \rho$*(d1, d2)* $\forall\varphi\in$*f W,* $\beta(\varphi) \leq \gamma(\varphi)$ $\forall\varphi\in$*f,* $\sum$ $\varphi\in\mathbb{R}(\varphi)$ $\varphi$ *= 1* $\forall\varphi\in$*f,* $\sum$ $\varphi\in$*f* $.\kappa.(\varphi\in\mathbb{R}(\varphi)) \geq \psi(\varphi)$ other constraints as needed where $\rho$, $\gamma$, $\kappa$ and $\psi$ are appropriate distance, cost, indicator, and threshold functions, respectively, and *deg_D(d)* is the degree of *d* in *D*.

### 3.6 HETEROGENEITY DISTRIBUTIVENESS MEASURE

Adversarial training with covariate shift is a method for handling covariate shift, where the distribution of the input data changes over time. The idea behind this method is to use adversarial loss functions to encourage the model to be robust to changes in the data distribution. The formulation of adversarial training with covariate shift typically involves two components: a main task loss function, which is used to train the model to perform the target task, and an adversarial loss function, which is used to encourage the model to be robust to covariate shift. The adversarial loss function is usually defined as the difference between the predictions of the model on the training data and on a synthetic dataset that is generated to have a similar distribution to the target data. The synthetic data can be generated, for example, by using generative models or by re-sampling the training data. The final loss function for adversarial training with covariate shift is a weighted combination of the main task loss and the adversarial loss:

$$f_L{=}\zeta_L{+}\mathit{\Delta}x{\times}\mathit{\Theta}_L \tag{10}$$

where $\zeta_t$ is the main task loss, $\mathit{\Theta}_t$ is the adversarial loss, and $\mathit{\Delta}x$ is a weight that determines the trade-off between the two losses. The equation (10) represents the loss function used in adversarial training with covariate shift. In this equation, $\zeta_t$ which represents the loss function for the main task, which is typically a supervised learning problem where the goal is to predict a target variable based on some input data. This could be a regression problem where the target variable is continuous or a classification problem where the target variable is categorical. The main task loss function is designed to measure the difference between the predicted values and the ground truth values for the target variable. $\mathit{\Theta}_t$represent the loss function for the adversarial network, which is designed to minimize the difference between the distributions of some selected feature between the training and test data. The idea is to train the adversarial network to generate synthetic samples that are similar to the test data, so that the main network can learn to be robust to distribution shifts. $\mathit{\Delta}x$is a hyperparameter that controls the relative weight of the adversarial loss compared to the main task loss. It is chosen based on the desired trade-off between improving the performance on the main task and increasing the robustness of the model to distribution shifts. The final loss function $f_L$ is the sum of the main task loss and the adversarial loss, weighted by $\mathit{\Delta}x$. This loss function is optimized during training by adjusting the parameters of both the main network and the adversarial network using gradient descent or a related optimization algorithm. The goal is to find values of the network parameters that minimize the final loss function and produce a model that performs well on the main task and is robust to distribution shifts.

The A-GAN is trained by minimizing the final loss, encouraging it to perform well on the main task while also being robust to changes in the data distribution. This can improve the generalization performance of the model, especially when the target data distribution is significantly different from the training data distribution.

### 3.7 SECURITY STRATEGIES

In this work, blockchain technology is adopted to provide a number of features that can be used to implement security strategies for storing optimized heterogeneous data in a decentralized and secure manner. These features can provide a way to store and track data securely over time, control access to data based on rules and policies, and protect sensitive data by incorporating hashing technique. Here, AES integrated with SHA-3 256 technique is utilized to encrypt and hash the optimized data, before storing the data in each blocks of the blockchain.

The AES (Advanced Encryption Standard) and SHA-3 256 algorithms are often used together to provide secure data transmission and storage. Here's a high-level overview of how they can be integrated:

*Step 1*- Encryption with AES: The data to be transmitted or stored is first encrypted using the AES algorithm. AES is a symmetric key encryption algorithm that operates on fixed-length blocks of data. The encryption process involves a series of substitution and permutation operations, followed by a key mixing step.

*Step 2*- Hashing with SHA-3 256: After the data has been encrypted with AES, the resulting ciphertext is hashed using the SHA-3 256 algorithm. The hash function takes the ciphertext as input and produces a fixed-length output that represents a digital fingerprint of the data.

*Step 3*- Transmission or Storage: The encrypted and hashed data can now be transmitted or stored securely. The recipient of the data can use the same AES key to decrypt the ciphertext and verify the integrity of the data by hashing it with SHA-3 256 and comparing the result to the original hash value.

In summary, integrating AES with SHA-3 256 provides both encryption and hash-based authentication for secure data transmission and storage.

SHA-3-256 is a specific variant of the Secure Hash Algorithm 3 (SHA-3) family of cryptographic hash functions. It is a 256-bit hash function that takes an input (also known as a message) and produces a fixed-size output of 256 bits. The working of SHA-3-256 can be divided into the following steps:

1: Initialize the state array with 0's.

2: Absorb the input data into the state array using the XOR operation.

3: Permute the state array using the theta, rho, pi, and chi functions for a fixed number of rounds.

***Theta Function:***

For each column c, calculate the parity of the elements in that column:

C_parity(c) = S[0, c] XOR S[1, c] XOR S[2, c] XOR S[3, c] XOR S[4, c]

For each row r, XOR the parity of the two adjacent rows to update the state array:

for r in 0 to 4:

S[r, c] = S[r, c] XOR C_parity(c-1) XOR C_parity(c+1)

where S is the state array, c is the index of the current column, and r is the index of the current row.

***Rho Function:***

For each (i,j) pair, calculate the offset value:

rho_offset(i, j) = (j + 2*i) % 5

For each (i,j) pair, rotate the corresponding lane of the state array by the calculated offset value:

for i in 0 to 4:

for j in 0 to 4:

S[i, j] = rot(S[i, j], rho_offset(i, j))

where S is the state array, rot(S, n) is a function that rotates the elements of S to the left by n positions, and (i,j) are the indices of the current element.

***Pi Function:***

For each (i,j) pair, permute the corresponding lane of the state array to a new location:

for i in 0 to 4:

for j in 0 to 4:

S_new[j, (2*i + 3*j) % 5] = S[i, j]

***Chi Function:***

For each row r, update the elements in that row based on the values in the other two rows:

for r in 0 to 4:

C0 = S[r, 0] XOR (∼S[r, 1] AND S[r, 2])

C1 = S[r, 1] XOR (∼S[r, 2] AND S[r, 3])

C2 = S[r, 2] XOR (∼S[r, 3] AND S[r, 4])

C3 = S[r, 3] XOR (∼S[r, 4] AND S[r, 0])

C4 = S[r, 4] XOR (∼S[r, 0] AND S[r, 1])

S[r, 0], S[r, 1], S[r, 2], S[r, 3], S[r, 4] = C0, C1, C2, C3, C4

makefile: S = S_new

where S is the state array and S_new is a temporary array used to store the permuted elements. (i,j) are the indices of the current element.

where S is the state array, r is the index of the current row, AND is the bitwise logical AND operator, and ∼ is the bitwise logical NOT operator. The Chi function updates each element in a row by performing a bit-wise logical operation with the neighboring elements in the same row.

4: Squeeze the output data from the state array by permuting the state array and extracting the output bits.

5: Return the output data.

# 4 Experimental analysis and discussions

## 4.1 MEASURES

It's crucial to consider each measure's constraints and presumptions before settling on one that's a good fit for the issue in question. It is also essential to evaluate and interpret the selected indicator entirely and concisely to confirm that the findings are relevant and helpful. Few vital measures are incorporated to evaluate the models performance. Some are briefed as follow,

*Simpson Diversity Index:* SDI can also be applied to measure the data heterogeneity. These metrics can be used to assess the degree to which the optimization process has reduced the heterogeneity of the data and made it more uniform.

To estimate the SDI for data and device heterogeneity, we can follow the same formula used in ecology:

$$SDI{=}1{-}\sum\left[(\alpha\left(\alpha{-}1\right))/\mu\left(\mu{-}1\right)\right] \qquad (11)$$

where, $\alpha$ is the content count belonging to a particular class or subgroup, $\mu$ is the total count of content in the dataset.

By calculating the SDI for the training data, we can get a sense of how diverse the data is and whether it may suffer from issues such as class imbalance or sub-population bias. A higher value of SDI indicates greater data and device heterogeneity and may result in better model performance and generalization.

*Accuracy:* It is a commonly used metric to evaluate the performance of a classification model. It measures the proportion of correct predictions made by the model out of the total number of predictions. Specifically, accuracy is calculated as the number of true positive and true negative predictions divided by the total number of predictions. However, accuracy may not always be the best metric to use, especially in imbalanced datasets where one class may dominate the other. In such cases, other metrics such as precision, recall, and F1-score may be more informative.

Precision is the proportion of true positive predictions out of all positive predictions made by the model, while recall is the proportion of true positive predictions out of all actual positive samples in the dataset. F1-score is the harmonic mean of precision and recall, providing a balanced evaluation of the model's performance. Other metrics that may be used to evaluate model performance include ROC-AUC, which measures the trade-off between true positive rate and false positive rate

## 4.2 ANALYSIS OF FL PROCESSES

Adjusting the weight given to each data source based on its reliability or using pretrained procedures to leverage knowledge from associated activities or contexts are just two instances of how the proposed FL model dynamically adapts to the context and the learning process to the heterogeneity of the data sources. The benefit of the proposed FL model is due to the fact that it incorporates a generative model, which is employed throughout the learning procedure to produce synthetic data that could enhance the model's performance and resilience. Furthermore, it reduces processing costs, enabling models to be trained even in constrained networks with limited resources. Figures 5(a) and (b) demonstrate that the proposed FL model is flexible and effective despite more than 70% SDI statistical and data variation. Furthermore, as the number of epochs increases, the model gradually optimizes the heterogeneity, as illustrated in figure 5(a).

On the other hand, existing models performed poorly with low SDI values (see figure 5(b)) whenever statistical and data heterogeneity (discrepancies in data distribution, data format, or data quality) across data sources were present. This is because the model is biased and has poor generalization since it was trained on a subset of information that may not be inclusive of the complete dataset. In addition, noise and inconsistency may also be introduced during the transmission and aggregation of the modeling updates from various sources, which can have a negative effect on performance.

The proposed FL model dynamically adjust to the context and the learning process to the heterogeneity of the data sources, such as by weighting the contribution of each data source based on its reliability or by using transfer learning to leverage knowledge from related tasks or domains. The reason behind the advantage of FL model is the inclusion of generative model that has been used in learning process to generate synthetic data that can improve the performance and robustness of the model. Additionally, it reduces the process overhead, making it feasible to train models even in low-bandwidth or low-power settings. The resultant from figures 5(a) and (b) shows that proposed FL model adapts to the condition and performs well in the presence of statistical and data heterogeneity.

The number and variety of factions, the suitability of the data, the correlation of the data distributions across factual domains, and the model's efficacy all contribute to the accuracy attained by FL against statistical and data heterogeneity in the MHEALTH and MIMIC-II datasets. Furthermore, figures 6 (a) and (b) show that the results of using the suggested model for the learning process are more accurate than those obtained using more conventional FL models. In accordance with the utilization of the MMHEALTH dataset, it is notable that the proposed model registers 97.14% accuracy under statistical heterogeneity, whereas for data heterogeneity; it was noted to be 96.23%. In the case of

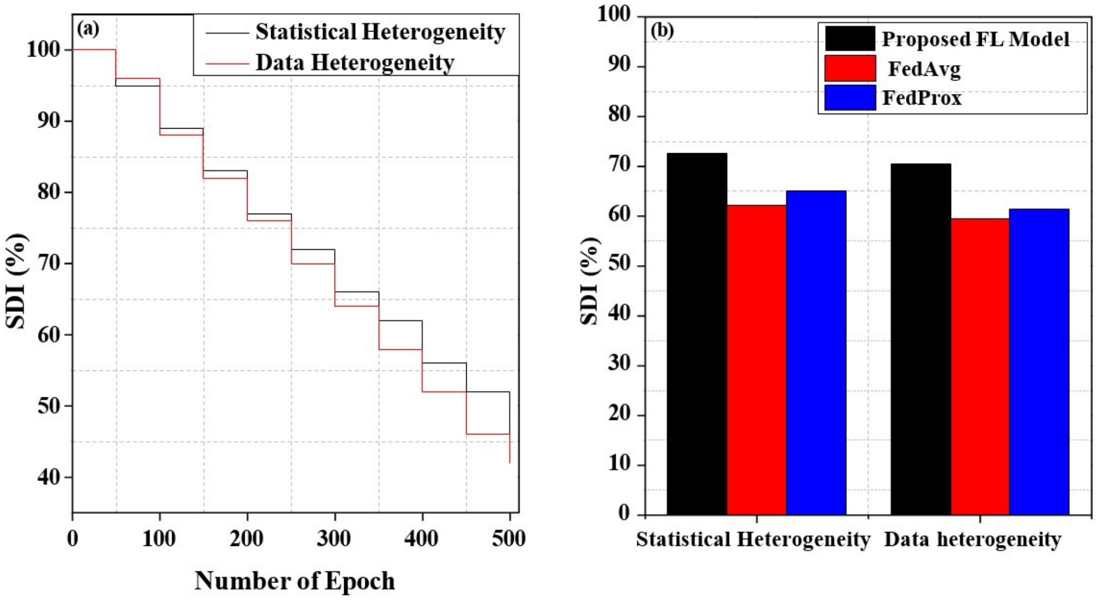

Figure 5: Analysis of SDI over Statistical and Data Heterogeneity

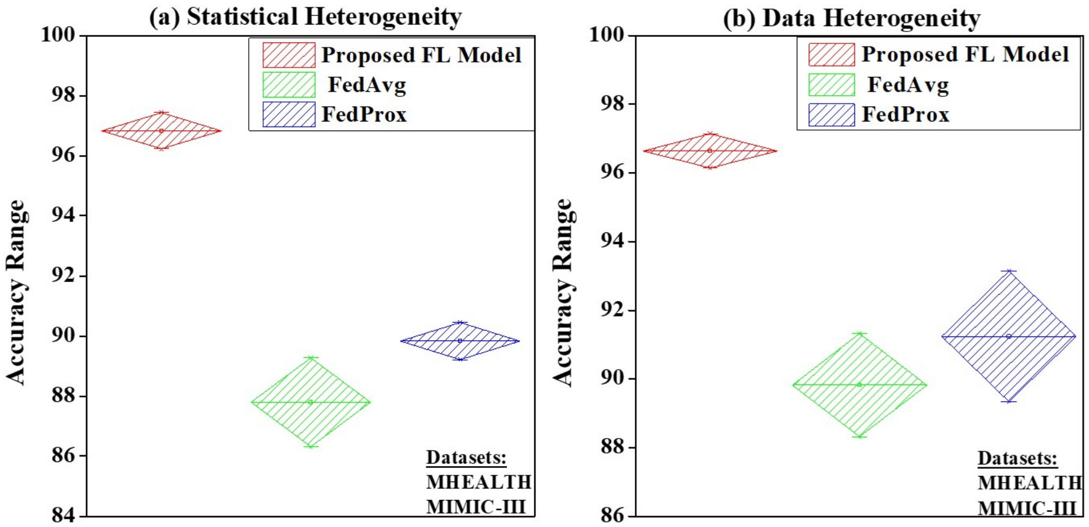

Figure 6: Analysis of Accuracy against (a) Statistical and (b) Data Heterogeneity based on MHEALTH and MIMIC-II Datasets.

MIMIC-III, it is around 96.14% and 97.43% for both statistical and data heterogeneity, respectively. As a result, the proposed FL technique was discovered to be an effective method for overcoming statistical and data heterogeneity in order to create reliable prediction models for the MHEALTH and MIMIC-II datasets.

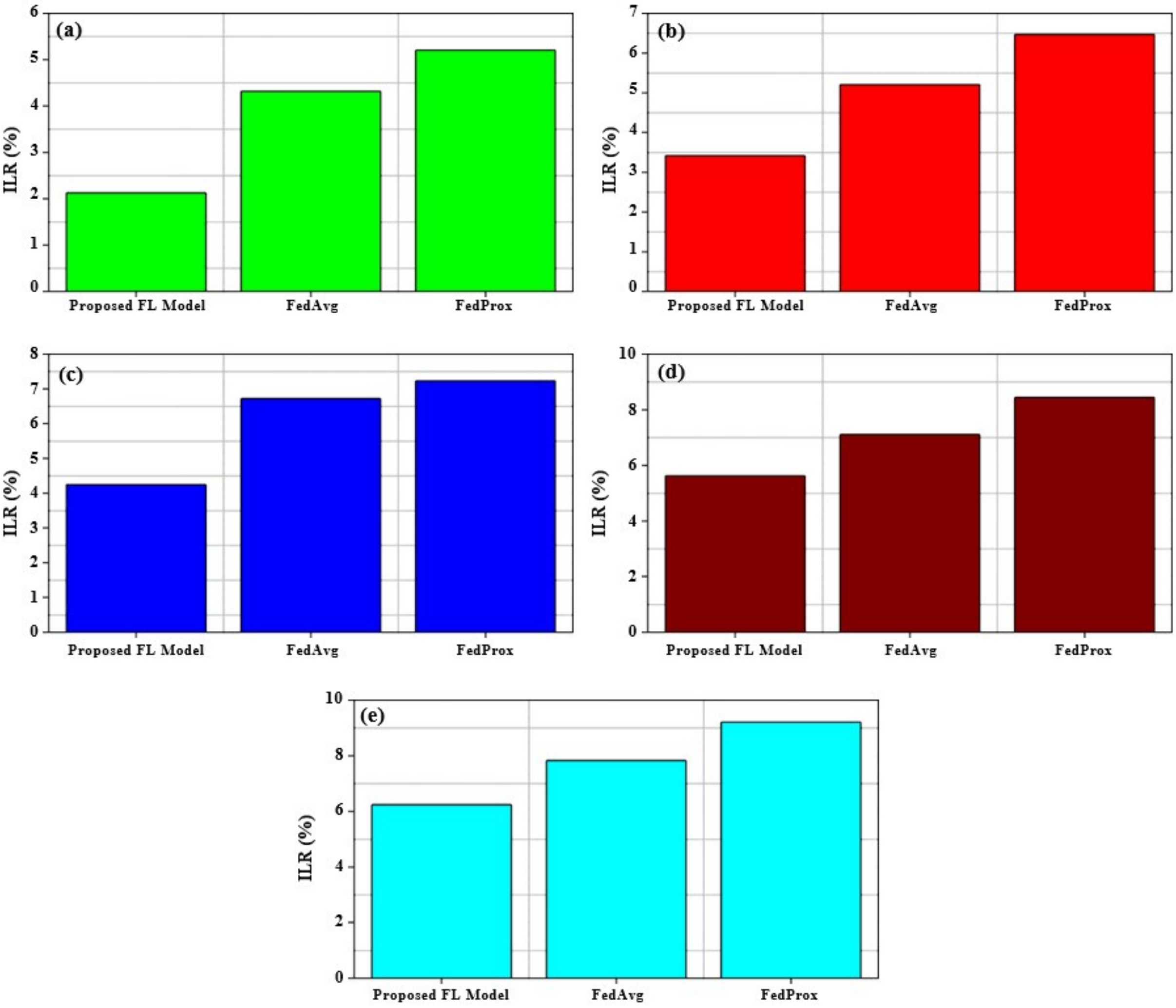

Figure 7: Analysis of Accuracy against (a) Statistical and (b) Data Heterogeneity based on MHEALTH and MIMIC-II Datasets.

ILR Assessment on three different model at varying epochs (a) 100 epochs, (b) 200 epochs, (c) 300 epochs, (d) 400 epochs, and (e) 500 epochs.

In order to make reliable predictions from heterogeneous datasets, it is essential to keep the rate of information loss as low as possible. Standard methods for calculating ILR include contrasting the pre-merge and post-merge datasets and measuring the degree to which they vary. The ILR in FL is the percentage of data that is lost or altered when combining model updates from many sources, each of which has some of the data. From ILR results exhibited in table 2 shows that the gradual increase in epoch count impacts the loss ratio as the amount of information and its associated FL process eventually increases. However, despite such increases, the proposed model tends to lose only a negligible percentage of data. In contrast, the existing models (FedAvg and FedProx) tend to lose maximum percentage information, which is steeply elevating at the epoch counts 400 and 500 (see figure 7(a), 7(b), 7(c), 7(d), and 7(e)). As a result, the suggested model may reduce the drop in precision brought on by data loss by using optimization techniques.

| **Methods** | **ILR(%)** | | | | |
|---|---|---|---|---|---|
| | **100** | **200** | **300** | **400** | **500** |
| Proposed FL Model | 2.13 | 3.42 | 4.25 | 5.63 | 6.24 |
| FedAvg | 4.32 | 5.21 | 6.72 | 7.11 | 7.83 |
| FedProx | 5.21 | 6.47 | 7.23 | 8.45 | 9.21 |

Table 2: ILR Analysis on three different FL model

## 5 Security evaluation

Since FL relies on many different parties exchanging data and making model changes, security is paramount. Multiple methods are used to assess the FL process's safety to protect the data's confidentiality and integrity. In secure aggregation, model updates from several parties are combined without any of the participants' personal information being compromised because of the utilization of AES methods. In addition, blockchain integration improves security, particularly in the face of adversarial attacks. The encryption and decryption times are used to measure the efficiency of the AES algorithm when used with blockchain technology. To combat such threats, the blockchain's SHA-3 256 hashing algorithm is validated in each block of blockchains. The effectiveness of applications that depend on encryption and decryption can be enhanced by reducing the time it takes to conduct these operations. The period that encrypted data is subject to attack can be decreased if the process of encrypting and decrypting it takes less time. Table 3 represents the encryption and decryption time at local and global model. From the observations, it is noted that the proposed model maintains the least encryption and decryption time which increases the conductions of base operation, effectively.

| **Stages** | **Encryption time** | **Decryption time** |
|---|---|---|
| **Local Model** | 1.53 | 1.21 |
| **Global Model** | 2.11 | 1.89 |

Table 3: Encryption and decryption time at local and global model

The success rate is the percentage of attacks that cause the machine-learning model to misclassify the input or produce incorrect output. A high success rate indicates that the attack is effective in compromising the system.

The success rate ($\phi$) of an adversarial attack can be calculated using the following equation:

$$\phi = \frac{\mathcal{Z}}{\mathcal{G}} \tag{12}$$

$\mathcal{Z}$ is the number of adversarial instances that cause misclassification
$\mathcal{G}$ denotes total number of adversarial instances.
For example, if an attacker generates 200 adversarial instances and 40 of them cause misclassification, the success rate of the attack would be: Success rate = 40 / 200 = 0.2 or 20%. Figure 8 shows how the suggested model's success rate steadily decreases despite the high likelihood of vulnerabilities. Likewise, when it comes to protecting training data, FedAvg is superior to FedProx in terms of its performance. This result unequivocally demonstrates the value of using the blockchain-based, sophisticated hashing technology, which guarantees security and gives the training data complete privacy. Fig 8 depicts the Vulnerability Index versus success rate.

## 6 Conclusion and future work

In summary, FL with A-GANs provides a way to train ML models on decentralized data while handling data heterogeneity and privacy concerns. For the purpose of cooperative learning and the safekeeping of vital data in a smart IoT network, this article implements FL between edge-based devices and

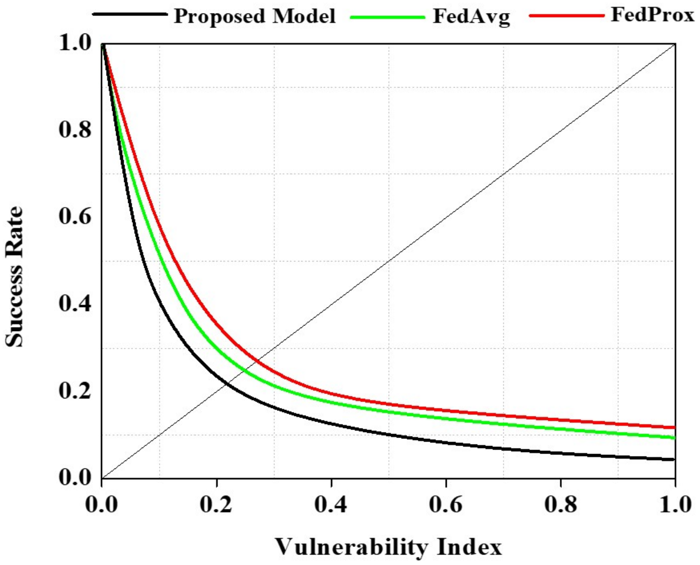

Figure 8: Vulnerability Index versus success

servers in a sparsely populated cloud. By pooling together independent unit models via supervised edge network participants, FL allows several users to train from the same base model in tandem. Even more importantly, blockchain technology handles all information and sensitive messaging activities related to the vulnerable device. Furthermore, a blockchain-based security mechanism has been included to protect user privacy and promote wider practical usage. Finally, the suggested model is contrasted with the top three free, open-source FL models currently in use (FedPD, FedProx, and FedAvg). Experiments indicate that the suggested model outperforms the state-of-the-art methods in terms of statistical significance and device heterogeneity.

Future revisions of our approach will include differential privacy to shield individual identities while exchanging information. To optimize the system's heterogeneity and boost its overall performance, adaptive algorithms are used to choose which client devices will participate in the FL process. The security of FL could be improved by using secure multi-party quantum computing methods. These methods allow information and variables from multiple participants to be safely combined without letting other participants see the original report.

## Funding

The research carried out has not received funds from any organizations.

## Author contributions

The authors contributed equally to this work.

## Conflict of interest

The authors declare no conflict of interest.

# References

[1] Rajagopal A, Nirmala V. Federated AI lets a team imagine together: federated learning of GANs. Int. J. Comput. Sci. Eng. 2019;7(5):704-9.

[2] Banos O, Garcia R, Holgado-Terriza JA, Damas M, Pomares H, Rojas I, Saez A, Villalonga C. mHealthDroid: a novel framework for agile development of mobile health applications. InAmbient

Assisted Living and Daily Activities: 6th International Work-Conference, IWAAL 2014, Belfast, UK, December 2-5, 2014. Proceedings 6 2014 (pp. 91-98). Springer International Publishing.

[3] Banos O, Villalonga C, Garcia R, Saez A, Damas M, Holgado-Terriza JA, Lee S, Pomares H, Rojas I. Design, implementation and validation of a novel open framework for agile development of mobile health applications. Biomedical engineering online. 2015 Dec;14(2):1-20.

[4] Deng S, Zhao H, Fang W, Yin J, Dustdar S, Zomaya AY. Edge intelligence: The confluence of edge computing and artificial intelligence. IEEE Internet of Things Journal. 2020 Apr 1;7(8):7457-69.

[5] Dillon T, Wu C, Chang E. Cloud computing: issues and challenges. In2010 24th IEEE international conference on advanced information networking and applications 2010 Apr 20 (pp. 27-33). Ieee.

[6] Hassan N, Yau KL, Wu C. Edge computing in 5G: A review. IEEE Access. 2019 Aug 30;7:127276-89.

[7] Ahmed, S. T., Kumar, V., & Kim, J. (2023). AITel: eHealth Augmented Intelligence based Telemedicine Resource Recommendation Framework for IoT devices in Smart cities. IEEE Internet of Things Journal..

[8] Hu B, Fang Y, Shi C. Adversarial learning on heterogeneous information networks. InProceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining 2019 Jul 25 (pp. 120-129).

[9] Johnson AE, Pollard TJ, Shen L, Lehman LW, Feng M, Ghassemi M, Moody B, Szolovits P, Anthony Celi L, Mark RG. MIMIC-III, a freely accessible critical care database. Scientific data. 2016 May 24;3(1):1-9.

[10] Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, Bonawitz K, Charles Z, Cormode G, Cummings R, D'Oliveira RG. Advances and open problems in federated learning. Foundations and Trends® in Machine Learning. 2021 Jun 22;14(1–2):1-210.

[11] Karimireddy SP, Kale S, Mohri M, Reddi S, Stich S, Suresh AT. Scaffold: Stochastic controlled averaging for federated learning. InInternational Conference on Machine Learning 2020 Nov 21 (pp. 5132-5143). PMLR.

[12] K. Gunasekaran, V. V. Kumar, A. C. Kaladevi, T. R. Mahesh, C. R. Bhat and K. Venkatesan, "Smart Decision-Making and Communication Strategy in Industrial Internet of Things," in IEEE Access, vol. 11, pp. 28222-28235, 2023, doi: 10.1109/ACCESS.2023.3258407..

[13] Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V. Federated optimization in heterogeneous networks. Proceedings of Machine learning and systems. 2020 Mar 15;2:429-50.

[14] Li T, Sanjabi M, Beirami A, Smith V. Fair resource allocation in federated learning. arXiv preprint arXiv:1905.10497. 2019 May 25.

[15] KarthickRaghunath KM, Koti MS, Sivakami R, Vinoth Kumar V, NagaJyothi G, Muthukumaran V. Utilization of IoT-assisted computational strategies in wireless sensor networks for smart infrastructure management. International Journal of System Assurance Engineering and Management. 2022 Jan 30:1-7.

[16] Ro J, Chen M, Mathews R, Mohri M, Suresh AT. Communication-efficient agnostic federated averaging. arXiv preprint arXiv:2104.02748. 2021 Apr 6.

[17] Venkatesan, Vinoth Kumar, Ivan Izonin, JayalakshmiPeriyasamy, AlagiriIndirajithu, Anatoliy-Batyuk, and Mahesh Thyluru Ramakrishna. "Incorporation of Energy Efficient Computational Strategies for Clustering and Routing in Heter-ogeneous Networks of Smart City." Energies 15, no. 20 (2022): 7524

[18] Tarcar AK. Advancing Healthcare Solutions with Federated Learning. InFederated Learning: A Comprehensive Overview of Methods and Applications 2022 Feb 8 (pp. 499-508). Cham: Springer International Publishing.

[19] Thapa C, Chamikara MA, Camtepe SA. Advancements of federated learning towards privacy preservation: from federated learning to split learning. Federated Learning Systems: Towards Next-Generation AI. 2021:79-109.

[20] Wang S. Edge computing: applications, state-of-the-art and challenges. Advances in Networks. 2019 Nov 15;7(1):8-15.

[21] Kumar, V. Vinoth, V. Muthukumaran, N. Ashwini, I. S. Beschi, K. Gunasekaran, and V. R. Niveditha. "An efficient sign-cryption scheme using near-ring hybrid approach for an IoT-based system." International Journal of e-Collaboration (IJeC) 18, no. 1 (2022): 1-31.

[22] Zhang X, Hong M, Dhople S, Yin W, Liu Y. FedPD: A federated learning framework with adaptivity to non-iid data. IEEE Transactions on Signal Processing. 2021 Oct 1;69:6055-70.

[23] Zhou P, Lin Q, Loghin D, Ooi BC, Wu Y, Yu H. Communication-efficient decentralized machine learning over heterogeneous networks. In2021 IEEE 37th International Conference on Data Engineering (ICDE) 2021 Apr 19 (pp. 384-395). IEEE.

[24] Muthukumaran, V., Vinoth Kumar, V., Joseph, R. B., Munirathnam, M., Beschi, I. S., & Niveditha, V. R. (2022, November). Efficient Authenticated Key Agreement Protocol for Cloud-Based Internet of Things. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2022, Volume 3 (pp. 365-373). Singapore: Springer Nature Singapore.

[25] Jatain, D., Singh, V., &Dahiya, N. (2021). A Contemplative Perspective on Federated Machine Learning: Taxonomy, Threats & Vulnerability Assessment and Challenges. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.05.016

[26] Qureshi, J. N., Farooq, M. S., Abid, A., Umer, T., Bashir, A. K., &Zikria, Y. B. (2022). Blockchain applications for the Internet of Things: Systematic review and challenges. *Microprocessors and Microsystems*, *94*, 104632. https://doi.org/10.1016/j.micpro.2022.104632

[27] Jatain, D., Singh, V., &Dahiya, N. (2022). Blockchain Base Community Cluster-Federated Learning for Secure Aggregation of Healthcare Data. Procedia Computer Science, 215, 752–762. https://doi.org/10.1016/j.procs.2022.12.077

[28] Mallah, R. A., López, D., & Halabi, T. (2023). Blockchain-enabled Efficient and Secure Federated Learning in IoT and Edge Computing Networks. 2023 International Conference on Computing, Networking and Communications (ICNC). https://doi.org/10.1109/icnc57223.2023.10074277

[29] Waheed, N., & Usman, M. (2020). Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. Corpus ID: 221137844

[30] Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2021). Communication-Efficient Federated Learning and Permissioned Blockchain for Digital Twin Edge Networks. IEEE Internet of Things Journal, 8(4), 2276–2288. https://doi.org/10.1109/jiot.2020.3015772

COPE

Member since 2012
JM08090

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

*Cite this paper as:*

Muthukumaran, V.; Sivakami, R.; Venkatesan, V.K.; Balajee, J.; Mahesh, T. R.; Mohan, E.; Swapna, B. (2023). Optimizing Heterogeneity in IoT Infra Using Federated Learning and Blockchain-based Security Strategies, *International Journal of Computers Communications* & *Control*, 18(6), 5890, 2023.

https://doi.org/10.15837/ijccc.2023.6.5890