Austin Journal of Business Administration and Management

Open Access

Austin Publishing Group

Review Article

Unlocking the Power of Federated and Transfer Learning: A Unified Architecture for Enhanced Privacy and Scalability in AI

Venkatesh Upadrista[1*]; Rahil Burhani[2]

[1]Research Scholar, Glasgow Caledonian University, Scotland

[2]Former CIO at Essar Oil, Essar Energy, Executive Director of Innovations at Trinity ESG Consulting Ltd., UK

[*]**Corresponding author: Venkatesh Upadrista**
Research Scholar, Glasgow Caledonian University, Glasgow G4 0BA, Scotland.
Tel: +44(0)7424991399
Email: vupadr200@caledonian.ac.uk

Received: September 27, 2024
Accepted: October 17, 2024
Published: October 24, 2024

Abstract

Federated Learning and Transfer Learning are two distinct machine learning methodologies that have typically been applied independently. However, combining these approaches offers the potential to deliver significant value across various industries. This paper systematically reviews existing literature on both technologies and introduces a novel framework that integrates Federated Learning and Transfer Learning to improve machine learning model performance. The proposed framework can be utilized in a range of applications, including healthcare (for detecting heart attacks, cancer, and strokes), retail (for predicting customer churn), and industrial sectors like Power Grids, Oil & Gas and Manufacturing (for identifying equipment failures, grid loads etc). By merging these technologies, this framework enhances model accuracy and scalability while ensuring data privacy in distributed environments.

Keywords: FL; TL; Architecture; Federated TL

Introduction

Federated Learning (FL) and Transfer Learning (TL) are often confused as being the same concept, although they have distinct differences despite some similarities in reusing knowledge across tasks. TL involves using a pre-trained model (typically trained on a large dataset) and fine-tuning or adapting it to a new, related task or domain [1-3]. This allows the model to leverage knowledge gained from a source task to improve performance on a target task, especially when the target task has limited data. For example, a model trained on ImageNet (a large dataset of images) can be fine-tuned to classify medical images. Federated TL (FTL) is a combination of FL and TL. In FL, models are trained across multiple decentralized devices or servers, with data remaining on the local devices instead of being shared or centralized [1,4,5]. In FTL, the goal is to allow models at different locations or with different datasets to learn collaboratively without sharing data. This approach is particularly useful when datasets from different organizations (such as companies or institutions) are related but cannot be shared due to privacy concerns or regulatory restrictions. For example, different insurance companies can contribute to a shared model without sharing proprietary data but can still benefit from the insights across their datasets. The advantage of using these two technologies together is that it brings the best of both approaches. A model trained using TL can be further enhanced by FL, enabling it to benefit from diverse, distributed datasets without requiring direct data sharing. This approach leverages pre-trained knowledge from a source domain while simultaneously training the model across multiple organizations or devices in a privacy-preserving manner, leading to improvements in accuracy, generalization, and applicability in scenarios with sensitive or proprietary data. Imagine a model pre-trained on a specific dataset within an industry, which is then fine-tuned to be organization specific. FL can further amplify this learning by allowing the model to train on data from multiple organizations, resulting in a highly accurate model which is one of the most innovative techniques in machine learning. In healthcare, privacy is of utmost importance due to regulations like HIPAA and GDPR [1,4]. FL allows hospitals and medical institutions to collaboratively train models on patient data without sharing sensitive information, ensuring privacy [1]. TL can be used to apply pre-trained models (such as those trained on large, public medical datasets) to specific tasks, like diagnosing rare diseas-

Citation: Upadrista V, Burhani R. Unlocking the Power of Federated and Transfer Learning: A Unified Architecture for Enhanced Privacy and Scalability in AI. Austin J Bus Adm Manage. 2024; 8(3): 1077.

es or analyzing medical imaging data [4]. For instance, a pre-trained model for general image recognition (TL) can be fine-tuned to recognize brain tumors in MRI scans using FL across hospitals [1]. Each hospital can adapt the model using its local data without sharing patient information, resulting in a high-performance model while maintaining data privacy.

In the insurance industry, companies have vast amounts of private data, such as claims data and customer profiles. FL allows different branches or companies to collaboratively train models to detect fraudulent claims or assess risks without exposing sensitive customer information [3]. TL helps these companies quickly adapt models pre-trained on general insurance data to specific local markets or types of insurance products. For example, a global insurance company can use a fraud detection model trained on generic fraud cases (TL) and refine it for local regions using FL. Local branches can use their own claims data to update the model without sharing sensitive customer information with other branches or regions.

In the banking sector, privacy and security are critical due to regulations like PSD2. FL enables different banks to collaboratively train models on transaction data to detect fraud or assess credit risk, without sharing actual customer data [6,7]. TL allows pre-trained models from one bank to be adapted to new regions or product offerings [6,7]. For instance, a pre-trained credit scoring model (TL) can be shared and adapted across different banks or regions. Using FL, banks can refine the model using their local customer data, ensuring the model reflects the credit behavior of their clients while maintaining data privacy compliance.

In the retail sector, FL helps companies personalize product recommendations by training models across multiple retail outlets or online platforms without sharing customer data [8]. TL allows retailers to use pre-trained models for general customer behavior and adapt them to specific demographics or regions. For example, a pre-trained model for general customer purchasing behavior (TL) can be fine-tuned for specific stores or regions using FL. Each retail store can locally train the model on its customer data to create personalized recommendations without sharing purchase histories with other stores or a central server.

Several pre-trained models are available from leading cloud providers. For healthcare, examples include Amazon HealthLake [9], which uses machine learning to extract meaningful information from healthcare data, and Google Cloud's AutoML [10], which provides models for medical image classification and natural language processing for clinical text. In retail, Amazon Personalize [11] offers individualized product recommendations, while Google Cloud's Recommendations AI [10] provides tailored shopping recommendations for e-commerce platforms. In financial services, Amazon Fraud Detector is specialized in identifying fraudulent activities based on transaction data, while Google Cloud offers tools for building fraud detection systems. These models can be used as the initial TL models, after which specific FL can be applied to tailor them to individual organizations.

In conclusion, combining FL and TL offers significant potential across industries by integrating the privacy-preserving capabilities of FL with the knowledge reuse of TL. This hybrid approach allows models to be collaboratively trained on decentralized datasets without compromising data privacy, while also adapting pre-trained models to specific tasks in different domains. The integration not only enhances the accuracy and generalization of models but also ensures compliance with regulatory standards, making it particularly useful in sensitive sectors such as healthcare, insurance, finance, and retail. As industries continue to evolve, this combined approach will play a pivotal role in building scalable, secure, and efficient machine learning systems.

Literature Review

FL and TL have been extensively utilized across industries to enhance privacy, boost model efficiency, and adapt models to new tasks. FL enables decentralized model training by distributing computation across multiple devices or institutions, ensuring that sensitive data remains localized. TL, meanwhile, facilitates the use of pre-trained models to transfer knowledge from one domain to another, improving performance and reducing the reliance on large datasets for new tasks. Through a comprehensive literature review, we explored various applications of FL and TL across industries like healthcare, autonomous systems, IoT, smart manufacturing, and more. Studies indicate that integrating FL and TL improves accuracy, reduces training time, and enhances privacy, making them vital tools for modern AI applications.

Literature Review

Authors in [1] integrated FL and TL for brain tumor classification using MRI images. FL was used to decentralize model training across multiple institutions while ensuring data privacy. TL, using a pre-trained VGG16 CNN, improved the model's performance by leveraging knowledge from large datasets. The model achieved high accuracy, precision, and recall rates, with an overall accuracy of 98%. This method outperformed traditional approaches, maintaining data privacy and ensuring accurate classification of brain tumors.

As part of their work in [2], the authors developed a method called PrivateKT, integrating FL with differential privacy. FL allowed the decentralized training of models, while knowledge was transferred via small, carefully selected public datasets to ensure privacy. TL leveraged these public datasets to enhance model training efficiency without accessing sensitive data. Experimental results demonstrated that PrivateKT reduced performance degradation in privacy-constrained environments, achieving up to 84% of the performance of centralized learning models, even under strict privacy measures. The model performed well on tasks like digit classification, disease prediction, and pneumonia detection.

As part of [3], the authors reviewed the integration of FL and TL. FL was utilized for decentralized model training, ensuring privacy by preventing data sharing across participants. TL enabled knowledge transfer between participants, minimizing data distribution disparities and enhancing model utility. The authors demonstrated that combining these methods mitigated challenges like data and system heterogeneity. Experimental results showcased improved performance in scenarios involving multiple domains and incremental data.

As part of their research, the authors in [4] employed FL combined with TL to enhance privacy-preserving breast cancer classification. FL enabled collaborative model training across multiple medical centers while ensuring data privacy. TL was integrated with a pre-trained ResNet model to fine-tune breast cancer classification tasks. The model achieved a classification accuracy of 98.8%, with an F1-score of 98.2% and a computational time of 12.22 seconds. This approach demonstrated im-

proved generalization across diverse datasets without compromising data privacy.

As part of their research [5], the authors employed federated TL to enhance flow-based traffic classification. FL was used to collaboratively train models across different silos while preserving data privacy. TL allowed the transfer of knowledge from a source model to a target model, improving both accuracy and training efficiency. The source model was trained for application-level traffic classification, while the target model was trained for VPN/non-VPN identification. The target model outperformed the baseline model in validation accuracy (0.90 vs. 0.85) and training time.

Authors in [12] proposed FTLIoT, a Federated TL (FTL) framework to enhance security in IoT networks. FL was employed to allow multiple IoT devices to collaboratively train intrusion detection models without sharing raw data, ensuring privacy. TL enabled the model to adapt to new tasks quickly by leveraging previously trained models. Experimental results showed that using CNN and DNN algorithms led to an accuracy improvement of 1.44% and 5.55%, respectively. The model also reduced training time by 36.11% for CNN and 38.62% for DNN.

Authors in [13] proposed a blockchain-enabled Federated TL (FTL) schema for autonomous vehicular systems to reduce latency and enhance security. The FTL framework enabled distributed learning across edge devices, minimizing data transfer and improving model accuracy. Blockchain integration ensured privacy and security in the communication process. The experimental results demonstrated better scalability, reduced latency, and improved data rate efficiency in vehicular networks. The proposed model outperformed traditional methods, showing a higher reliability in autonomous vehicular environments.

As part of [14], the authors introduced TinyFedTL, the first open-source implementation of Federated TL (FTL) on resource-constrained IoT devices. FL enabled decentralized model training on devices with limited memory (less than 1MB), while TL allowed the use of pre-trained models for new tasks. The system was tested on the Arduino Nano 33 BLE Sense with CIFAR-10 datasets. Results showed that TinyFedTL maintained constant memory usage while learning continuously, using only 210KB of dynamic memory and reducing training time compared to existing models.

As part of their study, the authors in [15] proposed a hierarchical federated TL (HFTL) model for secure and efficient fault classification in additive manufacturing. FL was used to enable distributed training across multiple servers while preserving privacy. TL was applied to adapt pre-trained models for fault detection in 3D printing. Experimental results demonstrated that HFTL reduced training time by 24%, improved accuracy by 45%, and increased F1-scores by 59% on non-IID data compared to traditional methods. The model efficiently handled distributed data and improved performance in the fault classification of 3D-printed products.

As part of their research [16], the authors introduced a novel federated TL framework called CPFTL-CGAN for smart manufacturing. FL enabled decentralized model training across different clients, while TL allowed knowledge transfer from a pre-trained model to a target task. The Collaborative Generative Adversarial Network (CGAN) generated high-quality synthetic data to facilitate TL without compromising data privacy. Experimental results demonstrated that the proposed framework improved classification accuracy by up to 93.6%, with enhanced precision, recall, and F1 scores, while significantly reducing communication rounds compared to baseline methods.

As part of their research, the authors [17] developed a Hashgraph-based FL approach (HFLA) for securing multi-domain 5G networks. FL was used to train models across decentralized devices without compromising data privacy. The hashgraph technology ensured robust protection against Sybil, DDoS, and other attacks by utilizing asynchronous Byzantine fault tolerance. Experimental results from the Federated 5G testbed showed that the proposed method effectively prevented poisoning and membership inference attacks while maintaining high model accuracy and training efficiency.

As part of [6], the authors proposed a digital currency system that integrates FL and TL to enhance transaction privacy while maintaining regulatory oversight. FL was used to allow multiple nodes to collaboratively train models without sharing sensitive transaction data, preserving privacy across different participants. TL enabled the adaptation of pre-trained models to new environments, reducing the time and data needed for implementation in different contexts. The authors demonstrated that the system successfully protected transaction amounts using homomorphic encryption and offered controllable anonymity, meeting both privacy and regulatory requirements.

As part of [7], authors have developed a graph mining approach for detecting suspicious transactions, specifically those related to money laundering. The method built a model that identified subgraphs of transactions based on fuzzy parameters, which captured both transaction values and their structural relationships. FL was used to aggregate data from various financial institutions without revealing sensitive information, and TL helped adapt models to new transaction data. The experimental results showed that the method effectively detected illegal transactions while minimizing false positives, improving the efficiency of human review processes.

In research [8], the authors introduced a FL approach to detect data hidden in mobile application icons delivered through web and multiple stores. FL was used to allow distributed nodes to train models on local datasets, preserving data privacy while identifying steganographic threats. TL facilitated adapting the models to different types of encoding schemes like Base64 and zip compression. Experimental results showed that the federated approach achieved detection performance comparable to centralized models, with an AUC of 97.1% for plain text and significant improvements in detecting obfuscated payloads.

Summary

Based on the reviews performed, FL and TL have demonstrated significant potential in medical image classification, such as brain tumor and breast cancer detection. These methods enable institutions to collaborate on improving diagnostic models while maintaining patient data privacy. Pre-trained models like VGG16 and ResNet have been critical in enhancing classification accuracy and efficiency. In the automotive and smart manufacturing sectors, FL and TL have shown improvements in fault detection, operational efficiency, and security. Autonomous vehicular systems benefited from reduced latency and improved accuracy, while smart manufacturing processes saw higher performance in fault classification. Technologies such as blockchain and generative adversarial networks (GANs) further bolstered privacy and security. In 5G networking, FL and TL help safeguard

networks against DDoS and Sybil attacks, with hashgraph technology ensuring robust protection while maintaining model accuracy and training efficiency. The benefits observed in these reviews include improved data privacy, better model accuracy, reduced training time, and enhanced scalability across industries like healthcare, automotive, smart manufacturing, and 5G networking.

A Framework for Transfer Learning and Federated learning

As part of this section, we will discuss a novel framework that combines TL and FL to enhance prediction accuracy while maintaining privacy-preserving data processing. This approach leverages pre-trained models for knowledge transfer across different domains, improving the model's efficiency without needing large datasets, and ensuring that sensitive data remains localized across institutions. The privacy-preserving aspect is achieved through FL, where data is not shared across clients, but models are trained collaboratively.

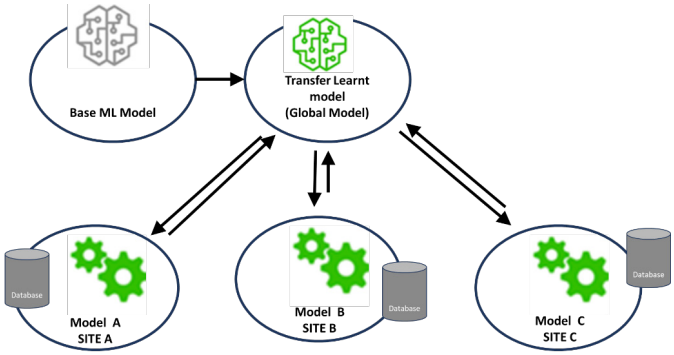
1. Figure.1 illustrates the five tasks involved in this p**Model Initialization using TL**: A global machine learning model (base ML Model) is trained using publicly available datasets.

2. Model Distribution: The global model is then shared with each Site unit.

3. Local Model Training: Each site trains its local model using local data stored locally in its database.

4. Parameter Update: The locally trained models update their parameters, which are encrypted and sent back to the server to create an updated global model. No raw data (e.g., local data) is shared, ensuring privacy.

5. Personalized Model: TL is applied to fine-tune the global model for each site, resulting in personalized settings based on their local data.



This combination of FL and TL allows the system to balance global model performance with individual customization, maintaining privacy throughout the data sharing process.

TL Initialization

The process begins with the application of TL to initialize the models at each local node (e.g., healthcare institution or device). The key steps are:

Pretrained Model Setup: A global model, trained on a large dataset from a source task, such as a general health or diagnostic dataset, is distributed to each local node. This pretrained model already contains features that are likely generalizable across different health conditions.

The model's initial parameters, $\theta\ pretrained$, are shared with all participating nodes.

$$\theta^{(0)} local = \theta\ pretrained$$

Local Fine-Tuning: Each node fine-tunes the global pretrained model on its local dataset, which contains data specific to the node's medical practice or region (e.g., patient demographics or localized health issues). This step adjusts the model parameters to better suit the node's specific task.

The objective is to minimize the local loss function Li with respect to the parameters θi (where i represents the node):

$$\theta_{local}^{(t+1)} = \theta_{local}^{(t)} - \eta \nabla L_i(\theta_{local}^{(t)})$$

Where η is the learning rate and Li is the gradient of the local loss function.

FL for Collaborative Model Training

Once TL has enabled local fine-tuning of the pretrained model, the system moves to the FL phase to collaboratively improve the model across all nodes without sharing raw data.

Local Model Training (On-Device Training): Each node continues training the locally fine-tuned model using its private dataset. No data is shared with other nodes or the central server. Instead, each node updates its local model's parameters based on its specific data, ensuring data privacy and security.

The goal is to minimize the local objective function at each node iii:

$$\min_{\theta_i} \sum_{j=1}^{N_i} L(\theta_i; X_j, y_j)$$

Where:

- Ni is the number of data points at node i,
- $L(\theta_i; X_j, y_j)$ is the local loss function using local data
- (X_j, y_j).

Model Aggregation at Central Server: After a round of local training, the updated model parameters (not the data) from each node are sent to the central server for aggregation. This is typically done using Federated Averaging (FedAvg), where the server computes the weighted average of the local models based on the size of their local datasets.

The global model parameters are updated as follows:

$$\theta_{global}^{(t+1)} = \sum_{i=1}^{K} \frac{N_i}{N} \theta_i^{(t)}$$

Where:

- K is the number of nodes,
- N is the total number of data points across all nodes,
- $\theta^{(t)} i$ represents the model parameters from node i at iteration t.

Global Model Distribution: After aggregation, the updated global model is sent back to all local nodes for further fine-tuning based on local data. This creates an iterative loop where the global model benefits from the knowledge learned at each node.

Iterative Training and Model Convergence

The above steps are repeated over multiple iterations:

- Local nodes continue to fine-tune their models on the

local datasets.

- The central server aggregates the updated models after each iteration.

- The global model gradually converges, learning from the diversity of local datasets across all nodes, ensuring that the final model generalizes well across different healthcare settings.

Final Model Deployment

After several rounds of aggregation and local fine-tuning, a robust global model is obtained. This model can then be deployed across all participating nodes to provide a high-quality second health opinion for patients, benefiting from the collective knowledge learned from different healthcare institutions.

Advantages

The integration of FL and TL brings numerous advantages to industries like healthcare, retail, insurance and finance, where data privacy and efficiency are critical. By enabling collaborative learning across multiple institutions without sharing sensitive data, this approach fosters innovation while safeguarding privacy. Below are some of the key benefits:

- **Data Privacy**: No raw data is shared between nodes or with a central server. Only model updates are exchanged, ensuring the protection of sensitive information.

- **Knowledge Sharing**: FL allows all nodes to benefit from diverse data across multiple healthcare providers, improving model generalization.

- **Specialized Local Models**: TL ensures models are tailored to local data needs while still leveraging insights from a global model.

- **Efficient Learning**: TL accelerates model adaptation to new tasks, minimizing the need for large labeled datasets.

- **Collaboration**: Enables institutions to collaborate and train high-performing models without exposing sensitive data directly.

- **Cost-Effectiveness**: Reduces the requirement for extensive data collection efforts by allowing pre-trained models to be fine-tuned locally.

- **Cyber Defence**: Building nationwide or regional cyber-defence models by sharing threats and malicious attempt patterns across industries, without exposing the actual types and strategies of defence system design.

By beginning with TL, which fine-tunes a pre-trained model on specific local datasets, and subsequently applying FL, organizations across various industries can collaboratively enhance model performance while safeguarding sensitive data.

This approach enables the development of high-performing models that capitalize on knowledge from diverse, distributed data sources, making it ideal for applications like fraud detection in finance, personalized recommendations in retail, or risk assessment in insurance.

The process ensures that proprietary or private data remains secure, while still benefiting from the collective insights of all participating entities.

Discussion

The integration of FL and TL represents a significant advancement in the field of machine learning, particularly in areas where data privacy, scalability, and domain adaptation are crucial. These technologies, traditionally employed independently, have been successfully merged in various domains such as healthcare, finance, retail, and manufacturing, where data sharing across organizations is restricted due to privacy or regulatory concerns. A significant body of research has demonstrated the potential of combining these two approaches into Federated TL (FTL). For example, in healthcare, Federated TL (FTL) was used for decentralized brain tumour classification using MRI data [1], achieving a high accuracy of 98% while preserving patient privacy. Similarly, authors in [2] developed the PrivateKT framework for privacy-preserving tasks like fraud detection, with up to 84% of centralized model performance in constrained environments. In IoT, FTL was applied for intrusion detection, leading to an accuracy improvement of up to 5.55% and reduced training time by 36.11% [12]. And a blockchain-enabled FTL was proposed for autonomous vehicular systems, improving latency, scalability, and security [13].

In conclusion, by starting with TL to fine-tune models based on localized data and proceeding to FL to aggregate knowledge without sharing data, this integrated approach is poised to transform industries by offering solutions that are both highly accurate and privacy-compliant across distributed environments.

Conclusion

FL and TL offer significant benefits by enhancing model accuracy, preserving data privacy, and enabling collaboration across industries. The combination of these technologies has been shown to improve outcomes in sectors ranging from healthcare to finance, manufacturing, and networking. The ability to leverage pre-trained models while maintaining privacy makes this approach an ideal solution for modern AI applications in privacy-sensitive environments.

Author Statements

Authors' Contributions

All authors read and approved the final manuscript. The corresponding author was responsible for the study's conception and design. Venkatesh Upadrista authored the first draft of the manuscript. All authors have read and approved the final version of the manuscript.

Funding

No Funding was received.

Conflict of Interests

The authors have no relevant financial or non-financial interests to disclose.

Ethical Approval

This work does not involve the use of human subjects.

Data Availability

No datasets were used and/or analyzed during the current study. rocess:

References

1. Albalawi E, Mahesh TR, Thakur A, Kumar VV, Gupta M, Khan SB, et al. Brain tumor classification using MRI images: a federated learning-based approach leveraging VGG16 architecture and transfer learning. BMC Medical Imaging. 2024; 24: 1-15.
2. Qi T, Wu F, Wu C, He L, Huang Y, Xie X. Differentially private knowledge transfer for federated learning. Nature Communications. 2023; 14: 3785.
3. Guo W, Zhuang F, Zhang X, Tong Y, Dong J. A Comprehensive Survey of Federated Transfer Learning: Challenges, Methods, and Applications. Frontiers of Computer Science. 2024; 18: 186356.
4. Selvakanmani S, Devi GD, Rekha V, Jeyalakshmi J. Privacy-Preserving Breast Cancer Classification: A Federated Transfer Learning Approach. Journal of Imaging Informatics in Medicine. 2024; 37: 1488-1504.
5. Majeed U, Hassan SS, Hong CS. Cross-Silo Model-Based Secure Federated Transfer Learning for Flow-Based Traffic Classification. IEEE International Conference on Information Networking (ICOIN). 2021: 588-593.
6. Xu B, Chen H, Jin S, Jiao Q. A Digital Currency System with Transaction Amount Privacy Protection. IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technol. 2021: 535-540.
7. Michalak K, Korczak J. Graph Mining Approach to Suspicious Transaction Detection. Proceedings of the Federated Conference on Computer Science and Information Systems. 2011: 69–75.
8. Cassavia N, Caviglione L, Guarascio M, Liguori A, Manco G, Zuppelli M. A federated approach for detecting data hidden in icons of mobile applications delivered via web and multiple stores. Social Network Analysis and Mining. 2023; 13: 1-15.
9. Wang E, Tayebi P, Song YT. Cloud-Based Digital Twins' Storage in Emergency Healthcare. International Journal of Networked and Distributed Computing. 2023: 75–87.
10. Lloyd J. Infrastructure Leader's Guide to Google Cloud: Lead Your Organization's Google Cloud Adoption, Migration and Modernization Journey, Apress Media LLC. 2023.
11. Kanellopoulos P, Kyropoulou M, Voudouris A. Algorithmic Game Theory, 15th International Symposium, SAGT 2022, Colchester, UK, September 12–15, 2022, Proceedings. Lecture Notes in Computer Science. 2022: 13584.
12. Otoum Y, Yadlapalli SK, Nayak A. FTLIoT: A Federated Transfer Learning Framework for Securing IoT. IEEE Global Communications Conference. 2022: 1146-1151.
13. Basha SM, Iyengar NSN, Ahmed ST, Caytiles RD. Inter-Locking Dependency Evaluation Schema based on Blockchain-Enabled Federated Transfer Learning for Autonomous Vehicular Systems. IEEE International Conference on Innovative Technology Convergence (CITC). 2021: 46-51.
14. Kopparapu K, Lin E, Breslin JG, Sudharsan B. TinyFedTL: Federated Transfer Learning on Ubiquitous Tiny IoT Devices. IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). 2022: 79-81.
15. Putra MAP, Rachmawati SM, Abisado M, Sampedro GA. HFTL: Hierarchical Federated Transfer Learning for Secure and Efficient Fault Classification in Additive Manufacturing. IEEE Access. 2023; 11: 54795-54807.
16. Li S, Cui Q, Li X, Liao T, Zhao X, Tao X. A Novel Federated Transfer Learning Framework Based on Collaborative GAN for Smart Manufacturing. 2024 IEEE Wireless Communications and Networking Conference. 2024: 20-24.
17. Kholidy HA, Kamaludeen R. An Innovative Hashgraph-based Federated Learning Approach for Multi-Domain 5G Network Protection. IEEE Future Networks World Forum (FNWF). 2022: 139-146.
18. Sakib S, Fouda MM, Fadlullah ZM, Abualsaud K, Yaacoub E. Asynchronous Federated Learning-based ECG Analysis for Arrhythmia Detection. IEEE International Mediterranean Conference on Communications and Networking (MeditCom). 2021: 277-282.
19. Soni G, Verma S, Sharan A, Ahmad O. BioBERT-Based Model for COVID-Related Named Entity Recognition. Advances in IoT and Security with Computational Intelligence. 2023: 335-345.
20. Soni G, Verma S, Sharan A, Ahmad O. BioBERT-Based Model for COVID-Related Named Entity Recognition. Published in a Springer compilation. 2023: 332-346.
21. Soni G, Verma S, Sharan A, Ahmad O. BioBERT-Based Model for COVID-Related Named Entity Recognition. Springer compilation. 2023: 332-346.
22. Sujie X, Ruipeng H, Gaofeng C, Xiaoyan X, Ta L. EC-BERT: A BERT Language Model with Error Correction for Mandarin Chinese Speech Recognition. J Shanghai Jiao Tong Univ (Sci). 2024.
23. Baghersalimi S, Teijeiro T, Atienza D, Aminifar A. Personalized Real-Time Federated Learning for Epileptic Seizure Detection. IEEE Journal of Biomedical and Health Informatics. 2022; 26: 2.
24. Brophy E, Vos MD, Boylan G, Ward T. Estimation of Continuous Blood Pressure from PPG via a Federated Learning Approach. Sensors. 2021; 21: 6311.
25. Yuan B, Ge S, Xing W. A Federated Learning Framework for Healthcare IoT devices. Distributed, Parallel, and Cluster Computing. 2020.
26. Polamuri SR. Stroke detection in the brain using MRI and deep learning models. Multimedia Tools and Applications. 2024.
27. Sarwat H, Alkhashab A, Song X, Jiang S, Jia J, Shull PB. Post-stroke hand gesture recognition via one-shot transfer learning using prototypical networks. Journal of Neuro Engineering and Rehabilitation. 2024: 21: 100.
28. Carino-Escobar RI, Franceschi-Jimenez LA, Carrillo-Mora P, Cantillo-Negrete J. Subject-Specific Session-to-Session Transfer Learning Strategies for Increasing Brain-Computer Interface Performance during Upper Extremity Neurorehabilitation in Stroke. Journal of Medical and Biological Engineering. 2024; 44: 596-606.
29. Reddy R. Generative AI in healthcare: an implementation science informed translational path on application, integration and governance. Implementation Science. 2024; 19: 27.
30. AK, "MIMIC-III - Deep Reinforcement Learning," Kaggle. 2022.