International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Survey on Federated Learning Utilising Deep Learning Models for Diverse Applications

Mr. Nandakumar M[1], Dr. N. Ranjith[2]

[1]Research Scholar, Computer Science, K.S.G College of Arts and Science, Coimbatore, Tamilnadu, India.
[2]Head & Assistant Professor, Computer Science, K.S.G College of Arts and Science, Coimbatore, Tamilnadu, India.

ABSTRACT
In the rapidly advancing field of artificial intelligence (AI), Federated Learning (FL) is a distributed learning enhanced to preserve the privacy of individual's data. FL models often captures boarder patterns and generalize well across user groups by learning from diverse and decentralized data sources. FL also supports on-device learning updates for enabling real-time personalization in dynamic environments. Despite its advantages, FL faces key challenges like difficulty in handling Non-Independent and Identically Distributed (Non-IID) client data, communication overhead, slow convergence, data heterogeneity and potential security and privacy risks during model updates. To solve this, Machine Learning (ML) and Deep Learning (DL) models are integrated within the FL model. ML models are lightweight and less computational demanding, making them suitable for resource-constrained environments. But, ML models often fails to capture complex patterns especially when dealing with high-dimensional or unstructured data. In contrast, DL models are capable of extracting complex features and patterns making them more suitable for FL settings for various application applications like healthcare diagnostic, Internet of Things (IoT) security and financial anomaly prediction. By leveraging the strengths of DL, FL systems can achieve improved performance and provides more effective learning across diverse and distributed environments. This paper presents a detailed review of various FL-DL frameworks developed for predictive modeling across various domains. Initially, several federated systems proposed by researchers integrating DL algorithms are briefly studied and analyzed. A comparative evaluation is then conducted to understand the drawbacks of those algorithms and suggest a new solution for better decision making in real-time, distributed and privacy-sensitive environments.

Keywords: Artificial Intelligence, Federated Learning, Machine Learning, Deep Learning, Dynamic Environments

1. INTRODUCTION

Federated learning (FL) is a machine learning approach in which numerous devices or entities train a model together without explicitly exchanging raw data [1]. In FL, users train the model locally on their own data and then send model updates or parameters to a central server, which combines them to enhance the global model. This technique helps to protect data privacy and security by keeping sensitive data locally [2]. FL is a decentralized approach in terms of training data and on-device processing of computations dedicated to train a model [3]. In FL, raw data is kept on end user devices, which cooperate

on training a joint model. On a central server, only locally computed updates and analysis results are received and aggregated for an enhanced global model benefiting from the distributed learning. The new model is then shared with the clients to share knowledge among them [4]. Figure 1 depicts the structure of federated learning

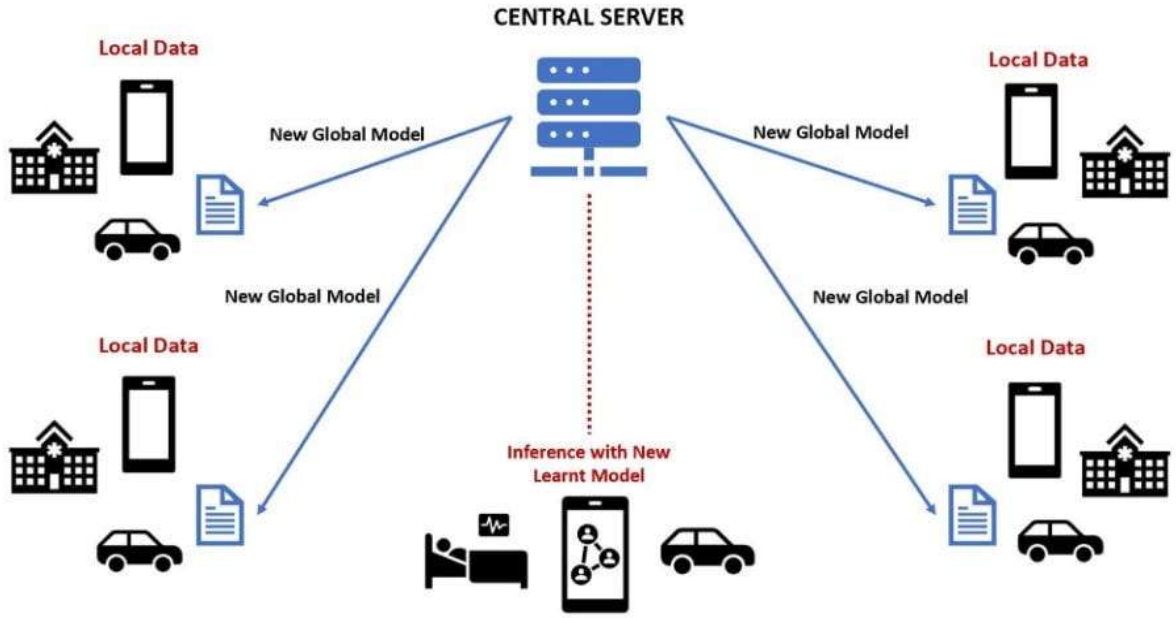

Figure 1 Overview of Federated Learning System

1.1 FL types based on Data Distribution

FL can be broadly categorized into three main types based on data distribution like Horizontal FL (HFL), Vertical FL (VFL) and Federated TL (FTL) [5]. These categories reflect how data is distributed across different clients or parties involved in the learning process.

- **Horizontal Federated Learning (HFL):** In HFL, datasets from different clients share the same feature space but have different sample IDs. Each client possesses a subset of the overall population, with the same features but different individuals or records. For example, multiple hospitals might have data on different sets of patients but with the same set of medical records like lab results.
- **Vertical Federated Learning (VFL):** VFL is used when datasets share the same sample IDs but have different feature spaces. This implies that clients have data on the same individuals or entities, but with different attributes or features. For example, a bank and a credit bureau might collaborate using VFL, where the bank has customer transaction data and the bureau has credit history information, both pertaining to the same customers.
- **Federated Transfer Learning (FTL):** FTL applies when datasets across clients differ in both features and samples. FTL leverages transfer learning techniques to enable knowledge sharing between domains with little or no overlap in data. For example, if two hospitals have data on different diseases with little overlap in patients or features, FTL could be used to transfer knowledge about one disease to improve diagnosis of the other.

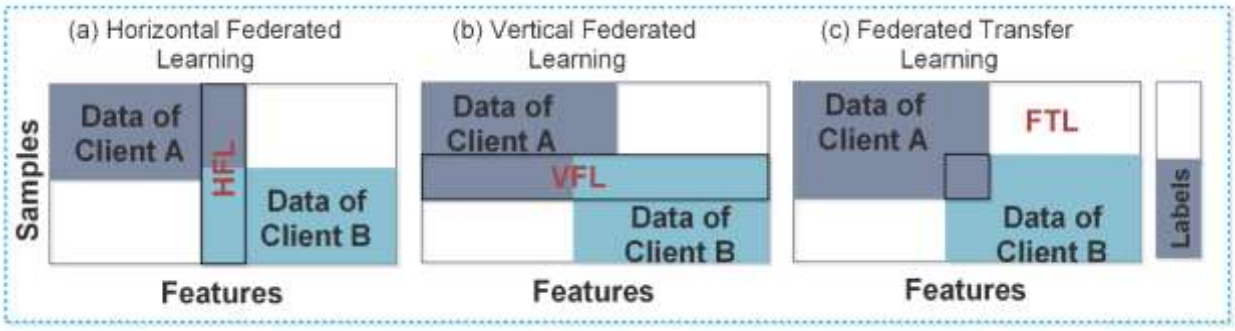

Figure 2 Working Design of FL types based on Data Distribution

1.2 System Architecture in Federated Learning

They are 3 types of system architecture involved in federated learning

1. Centralized Architecture: In centralized federated learning [6], a central server orchestrates the training process. Clients perform local model training on their data and send the model updates to the server. The server aggregates these updates to form a global model and sends it back to the clients. This setup is easier to manage and scales well but has a single point of failure. It is commonly used in real-world applications like mobile keyboards and healthcare.

2. Distributed (Decentralized) Architecture: Distributed FL [7] eliminates the need for a central server by allowing clients to share updates directly with one another in a peer-to-peer manner. Clients collaborate using consensus protocols or gossip-based communication to update and refine the global model. This approach is more robust and privacy-preserving but harder to coordinate. It is useful in scenarios where central coordination is not feasible. Training may take longer due to network delays and synchronization issues.

3. Hybrid Architecture: Hybrid FL [8] combines aspects of both centralized and distributed architectures. It may involve multiple central servers coordinating with clusters of clients or partial peer-to-peer communication among clients within a centralized setup. This model balances scalability, reliability, and privacy. Hybrid setups are particularly useful in large-scale or hierarchical networks, like edge-cloud systems. They offer flexibility in design and can be adapted to varying network and device conditions.

1.3 Strategies Involved in FL

In FL, multiple parties can collaborate without sharing raw data. Each party shares model updates with a central server. The data undergoes aggregation by the central server and are sent to local sources [9]. In this way, the model is trained while benefiting all parties by providing privacy. Distributing the data across different devices is more convenient than gathering all the data in one location or device. To achieve this, a variety of federated learning strategies [10] have been developed which are listed below

Federated Averaging (FedAvg): A basic FL method where clients train local models and the server averages their parameters. It ensures data privacy, lowers communication costs, and scales well for large networks.

FedAdam: An FL variant of the Adam optimizer that combines adaptive learning rates with momentum. It improves convergence on non-Independent and Identically Distributed (IID) data by adjusting updates based on gradient history.

FedYogi: Based on the Yogi optimizer, it stabilizes FL training on heterogeneous data by conservatively adjusting learning rates, preventing aggressive updates and model divergence.

FedAdagrad: Uses the Adagrad optimizer in FL to adapt learning rates per parameter. It improves convergence by giving smaller updates to frequent features and larger ones to infrequent ones.
FedNova: Normalizes client updates to correct for client-side heterogeneity in data and computation, preventing bias from unbalanced local training.
FedProx: Enhances FedAvg by adding a regularization term to reduce local model divergence. It improves training stability in settings with highly non-IID client data.
Scaffold: Corrects client drift using control variates and server-side updates. It improves convergence and reduces communication rounds, especially under non-IID data conditions.

1.4 Applications

FL is gaining traction across various industrial application where data privacy, security and decentralization are crucial [11]. Some of those application are listed below

- In **healthcare**, FL enables hospitals to collaboratively train models for disease diagnosis or drug discovery without sharing sensitive patient data.
- In the **financial sector**, banks and institutions use FL to detect fraud or assess credit risk while preserving user confidentiality.
- **Mobile and IoT devices** (e.g., smartphones, wearables) use FL to personalize services like voice recognition, keyboard suggestions, and activity tracking without uploading private user data to the cloud.
- In **smart manufacturing and edge computing**, FL supports predictive maintenance and quality control by learning from data across multiple distributed machines.
- **An autonomous vehicles** use FL to share insights from real-world driving experiences across fleets, improving safety and decision-making while keeping raw sensor data local.

1.5 Advantages

FL allows model training directly on devices where data is generated, which enhances data privacy by ensuring that raw data never leaves the local device. This makes FL especially suitable for industries with sensitive information, such as healthcare or finance. It also reduces network bandwidth usage, since only model updates (like gradients or weights) are communicated instead of full datasets. Furthermore, FL enables personalized models tailored to individual users without compromising their privacy. It supports real-time learning as new data is continuously generated on edge devices and is highly scalable, operating efficiently across thousands or even millions of distributed clients.

1.6 Disadvantages

The key issue in FL is non-IID data, where client data distributions vary significantly, leading to poor model performance; this can be addressed using meta-learning, domain adaptation, or personalized FL approaches. Another challenge is unreliable or slow clients, which can disrupt training solvable through asynchronous updates and smart client selection. Communication overhead from frequent model updates can be reduced using model compression, quantization, or adaptive update strategies. Although raw data isn't shared, gradients may still leak private information, which can be protected using techniques like differential privacy, secure multiparty computation, or homomorphic encryption. Additionally, FL is vulnerable to malicious participants who may send corrupted or poisoned updates, potentially degrading the performance of the global model or causing it to behave incorrectly. Lastly, as user behavior changes over time, models may become outdated a problem that can be handled using continual and online learning methods that adapt the model to evolving data patterns.

1.7 Artificial Intelligence in Federated Learning

Artificial Intelligence (AI) refers to the ability of machines or systems to mimic human intelligence by learning from data and making decisions or predictions [12]. In the context of FL, AI plays a crucial role in enabling smart, secure, and efficient training of models across distributed clients without compromising user privacy [13]. AI techniques allow FL systems to handle complex tasks such as intelligent client selection, adaptive model training, and anomaly detection [14]. AI composed of two subsections i.e., Machine Learning (ML) and Deep Learning (DL).

Machine Learning (ML) is one of the most commonly applied methods in FL. ML algorithms in FL allow devices to collaboratively train models on local data and share only model updates with a central server [15]. ML models collaboratively train systems without sharing raw data. Some ML models include Logistic Regression (LR), Support Vector Machines (SVMs), K-Nearest Neighbors (KNN) and Random Forest (RF). These models are widely applied in FL for classification and regression tasks, offering simplicity and effectiveness on structured data while preserving data privacy across distributed clients [16]. FL can also incorporate Reinforcement Learning models, such as Q-Learning and Policy Gradient Methods, to optimize decision-making in dynamic environments [17]. However, traditional ML techniques often struggle with challenges like non-IID data, limited feature representation, and the inability to generalize well in heterogeneous environments. When integrated with FL, these models also face issues such as increased communication overhead, difficulty in handling asynchronous client updates and reduced performance due to limited local data on each client. Figure 3 depicts the integration of FL with DL model.

DL models like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and their variants like Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU) are well-suited for sequential and time-series data across distributed clients. These models enable decentralized training on complex data while preserving user privacy [20]. Transformer-based models have also been adopted in FL settings for natural language tasks, as they support parallel processing and perform well even in non-IID and resource-constrained environments commonly found in federated systems [21]. Despite being computationally intensive, DL models integrated with FL enable powerful, privacy-preserving AI applications across domains such as healthcare, finance, smart homes, and autonomous systems [22].

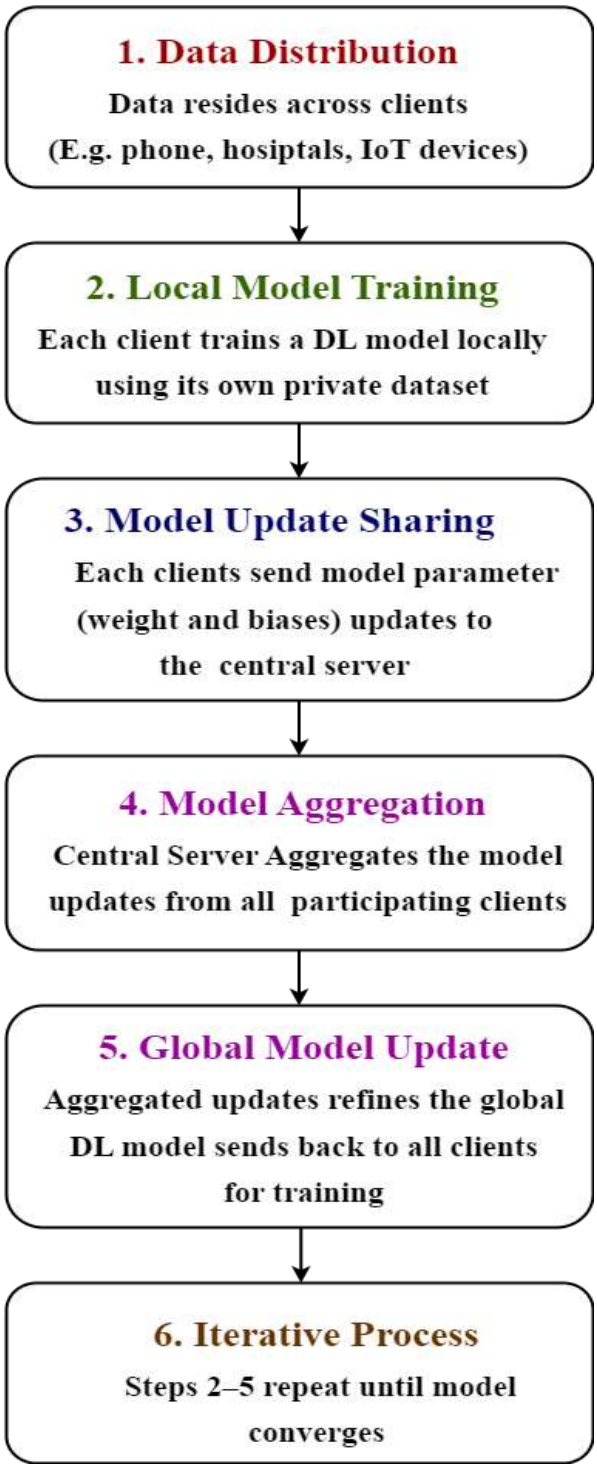

Figure 3 Training Workflow: Federated Learning with Deep Learning

In this paper, a comprehensive overview of the state-of-the-art FL methods integrated with DL models are illustrated for various applications. By categorizing and analyzing existing approaches, this study highlights their strengths and limitations, providing valuable insights into the current state of the field. The remaining parts are organized in the following manner: Section II provides a survey of various papers related to FL integrated with DL algorithms designed for different environments, focusing on their methodologies and applications. Section III presents a comparison of these survey papers, highlighting their strengths, weaknesses and differences. Section IV evaluates the performance of the discussed

approaches, analyzing key performance metrics and their impact on system efficiency. Section V concludes the survey by summarizing the key findings and proposing potential future directions for research in this area.

2. SURVEY ON FEDERATED LEARNING WITH DEEP LEARNING MODEL FOR VARIOUS APLICATIONS

Reddy et al. [23] developed a Jellyfish Namib Beetle Optimization Algorithm-SpinalNet (JNBO-SpinalNet) with FL for fraudulent credit card transaction detection. The input data was pre-processed using quantile normalization and the features were selected using various distance measures. The selected features were augmented using Bootstrapping method and SpinalNet is finally allowed to detect credit card frauds. The hyper-parameter of SpinalNet was optimized by JNBO model for credit card transaction fraudulent detection. FL was incorporated to ensure privacy-preserving, decentralized training across multiple financial institutions.

Guo & Jiang, [24] presented a weakly supervised anomaly detection with privacy preservation called bi-level federated learning framework (BFL). Initially, a Pairwise Relation prediction-based Ordinal Regression Network (PRO) was employed to train a Deep Anomaly Detection (DAD) model within a Federated Learning (FL) framework. The model detected anomalies with minimal labels, which were manually categorized and combined with normal data to train a multi-class defect classifier under the same FL setup. The BFL framework enables accurate defect classification while preserving data privacy.

Sikandar et al. [25] developed generative AI and FL for privacy preserved sequence-based stomach adenocarcinoma detection. In this model, amino acid sequences altered by STAD were used as input, and features were extracted using Electro-Ion Interaction Pseudopotential (EIIP) values and Kidera factors. To address class imbalance, generative AI was employed to create synthetic data samples. The federated artificial neural network (Fed_ANN11) was used to ensure the data privacy while achieving high diagnostic accuracy particularly with EIIP-based features.

Abbas et al. [26] presented a federated DL (FDL) framework using deep neural network (DNN) to predict thermal comfort in smart buildings. The model allows clients (e.g., smart devices) to train locally on private data while only sharing model updates, thus preserving user privacy. The min-max normalization and Synthetic Minority Over-Sampling Technique (SMOTE) were integrated to balance and prepare the dataset before training. The horizontal FL architecture were used to ensure data confidentiality across distributed clients. This system supports energy-efficient HVAC control and occupant comfort prediction in privacy-sensitive building environments.

Chawla et al. [27] constructed a lightweight and privacy-preserved FL framework for classifying emotions from verbal communication. Mel-Frequency Cepstral Coefficients (MFCC) was used to extract features from audio data and trains a Bidirectional Long Short-Term Memory (Bi-LSTM) model locally on edge devices, ensuring user data privacy. This FL system was designed to handle both Independent and Identically Distributed (IID) and non-IID datasets making it robust across diverse data sources. The approach ensures secure emotion recognition for social communication deficits, aiding mental health, assistive tools and private customer interactions.

Bhavsar et al. [28] introduced a federated learning-based intrusion detection system (FL-IDS) to enhance the vehicular network security in Internet of Things (IoT) edge device implementations. The FL-IDS system protects data privacy by using local learning in which devices share only model updates with an

aggregation server. Logistic Regression (LR) and Pearson Correlation Coefficient (CNN) was performed for IDS to prevent attacks in transportation IoT environments.

Sarker et al. [29] presented an optimized Attention-based One-Dimensional Convolutional Neural Network - Gated Recurrent Unit model (Att-1D-CNN-GRU) with FL for secure and effective load forecasting in smart grid systems. An attention-based 1D-CNN-GRU model was performed to capture the temporal patterns from the time-series data. The hyperparameters were optimized by particle swarm optimization (PSO) algorithm that improves the convergence in model training. Moreover, the explainable AI (XAI) technique was applied using Shapley Additive explanations (SHAP) to interpret the model prediction providing the feature ranking based on their prediction score.

Huang et al. [30] proposed a novel IDS called DVACNN-Fed which integrates Deep Variational Autoencoders (DVAE) and Convolutional Neural Networks (CNN) with attention mechanisms within a FL architecture. The DVAE enhances privacy by encoding data before transmission, while the CNN-attention hybrid improves anomaly detection accuracy. This decentralized training method allows multiple Industrial IoT (IIoT) devices to collaboratively build a strong intrusion detection model without exposing raw data. The model also incorporates differential privacy and data augmentation techniques to boost robustness and generalization.

Nobakht et al. [31] suggested a secure IoT malware detection model with FL model (SIM-FED). The SIM-FED offers a privacy-preserving solution for IoT malware detection, without sharing data and enhancing security in distributed environments. The model utilizes a lightweight one-dimensional CNN to reduce preprocessing time and computational overhead, enabling automatic feature extraction. Furthermore, Grid search was used to optimize the CNN parameter for efficient malware prediction in IoT.

Olanrewaju-George et al. [32] presented Federated learning-based intrusion detection system (FL-IDS) for the Internet of Things (IoT) using unsupervised and supervised deep learning models. This model specifically utilizes Deep Auto Encoder (DAE) as the unsupervised model to detect anomalies and Deep Neural Network (DNN) as the supervised model for attack classification. These models were trained locally on individual IoT devices using the FedAvgM model, which preserves the data privacy while enabling the collaborative learning for best IDS performance.

Albogami, [33] developed an Intelligent Deep Federated Learning Model for Enhancing Security (IDFLM-ES) strategy for IoT-enabled edge computing. Federated hybrid deep belief network (FHDBN) model was applied in FL to analyze the time series data generated by IoT edge devices. Data normalization and golden jackal optimization (GJO) was employed for feature selection. This model learns individual and distributed feature representations over distributed databases to improve model convergence. Finally, the dung beetle optimizer (DBO) model was used to choose the optimal hyperparameter for the FHDBN model.

Çıplak et al. [34] suggested a FL-based malware detection and classification using DNN algorithms called FEDetect. The collected dataset was pre-processed to create separate dataset versions for binary and multiclass classification. Feedforward Neural Networks (FNN) and Long Short-Term Memory networks (LSTM) were applied for both classification types. Federated and non-federated versions were developed with total 22 base models with additional variants for testing. Model aggregation in the FL setup used the FedAvg algorithm with the Adam optimizer to suit low-power devices.

Zhang et al. [35] presented a Differential Privacy based FL algorithm with Clustered Model Random Selection (DPFedCMRS) for privacy preserving data. This model first groups clients based on similar data distributions. In order to address data heterogeneity, each cluster then selects a model at random from

other clusters during the iteration to learn the properties of various data distributions. To achieve sample-level differential privacy and safeguard the client's data privacy, the algorithm was subjected to differential privacy. An adaptive clustering algorithm (ACA) incorporates gradient quantile smartification (GQS) to guarantee high-accuracy clustering results while preserving high privacy.

Yang et al. [36] presented a clustering-based federated deep learning (Clu-FDL) model for personalized glucose prediction in diabetes management. This model utilizes Simple Recurrent Neural Network (SimpleRNN) and Gated Recurrent Units (GRU) to capture temporal patterns in patient glucose data. The integration combines clustering patients according to their intake of carbohydrates (CHO) with FL which protects data privacy by training models on local devices. For every patient group, this aids in producing more precise and customized predictions.

Li et al. [37] developed a Split Federated Learning (SFL) framework that synergistically integrates FL and split learning (SL) for enhancing cancer detection capabilities in medical consumer electronics. The SFL framework introduces a novel hybrid architecture where DL models were partitioned between client-side and server-side components. This model enabling efficient local feature extraction while preserving data privacy through secure and encrypted intermediate feature transmission for enhancing cancer detection.

Onaizah et al. [38] developed Siamese Convolutional Neural Network (SiCNN) in a peer-to-peer FL approach (FL-SiCNN) to improved brain tumor diagnosis. The SiCNN was used to improve the feature extraction and classification of brain tumor using paired medical images. The peer-to-peer FL approach (P2P-FL) approach ensured data security and privacy making it a privacy–preserving automated medical diagnosis solutions in collaborative healthcare settings.

Basnin et al. [39] integrated CNN, Belief Rule Base (BRB) system and FL models to improve the Alzheimer's disease prediction. In this model, modified CNN was used to process the MRI images for initial disease stage classification. These CNN outputs were than integrated with demographic data and passed into BRB system for handling uncertainty. This system works under Horizontal FL (HoFL) design to secure data privacy across multiple clients like hospitals. Moreover, Particle Swarm Optimization (PSO) was used to BRB parameters for enabling uncertainty-aware diagnosis of Alzheimer's Disease in multi-modal healthcare data.

Table 1 provides the comparison of various FL with DL models across different applications.

Table 1 Comparison of various FL with DL models across different applications

Ref No	Techniques Used	Advantage	Disadvantage	Dataset	Performance Evaluation
[23]	FL, JNBO, SpinalNet	Ensures secure collaboration between banks without data sharing, well optimized parameters	Low model interpretability, complex architecture harder to analysis	Private credit card transaction dataset	Accuracy = 89.10%; Mean Square Error (MSE) = 28.68%
[24]	FL, DAD, PRO	Preserves data privacy across clients, Works	Manual labeling still required for defect types, Higher	Industrial data from pre-baked carbon anodes (real-world case	Accuracy= 94.2% Precision= 91.3%

		with weak and limited labels	computational complexity due to two-stage training	study); data not directly shared due to privacy constraints	Recall = 90.3%
[25]	Generative AI, FL, EIIP, Fed_ANN11	Ensures data privacy by avoiding data centralization through FL, Effectively handles class imbalance	System heterogeneity and communication overhead	Genomic data from patients with Stomach Adenocarcinoma (STAD)	Training Accuracy = 99%, Testing Accuracy = 94%
[26]	FDL, DNN, SMOTE, Max Normalization	Reduces overfitting by decentralized training, Supports scalable training across devices	Slower model convergence, Communication between clients and server can increase latency and complexity.	ASHRAE RP-884 dataset with records, 56 features thermal comfort votes environmental conditions	Overall Accuracy: 82.40% Client 1 Accuracy: 85% Client 2 Accuracy: 83%
[27]	MFCC, FL, Bi-LSTMS	Handles diverse and imbalanced audio emotion data effectively across multiple sources.	Ineffective synchronization and coordination between clients and server during training	RAVDESS, CREMA, TESS, SAVEE with Happy, Sad, Angry, Neutral of 668,376 samples	Validation Accuracy = 99.97%; Precision: 99.97%; Recall: 99.97%
[28]	FL, LR, PCC CNN	Effective attack prediction, works efficiently on larger dataset	Works on imbalanced data high processing time, slightly overfitting issues	NSL-KDD and Car-Hacking dataset	Accuracy (LR) = 94%; Accuracy (CNN) = 99%
[29]	attention-based 1D-CNN-GRU, PSO, XAI, SHAP	captures complex temporal-spatial patterns in electricity data, improved interpretability	Pruning and multi-component optimization increase system design complexity	Panama Case Study data, Victoria State Electricity Dataset Australian Load Dataset, Household Electric Power	RMSE (Victoria State) = 0.18 RMSE (Household) = 1.05 RMSE (Australian Load) 39.23

				Consumption Dataset	RMSE (Panama) = 117.88
[30]	DVAE, CNN, Attention Mechanism, FL	Combines feature-rich learning with strong privacy protection, enabling secure IDS across distributed IIoT devices.	High model complexity and communication overhead can make real-time deployment on limited-resource IIoT devices challenging.	Telemetry Operation and Network dataset for IoT (TON-IoT) and Botnet IoT (BoT-IoT) dataset	Accuracy (TON-IoT) = 96.51%; Accuracy (BOT-IoT) = 99.35%;
[31]	1D-CNN, FL	Reduced preprocessing time and low computational overhead	Susceptible to communication delays and synchronization issues	IoT-23 dataset	Accuracy = 99.52%
[32]	FL-IDS, IoT, DAE, DNN and FedAvgM	Lower False Positive Rates (FPR), captures local anomaly patterns, better data distributions	High communication costs, challenge in identifying non-identical data affects convergence	N-BaIoT (9 IoT devices, 10 attack classes)	Accuracy = 90.39%; Precision = 99.99%; Recall = 90.10%
[33]	FL, FHDBN, GJO, DBO, IoT	Privacy preserving, improved accuracy, low data transfer	Not scalable in real time, potential computational cost, limited to specific attacks	Edge-IIoTset dataset (15,000 samples, 15 attack classes)	Accuracy = 98.24%; Precision = 86.79%; Recall = 86.78%
[34]	FL, FNN, LSTM	Avoids the risks of data breaches, lightweight models with limited computing power	Longer training time, Actual network communication between devices were not tested properly	CIC-MalMem-2022 dataset	Accuracy (Binary classification) = 99.99%; Accuracy (Multi classification) = 84.5%
[35]	Differential privacy, ACA, GQS	Eliminates the data leak risk from the central database, works	Lower computation and communication overhead, Complex model	MNIST, FMNIST and CIFAR10	Accuracy (MNIST) = 93.45%; Accuracy (FMNIST) =

		well on large users	syncing, cache overhead		82.36%; Accuracy (CIFAR10) = 65.71%
[36]	SimpleRNN, GRU, FL	Easy new patients adaptability, well-suited for diverse and privacy- sensitive healthcare applications.	Challenged computational demands on edge devices with limited resource-limited settings.	UVA/Padova Type 1 Diabetes Simulator (Python version by Xie) with 30 virtual patients: 10 each from adult, adolescentand child groups	Precision = 93%; Recall = 96%; F1-score = 95%
[37]	FL, SL, DL	Strong data privacy, Efficient local processing, high adapa ability on local devices	High latency demands and maintenance complexity, High security risks in transmission	BreakHis dataset	Accuracy = 93.1%
[38]	FL, SiCNN, P2P-FL	Highly suitable for decentralized environments, ensures data privacy	Difficult in handling larger datasets, more complex, multi-class classifications	MRI dataset by cheng et al. [40]	Accuracy = 97.11%; Precision = 96.03%; Recall = 95.89%
[39]	CNN, BRB, FL, PSO	Effectively handling multimodal data (image +demographics) and uncertainty, tested with multiple clients	Limited data interpretability, needs to improve in parameter optimization, adequate error rate	Alzheimer's Disease Neurology Initiative (ADNI) and NIfTI files dataset	Accuracy (CNN) = 98% Accuracy (FL) = 99.9%

3. RESULT AND DISCUSSION

In this section, the performance analysis of the FL combined with DL techniques, as presented in Table 1 underscores their effectiveness across a wide spectrum of application domains like healthcare diagnostics, financial fraud detection, IoT security, smart energy systems and more. The models were evaluated using diverse datasets some publicly available, capturing a range of real-world environments and data distribution scenarios. This section offers a comparative evaluation of these FL-DL approaches, focusing primarily on their classification accuracy and demonstrating how these integrated models perform under different conditions and use cases.

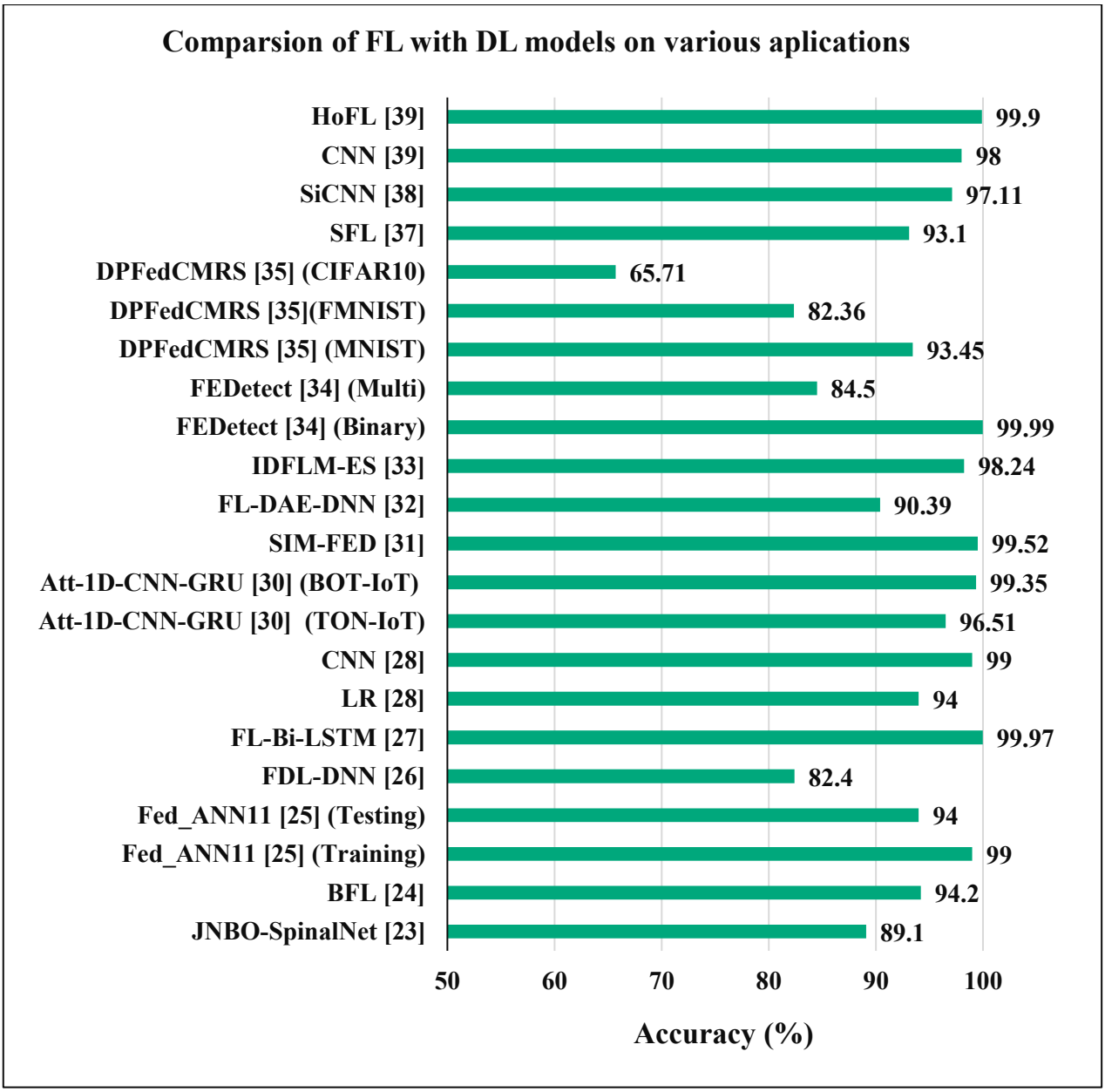

Figure 4 Graphical analysis of various FL with DL models for various application

Figure 4 depicts the graphical representation of different FL with DL based models for different application domains using the accuracy metric. Among the compared models, FEDetect (Binary) [34], HoFL [39] and SIM-FED [31] achieves highest accuracy of 99.99%, 99.9% and 99.52% respectively.

The FEDetect model [34] is a federated malware detection framework utilizing deep neural networks, where both binary and multiclass versions were trained using FNN and LSTM networks. It employs the FedAvg aggregation strategy along with the Adam optimizer to support low-power devices. This model effectively avoids the risk of data breaches and is well-suited for environments requiring lightweight computational models. The HoFL model [39] integrates CNN, BRB and Federated Learning to enhance Alzheimer's disease prediction. This model is particularly effective in handling multimodal data and managing uncertainty, making it suitable for deployment across multiple healthcare institutions. The SIM-FED model [31] provides a secure solution for IoT malware detection through a lightweight 1D-CNN architecture optimized via grid search. It significantly reduces preprocessing time and minimizes

computational overhead, making it an efficient and privacy-preserving approach for resource-constrained IoT environments.

Despite their advantages, these top-performing models also exhibit certain limitations. For instances, FEDetect model suffers from longer training times and lacks proper validation of real-world network communication between devices. Similarly, the HoFL model faces challenges related to limited interpretability of data, suboptimal parameter tuning, and a non-negligible error rate. The SIM-FED model is susceptible to communication delays and synchronization issues during deployment in distributed environments.

Thus, the limitations of these future models will be resolved in the future proposed models by developing an advanced and lightweight federated architectures integrated with DL models. The future model will emphasize efficient training techniques like model compression, adaptive federated optimizations and synchronous update mechanisms which collectively aims to improve scalability and reduce computational overhead. Also, in order to improve the interpretability, future model may incorporate attention models or transformers within FL models enabling the good decision making. Synchronization issues will be addressed by adopting the flexible communication strategies like client selection policies or asynchronous FL architectures.

Also, future research will explore the integration of multimodal data sources like sensor data, medical data and network traffic within FL-DL models for secure and collaborative learning. This approaches will enable more efficient learning across various different like IoT security, health care diagnosis, banking sector, government and financial fraud prediction. Also, these architectural improvements will aim to enhance scalability and make the models better suited for real-time, privacy preserving and distributed environments across diverse application domains.

4. CONCLUSION

FL combined with ML and DL models have shown great promise across various application domains like diagnostics, IoT security and financial anomaly detection. Compared to ML models, DL models results in superior performance in handling complex, high-dimensional and unstructured data. This paper presents a comphrensive review of FL-DL based models, analyzing the techniques used, their advantage and disadvantage, dataset types and performance evaluation. This study provides a valuable insight for researchers aiming to develop robust and secure predictive models in real-time deployment in distributed environments on various domains. Future work will focus on designing an advanced and lightweight FL-DL architectures to improve scalability, reduce computational complexity and resolve the synchronization issues in distributed systems. Efforts will also focus on improving the models interpretability in enabling efficient real-time deployment in various application domains.

REFERENCES

1. Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854.
2. Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.
3. Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 8, 140699-140725.

4. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE communications surveys & tutorials, 23(3), 1622-1658.
5. Huang, Y., Yang, X., Guo, J., Cheng, J., Qu, H., Ma, J., & Li, L. (2022). A high-precision method for 100-day-old classification of chickens in edge computing scenarios based on federated computing. Animals, 12(24), 3450.
6. Chou, L., Liu, Z., Wang, Z., & Shrivastava, A. (2021, September). Efficient and less centralized federated learning. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 772-787). Cham: Springer International Publishing.
7. Beltrán, E. T. M., Pérez, M. Q., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., ... & Celdrán, A. H. (2023). Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials*, *25*(4), 2983-3013.
8. AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal, 8(7), 5476-5497.
9. Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.
10. Yurdem, B., Kuzlu, M., Gullu, M. K., Catak, F. O., & Tabassum, M. (2024). Federated learning: Overview, strategies, applications, tools and future directions. Heliyon, 10(19).
11. Bharati, S., Mondal, M. R. H., Podder, P., & Prasath, V. S. (2022). Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems*, *18*(1-2), 19-35.
12. Hao, M., Li, H., Luo, X., Xu, G., Yang, H., & Liu, S. (2019). Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Transactions on Industrial Informatics, 16(10), 6532-6542.
13. Haggenmüller, S., Schmitt, M., Krieghoff-Henning, E., Hekler, A., Maron, R. C., Wies, C., ... & Brinker, T. J. (2024). Federated learning for decentralized artificial intelligence in melanoma diagnostics. JAMA dermatology, 160(3), 303-311.
14. Bárcena, J. L. C., Daole, M., Ducange, P., Marcelloni, F., Renda, A., Ruffini, F., & Schiavo, A. (2022, January). Fed-XAI: Federated Learning of Explainable Artificial Intelligence Models. In XAI. it@ AI* IA (pp. 104-117).
15. Liu, J., Huang, J., Zhou, Y., Li, X., Ji, S., Xiong, H., & Dou, D. (2022). From distributed machine learning to federated learning: A survey. Knowledge and information systems, 64(4), 885-917.
16. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.
17. Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. arXiv preprint arXiv:2107.10976.
18. Sarma, K. V., Harmon, S., Sanford, T., Roth, H. R., Xu, Z., Tetreault, J., ... & Arnold, C. W. (2021). Federated learning improves site performance in multicenter deep learning without data sharing. Journal of the American Medical Informatics Association, 28(6), 1259-1264.
19. Gugueoth, V., Safavat, S., & Shetty, S. (2023). Security of Internet of Things (IoT) using federated learning and deep learning—Recent advancements, issues and prospects. ICT express, 9(5), 941-960.

20. Guo, P., Wang, P., Zhou, J., Jiang, S., & Patel, V. M. (2021). Multi-institutional collaborations for improving deep learning-based magnetic resonance image reconstruction using federated learning. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 2423-2432).
21. Li, H., Cai, Z., Wang, J., Tang, J., Ding, W., Lin, C. T., & Shi, Y. (2023). Fedtp: Federated learning by transformer personalization. IEEE transactions on neural networks and learning systems, 35(10), 13426-13440.
22. Zhu, H., Zhang, H., & Jin, Y. (2021). From federated learning to federated neural architecture search: a survey. Complex & Intelligent Systems, 7(2), 639-657.
23. Reddy, V. V. K., Reddy, R. V. K., Munaga, M. S. K., Karnam, B., Maddila, S. K., & Kolli, C. S. (2024). Deep learning-based credit card fraud detection in federated learning. Expert Systems with Applications, 255, 124493.
24. Guo, W., & Jiang, P. (2024). Weakly Supervised anomaly detection with privacy preservation under a Bi-Level Federated learning framework. Expert Systems with Applications, 254, 124450.
25. Sikandar, M., Din, I. U., & Almogren, A. (2024). Integrating generative AI and federated learning for privacy preserved sequence-based stomach adenocarcinoma detection. IEEE Transactions on Consumer Electronics, 70(3), 5278-5285.
26. Abbas, S., Alsubai, S., Sampedro, G. A., Abisado, M., Almadhor, A., & Kim, T. H. (2024). Privacy preserved and decentralized thermal comfort prediction model for smart buildings using federated learning. PeerJ Computer Science, 10, e1899.
27. Chawla, M., Panda, S. N., Khullar, V., Kumar, S., & Bhattacharjee, S. B. (2024). A lightweight and privacy preserved federated learning ecosystem for analyzing verbal communication emotions in identical and non-identical databases. *Measurement: Sensors*, *34*, 101268.
28. Bhavsar, M. H., Bekele, Y. B., Roy, K., Kelly, J. C., & Limbrick, D. (2024). Fl-ids: Federated learning-based intrusion detection system using edge devices for transportation iot. IEEe Access, 12, 52215-52226.
29. Sarker, M. A. A., Shanmugam, B., Azam, S., & Thennadil, S. (2024). Enhancing smart grid load forecasting: An attention-based deep learning model integrated with federated learning and XAI for security and interpretability. Intelligent Systems with Applications, 23, 200422.
30. Huang, J., Chen, Z., Liu, S. Z., Zhang, H., & Long, H. X. (2024). Improved intrusion detection based on hybrid deep learning models and federated learning. Sensors, 24(12), 4002.
31. Nobakht, M., Javidan, R., & Pourebrahimi, A. (2024). SIM-FED: Secure IoT malware detection model with federated learning. Computers and Electrical Engineering, 116, 109139
32. Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. Cyber Security and Applications, 3, 100068.
33. Albogami, N. N. (2025). Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment. *Scientific Reports*, *15*(1), 4041.
34. Çıplak, Z., Yıldız, K., & Altınkaya, Ş. (2025). FEDetect: a federated learning-based malware detection and classification using deep neural network algorithms. Arabian Journal for Science and Engineering, 1-28.
35. Zhang, Y., Long, S., Liu, G., & Zhang, J. (2025). DP-FedCMRS: Privacy-preserving federated learning algorithm to solve heterogeneous data. IEEE Access.

36. Yang, X., & Li, J. (2025). A clustering-based federated deep learning approach for enhancing diabetes management with privacy-preserving edge artificial intelligence. Healthcare Analytics, 7, 100392.
37. Li, X., Lin, Q., Khan, F., Kumari, S., Alenazi, M. J., & Yang, J. (2025). Enhancing Cancer Detection Capabilities in Medical Consumer Electronics through Split Federated Learning and Deep Learning Optimization. IEEE Transactions on Consumer Electronics.
38. Onaizah, A. N., Xia, Y., & Hussain, K. (2025). FL-SiCNN: An improved brain tumor diagnosis using siamese convolutional neural network in a peer-to-peer federated learning approach. Alexandria Engineering Journal, 114, 1-11.
39. Basnin, N., Mahmud, T., Islam, R. U., & Andersson, K. (2025). An evolutionary federated learning approach to diagnose alzheimer's disease under uncertainty. Diagnostics, 15(1), 80.
40. Cheng, J., Huang, W., Cao, S., Yang, R., Yang, W., Yun, Z., ... & Feng, Q. (2015). Enhanced performance of brain tumor classification via tumor region augmentation and partition. PloS one, 10(10), e0140381.