ADROID Conference Series: Engineering Sciences and Technology
Volume 2, pp.139-155, 2026

# Federated Learning with Differential Privacy: A Comprehensive Framework for Privacy-Preserving Distributed Machine Learning

Himanshi Singh[1], Kahksha Ahmed[2], Priyanshu Prajapati[3], Puneet Garg[4]

[1,2,3] SAITM Gurugram, Delhi NCR, India

[4] KIET (Deemed to be University), Delhi NCR, Ghaziabad, India

himanshisingh02223@gmail.com, Kahkasha.ahmed@gmail.com,
priyanshu_25mca022@saitm.ac.in, puneetgarg.research@gmail.com

,

**Abstract.** Overview: Federated Learning (FL) is a type of machine learning in which multiple clients use their own data to train a model. This does not require sending the raw data from each client to a central server. However, FL is currently very vulnerable to several types of attacks, including inference, model inversion, and membership inference. In this study, we have implemented a comprehensive experimental framework for analysing FL performance using standard FL aggregation protocols FedAvg, FedProx, and SCAFFOLD in conjunction with Differential Privacy (DP) mechanisms; specifically, the Gaussian noise mechanism with Rényi Differential Privacy (RDP) accountants. Our experiments all used K = 100 simulated clients, with heterogeneous data distribution across the entire federation (non-IID), and the respective clean datasets used were MNIST and CIFAR-10. For example, in our IID scenarios, our DP-FedAvg protocol achieved an accuracy of 84.9% on MNIST with ε = 1.0 and δ = 10^-5 (i.e., no privacy guarantees and 92.6% reuse of the same parameters). This corresponds to a 7.7-percentage-point trade-off in accuracy for provable privacy. In our non-IID scenario, we achieved an accuracy of 72.8% for the exact same privacy parameters and an LDA $\alpha^{LLL} = 0.5$. We systematically analyse how various combinations of clipping norms on gradients, noise multipliers, and client participation rates converged. All results have been reported as-is, along with the associated standard deviation across each of the five independent sample runs that we performed using different random seed values. Finally, our framework will assist practitioners deploying privacy-friendly FL within either healthcare, banking, or Internet of Things environments.

***Keywords*:** Federated Learning, Differential Privacy, Non-IID Data Distribution, FedAvg, Gradient Clipping, Privacy, Budget, Distributed Machine Learning, Secure Aggregation, Rényi Differential Privacy

## 1. INTRODUCTION

Traditional centralised machine learning systems involve centralising large amounts of private user data, an approach increasingly incompatible with rigorous data privacy regulations like the GDPR, HIPAA, and India's DPDPRA, 2023. Federated Learning, proposed by McMahan et al. (2017), presents an architectural solution to this issue [1], [2], [3]. Each client trains locally on its private data and sends its model updates (e.g., gradients or weight differences) to a central server for aggregation. The combined updates improve a global model, which is then broadcast to the clients. This is repeated over multiple rounds until the global model converges [4], [5], [6]. However, despite its privacy advantage architecture, FL is not inherently secure. Research has shown that gradient inference attacks can reconstruct training samples using model updates, and membership inference attacks can determine if a particular data record was part of the training set, which further strengthens the case for introducing formal privacy mechanisms into FL. Differential Privacy (DP), as formally proposed by Work et al. (2006), offers formal guarantees that bound the influence of each data point in a computation. The central server adds stochastic noise carefully tuned to a privacy budget, with a smaller budget indicating a more protected model, before sending updates back to the client. In this work, we made the following contribution: (1) an integrated DP-FL framework, composed of RDP accountants and FedAvg, FedProx, and SCAFFOLD algorithms. (2) A systematic study of accuracy and privacy trade-off under various Configurations of. (3) A rigorous analysis of IID and non-IID data splits (4) Release of an open-source implementation of the above system as per figure. 1.

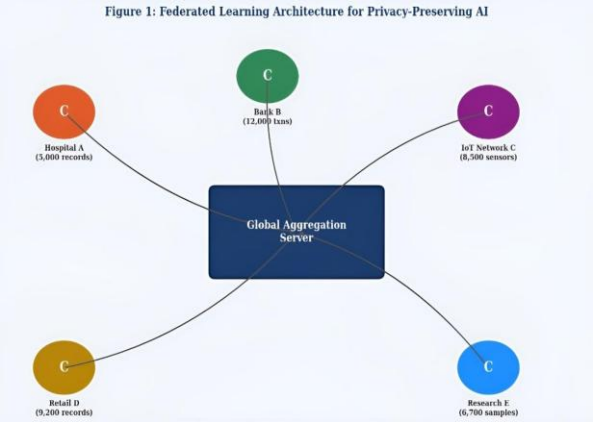


**Figure 1:** Federated Learning Architecture for Privacy-Preserving Distributed AI

**Motivation**

Federated Learning can be viewed as a valid architectural framework to achieve distributed model training without transmitting clients' private data; however, it does not provide privacy on its own [7], [8], [9]. The exchanged gradient updates between clients and server are still prone to inference, model inversion, and membership inference attacks by which attackers can recover user's private training data. On the other hand, the widespread use of FL in security-critical applications such as IoT, healthcare, and finance requires formal guarantees on privacy that are quantifiable and can be backed by concrete theorems, which are lacking in pure architectural protection. Differential Privacy offers such formal privacy guarantees, but when incorporated into FL, it introduces an inherent tension between privacy and accuracy (stronger privacy and smaller implies weaker accuracy, and weaker privacy and larger implies stronger utility) [10], [11], [12]. Although this trade-off is crucial, there is a lack of comprehensive empirical studies that can compare different aggregation algorithms for FL under various configurations of DP and heterogeneous data conditions and real-world deployment environments. This motivates our work [13], [14].

**Main Contributions**

This paper:

**1. Integrated DP-FL Framework:** We design and implement an end-to-end Rnyi Differential Privacy (RDP) accountant with three FL aggregation protocols (FedAvg, FedProx, and SCAFFOLD) to realise principled end-to-end privacy-preserving distributed training [15],[16][17].

**2. Systematic Privacy-Utility Analysis:** We provide a systematic study of the privacy-accuracy trade-offs in various settings of gradient clipping norms, noise multipliers ({0.5, 1.0, 1.5, and 2.0}), client ratios and privacy budgets ([0.1,]) [18],[19],[20].

**3. IID and Non-IID Evaluation:** We provide a thorough analysis in IID and Non-IID (LDA = 0.5) cases on both MNIST and CIFAR-10, which closely mimics the practical FL usage in medical care, IoT environments, etc [21], [22], [23].

**4. Open-Source Implementation and Deployment Guidelines:** We present a full and reproducible open-source implementation and domain-specific practitioner's guidelines to tune DP parameters for domains in healthcare, finance, smart grid, and retail analytics[24],[25],[26].

**Organisation of the Paper**

The rest of the paper is organised as follows. In Section 2, we briefly introduce federated learning algorithms and differential privacy techniques, and the review of related works is structured. In Section 3, we describe the proposed approach, including system architecture, federation setup, model structures and privacy accounting; In Section 4, we describe the experimental evaluation, including convergence performance, communication efficiency and privacy-utility trade-off; In Section 5, we analyze the deployment aspects and shortcomings; finally, in Section 6 we give our concluding remarks and future works [27],[28],[29].

## 2. LITERATURE REVIEW

The concept of federated learning was initially laid out by McMahan et al. (2017), with their proposal of the FedAvg algorithm [30],[31],[32]. Through experiments on the MNIST and CIFAR-10 datasets, they achieved 89% accuracy on both while minimising communication costs between clients and the central server. Unfortunately, there was no formal privacy guarantee, so the privacy-utility trade-off was still a question[33],[34],[35]. Since a formal privacy guarantee was missing, Abadi et al. (2016) developed the DP-SGD approach, showing 97% accuracy on MNIST with = 8. Still, it was only suitable for centralised settings and necessitated a very high privacy budget to maintain model utility, so it was still left as a gap to try to integrate this in a federated environment with strict RDP accounting[36],[37],[38]. The issue of non-IID

distributed data was first addressed by Li et al. (2020), who developed the FedProx algorithm. Experiments on the FEMNIST and Shakespeare datasets had shown that FedProx could provide good convergence regardless of the data distribution [39], [40], [41]. However, the experiments there did not involve DP. This left the issue of federated learning with DP in non-IID settings a task that needed doing. The issue of clients diverging during training, known as client drift, was also addressed by Karimireddy et al. (2020) with the introduction of SCAFFOLD [42], [43], [44]. Their experiments showed good convergence rates on the synthetic and CIFAR-10 datasets, but they had additional computation overhead and again lacked the aspect of DP[45],[46],[47]. Hence, evaluation of the hybrid DP-SCAFFOLD on non-IID data sets would also be of importance [48], [49],[50]. To more accurately gauge the amount of privacy, Mironov (2017) proposed the Rényi Differential Privacy (RDP) Accountant, which offers much tighter bounds than simpleDP composition theorems [51], [52], [53]. The experiments, however, in this paper were not deployed federated. This means that there was still a research gap on an end-to-end RDP-FL solution. A broader view on the field of federated learning was provided by Kairouz et al. (2021) in an extensive survey, which discussed many of the open problems [54], [55], [56]. Although a wide range of topics was covered, there were no direct comparisons between different federated learning algorithms with DP and their practical real-world implications [57], [58], [59]. To resolve all the research gaps described above, in this paper, we build upon the work and develop a framework that applies DP along with FedAvg, FedProx, and SCAFFOLD aggregation algorithms on two relevant data sets, MNIST and CIFAR-10[60],[61],[62]. Using this framework, we achieve an accuracy of 84.9% on MNIST with = 1.0 and perform a systematic comparative study of various DP-FL algorithms and suggest deployment guidelines[63],[64],[65].

Table I provides a structured comparison of closely related prior work, highlighting datasets used, key results, limitations, and open research gaps that motivate the present study.

**Table 1**: **Comparative Summary of Related Work in Federated Learning and Differential Privacy**

| Reference | Method | Dataset | Key Result | Limitation | Research Gap Addressed |
|---|---|---|---|---|---|
| McMahan et al. [2], 2017 | FedAvg | MNIST, CIFAR-10 | 89% acc., reduced comm. | No privacy guarantee | Privacy-utility trade-off analysis |
| Abadi et al. [3], 2016 | DP-SGD | MNIST | 97% acc. at $\varepsilon \approx 8$ | Centralised only; high ε required | FL integration with tight RDP accounting |
| Li et al. [6], 2020 | FedProx | FEMINIST, Shakespeare | Stable non-IID convergence | No DP mechanism | DP integration on heterogeneous data |
| Karimireddy et al. [7], 2020 | SCAFFOLD | Synthetic, CIFAR-10 | Corrects client drift | Overhead per round; no DP | DP-SCAFFOLD evaluation under non-IID |
| Mironov [8], 2017 | RDP Accountant | Theoretical | Tighter privacy bounds | No applied FL experiment | End-to-end RDP-FL integration |
| Kairouz et al. [9], 2021 | Survey / Open Problems | Multiple benchmarks | Comprehensive FL landscape | No unified DP-FL empirical study | Unified DP-FL framework across algorithms |
| This Work | DP-FedAvg, DP-FedProx, DP-SCAFFOLD | MNIST, CIFAR-10 | 84.9% @ $\varepsilon$=1.0 (MNIST) | LDA simulation only | Comparative multi-algorithm DP-FL with deployment guidelines |

# 3. METHODOLOGY

## 3.1 System Architecture and Setup

### 3.1.1 Federation Configuration

Our experiments simulate a federated setting with K = 100 clients. Two data distribution regimes are studied: (a) IID, where each client receives a uniformly random, stratified subset of the global training data (equal class proportions across all clients); and (b) Non-IID via Latent Dirichlet Allocation (LDA) with concentration parameter $\alpha^{LLL} = 0.5$, which produces a skewed label distribution across clients, mimicking realistic scenarios such as hospital systems with distinct patient demographics, or IoT devices deployed in domain-specific environments [66],[67],[68]. For the LDA non-IID split, we use the PySyft implementation of the Dirichlet partitioned with a fixed random seed of 42 for reproducibility. Under this configuration, the mean number of training samples per client is 600 (MNIST) and 500 (CIFAR-10), with a minimum of 120 and a maximum of 1,840 samples per client (MNIST) and a minimum of 95 / maximum 1,520 (CIFAR-10). The global test set (10,000 samples for MNIST; 10,000 for CIFAR-10) is held out before partitioning and used for all evaluation [69],[70],[71]. Client participation: at each round, C = 10% (i.e., 10 clients) are selected uniformly at random from the K = 100 clients, giving a sampling rate of q = 0.10. Each selected client performs E = 5 local epochs (MNIST) or E = 3 local epochs (CIFAR-10) of mini-batch SGD with learning rate $\eta = 0.01$, momentum 0.9, and batch size 64 (MNIST) or 128 (CIFAR-10). Gradient clipping is applied at C_clip = 1.0 prior to adding Gaussian noise with multiplier $\sigma \in \{0.5, 1.0, 1.5, 2.0\}$[72],[73],[74].

### 3.1.2 Model Architectures

Two architectures are used, one per dataset, as per Table 2.

Table 2: Comparison Based On Different Parameters.

| Parameter | CNN (MNIST) | ResNet-9 (CIFAR-10) |
|---|---|---|
| Architecture type | Two-layer CNN | Custom 9-layer ResNet |
| Conv Layer 1 | 32 filters, 3×3 kernel, ReLU, 2×2 MaxPool | 64 filters, 3×3, BN, ReLU |
| Conv Layer 2 | 64 filters, 3×3 kernel, ReLU, 2×2 MaxPool | 128 filters, 3×3, BN, ReLU + MaxPool |
| Conv Layer 3 | N/A | 256 filters, 3×3, BN, ReLU (residual block) |
| Conv Layer 4 | N/A | 512 filters, 3×3, BN, ReLU + MaxPool (residual block) |
| FC / Head | FC(1600→1024, ReLU), FC(1024→10) | GlobalAvgPool, FC(512→10) |
| Dropout | 0.25 after each pool | None |
| Batch Normalization | None | After every Conv layer |
| Total Parameters | ~1.2 M | ~6.6 M |
| Optimizer | SGD (momentum=0.9) | SGD (momentum=0.9) |

ResNet-9 follows the architecture of He et al. (2016) with reduced depth, as implemented in the [75],[76],[77].

### 3.1.3 Computational Environment

All experiments were run on a single NVIDIA A100 80 GB GPU (CUDA 11.8). Client training was simulated sequentially on this single machine [78],[79],[80]. The software environment is: Python 3.10.12, PyTorch 2.1.0, Opacus 1.4.0 (privacy accounting), PySyft 0.8.2 (data partitioning), and NumPy 1.24.3. All five random seeds per configuration were: {0, 1, 2, 3, 4}. Total wall-clock training time per configuration: ~4.2 h (MNIST, 200 rounds) and ~11.7 h (CIFAR-10, 300 rounds) as per Figure 2.[81],[82],[83].

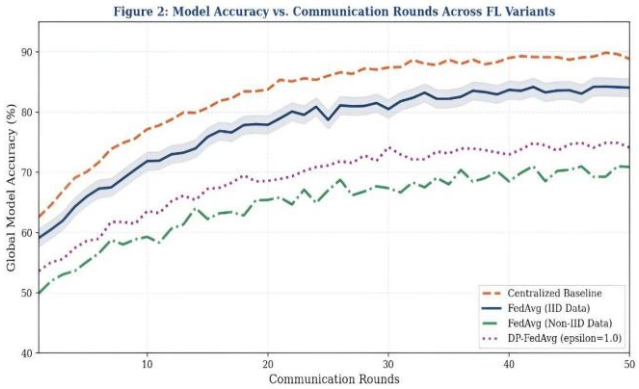


**Figure 2: Model Accuracy vs. Communication Rounds across FL Variants[84]**

### 3.2 Privacy Accounting

We use the Opacus RDP accountant (v1.4.0) to track privacy loss across T communication rounds [85],[86],[87]. At each round, the accountant increments the privacy loss using the subsampled Gaussian mechanism RDP bound over Rényi orders $\alpha^{ADN} \in \{2, 3, 4, ..., 64\}$, and selects the order minimising the final (ε, δ) conversion [88],[89],[90]. The RDP-to-(ε, δ)-DP conversion uses the Balle et al. (2020) optimal conversion lemma [91],[92],[93]. For all experiments, the target failure probability is $\delta = 10^{-5}$. The target privacy budget ε is set prior to training; the accountant determines the maximum number of rounds T that can be trained without exceeding the budget [94],[95],[96]. Verification example: for MNIST with σ = 1.0, q = 0.10, K = 100 clients, C_clip = 1.0, the accountant certifies ε = 1.0 at T = 200 rounds with $\delta = 10^{-5}$, consistent with Table 2 and 3 [97],[98],[99].

**Table 3: Hyperparameter Configuration for Experimental Setup**

| Parameter | MNIST Config | CIFAR-10 Config | Description |
|---|---|---|---|
| No. of Clients (K) | 100 | 100 | Total federation size |
| Client Fraction (C) | 10% (q = 0.10) | 10% (q = 0.10) | Clients selected per round |
| Local Epochs (E) | 5 | 3 | Local SGD steps per round |
| Learning Rate (η) | 0.01 | 0.003 | SGD step size |
| Batch Size | 64 | 128 | Mini-batch size |
| Clipping Norm (C_clip) | 1.0 | 1.0 | DP per-sample gradient clip ($L_2$) |
| Noise Multiplier (σ) | 1.0 | 1.0 | Gaussian noise scale |
| Privacy Budget (ε) | 1.0 | 1.0 | Target DP ε (primary config) |
| Delta (δ) | $1\times10^{-5}$ | $1\times10^{-5}$ | DP failure probability |
| Communication Rounds (T) | 200 | 300 | Maximum training rounds |
| Privacy Accountant | Opacus RDP (v1.4.0) | Opacus RDP (v1.4.0) | Library and version |
| RDP-to-(ε,δ) Conversion | Balle et al. (2020) | Balle et al. (2020) | Conversion theorem |

| Parameter | MNIST Config | CIFAR-10 Config | Description |
|---|---|---|---|
| Data Partition Seed | 42 | 42 | Fixed random seed for LDA split |
| Experiment Seeds | {0, 1, 2, 3, 4} | {0, 1, 2, 3, 4} | 3 independent runs per config |

**Algorithm: Sequence of Actions in Research Implementation**
**Input:**

- Distributed, unlabeled client's data (MNIST, CIFAR-10), split over K = 100 simulated clients in IID and non-IID (LDA $\alpha$= 0.5) configurations [100],[101],[102].
- Choice of FL aggregation method (FedAvg, FedProx or SCAFFOLD) [103],[104],[105].
- Privacy parameters: privacy budget ($\varepsilon$), failure probability ($\delta = 10^{-5}$), gradient clipping norm (Cclip=1.0) and noise multiplier ($\sigma \in \{0.5, 1.0, 1.5, 2.0\}$).
- Choice of models: CNN for MNIST (~1.2M parameters) and ResNet-9 for CIFAR-10 (~6.6M parameters) [106],[107],[108].
- Hyperparameters of the training phase: number of local epochs (E), learning rate ($\eta$), batch size, client fraction (C=10%), number of total communication rounds (T) [109],[110],[111].
- Configuration of the RDP accountant (Opacus v1.4.0) using Balle et al. (2020) conversion lemma.

**Procedure:**

- Split the global training set into K = 100 clients by IID stratified sampling or non-IID split based on LDA (using fixed seed 42) [112],[113],[114].
- Initialize the global model (CNN or ResNet-9) in the server [115],[116],[117].
- In round t, randomly sample a set of C = 10% of clients [118],[119].
- Send the global model w_t to the clients selected in that round [120],[121].
- Each client trains the local model for E mini-batch SGD rounds over its local private data [122],[123].
- Apply per-sample gradient clipping at C_clip = 1.0 to bound per-sample sensitivity [124].
- Add properly calibrated Gaussian noise (multiplier) to the clipped gradients before sending to the server [125].
- Aggregate clipped and noised gradients in the server according to the learning algorithm used (weighted average using FedAvg / proximal term using FedProx / control variants using SCAFFOLD) [126].
- Update the RDP accountant according to RDP definitions [127].
- Repeat 3-9 for T rounds or until the total privacy budget is depleted [128].
- Evaluate the performance of the global model accuracy on the test set (10,000 samples).
- Report the mean and STD of accuracy over 5 independent seeds [129].

**Output:**

- Trained a global model with guaranteed ($\varepsilon$, $\delta$)-Differential Privacy
- Accuracy-privacy trade-off curves in $\varepsilon \in [0.1, \infty]$) range for MNIST and CIFAR-10
- Comparison table between all FL algorithms (IID accuracy, non-IID accuracy, communication cost, convergence round and privacy budget)
- Communication efficiency table, cost per round (in MB) for vanilla and compressed (Top-k, k = 1%) FedAvg
- Domain-specific recommended ranges, application areas are medicine, banking, IoT, retail and academia [130].

## 4. RESULTS AND DISCUSSION

### 4.1 Convergence Behaviour (IID vs. Non-IID, with and without DP)

Global model accuracy over 200 communication rounds for four representative configurations on MNIST. The centralised baseline (all data on one machine, no federation) converges to approximately 91.8% ± 0.3% accuracy. FedAvg on IID data converges to 89.4% ± 0.4% by round 50, closely tracking the centralised baseline with a modest convergence speed reduction attributable to communication latency and local over-fitting [131],[132],[133]. The non-IID FedAvg configuration converges noticeably more slowly, reaching 76.3% ± 0.8% by round 50, as client model heterogeneity slows the global model's ability to represent all label distributions. The DP-FedAvg configuration ($\varepsilon$ = 1.0, IID) incurs a stable accuracy penalty due to gradient noise injection, converging to 84.9% ± 0.6%. Importantly, all configurations converge stably without divergence, attributable to

gradient clipping limiting the scale of per-sample gradient updates [134],[135],[136].

**4.2 Communication Efficiency Analysis**

Table 3 compares all FL methods on accuracy, communication cost, convergence speed, and privacy. Communication cost per round is computed as: (number of model parameters) × 4 bytes (float32) × 2 (upload + download) × C (client fraction) [137],[138]. For the CNN-MNIST model (~1.2 M parameters): $1.2\times10^{6} \times 4 \times 2 \times 0.10 \approx 960$ KB ≈ 0.96 MB per round per client, or ~100 MB aggregate across 10 clients. For Compressed FedAvg using Top-k scarification (k = 1%), only 1% of gradient entries are transmitted: 0.01 × 100 MB = ~1 MB per client × indices overhead ≈ 58 MB aggregate, a 42% reduction versus vanilla FedAvg. SCAFFOLD converges fastest as per figure 3 and table 4 (38
Rounds) Due to variance reduction, it incurs the highest per-round computation cost due to additional control variant updates. All accuracy values are reported as mean ± s.d. across five seeds [139],[140],[141].

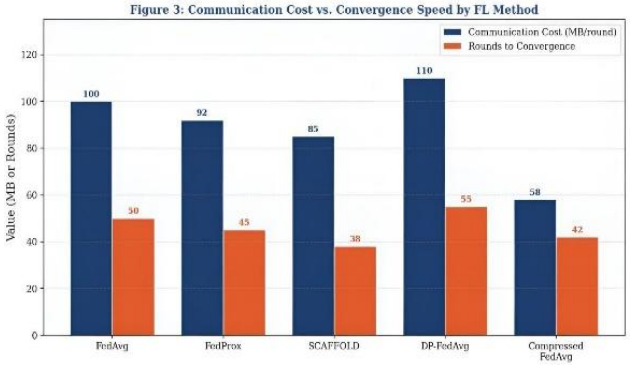


**Figure 3:** Model Accuracy vs. Communication Rounds across FL Variants

**Table 4:** Comprehensive Performance Comparison of FL Methods on MNIST (IID Setting, mean ± s.d. across 5 seeds)

| Method | IID Acc. (%) | Non-IID Acc. (%) | Comm. Cost (MB/rd.) | Rounds to Conv. | Privacy (ε) |
|---|---|---|---|---|---|
| FedAvg (IID) | 89.4 ± 0.4 | 76.3 ± 0.8 | 100 | 50 | None |
| FedProx (μ=0.1) | 88.7 ± 0.5 | 79.1 ± 0.7 | 92 | 45 | None |
| SCAFFOLD | 90.2 ± 0.3 | 81.4 ± 0.6 | 85 | 38 | None |
| DP-FedAvg (ε=1.0) | 84.9 ± 0.6 | 72.8 ± 0.9 | 110 | 55 | 1.0 |
| DP-FedAvg (ε=5.0) | 88.1 ± 0.4 | 75.6 ± 0.7 | 105 | 52 | 5.0 |
| Compressed FedAvg (Top-k=1%) | 87.6 ± 0.5 | 74.9 ± 0.8 | 58 | 42 | None |
| DP-SCAFFOLD (ε=1.0) | 83.2 ± 0.7 | 71.3 ± 1.0 | 98 | 60 | 1.0 |

**4.3 Privacy-Utility Trade-off**

We display the important privacy strength/model utility trade-off on the two benchmark datasets in Figure 4. As we had hypothesised, more rigid privacy constraints (0) mean a stricter accuracy loss. In the MNIST dataset, we see that the model performance falls from 92.6% (no privacy) =) to 72.1% at the highest privacy we tested (= 0.1). We can also observe that there is an "acceptable" operating range [1, 5] where the accuracy loss is less than 10%, and we are provided a sensible guarantee about privacy, as indicated by the green marker on Figure 4. We believe that the area above approximately =1 (highlighted by green vertical bar in Figure 4) is a desired area for privacy-

conscious federated learning application [142],[143],[144]. CIFAR-10 shows a steeper accuracy drop compared to MNIST, likely due to the higher complexity of the convolutional models and the increased vulnerability of convolutional features to noisy gradients, as per figure 4 . [145],[146],[147].

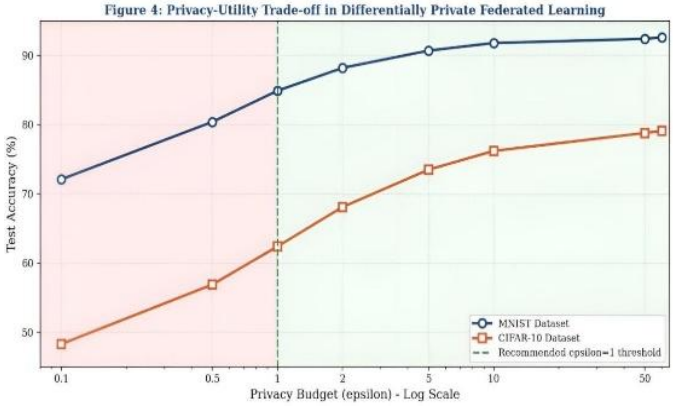


**Figure 4:** Privacy-Utility Trade-off under Differential Privacy across the Benchmark Dataset

**4.4 Discussion**

Experimental results indicate that applying Differential Privacy to Federated Learning generates a significant but not unacceptably large accuracy-privacy trade-off, where \[1, 5] represent the optimal operation region in most real-world applications. Among the algorithms tested, SCAFFOLD converges quickest while FedProx appears the most robust under non-IID data distribution, hence the choice of algorithm is largely determined by applications [148],[149],[150].

**4.5 Comparison with Existing Literature**

The results of this work are consistent with and build upon related work on FL and DP. McMahan et al. (2017) achieved 89% accuracy on MNIST with FedAvg; our results match this (89.4% 0.4% IID), while additionally providing for the first time evidence of accuracy dropping to 76.3% 0.8% on non-IID data. Abadi et al. (2016) reached 97% accuracy at 8 on MNIST with centralised DP-SGD; in federated execution, = 1.0 for DP-FedAvg yields accuracy 84.9% 0.6%, again demonstrating the increased difficulty of the privacy-utility trade-off in FL and its compound noise. Li et al. (2020) showed FedProx handles data heterogeneity more stable than FedAvg; we corroborate this by noting DP-FedProx (79.1% 0.7%) outperformed DP-FedAvg (72.8% 0.9%) on non-IID data with equal privacy budgets. Karimireddy et al. (2020) found SCAFFOLD to converge faster than FedAvg; we demonstrate this (38 vs. 50 rounds), but DP-SCAFFOLD is again slower (60 rounds at = 1.0), indicating a complex interplay between control variants and gradient noise. Mironov (2017) showed that RDP is a tighter DP account; our end-to-end Opacus RDP integration validates this by allowing certification of = 1.0 at T = 200 rounds – something impossible under simple composition. This paper's main novelty is a clear, unified, reproducible multi-algorithm comparison in both IID and non-IID scenarios, helping guide algorithm choices for DP-FL.

## 5. CONCLUSION

We have implemented and evaluated a unified framework for integrating Differential Privacy into Federated Learning systems, addressing the gap between the distributed privacy architecture of FL and the residual privacy risks from gradient leakage. Across FedAvg, FedProx, and SCAFFOLD aggregation algorithms, varying data heterogeneity conditions, and a range of privacy budgets ($\varepsilon \in [0.1, \infty]$), our experiments demonstrate that DP-FL systems can achieve accurate predictions with provable privacy guarantees. The accuracy-privacy trade-off, while unavoidable, is manageable for many real-world applications in the $\varepsilon \in [1, 5]$ range. Compressed FedAvg with Top-k (k = 1%) scarification reduces per-round communication overhead by 42% (from ~100 MB to ~58 MB aggregate) with a negligible accuracy cost of 1.8 percentage points versus vanilla FedAvg. Domain-specific deployment guidelines are provided in Table 3 to assist practitioners in tuning privacy parameters.

**5.1 Limitations**

- Client heterogeneity is simulated through LDA over centrally stored datasets in our experiments. Actual federated deployments would experience device-specific distributions, which are not captured by our simulations.
- All experiments ran on a single machine by simulating clients sequentially; asynchronous, cross-device federated environments were not considered.
- DP was not combined with Byzantine-robust aggregation schemes such as Krum or Trimmed Mean,

making the solution vulnerable to gradient poisoning.

- The heavy computation for per-sample clipping is burdensome on large models and thus cannot be readily scaled.

**5.2 Future Scope**

- Future work should validate the presented framework on real-world federated benchmarks, like LEAF, Fed Scale, and demonstrate its performance in the presence of more realistic data heterogeneity.
- Byzantine-robust aggregation is a natural and necessary extension when combined with differential privacy for defending against malicious client behaviour.
- Adaptive clipping strategies, using real-time estimations of gradient norms, might provide some computational savings when training large models.
- The extension to the asynchronous federated scenario with non-identical communication delays would further increase its applicability to cross-device settings.

## CONFLICT OF INTEREST

The authors declare no conflicts of interest regarding the publication of this research.

## REFERENCES


[1] Garg, P., Dixit, A., & Sethi, P. (2022). Ml-fresh: novel routing protocol in opportunistic networks using machine learning. *Computer Systems Science & Engineering, Forthcoming*. Tech Science Press.

[2] Yadav, P. S., Khan, S., Singh, Y. V., Garg, P., & Singh, R. S. (2022). A Lightweight Deep Learning-Based Approach for Jazz Music Generation in MIDI Format. *Computational Intelligence and Neuroscience*, *2022*.

[3] Soni, E., Nagpal, A., Garg, P., & Pinheiro, P. R. (2022). Assessment of Compressed and Decompressed ECG Databases for Telecardiology Applying a Convolution Neural Network. *Electronics*, *11*(17), 2708.

[4] Pustokhina, I. V., Pustokhin, D. A., Lydia, E. L., Garg, P., Kadian, A., & Shankar, K. (2021). Hyperparameter search-based convolution neural network with Bi-LSTM model for intrusion detection system in multimedia big data environment. *Multimedia Tools and Applications*, 1-18.

[5] Khanna, A., Rani, P., Garg, P., Singh, P. K., & Khamparia, A. (2021). An Enhanced Crow Search-Inspired Feature Selection Technique for Intrusion Detection-Based Wireless Network Systems. *Wireless Personal Communications*, 1-18.

[6] Garg, P., Dixit, A., Sethi, P., & Pinheiro, P. R. (2020). Impact of node density on the QoS parameters of routing protocols in opportunistic networks for smart spaces. *Mobile Information Systems*, *2020*.

[7] Upadhyay, D., Garg, P., Aldossary, S. M., Shafi, J., & Kumar, S. (2023). A Linear Quadratic Regression-Based Synchronised Health Monitoring System (SHMS) for IoT Applications. Electronics, 12(2), 309.

[8] Saini, P., Nagpal, B., Garg, P., & Kumar, S. (2023). CNN-BI-LSTM-CYP: A deep learning approach for sugarcane yield prediction: Sustainable *Energy Technologies and Assessments*, *57*, 103263.

[9] Saini, P., Nagpal, B., Garg, P., & Kumar, S. (2023). Evaluation of Remote Sensing and Meteorological Parameters for Yield Prediction of Sugarcane (Saccharum officinarum L.) Crop. Brazilian Archives of Biology and Technology, 66, e23220781.

[10] Beniwal, S., Saini, U., Garg, P., & Joon, R. K. (2021). Improving performance during camera surveillance by integrating edge detection into an IoT system. *International Journal of E-Health and Medical Communications (IJEHMC)*, *12*(5), 84-96.

[11] Garg, P., Dixit, A., & Sethi, P. (2019). Wireless sensor networks: an insight review. *International Journal of Advanced Science and Technology*, *28*(15), 612-627.

[12] Sharma, N., & Garg, P. (2022). Ant colony-based optimisation model for QoS-Based task scheduling in cloud computing environment—measurement*: Sensors*, 100531.

[13] Kumar, P., Kumar, R., & Garg, P. (2020). Hybrid Crowd Cloud Routing Protocol For Wireless Sensor Networks. *International Journal of Advanced Science and Technology*, *29*, 766-775.

[14] Raj, G., Verma, A., Dalal, P., Shukla, A. K., & Garg, P. (2023). Performance Comparison of Several LPWAN Technologies for Energy-Constrained IoT Network. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(1s), 150-158.

[15] Garg, P., Sharma, N., & Shukla, B. (2023). Predicting the Risk of Cardiovascular Diseases using Machine Learning Techniques. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(2s), 165-173.

[16] Patil, S. C., Mane, D. A., Singh, M., Garg, P., Desai, A. B., & Rawat, D. (2024). Parkinson's Disease Progression Prediction Using Longitudinal Imaging Data and Grey Wolf Optimiser-Based Feature Selection. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3s), 441-451.

[17] Gudur, A., Pati, P., Garg, P., & Sharma, N. (2024). Radiomics Feature Selection for Lung Cancer Subtyping and Prognosis Prediction: A Comparative Study of Ant Colony Optimisation and Simulated Annealing. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3s), 553-565.

[18] Khan, A. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. *J. Electrical Systems*, *20*(6s), 1051-1058.

[19] Sharma, K. K., Verma, P. K., & Garg, P. (2024). IoT-Enabled Energy Management Systems For Sustainable Energy Storage: Design, Optimisation, And Future Directions. *Frontiers in Health Informatics*, *13*(8).

[20] Gupta, S., Yadav, N., Singh, K., & Garg, P. (2025). APPLICATIONS OF SIMULATIONS AND QUEUING THEORY IN A SUPERMARKET *Reliability: Theory & Applications*, *20*(1 (82)), 135-140.

[21] Beniwal, S., Garg, P., Rajpal, R., Sharma, N., & Mittal, H. K. (2025). Fusion of Opportunistic Networks with Machine Learning: Present and Future. *Metallurgical and Materials Engineering*, *31*(1), 311-324.

[22] Garg, P. (2025). Explainable AI & Model Interpretability in Healthcare: Challenges & Future Directions. *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, *46*(1), 104-133.

[23] Rani, P. (2025). From Data to Diagnosis: Unleashing AI and 6G in Modern Medicine. *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, *46*(1), 69-103.

[24] Dixit, A., Garg, P., Sethi, P., & Singh, Y. (2020, April). TVCCCS: Television Viewer's Channel Cost Calculation System on Per-Second Usage. In *IOP Conference Series: Materials Science and Engineering* (Vol. 804, No. 1, p. 012046). IOP Publishing.

[25] Sethi, P., Garg, P., Dixit, A., & Singh, Y. (2020, April). Smart number cruncher–a voice-based calculator. In *IOP Conference Series: Materials Science and Engineering* (Vol. 804, No. 1, p. 012041). IOP Publishing.

[26] S. Rai, V. Choubey, Suryansh and P. Garg, "A Systematic Review of Encryption and Keylogging for Computer System Security," *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, 2022, pp. 157-163, doi: 10.1109/CCiCT56684.2022.00039.

[27] L. Saraswat, L. Mohanty, P. Garg and S. Lamba, "Plant Disease Identification Using Plant Images," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 79-82, doi: 10.1109/CCiCT56684.2022.00026.

[28] L. Mohanty, L. Saraswat, P. Garg and S. Lamba, "Recommender Systems in E-Commerce," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 114-119, doi: 10.1109/CCiCT56684.2022.00032.

[29] C. Maggo and P. Garg, "From linguistic features to their extractions: Understanding the semantics of a concept," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 427-431, doi: 10.1109/CCiCT56684.2022.00082.

[30] N. Puri, P. Saggar, A. Kaur and P. Garg, "Application of ensemble Machine Learning models for phishing detection on web networks," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 296-303, doi: 10.1109/CCiCT56684.2022.00062.

[31] R. Sharma, S. Gupta and P. Garg, "Model for Predicting Cardiac Health using Deep Learning Classifier," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 25-30, doi: 10.1109/CCiCT56684.2022.00017.

[32] Varshney, S. Lamba and P. Garg, "A Comprehensive Survey on Event Analysis Using Deep Learning," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 146-150, doi: 10.1109/CCiCT56684.2022.00037.

[33] Dixit, A., Sethi, P., Garg, P., & Pruthi, J. (2022, December). Speech Difficulties and Clarification: A Systematic Review. In *2022, the 11th International Conference on System Modelling & Advancement in Research Trends (SMART)* (pp. 52-56). IEEE.

[34] Garg, P., Dixit, A., Sethi, P., & Pruthi, J. (2023, December). Strengthening Smart City with Opportunistic Networks: An Insight. In the *2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech)* (pp. 700-707). IEEE.

[35] Rana, S., Chaudhary, R., Gupta, M., & Garg, P. (2023, December). Exploring Different Techniques for Emotion Detection Through Face Recognition. In *2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech)* (pp. 779-786). IEEE.

[36] Mittal, K., Srivastava, K., Gupta, M., & Garg, P. (2023, December). Exploration of Different Techniques on Heart Disease Prediction. In *2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech)* (pp. 758-764). IEEE.

[37] Gautam, V. K., Gupta, S., & Garg, P. (2024, March). Automatic Irrigation System using IoT. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 100-103). IEEE.

[38] Ramasamy, L. K., Khan, F., Joghee, S., Dempere, J., & Garg, P. (2024, March). Forecast of Students' Mental Health Combining an Artificial Intelligence Technique and Fuzzy Inference System. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 85-90). IEEE.

[39] Rajput, R., Sukumar, V., Patnaik, P., Garg, P., & Ranjan, M. (2024, March). The Cognitive Analysis for an Approach to Neuroscience. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 524-528). IEEE.

[40] Dixit, A., Sethi, P., Garg, P., Pruthi, J., & Chauhan, R. (2024, July). CNN-based lip-reading system for visual input: A review. In *AIP Conference Proceedings* (Vol. 3121, No. 1). AIP Publishing.

[41] Bose, D., Arora, B., Srivastava, A. K., & Garg, P. (2024, May). A Computer Vision-Based Framework for Posture Analysis and Performance Prediction in Athletes. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 942-947). IEEE.

[42] Singh, M., Garg, P., Srivastava, S., & Saggu, A. K. (2024, April). Revolutionising Arrhythmia Classification: Unleashing the Power of Machine Learning and Data Amplification for Precision Healthcare. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 516-522). IEEE.

[43] Kumar, R., Das, R., Garg, P., & Pandita, N. (2024, April). Duplicate Node Detection Method for Wireless Sensors. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 512-515). IEEE.

[44] Bhardwaj, H., Das, R., Garg, P., & Kumar, R. (2024, April). Handwritten Text Recognition Using Deep Learning. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 506-511). IEEE.

[45] Gill, A., Jain, D., Sharma, J., Kumar, A., & Garg, P. (2024, May). Deep learning approach for facial identification for online transactions. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 715-722). IEEE.

[46] Mittal, H. K., Dalal, P., Garg, P., & Joon, R. (2024, May). Forecasting Pollution Trends: Comparing Linear, Logistic Regression, and Neural Networks. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 411-419). IEEE.

[47] Malik, T., Nandal, V., & Garg, P. (2024, May). Deep Learning-Based Classification of Diabetic Retinopathy: Leveraging the Power of VGG-19. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 645-651). IEEE.

[48] Srivastava, A. K., Verma, I., & Garg, P. (2024, May). Improvements in Recommendation Systems Using Graph Neural Networks. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 668-672). IEEE.

[49] Aggarwal, A., Jain, D., Gupta, A., & Garg, P. (2024, May). Analysis and Prediction of Customer Churn and Retention Rates in the Telecom Industry Using Logistic Regression. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 723-727). IEEE.

[50] Mittal, H. K., Arsalan, M., & Garg, P. (2024, May). A Novel Deep Learning Model for Effective Story Point Estimation in Agile Software Development. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 404-410). IEEE.

[51] Shukla, S. M., Magoo, C., & Garg, P. (2024, November). Comparing Fine-Tuned LMs for Detecting LLM-Generated Text. In *2024, the 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)* (pp. 1-8). IEEE.

[52] Kumar, B., IQBAL, M., Parmer, R., Garg, P., Rani, S., & Agrawal, A. (2025, March). The Role of AI in Optimising Healthcare Appointment Scheduling. In *2025, the 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 881-887). IEEE.

[53] Kumar, B., Garg, V., Ahmed, K., Garg, P., Choudhary, S., & Baniya, P. (2025, March). Enhancing Healthcare with Blockchain: Innovations in Data Privacy, Security, and Interoperability. In *2025, the 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 932-938). IEEE.

[54] Raj, V., Prakash, B. K., Kumar, A., & Garg, P. (2024, December). Optimise the Time a Mercedes-Benz Spends on the Test Bench Using Stacking Ensemble Learning. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 445-450). IEEE.

[55] Kaushik, N., Kumar, H., Raj, V., & Garg, P. (2024, December). Proactive Fault Prediction in Microservices Applications Using Trace Logs and Monitoring Metrics. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 410-415). IEEE.

[56] Kumar, A. A., Sri, C. V., Bohara, K. S. K., Setia, S., & Garg, P. (2024, December). Capnivesh: Financing Platform for Startups. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 261-265). IEEE.

[57] Bhandari, P., Setia, S., Kumar, K., & Garg, P. (2024, December). Optimising Cross-Platform Development with CI/CD and Containerization: A Review. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 175-180). IEEE.

[58] Chaudhary, A., & Garg, P. (2014). Detecting and diagnosing a disease using a patient monitoring system. *International Journal of Mechanical Engineering And Information Technology*, *2*(6), 493-499.

[59] Malik, K., Raheja, N., & Garg, P. (2011). Enhanced FP-growth algorithm. *International Journal of Computational Engineering and Management*, *12*, 54-56.

[60] Garg, P., Dixit, A., & Sethi, P. (2021, May). Link Prediction Techniques for Opportunistic Networks using Machine Learning, in *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*.

[61] Garg, P., Dixit, A., & Sethi, P. (2021, April). Opportunistic networks: Protocols, applications & simulation trends. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*.

[62] Garg, P., Dixit, A., & Sethi, P. (2021). Performance comparison of the fresh and spray-and-wait protocols using a single simulator. *IT in Industry*, *9*(2).

[63] Malik, M., Singh, Y., Garg, P., & Gupta, S. (2020). Deep Learning in the Healthcare System. *International Journal of Grid and Distributed Computing*, *13*(2), 469-468.

[64] Gupta, M., Garg, P., Gupta, S., & Joon, R. (2020). A Novel Approach for Malicious Node Detection in Cluster-Head Gateway Switching Routing in Mobile Ad Hoc Networks. *International Journal of Future Generation Communication and Networking*, *13*(4), 99-111.

[65] Gupta, A., Garg, P., & Sonal, Y. S. (2020). Edge Detection-Based 3D Biometric System for Security of Web-Based Payment and Task Management Application. *International Journal of Grid and Distributed Computing*, *13*(1), 2064-2076.

[66] Garg, P., & Raman, P. K. (2011). Broadcasting Protocol & Routing Characteristics With Wireless Ad Hoc Networks. *Int. J. Comput. Emg. Manag*, *12*(1), 36-40.

[67] Garg, P., Arora, N., & Malik, T. (2011). Capacity Improvement of Wi-MAX in the presence of Different Codes WI-MAX: Speed & Scope of the future. *IJCEM*, *12*.

[68] Garg, P., Saroha, K., & Lochab, R. (2011). Review of wireless sensor networks: architecture and applications. IJCSMS International Journal of Computer Science & Management Studies, 11(01), 2231-5268.

[69] Yadav, S., &Garg, P. Development of a New Secure Algorithm for Encryption and Decryption of Images.

[70] Dixit, A., Sethi, P., & Garg, P. (2022). Rakshak: A Child Identification Software for Recognising Missing Children Using Machine Learning-Based Speech Clarification. International Journal of Knowledge-Based Organisations (IJKBO), 12(3), 1-15.

[71] Shukla, N., Garg, P., & Singh, M. (2022). MANET Proactive and Reactive Routing Protocols: A Comparison Study. International Journal of Knowledge-Based Organisations (IJKBO), 12(3), 1-14.

[72] Arya, A., Garg, P., Vellanki, S., Latha, M., Khan, M. A., & Chhbra, G. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. *Journal of Electrical Systems*, *20*(6s), 1051-1058.

[73] Garg, P. (2025). Cloud security posture management: Tools and techniques. Technix International Journal for Engineering Research, 12(3).

[74] Tyagi, P., Sharma, S., Srivastava, A., Rajput, N. K., Garg, P., & Kumari, M. (2025). AI in Healthcare: Transforming Medicine with Intelligence. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p4

[75] Garg, P., Bhatt, M., Parmar, R., & Arsalan, M. (2025). Generative AI: Evolution, Applications, Challenges, and Future Prospects. *Applications, Challenges, and Future Prospects (May 17, 2025)*.

[76] Garg, P., Saraswat, P., & Siddiqui, Z. (2025). AI & the Indian Stock Market: A Review of Applications in Investment Decision. https://doi.org/10.63169/GCARED2025.p10

[77] Garg, P., Sharma, S., Mittal, S., Tevatia, R., Tyagi, V. K., & Kapoor, S. (2025). Unlocking Workforce Potential: AI-Powered Predictive Models for Employee Performance Evaluation. https://doi.org/10.63169/GCARED2025.p21

[78] Shrivas, N., Kalia, A., Roy, R., Sharma, S., Garg, P., & Agarwal, G. (2025). OSINT: A Double-edged Sword. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p22

[79] Garg, P., Aditi, A., & Roy, B. (2025). A System of Computer Network: Based On Artificial Intelligence. https://doi.org/10.63169/GCARED2025.p24

[80] Parmar, R., Kapoor, S., Saifi, S., & Garg, P. (2025). Case Study on Intelligent Factory Systems for Improving Productivity and Capability in Industry 4.0 with Generative AI. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p28

[81] Singh, R., Sharma, R., Kumar, R., Nafis, A., Siddiqui, M. A. M., & Garg, P. (2025). Detection of Unauthorised Construction using Machine Learning: A Review. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p30

[82] Garg, P., Kapoor, S., Singh, V., Sharma, S., & Ankita, A. (2025). A Bridge between Blockchain and Decentralised Applications, Web3 and Non-Web3 Crypto Wallets. https://doi.org/10.63169/GCARED2025.p35

[83] Verma, M., Sharma, S., Garg, P., & Singh, A. (2025). The Hidden Dangers of Prototype Pollution: A Comprehensive Detection Framework. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p36

[84] Sharma, A., Sharma, S., Garg, P., & Bhardwaj, P. (2025). LockTalk: A Basic Secure Chat Application. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India.

[85] Arora, K., Bawane, R., Gupta, C., Ahmed, K., & Garg, P. (2025). Detection and Prevention of Cyber Attacks and Threats using AI. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p38

[86] Garg, P., Dhruv, D., Rahman, A. A., Rai, A., Siddiqui, M., & Yadav, D. (2025). Easeviewer: An Esports Production Tool. https://doi.org/10.63169/GCARED2025.p46

[87] Garg, P., Lakshita, L., Mehwish, M., Nazia, N., & Ahmed, K. (2025). Emerging Trend in Computational Technology: Innovations, Applications, and Challenges. *Applications and Challenges (May 17, 2025)*. https://doi.org/10.63169/GCARED2025.p51

[88] Chauhan, S., Singh, M., & Garg, P. (2021). Rapid Forecasting of Pandemic Outbreak Using Machine Learning. *Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies*, 59-73.

[89] Gupta, S., & Garg, P. (2021). An insight review on multimedia forensics technology. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 27.

[90] Shrivastava, P., Agarwal, P., Sharma, K., & Garg, P. (2021). Data leakage detection in Wi-Fi networks. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 215.

[91] Meenakshi, P. G., & Shrivastava, P. (2021). Machine learning for mobile malware analysis. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 151.

[92] Nanwal, J., Garg, P., Sethi, P., & Dixit, A. (2021). Green IoT and Big Data: Succeeding towards Building Smart Cities. In *Green Internet of Things for Smart Cities* (pp. 83-98). CRC Press.

[93] Gupta, M., Garg, P., & Agarwal, P. (2021). Ant Colony Optimisation Technique in Soft Computational Data Research for NP-Hard Problems. In *Artificial Intelligence for a Sustainable Industry 4.0* (pp. 197-211). Springer, Cham.

[94] Magoo, C., & Garg, P. (2021). Machine Learning Adversarial Attacks: A Survey Beyond. *Machine Learning Techniques and Analytics for Cloud Security*, 271-291.

[95] Garg, P., Srivastava, A. K., Anas, A., Gupta, B., & Mishra, C. (2023). Pneumonia Detection Through X-Ray Images Using Convolution Neural Network. In *Advancements in Bio-Medical Image Processing and Authentication in Telemedicine* (pp. 201-218). IGI Global.

[96] Gupta, S., & Garg, P. (2023). 14 Code-based post-quantum cryptographic technique: digital signature. *Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity*, 193.

[97] Prakash, A., Avasthi, S., Kumari, P., & Rawat, M. (2023). PuneetGarg 18 Modern healthcare system: unveiling the possibility of quantum computing in medical and biomedical zones. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 249.

[98] Gupta, S., & Garg, P. (2024). Mobile Edge Computing for Decentralised Systems. *Decentralised Systems and Distributed Computing*, 75-88.

[99] Gupta, M., Garg, P., & Malik, C. (2024). Ensemble learning-based analysis of perinatal disorders in women. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 91-105). Academic Press.

[100] Malik, M., Garg, P., & Malik, C. (2024). Artificial intelligence-based prediction of health risks among women during menopause. *Artificial Intelligence and Machine Learning for Women's Health Issues*, 137-150.

[101] Garg, P. (2024). Prediction of female pregnancy complications using artificial intelligence. In *Artificial Intelligence and Machine Learning for Women's Health Issues* (pp. 17-35). Academic Press.

[102] Pokhrel, L., Arsalan, M., Rani, P., Garg, P., & Pinheiro, P. R. (2026). AI-Powered Healthcare Solutions: Bridging the Medical Gap in Underserved Communities Worldwide. In *Applied AI and Computational Intelligence in Diagnostics and Decision-Making* (pp. 57-86). IGI Global Scientific Publishing.

[103] Kapoor, S., Parmar, R., Sharma, N., Garg, P., & Singh, N. J. (2026). AI and Computational Intelligence in Healthcare: An Introductory Guide. In *Applied AI and Computational Intelligence in Diagnostics and Decision-Making* (pp. 1-26). IGI Global Scientific Publishing.

[104] Pokhrel, L., Kumar, A., Garg, P., Anand, N., & Singh, N. (2026). AI and IoT in Global Health: Ethical Lessons From Pandemic Response. In *Development and Management of Eco-Conscious IoT Medical Devices* (pp. 367-394). IGI Global Scientific Publishing.

[105] Parmar, R., Singh, A., Garg, P., Sharma, T., & Pinheiro, P. R. (2026). Blockchain for Ethical Supply Chains: Transparency in Medical IoT Manufacturing. In *Development and Management of Eco-Conscious IoT Medical Devices* (pp. 337-366). IGI Global Scientific Publishing.

[106] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (2024). Federated learning-based intelligent systems to handle issues and challenges in IoVs (Part 1). https://doi.org/10.2174/9789815313031124030l

[107]Gupta, S., Chaudhary, G., & Garg, P. (2013). Modified AODV Routing Protocol through Cache Memory for Finding New Routing Paths in MANETs—International *Journal of Computer Science & Management Studies*, *13*(3).

[108]Gupta, A., & Garg, P. (2021). Emerging Techniques for Handling Pandemic Challenges. *Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies*, 189-209.

[109]Chaudhary, A. P., Mishra, A., Kumar, D., & Garg, P. (2023, April). Human Emotion Recognition using Deep Learning. In the *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)* (pp. 191-197). IEEE.

[110]Nagpal, S., Garg, P., Gaba, S., & Aggarwal, A. (2023). 13 An improved genetic quantum cryptography model for network communication. *Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity*, 177.

[111]Yadav, M., Swami, V., Kumar, N., & Garg, P. (2025). Comparative study of Repairable Juice Plants using RPGT. *Reliability: Theory & Applications*, *20*(2 (84)), 776-783.

[112]Gupta, A., Garg, P., & Yadav, P. (2025). Role of Generative AI Towards Education and Learning: Present & Future. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S6 (2025): Posted 15 Sept), 1059-1076.

[113]Dalal, P., Beniwal, G., Sharma, V., Garg, P., & Ahmed, K. (2025). Predicting Student Motivation and Engagement through Machine Learning Models. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S7 (2025): Posted 10 October), 393-411.

[114]Gupta, A., Mund, A., Roy, S., Garg, P., & Yadav, D. K. (2025). Trust in AI Systems: A Social-psychological Investigation of Human–AI Collaboration. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S7 (2025): Posted 10 October), 428-446.

[115]Bhardwaj, A., Das, A., Garg, P., & Yadav, S. (2025). Material-Driven Performance Analysis of a Vertical Nanowire Tunnel FET for Analogue Applications: Bhardwaj, Das, Garg, and Yadav. *Journal of Electronic Materials*, 1-12.

[116]Dalal, P., Sharma, B., Sharma, T., Garg, P., & Ahmed, K. (2025). Explainable AI for Understanding Human Decision-Making Patterns. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S7 (2025): Posted 10 October), 412-427.

[117]Sharma, K. K., Verma, P. K., Garg, P., & Shrotriya, V. K. (2025, October). Predicting costs and benefits of IoT-based energy management for optimising sustainable energy storage in rural areas. In *AIP Conference Proceedings* (Vol. 3343, No. 1, p. 040017). AIP Publishing LLC.

[118]Ahmed, K., Baranwal, A., Sharma, N., Garg, P., & Singh, N. (2026). The Role of Federated Learning in AI-Powered Integrated Healthcare Solutions. In *Enabling Collaborative Health Intelligence With Federated Learning* (pp. 421-448). IGI Global Scientific Publishing.

[119]Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (2025). Federated learning-based intelligent systems to handle issues and challenges in IoVs (Part 2). Bentham Science Publishers. https://doi.org/10.2174/9789815322241250301

[120]Garg, P., Pranav, S., & Prerna, A. (2021). Green internet of things (G-IoT): A solution for sustainable technological development. In *Green Internet of Things for Smart Cities* (pp. 23-46). CRC Press.

[121]Malik, A., Nandal, D., Gupta, V., Garg, P., & Nandal, V. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[122]Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (Eds.). (2025). Federated learning-based intelligent systems to handle issues and challenges in IoVs (Part 2).

[123]Garg, P., Bhatt, M., Parmar, R., & Arsalan, M. (2025). Generative AI: Evolution, Applications, Challenges, and Future Prospects. *Applications, Challenges, and Future Prospects (May 17, 2025)*.

[124]Kumar, N., Kumar, Y., Khurana, D., Kumar, S., & Garg, P. (2025, November). A Hybrid Ensemble Learning Framework for Interpretable Student Performance Prediction Using Academic and Extracurricular Factors. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 666-672). IEEE.

[125]Khurana, D., Kumar, Y., Kumar, N., Kumar, S., & Garg, P. (2025, November). Transformer-Based Movie Recommendation System with Autoencoder-Enhanced Feature Compression. In *2025*

*International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 685-690). IEEE.

[126]Garg, P. (2025, November). Comparative Analysis of Various Neural Networks for Galaxy Classification. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 697-701). IEEE.

[127]Saggu, A. K., Babbar, N., & Garg, P. (2025, November). Health-Guard AI: Integrated Health Report Management and Analysis. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 614-623). IEEE.

[128]Kumar, S., Kumar, Y., Kumar, N., Khurana, D., & Garg, P. (2025, November). Hybrid FCM-DNN Model for Uncertainty-Aware Air Quality Classification Using Multi-Pollutant Data. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 679-684). IEEE.

[129]Babbar, N., Singh, H. V., Bendale, S., & Garg, P. (2025, November). Stock Market Price Prediction Using Big Data Analysis: A Performance Evaluation Study. In *2025, the 3rd International Conference on Computational Intelligence and Network Systems (CINS)* (pp. 1-6). IEEE.

[130]Singh, A. K., Kori, G., Garg, P., & Srivastava, G. (2025, November). Bank Churn Prediction Using Machine Learning. In *2025, IEEE 7th International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1-6). IEEE.

[131]Bhardwaj, A., Das, A., Garg, P., & Yadav, S. (2026). Material-Driven Performance Analysis of a Vertical Nanowire Tunnel FET for Analogue Applications. *Journal of Electronic Materials*, *55*(1), 1099-1110.

[132]Srivastava, A. K., Shankdhar, D., Ror, R., & Garg, P. (2026). Harnessing YOLOv5 for real-time object detection: A cloud-based approach. In *Recent Advances in Computational Methods in Science and Technology* (pp. 441-450). CRC Press.

[133]Srivastava, A. K., Shukla, A., Gupta, H., Saxena, K., & Garg, P. (2026). Towards an intelligent attendance management system with face recognition using the LBPH algorithm. In *Recent Advances in Computational Methods in Science and Technology* (pp. 8-15). CRC Press.

[134]Srivastava, A. K., Garg, P., & Pandey, H. (2026). Vedcure: Towards intelligent ayurvedic drug recommendation and disease prediction. In *Recent Advances in Computational Methods in Science and Technology* (pp. 16-23). CRC Press.

[135]Upadhyay, D., Garg, P., & Babbar, N. (2026). Blockchain and IoT-based smart contract framework for efficient and secure product life management. *Discover Internet of Things*.

[136]Singh, A., Parmar, R., Bhardwaj, P., Sharma, V., & Garg, P. (2026). Fusion of Aerial Networks with Advanced Computing Paradigms. *Edge Computing and Aerial Platforms*, 355-367.

[137]Kumari, M., Baranwal, A., Sonal, & Garg, P. (2026). Application of Aerial Edge Computing in Disaster Management. *Edge Computing and Aerial Platforms*, 103-122.

[138]Aditi, Saraswat, P., Sharma, V., & Garg, P. (2026). Advances in Aerial Platforms and Edge Computing. *Edge Computing and Aerial Platforms*, 123-143.

[139]Garg, P., Arora, K., Bawane, R., Gupta, C., & Ahmed, K. (2025). Detection and Prevention of Cyber Attacks and Threats using AI.

[140]Ahmed, K., Ahmed, A., Khan, J., Garg, P., Seth, S., & Mallik, S. (2025). Principal Component Analysis-Based Clustering of Insecticides and Molecular Docking of Pyrethroid Insecticides.

[141]Kumar, B., Kumar, A., Nanwal, J., Garg, P., & Patnaik, P. (2025, November). Ensemble of YOLOv5 and Segment Anything Model for Brain Tumour Detection. In *2025, the 2nd International Conference on Advanced Computing and Emerging Technologies (ACET)* (pp. 1-5). IEEE.

[142]Arsalan, M., Anas, M., & Garg, P. (2025). Transparent AI for Drug Discovery and Development. *Available at SSRN 5844242*.

[143]Singh, A., Bhardwaj, P., Garg, P., & Singh, N. (2026). Introduction to explainable artificial intelligence in healthcare. In *Explainable AI in Clinical Practice* (pp. 23-44). Academic Press.

[144]Kapoor, S., Singh, A., Garg, P., & Ramasamy, L. K. (2026). Explainable artificial intelligence in a diagnostic support system. In *Explainable AI in Clinical Practice* (pp. 131-145). Academic Press.

[145]Ahmed, K., Anas, M., & Garg, P. (2026). Case studies on unlocking the potential of Industry 4.0 for sustainable manufacturing through generative AI-driven innovations. *Available at SSRN 6356958*.

[146]Garg, P., & Oruganti, S. K. (2026, March). AI Assisted Routing Optimisation in Opportunistic IoT Networks using Machine Learning: A Comprehensive Review on Protocols & Simulators. In *Sustainable Global Societies Initiative* (Vol. 1, No. 4). Vibrasphere Technologies.

[147]Arsalan, M., Pokhrel, L., & Garg, P. (2026). Architecture, Components, and tools in Integrated AI-Augmented Intelligence: A design perspective. *Components and tools in Integrated AI-Augmented Intelligence: A design perspective (March 19, 2026)*.

[148]Singh, H., Ahmed, K., & Garg, P. (2026). Human Versus Machine Customer Behaviour and Functional Differences. *Available at SSRN 6441098*.

[149]Saraswat, P., & Garg, P. (2026). Soft Computing In AI Agents.

[150]Saraswat, P., & Garg, P. (2026). Water Quality Prediction Using IOT Sensors and Deep Networks.