Expert Systems

WILEY

Expert Systems

ORIGINAL ARTICLE

Leveraging Transfer Learning Domain Adaptation Model With Federated Learning to Revolutionise Healthcare

Priyanka Verma[1] | Nitesh Bharot[1] | John G. Breslin[1] | Donna O'Shea[2] | Anand Kumar Mishra[3] | Ankit Vidyarthi[4] | Deepak Gupta[5]

[1]Data Science Institute, University of Galway, Galway, Ireland | [2]Department of Computer Science, Munster Technological University, Cork, Ireland | [3]Department of CSE, NIIT University, Neemrana, Rajasthan, India | [4]Department of CSE&IT, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India | [5]Department of CSE, Maharaja Agrasen Institute of Technology, Delhi, India

Correspondence: Ankit Vidyarthi (dr.ankit.vidyarthi@gmail.com)

Received: 31 January 2024 | **Revised:** 25 November 2024 | **Accepted:** 11 December 2024

Funding: This work was supported by European Union's Horizon (Grant Number 847577) and Science Foundation Ireland (Grant Numbers SFI/12/RC/3918) and also in part supported by Taighde Éireann - Research Ireland under grants 12/RC/2289-P2 (Insight) and 21/FFP-A/9174 (SustAIn).

Keywords: deep learning | federated learning | healthcare | transfer learning | UCI-HAR

ABSTRACT

The application of artificial intelligence (AI) in healthcare has been witnessing an increasing interest. Particularly, federated learning (FL) has become favourable due to its potential for enhancing model quality whilst maintaining data privacy and security. However, the effectiveness of present FL methodologies could underperform under non-IID conditions, characterised by divergent data distributions across clients. The globally constructed FL model may suffer potent issues by allowing the least-performing models to equal participation. Thus, we propose a new accuracy-based FL approach (FedAcc) which only takes into account the clients' validation accuracy to consider their participation during global aggregation, also called Smart Healthcare Amplified (SHA). However, with limited supervised data it is challenging to increase the model performance thus concept of transfer learning (TL) is used. TL enables the global model to integrate knowledge from precomputed systems, resulting in an efficient model. However, the complexity of the global system is amplified by these TL models, leading to challenges related to vanishing gradients, particularly when dealing with a substantial number of layers. To mitigate this, we present a Transfer Learning Domain Adaptation Model (TLDAM). TLDAM employs a two-layered sequentially trained TL model, which contains approximately 50% fewer layers compared to traditional TL models. TLDAM is trained on multiple datasets such as MNIST and CIFAR10, to enhance its knowledge and make it domain-adaptive. Moreover, experimental results conducted on the UCI-HAR dataset reveal the supremacy of our proposed framework with an accuracy of 94.2990%, F-score of 94.2820%, precision of 94.3058%, and recall of 94.2993% over traditional FL techniques and state-of-the-art techniques.

1 | Introduction

Healthcare is a growing area of research that has an unmeasurable effect to improve the quality of life. It aims at the prevention and treatment of diseases, and injuries along with monitoring all the steps to recovery. With enhanced artificial intelligence (AI) capabilities in the healthcare industry, the landscape of healthcare is undergoing a remarkable transformation driven by an escalating demand for security and privacy measures. The development of AI has led to more smart applications in the medical sector but has also increased the need for security (Verma et al. 2022).

In addition to that, Internet of Things (IoT) devices play a pivotal role in transforming the healthcare landscape by offering a multitude of benefits that enhance patient care, medical practices

https://doi.org/10.1111/exsy.13827

and overall healthcare efficiency (El-Sherif et al. 2022; Tam et al. 2023). They have evolved into independent data sources with the potential to revolutionise the healthcare sector. The integration of IoT in healthcare holds the promise of significantly enhancing healthcare capabilities. They enable the exchange of data and computational capabilities thus improving healthcare stats (Borgia 2014; Madakam et al. 2015; Sun, Liu, and Yue 2019), and pharmaceutical manufacturing pipelines and eventually enabling affordable good healthcare (Choi, Xiao, and Stewart 2018; Lu et al. 2022a; Unal, Akgun, and Pfeifer 2021).

These devices enable continuous tracking of vital signs, facilitate remote consultations, provide valuable health trend data, enhance treatment personalization and optimise healthcare workflows. Wearable health technology empowers individuals to engage in healthier behaviours, whilst IoT-driven emergency alerts and medication management systems ensure rapid responses and improved adherence. Moreover, IoT devices contribute to medical research, public health surveillance and cost-effective healthcare delivery, ultimately leading to enhanced patient outcomes, reduced costs and more patient-centred medical approaches (El-Sherif et al. 2022; Tam et al. 2023). However, there is not a reliable data source that can offer all the essential details, and frequently labels are absent for the vast bulk of training data. Due to the shortage of data and labels, machine learning (ML) models could not function properly, which causes a bottleneck for intelligent medical systems. Medical institutions are not willing to share their data due to data privacy and security issues. Thus, integrating federated learning (FL) is a viable approach to overcome the above issues.

FL (McMahan et al. 2017) presents a distributed architecture that adeptly addresses challenges associated with centralised learning paradigms (Xiong et al. 2020). These challenges encompass vulnerabilities like single points of failure and communication bottlenecks. A distinctive feature of FL is its ability to shift the computational burden from the central system to the individual client (Issa et al. 2023; Verma, Breslin, and O'Shea 2022). The amalgamation of FL within healthcare along with IoT has significant potential. FL plays a crucial role in healthcare (Chen et al. 2020) and smart healthcare systems (Li et al. 2021; Zhang, Kou, and Wang 2021; Zhou et al. 2022). This novel approach eliminates the need for data transfer to a centralised system for further processing and distribution of the workload (Manickam et al. 2022; Singh et al. 2022). The performance of these FL models could be then evaluated based on accuracy and communication rounds (Khan, Glavin, and Nickles 2023). Here, instead of aggregating data on a centralised server, learning takes place directly on user devices whilst only sharing model updates ensuring robustness, scalability and improved accuracy, setting it apart as a potent solution for contemporary ML challenges.

However, in FL the inherent variability in client data presents a hurdle, potentially leading to the inclusion of under-performing models on equal footing during global aggregation (Verma, Breslin, and O'Shea 2023). To surmount this issue, we propose FedAcc, a novel approach that selectively considers clients' validation accuracy levels for participation during the global aggregation process. The resulting aggregated system is poised to foster the development of an improved global framework with enriched capabilities.

The concept of transfer learning (TL) holds paramount importance in ML and deep learning (DL) due to its ability to enhance data efficiency, expedite training, improve generalisation, address limited data challenges, facilitate domain adaptation, aid in feature learning, mitigate over-fitting risks, conserve resources and enable state-of-the-art performance. By leveraging knowledge from pre-trained models, TL empowers models to transfer learned features and patterns across tasks and domains, ultimately advancing the capabilities of various applications and domains in the field of AI. In the realm of healthcare datasets, TL (Kishor and Chakraborty 2022; Nguyen et al. 2022), has emerged as a preeminent technique due to its demonstrated superiority in performance. TL empowers the global model to harness knowledge from precomputed systems, thereby elevating its performance levels. However, the integration of TL models introduces complexities that can lead to challenges, notably the issue of vanishing gradients, especially within models featuring a substantial number of layers. To address this concern, we introduce a Transfer Learning-based Domain Adaptation Model (TLDAM). This model design employs a two-layered sequentially trained TL architecture, boasting a streamlined structure with approximately 50% fewer layers compared to traditional TL models. Our TLDAM approach is honed through training on diverse datasets, including MNIST and CIFAR10, thereby enhancing its domain adaptability and performance capacity.

The superiority of our proposed framework which includes TLDAM and FedAcc methodologies, jointly called Smart Healthcare Amplified (SHA), is empirically established through rigorous experimentation on the UCI-HAR dataset. The experimental results of the SHA validate the efficacy of our approach over conventional FL techniques and state-of-the-art methodologies, reinforcing their potential to reshape and advance healthcare system paradigms. The contributions of the SHA framework are as follows:

- Proposed framework SHA adopted FL to enable secure and efficient distributed computation. By applying FL, the paper establishes a novel approach that addresses the challenge of the limited computational capacity of centralised systems, allowing for distributed model training whilst maintaining data privacy. Thus, exemplifying the potential of FL to advance healthcare capabilities in a secure and privacy-conscious manner.
- This work also contributes FedAcc, a novel approach that leverages clients' accuracy levels for participation in global aggregation. By selectively considering accuracy, FedAcc addresses the issue of under-performing models influencing aggregated results, leading to more accurate outcomes in healthcare data analysis.
- SHA introduces the streamlined two-layered TLDAM to overcome complexities in TL. With fewer layers than traditional models, TLDAM enhances adaptability whilst effectively integrating knowledge from diverse datasets. Empirical validation confirms TLDAM and FedAcc's superiority over existing methodologies, promising transformative healthcare advancements.

The subsequent sections of the paper are structured as follows: Section 2 delves into an exploration of related work in the field.

In Section 3, we present the foundational concepts and preliminary knowledge relevant to our study. The core of our contribution, the proposed framework, is elaborated upon in Section 4, where we outline its design and mechanics. Moving forward, Section 5 conducts a thorough examination of the experimental results and provides an insightful analysis. Lastly, Section 6 encapsulates the paper by summarising our findings, drawing conclusions from the study, and suggesting potential avenues for future research and development.

2 | Related Work

McMahan et al. (2017) introduced a robust methodology that employs a deep network model to effectively handle decentralised data through an efficient communication system. This approach demonstrates resilience in the face of challenges posed by unbalanced and non-IID data distribution. The concept of non-IID refers to the disparity between a user's local dataset and the overall population distribution, often stemming from individual mobile device usage patterns. Meanwhile, "unbalanced" data pertains to varying levels of usage amongst users, resulting in unequal local training data. By tackling these complexities, their proposed method showcases the adaptability of deep models in decentralised scenarios, shedding light on their efficacy in real-world applications with diverse data dynamics.

Jiménez-Sánchez et al. (2023) centre their research on enhancing the efficacy of computer-aided diagnosis (CAD) systems for breast cancer detection, a field challenged by the scarcity of representative positive cases in routine mammography imaging datasets. Their study introduces a novel memory-aware curriculum learning approach within the context of FL. In this method, local models operate on their private data to update the global model. The proposed curriculum guides the sequence of training samples, giving precedence to those that tend to be overlooked. This strategy is complemented by unsupervised domain adaptation, addressing domain shifts whilst ensuring data privacy. By merging these innovative techniques, the study endeavours to bolster the performance of CAD systems, particularly in scenarios characterised by data imbalance and domain variations. Xiong et al. (2021) tackle the challenge of FL with non-IID data, a common occurrence in real-world contexts. They employ multiple strategies to address this issue, encompassing data partitioning, model aggregation and TL techniques. Subsequently, the effectiveness of these methods is evaluated across diverse datasets. This study contributes to the advancement of FL methodologies, shedding light on techniques that can mitigate the impact of non-IID data distributions, thereby enhancing the reliability and adaptability of FL models across various application domains.

The proposal by Du et al. (2017) centres on employing Long Short-Term Memory (LSTM) networks to model system logs as sequences resembling natural language. Through the acquisition of log patterns during regular operations, their approach strives to identify anomalous behaviours by detecting deviations from the log-generated model established during normal execution. This method capitalises on LSTM's sequential learning capabilities to enhance anomaly detection in system logs, thereby contributing to improved system monitoring and ensuring timely identification of irregular activities.

In the healthcare landscape, data from diverse sources such as clinical institutions, patients and insurers are driving the significance of ML services. To ensure trustworthy ML models amid growing privacy concerns, FL gains prominence due to its ability to preserve data integrity across IoT devices. However, network instability challenges FL's accuracy. Houssein and Sayed (2023) present a novel approach using FedImpPSO, an enhanced Particle Swarm Optimization, for FL model updates. Their method exhibits improved accuracy and robustness in unstable networks, proven with case studies on COVID-19 classification and cardiovascular prediction, emphasising its potential in healthcare and privacy-driven domains.

Gupta et al. (2024) explores ML's transformative role in healthcare, detailing its applications in diagnosis, literature comparisons and real-life use cases. It discusses the challenges within the healthcare system, practical disease prediction implementations and the future of ML in enhancing global health outcomes, ultimately improving patient care and reducing costs. Another article (Puri, Kataria, and Sharma 2024) proposes an AI-enabled decentralised healthcare framework to address the challenges of remote patient monitoring, such as security and privacy issues. Utilising AI smart contracts and public blockchain, it authenticates IoT devices and ensures transparency in patient records whilst improving system metrics like energy consumption and latency in a real-time test environment.

Alkhdour et al. (2024) proposed a solution that integrates fuzzy logic algorithms with blockchain technology to improve authentication security in digital healthcare environments. Fuzzy logic helps reduce false positives and negatives, enhancing the system's defence against various cyber threats. Blockchain offers a decentralised, tamper-resistant structure for secure data management, ensuring transparency and trust. This dual approach not only efficiently handles authentication requests, promoting scalability, but also lowers communication overheads and improves system responsiveness. Tested against the NIST Special Database 302, the method shows superior performance, exhibiting robustness against attacks like replay, man-in-the-middle, DoS and impersonation, making it ideal for secure peer-to-peer cloud interactions.

In the study "Federated Learning for Healthcare Informatics" Zhang et al. focuses on harnessing FL's capabilities in healthcare informatics, a field dedicated to analysing medical data from diverse sources to enhance patient care and results. The paper delves into the myriad applications of FL within healthcare, spanning disease diagnosis, drug exploration and personalised treatment approaches. The authors underscore the significance of this approach whilst addressing the pertinent challenges posed by data heterogeneity, privacy concerns and regulatory adherence. The study also offers potential resolutions to these challenges and outlines promising avenues for future research, affirming the role of FL as a transformative tool in the realm of healthcare informatics.

While FedAvg is effective in various scenarios, challenges like non-IID data and the need for personalised client models persist

(Khodak, Balcan, and Talwalkar 2019; Smith et al. 2017; Zhu, Hong, and Zhou 2021). A comprehensive survey discussing FL on non-IID data can be found in Zhu et al. (2021). FedProx (Zhang et al. 2022) addresses non-IID data by allowing partial aggregation and integrating a proximal term with FedAvg. In Yeganeh et al. (2020), client model weights are aggregated via L1 distance. Some approaches concentrate on a universal model shared by all clients, whilst others strive for unique models for each. Arivazhagan et al. (2019) exchange base layer information whilst retaining a personalization layer to mitigate non-IID effects. Dinh, Tran, and Nguyen (2020) employs Moreau envelopes as client-regularised loss functions, decoupling personalised model optimization from global learning. Amid the surge in healthcare-oriented ML, FL gains traction for privacy-preserving models. FL's efficacy, however, diminishes with non-IID scenarios. Addressing this, propose FedAP (Lu et al. 2022b), harnessing batch normalisation layer stats for client similarity whilst retaining specificity through local normalisation. Across five healthcare benchmarks, FedAP outperforms state-of-the-art methods with notably enhanced accuracy (e.g. ≥10% for PAMAP2) and accelerated convergence.

While FedAvg, a commonly used aggregation technique, exhibits effectiveness, it grapples with issues concerning non-IID data distribution and the need for personalised models. Thus to overcome above issues we propose a FedAcc and TLDAM-based framework called SHA. TLDAM, a component of the SHA framework, introduces a two-layered sequential TL model with reduced complexity. This architecture enables the extraction of task-specific features from diverse healthcare datasets whilst minimising the risk of over-fitting or excessive model complexity. By leveraging TL techniques, TLDAM facilitates the adaptation of pre-trained models to new tasks or domains, thereby enabling the creation of personalised models that can effectively capture the nuances of individual patients or medical conditions.

3 | Preliminaries

3.1 | Centralised Learning

Centralised learning refers to a traditional approach in ML where data from various sources such as IoTs is collected at a single server to train the model. In this approach, a central server or processing unit is responsible for aggregating all the data from different clients or sources, conducting the training process, and then distributing the trained model back to the clients. Developments show that with increasing data size, security concerns and user restrictions day-by-day, it becomes arduous to implement a centralised approach (Ferrag et al. 2022; Haddad, Hedjazi, and Aouag 2022; Namalomba, Feihu, and Shi 2022).

3.2 | Federated Learning

FL is Google developed method that brings the computation to the client itself. Let there be K clients $k \in K$, and the number of communication rounds be Γ and client training data as $train_1$, $train_2$, $train_3$, ..., $train_k$, ..., $train_K$. Each $train_k = \left\{train\_X_k, train\_y_k\right\}_{k=1}^{K}$ and testing dataset as $test\_X, test\_y$ for all clients. Each training data has distinct distribution such that $P\left(train_a\right) \neq P\left(train_b\right)$. Every client has its individual local model τ_1 and it is trained with loss function as:

$$\zeta\left(train_k, w\right) = \frac{1}{\mid train_k \mid} \sum \zeta_k\left(train\_X_k, train\_y_k, w\right) \quad (1)$$

where $\sum$ varies for $\left(train\_X_k, train\_y_k\right) \in train_k$ and $\zeta_k\left(train\_X_k, train\_y_k, w\right)$ is a specific function to be minimised. So our goal is to finally aggregate the τ_1 to obtain global model τ_g for each client by maintaining the data privacy:

$$\min_{\left\{\tau_k\right\}_{k=1}^{K}} \frac{1}{K} \sum_{k=1}^{K} \frac{1}{\mid train_k \mid} \sum_{i=1}^{train_k} \zeta\left(\tau_1^{(k)}\left(train\_X_k\right), train\_y_k\right) \quad (2)$$

3.3 | Nesterov Accelerated Gradient Descent

The main idea of Nesterov Stochastic Gradient Descent (NSGD) is to look ahead before making the gradient update. This helps to anticipate the future position and adjust the update accordingly, allowing the algorithm to converge faster and with fewer oscillations compared to traditional Stochastic Gradient Descent (SGD). This concept is particularly beneficial when dealing with complex optimization landscapes like those encountered in Deep Neural Networks (DNN). The main idea of NSGD is to look ahead before making the gradient update. A standard SGD works on:

$$w_{i+1} = w_i - \eta \nabla \zeta\left(train_k, w_i\right) \quad (3)$$

$$\nabla \zeta\left(train_k, w_i\right) = \frac{\sum_{k=1}^{K} \Delta\mu_k^i}{\sum_{k=1}^{K} train_k} \quad (4)$$

where η is the learning rate and $\Delta\mu_k^i = \mid train_k^i \mid \nabla \zeta\left(train_k^i, w^i\right)$ is the locally computed client gradient and uploaded to server. However, NSGD works as:

$$\vartheta(i+1) = \gamma\vartheta(i) + \eta \nabla \zeta(w(i) - \gamma \times \vartheta(i)) \quad (5)$$

$$w(i+1) = w(i) - \vartheta(i+1) \quad (6)$$

where ϑ is velocity at ith iteration, and γ is momentum parameter with $\gamma \in \{0, 1\}$.

3.4 | Transfer Learning

TL is an DL technique where knowledge gained from training a model on one task is applied to improve performance on a related but different task. By leveraging the learned features or parameters, TL reduces the need for extensive training data and computation for the new task. This approach is particularly effective when data is limited, enhancing model accuracy, convergence speed and generalisation. Pre-trained models from large datasets serve as valuable starting points. Fine-tuning or feature extraction methods adapt the model for the target task. Here the layers of the model are frozen and then collaborated (or not) with different DL models to design domain-specific solutions. This concept of layer freezing deters the frozen layer weights to be updated thus enabling the pre-trained model to transfer its knowledge to the new model.

3.5 | Activation Functions

Activation functions play a pivotal role in neural networks, shaping their ability to model complex relationships within data. Three of the used activation functions in SHA are Rectified Linear Unit (ReLU), Softmax and Scaled Exponential Linear Unit (SELU). ReLU, a widely employed activation, defined as the max of zero and the input, effectively introducing non-linearity whilst disregarding negative values.

$$\mathrm{ReLu}(y) = \sigma(y) = \max(0, y) \tag{7}$$

Softmax, on the other hand, is often employed in multi-class classification tasks, normalising the input values into a probability distribution, making it suitable for selecting the most probable class.

$$\mathrm{softmax}(y) = \sigma(y) = \frac{e^{y_i}}{\sum_{i=1}^{N} e^{y_i}} \tag{8}$$

where $x = \left[y_1, y_2, y_3, \ldots, y_N\right]$.

SeLu is a self-normalising activation, designed to combat the vanishing/exploding gradient problem. It maintains mean and variance stability within layers, enhancing network training and potentially yielding improved performance. Each activation function serves a unique purpose, contributing to the neural network's capacity to model intricate patterns and produce accurate predictions in diverse scenarios.

$$\mathrm{SeLu}(y) = \lambda y \quad \text{or} \quad \lambda(\alpha e^{y} - \alpha) \tag{9}$$

depending on $y \geq 0$ or $y \leq 0$ respectively.

4 | Proposed Work

This section formulates the proposed work. It starts by describing the need for this approach, and the FL procedure and finally explains the various components involved in the proposed work. All the notations used in the proposed system are described in Table 1.

Existing TL methods in healthcare face several drawbacks that impede their effectiveness. Firstly, these methods often struggle with domain shifts, as healthcare data can exhibit variations across different sources and institutions, making it challenging to adapt models effectively. Secondly, the presence of non-IID data distribution, where data from different clients or sources have varying statistical properties, hinders the direct applicability of pre-trained models. Moreover, some TL models may suffer from scalability issues, especially when dealing with large and complex medical datasets, causing training times to increase significantly. To mitigate these challenges, we propose a multi-TL concept called TLDAM. This multi-TL concept strives to enhance the adaptability and performance of TL methods in healthcare, providing potential solutions to the sector's prevailing challenges.

TABLE 1 | Meanings and notations.

Meaning	Notation
TL model local and global	τ_l and τ_g
Moderation index at round r	$\varsigma^{(r)}$
Total communication rounds	Γ
Total clients	K
Scaling factor at round r	$\mathrm{sf}^{(r)}$
Aggregated weights at round r	$\omega_g^{(r)}$
Activation function	σ
Velocity at ith iteration	ϑ
Momentum parameter	γ
Loss function	ζ
Weights of local model	w
Iterations	i

Additionally, it has been observed and experimentally proved that centralised approaches for data scrutinization fall apart and face various issues (Ferrag et al. 2022; Haddad, Hedjazi, and Aouag 2022; Namalomba, Feihu, and Shi 2022). Therefore, FL has emerged as a potent solution for seamless integration into the healthcare sector. FL is a distributed approach where model training occurs locally on decentralised devices or clients, preserving data privacy. Models' updates are then aggregated on a central server, enhancing the global model collaboratively whilst keeping sensitive data localised and private.

This section delineates the architecture of the proposed framework which has two components: the TLDAM framework and FedAcc. The images or data captured by healthcare systems can serve as inputs to pre-trained TL models, synergistically amalgamated with DL techniques to formulate innovative solutions. As illustrated in Figure 1, the FL process within the healthcare domain is portrayed, specifically focusing on incorporating FedAcc. This integrated approach harnesses the power of distributed learning to address healthcare challenges, underpinned by TL's adaptability and the data-sharing potential of FL, ultimately culminating in enhanced healthcare outcomes.

Firstly, the TLDAM process commences with training the model using MNIST and CIFAR10 images. The TLDAM model is merged with convolutional neural networks (CNNs) and multilayer perceptrons (MLPs), producing a global model. The initialization involves sharing initial parameters between the global model and clients. Following this, clients train their individual models on personal datasets and transmit both model weights and validation accuracy to the global server. These validation

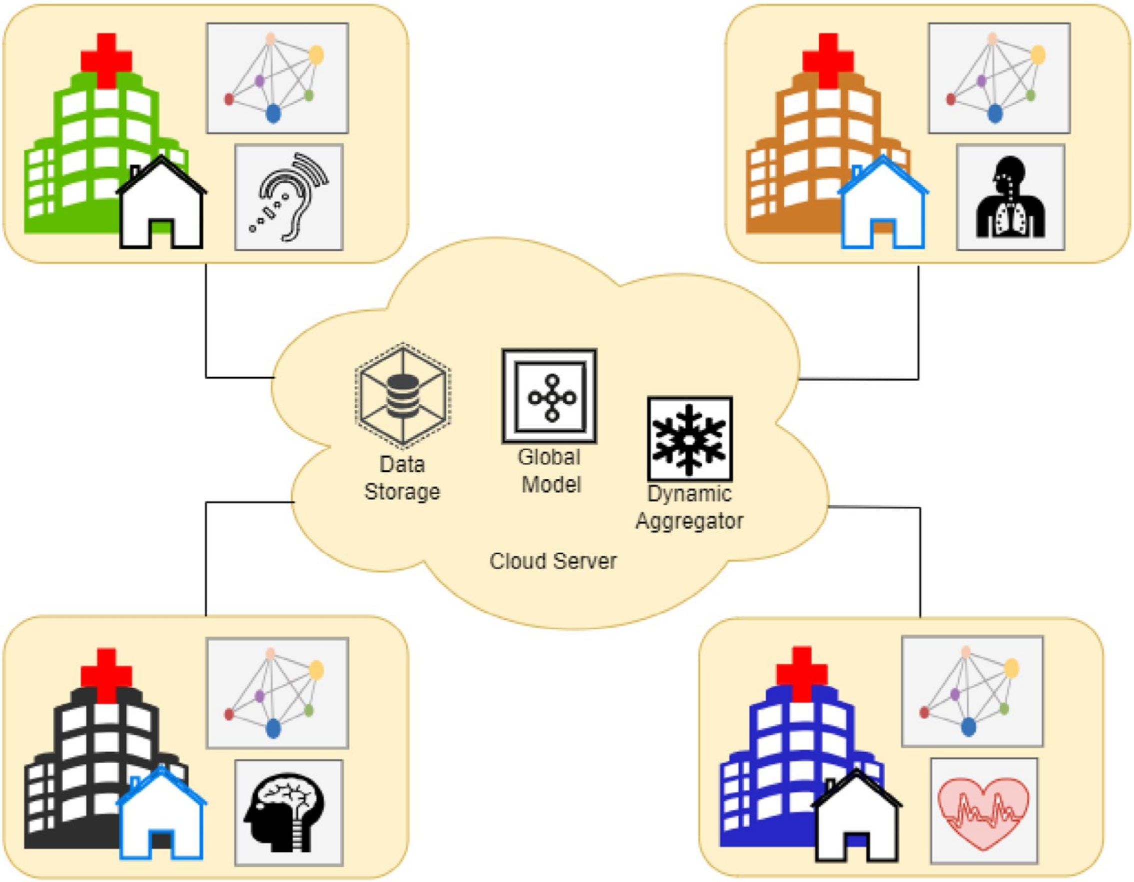

FIGURE 1 | Federated framework. (1) Server initializes the process by sharing model τ_g for training of each client, (2) Local model τ_l are then trained by each client with their data, (3) Client shares the local model τ_l parameters with their accuracy, (4) Server aggregates the local models τ_l to obtain global weights and shares them with clients, and (5) Repeat steps (2)–(4) for communication rounds Γ.

accuracy values serve to define the scaling parameters to apply FedAcc. Leveraging validation accuracy, the server aggregates the weights of clients using FedAcc. Once a communication round concludes, the server returns aggregated weights to clients for subsequent analysis or predictions, embodying a cyclic and collaborative learning approach.

4.1 | TLDAM Framework

TLDAM is a multi-layered sequential TL model which is trained on the MNIST and CIFAR10 images and then further used as TL model to transfer the concept. Figure 2 describes the TLDAM framework indicating that it is composed of two TL models combined together and weights transferred sequentially from the model preceding to the front. Let the TL model one has the following layers as represented:

$$\xi_1 = \text{Conv1D}_1(\text{input\_shape}, \text{activation} = \text{relu}, \text{filters} = 128, \text{kernel\_size} = 3) \tag{10}$$

$$\xi_2 = \text{MaxPooling1D}_1(2) \tag{11}$$

$$\xi_3 = \text{Conv1D}_2(\text{activation} = \text{relu}, \text{filters} = 64, \text{kernel\_size} = 3) \tag{12}$$

$$\xi_4 = \text{BatchNormalization}_1() \tag{13}$$

$$\xi_5 = \text{Flatten}_1() \tag{14}$$

$$\xi_6 = \text{Dense}_1(\text{activation} = \text{relu}, 64) \tag{15}$$

$$\xi_7 = \text{Dense}_2(\text{activation} = \text{softmax}, 10) \tag{16}$$

which are trained on MNIST images. Next, these TL model 1 layers $\xi_1, \xi_2, \xi_3, \xi_4$ are frozen, that is, the weights of the layers ξ_1, ξ_3, ξ_4 are fixed and set to non-trainable whereas with layer ξ_2 it is experimentally determined to allow it to be trainable for better systems. Therefore, the batch normalisation layer is set as trainable, and afterward $\xi_1, \xi_2, \xi_3, \xi_4$ are used in TL model 2. This way TL model 2 will have knowledge of one kind of dataset and knowledge of TL model 1 will be transferred to TL model 2. Using TL model 1 layers TL model 2 could be constructed as:

$$\psi_5 = \xi_1 + \left(\xi_2\right) + \xi_3 + \xi_4 + \text{Conv1D}_3\left(32, 3, \text{activation} = \}\text{selu}'\right) \tag{17}$$

$$\psi_6 = \text{MaxPooling1D}_2(2) \tag{18}$$

$$\psi_7 = \text{BatchNormalization}_2() \tag{19}$$

$$\psi_7 = \text{Flatten}_2() \tag{20}$$

$$\psi_8 = \text{Dense}(256, \text{activation} = \text{relu}) \tag{21}$$

$$\psi_9 = \text{Dense}(128, \text{activation} = \text{relu}) \tag{22}$$

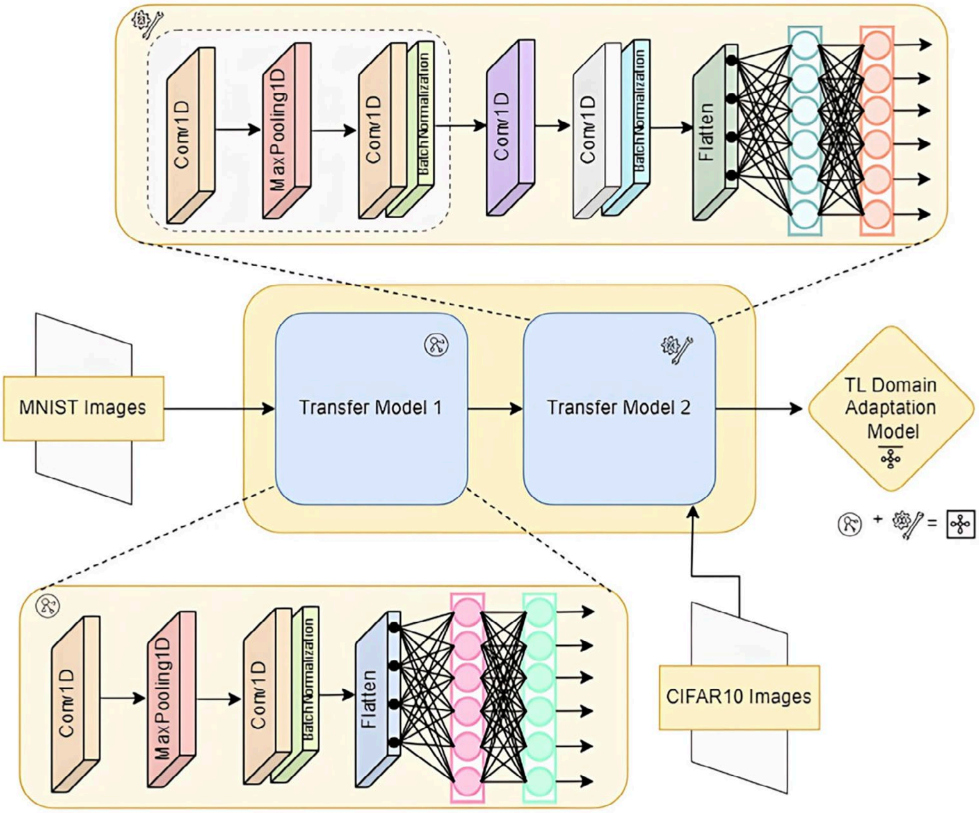

FIGURE 2 | TLDAM framework.

$$\psi_1 0 = \text{Dense}(10, \text{activation} = \text{softmax}) \tag{23}$$

which are trained using the CIFAR10 dataset and categorical cross-entropy as loss function defined as:

$$\zeta(train\_y, predict\_y) = -\sum_i train\_y_i \cdot \log\left(predict\_y_i\right) \tag{24}$$

Next, layers ψ_5, ψ_6 and ψ_7 are frozen and used as TLDAM model for future transfers and DL model constructions.

Figure 3 outlines the comprehensive TLDAM construction procedure. In summary, TL model 1 undergoes training using MNIST images. Subsequently, a selection of its layers is frozen and integrated with corresponding layers from TL model 2. This amalgamated TL model 2 is then subjected to training using CIFAR10 images, enhancing its overall generalisation capability. This meticulous training equips the TLDAM model to be seamlessly deployable across both centralised and federated scenarios, rendering it adaptable and versatile for diverse application contexts.

4.2 | FedAcc

In the conventional paradigm of weight aggregation, the potential influence of poorly performing models is often disregarded, resulting in suboptimal global models. These outliers can significantly undermine the efficacy of the aggregated model. To overcome this limitation, we introduce a novel approach termed FedAcc. By incorporating model accuracy as a pivotal criterion, FedAcc addresses the challenge of under-performing models. It dynamically adjusts model weights based on their respective accuracies, thus mitigating the impact of anomalies and enhancing the overall model robustness. The proposed FedAcc method effectively scales model weights according to accuracy prior to initiating the weight aggregation process. Consequently, the final set of aggregated weights is refined, leading to an improved global model that is more resilient to the influence of poorly performing models. Algorithm 1 presents the FL process used in the proposed framework and steps 4–10 indicate the FedAcc process. It takes into account only the accuracy of the models to determine their scaling factor sf and model their weights according to it.

5 | Experimental Evaluation

This section outlines the experimental setup and the obtained results. This section begins by detailing the experimental environment and dataset utilised. Subsequently, the scenario in which the experiments were conducted is described in detail. The section culminates with a comprehensive analysis of the achieved results, highlighting the performance and effectiveness of the proposed technique in comparison to existing methods.

5.1 | Experimental Setup

The experimental results were conducted on the GPU-enabled Asus Vivobook system which includes an Intel(R) Core(TM)

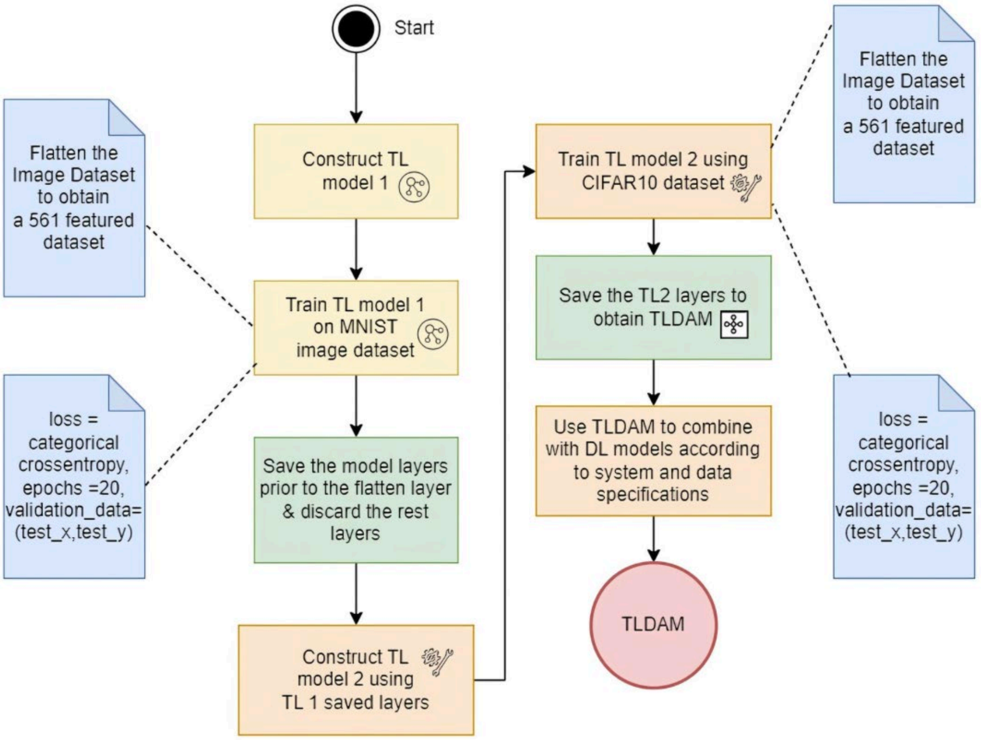
Start
Construct TL model 1
Train TL model 1 on MNIST image dataset
Save the model layers prior to the flatten layer & discard the rest layers
Construct TL model 2 using TL 1 saved layers
Train TL model 2 using CIFAR10 dataset
Save the TL2 layers to obtain TLDAM
Use TLDAM to combine with DL models according to system and data specifications
TLDAM
Flatten the Image Dataset to obtain a 561 featured dataset
loss = categorical crossentropy, epochs =20, validation_data= (test_x,test_y)
Flatten the Image Dataset to obtain a 561 featured dataset
loss = categorical crossentropy, epochs =20, validation_data= (test_x,test_y)

FIGURE 3 | TLDAM construction flow.

i5-9300H CPU running at a clock speed of 2.40 GHz. It is equipped with 8.00 GB of installed RAM, with 7.85 GB usable with a 64-bit operating system and an x64-based processor. The federated framework and DL models proposed were developed using TensorFlow and Keras, leveraging their powerful capabilities for building and training sophisticated models.

5.2 | Dataset Description, Experiment Design, and Performance Metrics

Experimental validation of our proposed approach is carried out using the UCI Human Activity Recognition (UCI-HAR) dataset, which is extensively utilised for activity recognition tasks. The dataset was gathered from 30 individuals, referred to as subjects, engaged in various activities whilst carrying a smartphone positioned at their waists. Data collection was facilitated through embedded sensors in the smartphone, specifically an accelerometer and a gyroscope. To ensure accurate labelling, the entire experiment was video recorded for manual annotation of the activities. The raw sensor data underwent pre-processing, where noise was minimised using filters, and the signals were segmented into fixed-width sliding windows of 2.56 s with a 50% overlap, resulting in 128 readings per window. This dataset was used by the proposed model in the process of FL where the sensor collected data of 30 individuals is divided between the clients in the process of FL.

The dataset consists of variety of activities such as walking, standing and other routine movements. It includes six distinct activities and a comprehensive range of sensor-derived features, making the UCI-HAR dataset a robust resource for developing and evaluating ML models in applications like wearable technology, health monitoring and activity tracking. The rich diversity of labelled activities and detailed sensor data positions it as an optimal benchmark for testing the efficacy of algorithms tailored for activity recognition and motion analysis.

Table 2 describes the class names for various class labels. The dataset is divided into 70-30 train test splits and further, the training data is divided between the clients for the process of FL. The results are compared based on the 10 clients and 30 communication rounds in the FL scenario. Moreover, to understand the efficacy of the proposed framework, it is also rigorously tested up to 20 clients as well.

To evaluate the proposed approach the metrics used for comparison are: Accuracy, Precision, Recall, F-score, Loss and time taken.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall (TPR)} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{TNR} = \frac{\text{TN}}{\text{TN} + \text{FP}}$$

$$\text{F-1 score} = \frac{2(\text{precision} \times \text{recall})}{\text{precision} + \text{recall}}$$

A true positive (TP) occurs when the model correctly identifies instances of the positive class, reflecting cases where the predicted

ALGORITHM 1 | Federated Framework.

```
Input: Clients $K$, Communication rounds ($\Gamma$)
Output: Federated FedAcc Framework
for $r$ in $\Gamma'$s:
  At client side
    for client $k$:
      history = $\tau_1^{(r)}$. fit($train\_X$, $train\_y$, validation_split = 0.15, verbose = 1)
      k. send$\left(\tau_1^{(r)}.\, localweights(), history\left['val\_accuracy'\right]\right)$
    end
  At server side
    if $r$ is 0:
      $sf\_list^{(r)} = \left[\frac{1}{K}\right]_{k=1}^{K}, moderation\_index\left(\varsigma^{(r)}\right) = 0.15$
      $val\_accuracy_{r-1} = val\_accuracy_r$
    else:
      for client $k$:
        if$\left(val\_accuracy_{r-1} \leq val\_accuracy_r: sf\_list[k]^{(r)} = sf\_list[k]^{(r)} + \left(sf\_list[k]^{(r)} \times \varsigma^{(r)}\right)\right)$
        if$\left(val\_accuracy_{r-1} \geq val\_accuracy_r: sf\_list[k]^{(r)} = sf\_list[k]^{(r)} - \left(sf\_list[k]^{(r)} \times \varsigma^{(r)}\right)\right)$
      end
  Tuning sf and weight scaling
  $sf\_list[k]^{(r)} = \frac{sf\_list[k]^{(r)}}{\sum_{j=1}^{K} sf\_list[j]^{(r)}}$
  for client $k$:
    $weight[k]^{(r)} = sf\_list[k]^{(r)} \times weight[k]^{(r)}$
  end
  $\omega_g^{(r)} = aggregate\left(weight[k]_{k=1}^{K}\right)$
  $\tau_g^{(r)}.\, set\_weights\left(\omega_g^{(r)}\right)$
  server. distribute$\left(\omega_g^{(r)}\right)$
  At client side
  $\tau_1^{(r)}.\, set\_weights\left(\omega_g^{(r)}\right)$
  $r = r + 1$
end
```

TABLE 2 | Class encoding and description.

Class label	Class name	Volume	Percentage
Class 1	Laying	136,865	18.3%
Class 2	Sitting	126,677	16.9%
Class 3	Standing	138,105	18.5%
Class 4	Walking	122,091	16.3%
Class 5	Stair up	116,707	15.6%
Class 6	Stair down	107,961	14.4%

outcome aligns with the actual positive outcome. Conversely, a true negative (TN) denotes instances where the model accurately identifies the negative class, reflecting correct predictions of absence or non-occurrence. On the other hand, false positives (FP) arise when the model incorrectly identifies instances as positive when they are actually negative, constituting errors of Type I. False negatives (FN) occur when the model fails to identify instances of the positive class, marking errors of Type II, as it predicts a negative outcome when the actual outcome is positive.

5.3 | Proposed Solution Scenario Discussion

The proposed solution for analysing the UCI-HAR dataset introduces a hybrid paradigm that combines CNNs and MLP with the innovative TLDAM in association with FL FedAcc. This approach aims to extract meaningful insights from the intricate sensor data within the dataset. The utilisation of CNNs facilitates robust feature extraction from the complex sensor inputs, enabling the model to capture relevant patterns and nuances. On the other hand, TLDAM's streamlined architecture stands as a testament to its efficiency in adapting to domain shifts and complexities. FedAcc additionally enables clients with greater performance to have a bigger contribution factor.

By integrating CNN, MLP and TLDAM, the proposed solution capitalises on their respective strengths. CNNs excel in processing visual data, which is pertinent given the nature of sensor inputs in the UCI-HAR dataset. Meanwhile, TLDAM's proficiency in domain adaptation ensures that the model learns and generalises effectively even in the presence of variations and challenges specific to the healthcare context.

This amalgamated approach holds the potential to enhance the accuracy and depth of analysis of the UCI-HAR dataset by considering the valid participation of each client. The synergy between CNN, MLP and TLDAM aligns with the intricacies of the dataset, catering to the unique intricacies of human activity recognition and motion analysis. By leveraging these advanced techniques, the proposed solution aspires to uncover deeper insights, optimise model performance using FedAcc and contribute to the refinement of healthcare applications through robust analysis of the UCI-HAR dataset.

5.4 | Results Analysis

In this section, a comprehensive analysis of the results is presented, covering various exhaustive phases. These analyses serve to assess the effectiveness and performance of the proposed framework across multiple scenarios. The examination of the framework's outcomes from different perspectives contributes to a holistic understanding of its capabilities and its adaptability to diverse contexts.

5.4.1 | Performance of Individual Client in Proposed Framework

Experimental results display the performance of each client participating in the FL process. Each client trains the collaborated TLDAM, CNN and MLP model and sends their model gradients to the global server along with their validation accuracy. The global server in turn aggregates the weights based on their accuracies as described in Algorithm 1.

Table 3 presents a detailed overview of individual client performance over 30 communication rounds. The study involves up to 20 clients used in the proposed framework and assesses various metrics mentioned above. Each client's performance is evaluated, providing valuable insights into the behaviour of the proposed framework across multiple rounds of communication.

The accuracy values for each client range from 96.73% to 99.73%, highlighting the clients' diverse proficiency in making accurate predictions. Clients 2, 3, 5, 9, 14, 15 and 17 consistently achieve accuracy levels above 99%, showcasing their proficiency in model training. On the other hand, clients like 6 and 19 exhibit slightly lower accuracies, suggesting potential areas for improvement in their training methodologies.

The loss values reflect the extent of discrepancy between predictions and actual values, with values varying from 0.1797 to 0.3214. Notably, F-score values range from 88.1982% to 93.485% for different clients.

TABLE 3 | Individual clients performance for 30 communication rounds.

Client	Accuracy	Loss	F-score	Precision	Recall	Time (ms)
Client 1	99.18	0.2990	88.1982	89.9983	88.2932	31
Client 2	99.46	0.1803	93.455	93.457	93.485	32
Client 3	99.46	0.1797	93.373	93.435	93.417	32
Client 4	98.64	0.1857	93.287	93.366	93.315	30
Client 5	99.46	0.222	92.462	92.727	92.501	35
Client 6	96.73	0.3214	88.626	91.039	88.734	35
Client 7	98.64	0.2272	92.234	92.626	92.297	34
Client 8	97.82	0.2383	91.562	92.654	91.72	34
Client 9	99.46	0.2094	92.61	93.263	92.637	32
Client 10	99.18	0.1838	93.351	93.375	93.381	33
Client 11	99.18	0.186	92.775	92.991	92.84	32
Client 12	98.64	0.2684	90.494	91.461	90.702	31
Client 13	98.64	0.2412	92.234	93.104	92.331	30
Client 14	99.46	0.1894	93.476	93.624	93.519	31
Client 15	99.73	0.2248	91.473	92.079	91.517	37
Client 16	98.91	0.1908	93.266	93.526	93.315	35
Client 17	99.73	0.1904	93.485	93.515	93.485	34
Client 18	99.46	0.2001	93.057	93.259	93.078	33
Client 19	98.09	0.1926	92.364	92.546	92.365	32
Client 20	99.18	0.2593	91.016	92.091	91.211	31

The time taken per step, showcases the training time for each client in milliseconds for each training step, vary from 30 to 37 ms. While the differences in training times are relatively marginal, they provide insights into the computational efficiency of each client's device during the FL process.

The diverse range of values across accuracy, loss, F-score and training time offer a multifaceted understanding of client behaviour, enabling us to fine-tune training strategies, address challenges and optimise the overall efficacy of the FL system. The performance trends observed across these metrics over 30 rounds offer insights into convergence trends, potential improvements and the stability of the model across different communication iterations.

5.4.2 | Multi-Class Comparison of Proposed Work With Varying Clients

This section entails the multi-class proficiency of the proposed work with a varying number of clients. It describes the efficiency of each class present in the UCI-HAR dataset.

A detailed breakdown of results for multi-class classification across different scenarios is shown in Table 4. The evaluation is carried out for varying numbers of clients, with each class displaying distinct performance characteristics.

Across different scenarios involving varying numbers of clients, consistent trends emerge in precision, recall and F-score values. For instance, in the case of two clients, precision ranges from 0.90 to 1.00, with Class 6 achieving perfect precision, whilst recall values span from 0.88 to 1.00, and F-scores between 0.91 and 1.00 indicate a balance between precision and recall. These results underscore the approach's scalability and robustness across different client numbers.

5.4.3 | Comparison of the Proposed Framework for Various Communication Rounds With Different Clients

This section provides insights into the effect of communication rounds on the global FL system. Additionally, it lays the overall accuracy of the global model built in the FL process.

A comprehensive analysis of the effect of varying communication rounds on different numbers of clients in a multi-class classification setting is shown in Table 5. The table is structured to highlight the performance metrics for different scenarios, combining the factors of the number of clients and the communication rounds.

In the scenario say, involving two clients, accuracy ranges from 92.9420% to 95.1140%, indicating models' proficiency in accurate predictions across communication rounds. Corresponding loss values decrease from 1.1306 to 1.0966, suggesting improved model convergence. F-score values span 92.9379%–95.0953%, highlighting the balance between precision and recall. Precision and recall remain consistent, reflecting stable predictions. As communication rounds increase, performance generally improves, demonstrating the models' learning capacity.

TABLE 4 | Multi-class classification results.

Number of clients	Class	Precision	Recall	F-score
2	Class 1	0.95	0.98	0.97
	Class 2	0.94	0.96	0.95
	Class 3	0.96	0.9	0.93
	Class 4	0.95	0.88	0.91
	Class 5	0.9	0.96	0.93
	Class 6	1	1	1
5	Class 1	0.96	0.98	0.97
	Class 2	0.92	0.94	0.93
	Class 3	0.95	0.89	0.92
	Class 4	0.95	0.87	0.91
	Class 5	0.90	0.96	0.93
	Class 6	0.99	1.00	1.00
10	Class 1	0.98	0.96	0.97
	Class 2	0.92	0.96	0.94
	Class 3	0.92	0.91	0.91
	Class 4	0.93	0.88	0.91
	Class 5	0.92	0.94	0.93
	Class 6	0.98	1.00	0.99
15	Class 1	0.92	0.99	0.95
	Class 2	0.92	0.91	0.92
	Class 3	0.94	0.87	0.90
	Class 4	0.95	0.86	0.90
	Class 5	0.90	0.96	0.93
	Class 6	0.99	1.00	0.99
20	Class 1	0.95	0.97	0.96
	Class 2	0.92	0.94	0.93
	Class 3	0.92	0.88	0.90
	Class 4	0.94	0.87	0.90
	Class 5	0.90	0.95	0.92
	Class 6	0.99	1.00	0.99

Consistently across scenarios involving 5, 10, 15 and 20 clients and 30 communication rounds, a notable trend unfolds the metrics of accuracy, loss, F-score, precision and recall all demonstrate a marginal dip with each increase in the client. Despite this slight decline, the overarching trend underscores the resilience and effectiveness of the proposed framework. The robustness of the system is evident, as it manages to enhance performance metrics despite encountering challenges associated with scaling up to larger client populations. This trend highlights the adaptability and potency of the framework in accommodating diverse scenarios and scaling gracefully with increasing client numbers.

TABLE 5 | Effect of communication rounds on different number of clients.

Number of clients	Communication rounds	Accuracy	Loss	F-score	Precision	Recall
2	2	92.9420	1.1306	92.9379	93.0710	92.9420
	5	94.0960	1.1102	94.0485	94.4413	94.0957
	10	94.6390	1.1036	94.6084	94.8043	94.6386
	15	95.1140	1.0966	95.0953	95.1644	95.1137
	20	94.8420	1.0977	94.8173	94.9346	94.8422
	25	94.9440	1.0965	94.9231	95.0062	94.9444
	30	94.8420	1.0965	94.8189	94.9202	94.8422
5	2	91.3470	1.1503	91.2811	91.3785	91.3471
	5	93.7900	1.1166	93.7413	93.8722	93.7903
	10	94.0620	1.1087	94.0142	94.2622	94.0618
	15	94.2990	1.1060	94.2629	94.4265	94.2993
	20	94.2650	1.1049	94.2237	94.3943	94.2654
	25	94.1970	1.1038	94.1602	94.2631	94.1975
	30	94.3330	1.1021	94.3016	94.4008	94.3332
10	2	87.4790	1.1907	86.9712	88.9526	87.4788
	5	92.0260	1.1464	91.9334	92.3031	92.0258
	10	93.4170	1.1233	93.3819	93.4517	93.4170
	15	94.164	1.1129	94.125	94.211	94.164
	20	93.078	1.1174	93.015	93.244	93.078
	25	93.926	1.1101	93.888	93.932	93.926
	30	94.2990	1.1054	94.2820	94.3058	94.2993
15	2	82.3890	1.3556	82.1664	83.4642	82.3889
	5	87.75	1.1881	87.345	89.476	87.75
	10	92.094	1.1396	91.991	92.438	92.094
	15	92.908	1.273	92.864	92.937	92.908
	20	93.112	1.1209	93.073	93.125	93.112
	25	93.451	1.1175	93.41	93.473	93.451
	30	93.417	1.1173	93.367	93.495	93.417
20	2	85.5450	1.3081	85.0982	86.3269	85.5446
	5	89.99	1.1742	89.809	90.482	89.99
	10	91.11	1.1533	90.965	91.557	91.11
	15	92.637	1.1364	92.576	92.841	92.637
	20	93.519	1.1275	93.479	93.638	93.519
	25	93.756	1.1237	93.715	93.949	93.756
	30	93.655	1.1192	93.618	93.661	93.655

5.4.4 | Comparison of Proposed With ML and DL Techniques in Centralised Approach

This section tests the robustness of the proposed work with the centralised ML and DL techniques.

Figure 4 showcases a comparison of different techniques based on their performance metrics in a classification task. It comprises five techniques: Logistic Regression (LR), Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Random Forest (RF) and the proposed technique. The performance of these techniques is evaluated based on key metrics.

Overall, Figure 4 provides a clear comparison of different classification techniques based on their performance metrics, highlighting the strengths and weaknesses of each method. The proposed technique performs competitively with other methods, showing promising results in the evaluated metrics. Although it is seen that the proposed framework achieves lower performance as compared to centralised settings, it accounts for the

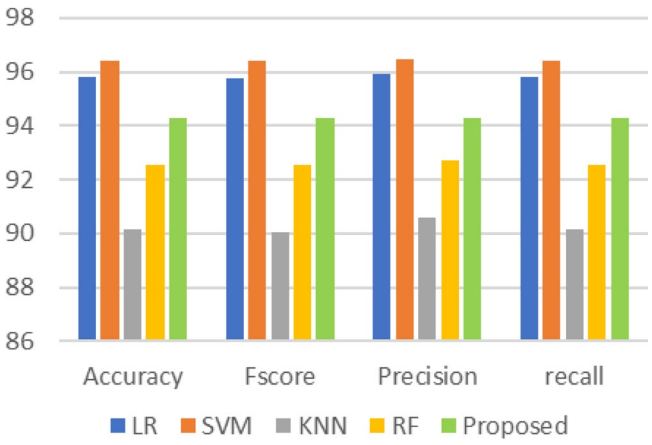

FIGURE 4 | Comparison of proposed with ML techniques.

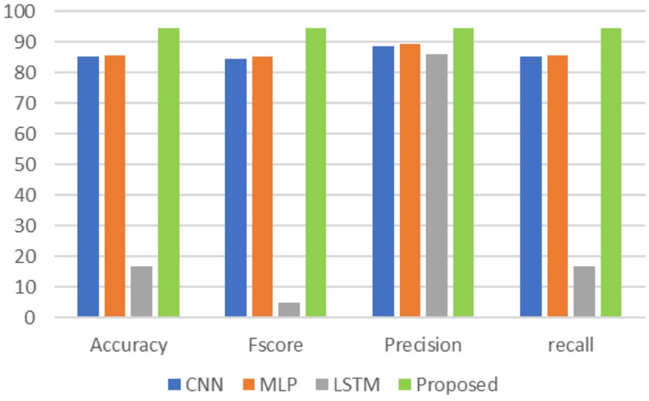

FIGURE 5 | Comparison of proposed with DL techniques.

fact that the centralised ML settings fail to resolve the security and privacy issues of the clients which limits this centralised approach to a very small scale.

Figure 5 provided is a comparison of different DL techniques in terms of their performance metrics. The techniques being compared are CNN, MLP, LSTM and the proposed approach.

The proposed technique achieves an accuracy of 94.2990%, an F-score of 94.2820%, a precision of 94.3058% and a recall of 94.2993%. These values suggest that the proposed approach performs better across all metrics compared to the other ML techniques, making it a promising choice for the given task. While the centralised DL settings in the experiment exhibit superior performance metrics compared to the proposed work, it is essential to recognise that these centralised approaches often come at the expense of security and computational efficiency. The proposed work, on the other hand, prioritises security and computational efficacy by utilising FL. This highlights the importance of striking a balance between performance and security considerations.

5.4.5 | Comparison With Other Federated Techniques

We compared the efficacy of FedAcc over existing FL techniques. This section describes the power of FedAcc over other techniques in federated scenarios with 10 clients for 30 communication rounds.

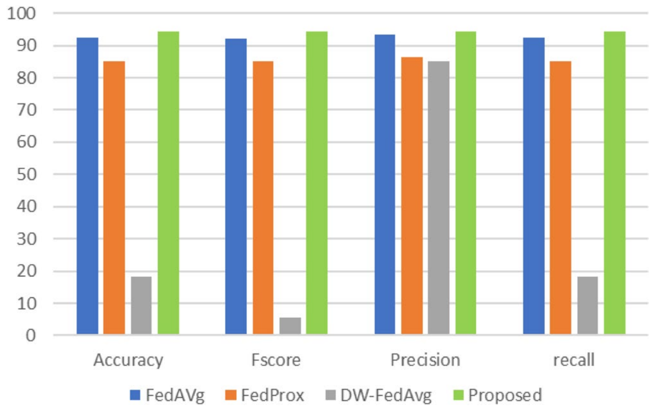

FIGURE 6 | Comparison with other federated techniques.

Figure 6 presented is a comparison of different FL techniques and the proposed approach based on their performance metrics. The techniques being compared are Federated Averaging (FedAvg), Federated Proximal (FedProx) (Zhang et al. 2022), Dynamic Weighted Federated Averaging (DW-FedAvg) (Chaudhuri, Nandi, and Pradhan 2023) and the proposed framework which uses FedAcc.

It is evident that the proposed method outperforms the other techniques in terms of accuracy, F-score, precision and recall. The proposed technique achieves an accuracy of 94.2990%, an F-score of 94.2820%, a precision of 94.3058% and a recall of 94.2993%. These values indicate that the proposed approach performs significantly better across all metrics compared to the other FL techniques evaluated, demonstrating its potential effectiveness in addressing the challenges of FL scenarios.

6 | Conclusion and Future Work

The proposed work has delved into the intricacies of TL, FL and their applications across various domains. We explored the challenges posed by domain shifts, non-IID data and scalability issues in existing TL methods, and introduced the innovative TLDAM as a potential solution. The FL framework's advantages in preserving data privacy and promoting computational efficiency were also underscored, achieving the client's accuracy of 99.73% on an average and high precision, recall and F-score values in multiclass classification. Through meticulous experimental setups, we witnessed the efficacy of the proposed techniques in comparison to traditional methods in terms of accuracy (94.2990%), F-score (94.2820%), precision (94.3058%) and recall (94.2993%). Future work focuses on improving the TLDAM model's adaptability and training it for TL on domain-specific healthcare datasets to ensure its applicability and effectiveness in real-world medical settings. Additionally, exploring advanced communication strategies in FL and devising techniques for handling heterogeneous data distribution amongst clients remain promising areas for further research.

Acknowledgements

The research presented emanated from the European Union's Horizon 2020 programme for research and innovation, which provided funding under Grant Number 847577 (SMART 4.0 Marie SkÅ‚odowska-Curie

Actions COFUND), and also by a grant from Science Foundation Ireland under Grant Number SFI/12/RC/3918 and also in part supported by Taighde Éireann - Research Ireland under grants 12/RC/2289-P2 (Insight) and 21/FFP-A/9174 (SustAIn). In order to promote open access, the author has chosen to apply a CC BY public copyright licence to any version of the Author Accepted Manuscript that results from this submission.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

Alkhdour, T., M. A. Almaiah, A. Ali, A. Lutfi, M. Alrawad, and T. Tin. 2024. "Revolutionizing Healthcare: Unleashing Blockchain Brilliance Through Fuzzy Logic Authentication." *Journal of Theoretical and Applied Information Technology* 102, no. 4: 29.

Arivazhagan, M. G., V. Aggarwal, A. K. Singh, and S. Choudhary. 2019. "Federated Learning With Personalization Layers." *arXiv Preprint arXiv:1912.00818*.

Borgia, E. 2014. "The Internet of Things Vision: Key Features, Applications and Open Issues." *Computer Communications* 54: 1–31.

Chaudhuri, A., A. Nandi, and B. Pradhan. 2023. "A Dynamic Weighted Federated Learning for Android Malware Classification." In *Soft Computing: Theories and Applications*, 147–159. Singapore: Springer.

Chen, Y., X. Qin, J. Wang, C. Yu, and W. Gao. 2020. "FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare." *IEEE Intelligent Systems* 35, no. 4: 83–93.

Choi, E., C. Xiao, W. Stewart, and J. Sun. 2018. "MiME: Multilevel Medical Embedding of Electronic Health Records for Predictive Healthcare." In *NIPS'18: Proceedings of the 32nd International Conference on Neural Information Processing Systems*, 4552–4562.

Dinh, C. T., N. Tran, and J. Nguyen. 2020. "Personalized Federated Learning With Moreau Envelopes." *Advances in Neural Information Processing Systems* 33: 21394–21405.

Du, M., F. Li, G. Zheng, and V. Srikumar. 2017. "DeepLog: Anomaly Detection and Diagnosis From System Logs Through Deep Learning." In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1285–1298. New York, NY, USA: Association for Computing Machinery.

El-Sherif, D. M., M. Abouzid, M. T. Elzarif, A. A. Ahmed, A. Albakri, and M. M. Alshehri. 2022. "Telehealth and Artificial Intelligence Insights Into Healthcare During the COVID-19 Pandemic." *Healthcare (Basel)* 10: 385.

Ferrag, M. A., O. Friha, D. Hamouda, L. Maglaras, and H. Janicke. 2022. "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning." *IEEE Access* 10: 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809.

Gupta, M., S. Tanwar, S. Bharany, et al. 2024. "Revolutionizing Healthcare by Unleashing the Power of Machine Learning in Diagnosis and Treatment." *International Journal of Advanced Computer Science and Applications (IJACSA)* 15, no. 3: 1111–1119.

Haddad, T. A., D. Hedjazi, and S. Aouag. 2022. "A Deep Reinforcement Learning-Based Cooperative Approach for Multi-Intersection Traffic Signal Control." *Engineering Applications of Artificial Intelligence* 114: 105019.

Houssein, E. H., and A. Sayed. 2023. "Boosted Federated Learning Based on Improved Particle Swarm Optimization for Healthcare IoT Devices." *Computers in Biology and Medicine* 163: 107195.

Issa, W., N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari. 2023. "Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey." *ACM Computing Surveys* 55, no. 9: 1–43.

Jiménez-Sánchez, A., M. Tardy, M. A. G. Ballester, D. Mateus, and G. Piella. 2023. "Memory-Aware Curriculum Federated Learning for Breast Cancer Classification." *Computer Methods and Programs in Biomedicine* 229: 107318.

Khan, M., F. G. Glavin, and M. Nickles. 2023. "Federated Learning as a Privacy Solution – An Overview." *Procedia Computer Science* 217: 316–325.

Khodak, M., M. F. F. Balcan, and A. S. Talwalkar. 2019. "Adaptive Gradient-Based Meta-Learning Methods." In *33rd Conference on Neural Information Processing Systems (NeurIPS 2019)*, 1–12.

Kishor, A., and C. Chakraborty. 2022. "Artificial Intelligence and Internet of Things Based Healthcare 4.0 Monitoring System." *Wireless Personal Communications* 127, no. 2: 1615–1631.

Li, J., Y. Meng, L. Ma, et al. 2021. "A Federated Learning Based Privacy-Preserving Smart Healthcare System." *IEEE Transactions on Industrial Informatics* 18, no. 3: 2021–2031.

Lu, W., J. Wang, Y. Chen, S. J. Pan, C. Hu, and X. Qin. 2022a. "Semantic-Discriminative Mixup for Generalizable Sensor-Based Cross-Domain Activity Recognition." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, no. 2: 1–19.

Lu, W., J. Wang, Y. Chen, et al. 2022b. "Personalized Federated Learning With Adaptive Batchnorm for Healthcare." *IEEE Transactions on Big Data* 10, no. 6: 915–925. https://doi.org/10.1109/TBDATA.2022.3177197.

Madakam, S., R. Ramaswamy, and S. Tripathi. 2015. "Internet of Things (IoT): A Literature Review." *Journal of Computer and Communications* 3, no. 5: 164.

Manickam, P., S. A. Mariappan, S. M. Murugesan, et al. 2022. "Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare." *Biosensors* 12, no. 8: 562.

McMahan, B., E. Moore, D. Ramage, S. Hampson, and y B A. Arcas. 2017. "Communication-Efficient Learning of Deep Networks From Decentralized Data." In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017*, 1273–1282.

Namalomba, E., H. Feihu, and H. Shi. 2022. "Agent Based Simulation of Centralized Electricity Transaction Market Using Bi-Level and Q-Learning Algorithm Approach." *International Journal of Electrical Power & Energy Systems* 134: 107415.

Nguyen, D. C., Q. V. Pham, P. N. Pathirana, et al. 2022. "Federated Learning for Smart Healthcare: A Survey." *ACM Computing Surveys (CSUR)* 55, no. 3: 1–37.

Puri, V., A. Kataria, and V. Sharma. 2024. "Artificial Intelligence-Powered Decentralized Framework for Internet of Things in Healthcare 4.0." *Transactions on Emerging Telecommunications Technologies* 35, no. 4: e4245.

Singh, S., S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon. 2022. "A Framework for Privacy-Preservation of IoT Healthcare Data Using Federated Learning and Blockchain Technology." *Future Generation Computer Systems* 129: 380–388.

Smith, V., C. K. Chiang, M. Sanjabi, and A. S. Talwalkar. 2017. "Federated Multi-Task Learning" In *NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems*, 4427–4437.

Sun, W., J. Liu, and Y. Yue. 2019. "AI-Enhanced Offloading in Edge Computing: When Machine Learning Meets Industrial IoT." *IEEE Network* 33, no. 5: 68–74.

Tam, P., R. Corrado, C. Eang, and S. Kim. 2023. "Applicability of Deep Reinforcement Learning for Efficient Federated Learning in Massive IoT Communications." *Applied Sciences* 13, no. 5: 3083.

Unal, A. B., M. Akgun, and N. Pfeifer. 2021. "ESCAPED: Efficient Secure and Private Dot Product Framework for Kernel-Based Machine Learning Algorithms With Applications in Healthcare." *Proceedings of the AAAI Conference on Artificial Intelligence* 35, no. 11: 9988–9996.

Verma, P., J. G. Breslin, and D. O'Shea. 2022. "FLDID: Federated Learning Enabled Deep Intrusion Detection in Smart Manufacturing Industries." *Sensors* 22, no. 22: 8974.

Verma, P., J. G. Breslin, and D. O'Shea. 2023. "PerCFed: An Effective Personalized Clustered Federated Learning Mechanism to Handle Non-IID Challenges for Industry 4.0." In *2023 IEEE 12th International Conference on Cloud Networking (CloudNet)*, 299–306.

Verma, P., J. G. Breslin, D. O'Shea, and R. Pateriya. 2022. "A Stacked Ensemble Method With Adaptive Attribute Selection to Detect DDoS Attack in Cloud-Assisted WBAN." In *International Conference on Machine Learning, Image Processing, Network Security and Data Sciences*, 329–344. Cham, Switzerland: Springer Nature Switzerland.

Xiong, J., R. Bi, M. Zhao, J. Guo, and Q. Yang. 2020. "Edge-Assisted Privacy-Preserving Raw Data Sharing Framework for Connected Autonomous Vehicles." *IEEE Wireless Communications* 27, no. 3: 24–30.

Xiong, Z., Z. Cai, D. Takabi, and W. Li. 2021. "Privacy Threat and Defense for Federated Learning With Non-IID Data in AIoT." *IEEE Transactions on Industrial Informatics* 18, no. 2: 1310–1321.

Yeganeh, Y., A. Farshad, N. Navab, and S. Albarqouni. 2020. "Inverse Distance Aggregation for Federated Learning With Non-IID Data." In *Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning. DART DCL 2020*, 150–159. Lima, Peru: Springer.

Zhang, D. Y., Z. Kou, and D. Wang. 2021. "Fedsens: A Federated Learning Approach for Smart Health Sensing With Class Imbalance in Resource Constrained Edge Computing." In *IEEE INFOCOM 2021 – IEEE Conference on Computer Communications*, 1–10.

Zhang, J., Z. Li, B. Li, et al. 2022. "Federated Learning With Label Distribution Skew via Logits Calibration." In *Proceedings of the 39th International Conference on Machine Learning*, PMLR 162, 26311–26329.

Zhou, X., W. Liang, J. Ma, Z. Yan, I. Kevin, and K. Wang. 2022. "2D Federated Learning for Personalized Human Activity Recognition in Cyber-Physical-Social Systems." *IEEE Transactions on Network Science and Engineering* 9, no. 6: 3934–3944.

Zhu, H., J. Xu, S. Liu, and Y. Jin. 2021. "Federated Learning on Non-IID Data: A Survey." *Neurocomputing* 465: 371–390.

Zhu, Z., J. Hong, and J. Zhou. 2021. "Data-Free Knowledge Distillation for Heterogeneous Federated Learning." In *Proceedings of the 38th International Conference on Machine Learning*, PMLR 139, 12878–12889.