ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/subhasis-kundu/547

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 2

Research Article

Multi-Brain Federated Learning for Decentralized AI: Collaborative, Privacy-Preserving Models Across Domains

Subhasis Kundu*

Citation: Kundu S. Multi-Brain Federated Learning for Decentralized AI: Collaborative, Privacy-Preserving Models Across Domains. *J Artif Intell Mach Learn & Data Sci 2023* 1(2), 2559-2562. DOI: doi.org/10.51219/JAIMLD/subhasis-kundu/547

Received: 02 April, 2023; **Accepted:** 18 April, 2023; **Published:** 20 April, 2023

***Corresponding author:** Subhasis Kundu, Solution Architecture & Design, Roswell, GA, USA, E-mail: subhasis.kundu10000@gmail.com

ABSTRACT

Multi-brain Federated Learning (MBFL) introduces an innovative approach to decentralized artificial intelligence, enabling joint model training across various fields while maintaining data privacy. This study clarifies the MBFL concept and explores its potential uses in industries such as healthcare, finance and defense. It covers the core principles of MBFL such as data decentralization, model aggregation and privacy-preserving techniques. The benefits of MBFL, including improved model performance and reduction of data silos, are examined along with possible challenges and limitations. A framework for implementing MBFL in different scenarios was provided and its impact on the future direction of AI development was discussed. The paper concludes by highlighting the transformative potential of MBFL in advancing collaborative AI, while ensuring data security and privacy.

Keywords: Multi-brain Federated Learning, Decentralized AI, Privacy-preserving, Collaborative models, Data security, Cross-domain learning, Model aggregation, Federated Learning, Healthcare, Finance, Defense

1. Introduction

A. Background on federated learning

Federated learning is a machine learning framework that enables model training on distributed datasets without the need to centralize data[1,2]. This method effectively tackles privacy issues and regulatory limitations by allowing participants to keep their data on local devices, while collectively improving a shared model. In recent years, this technique has gained significant attention because of its ability to leverage diverse datasets from various organizations and devices while maintaining data confidentiality. Federated earning effectively addresses challenges related to data silos, privacy regulations and the computational constraints of individual entities, making it especially useful in sensitive fields such as healthcare, finance and defense.

B. Concept of multi-brain federated learning

Multi-brain Learning enhances the traditional federated learning model by incorporating several independent AI models, known as "brains," which work together to improve their overall effectiveness[3-5]. This approach allows different AI systems from various fields or organizations to participate in collaborative training while maintaining their unique structures and areas of expertise. Multi brain federated learning enables these separate models to share knowledge and insights without directly exchanging raw data. By leveraging the strengths of different specialized models, this method can produce more resilient and comprehensive AI systems that gain from cross-domain expertise while preserving the distinct characteristics of each model involved.

C. Importance in various industries

The importance of Multi brain federated learning spans numerous sectors, especially those dealing with sensitive information and intricate, multifaceted issues. In healthcare, it enables hospitals and research centers to work together to create advanced diagnostic models, while ensuring patient confidentiality. Financial organizations can improve their fraud detection and risk evaluation models by utilizing diverse datasets from various entities. In the defense industry, Multi brain federated learning facilitates secure cooperation among different agencies and international allies, enhancing threat detection and strategic decision making[6]. This method also holds promise for smart cities where different municipal services can collaborate to enhance urban planning and resource management. By promoting cross-industry collaboration while maintaining decentralized data, Multi brain federated learning propels the development of advanced and privacy-conscious AI solutions in essential sectors.

2. Principles of Multi-Brain Federated Learning

A. Data decentralization

In Multi brain federated learning, data are stored and processed locally at its source rather than being centralized in one place. This approach allows organizations to maintain control over their sensitive data while participating in collaborative AI training. Data are spread across multiple "brains" or nodes, each representing a different entity or domain. These nodes can include individual devices organizations or even the entire industry. By keeping the data decentralized, multi-brain federated learning addresses privacy concerns, ensures regulatory compliance and reduces the risk of large-scale data breaches. This approach also allows for the integration of diverse datasets from multiple sources, resulting in the creation of more robust and generalizable AI models.

B. Model aggregation techniques

In multi-brain federated learning, model aggregation techniques are essential for merging insights from multiple decentralized models without requiring the sharing of raw data. These methods involve a series of iterative steps, where local models are trained on their respective datasets and only the updates or parameters from these models are shared with a central server or among peers. Federated averaging is a common method in which the central server calculates the weighted average of the model updates from the participating nodes[7]. More sophisticated techniques might include adaptive aggregation, which adjusts each node's contribution dynamically based on factors like data quality or model performance. Secure aggregation protocols ensure that individual updates remain private during the aggregation process, thus enhancing privacy protection.

C. Privacy-preserving mechanisms

Privacy-preserving techniques essential components in multi-brain federated learning, designed to protect sensitive data while such collaborative model development. These techniques include differential privacy, which introduces controlled noise to data or model updates to prevent the disclosure of individual information[8,9]. Secure multiparty computation allow multi-parties to collaboratively compute functions on their inputs while maintaining the privacy of those inputs. Additionally, encryption facilitates encrypted data operations, allowing nodes to exchange encrypted model updates that can be combined without decryption. In addition, methods such as federated learning with secure enclaves utilize hardware-based trusted execution environments to secure sensitive computations. Collectively, these privacy-preserving techniques ensure that the benefits of collaborative AI training are realized without compromising on data confidentiality or personal privacy.Same depicted in **(Figure 1)**.

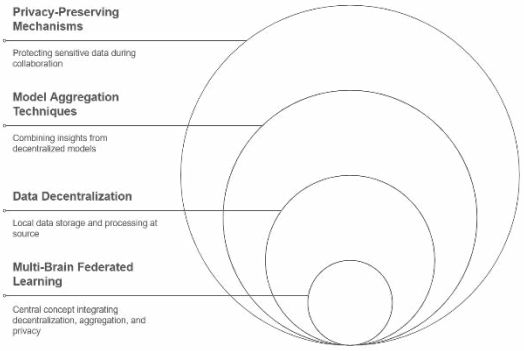

Figure 1: Multi-Brain Federated Learning Framework.

3. Benefits of Multi-Brain Federated Learning

A. Improved model performance

Multi brain federated learning significantly boosts the model performance by leveraging a variety of datasets from different sources without the need for data centralization. This approach allows artificial intelligence models to learn from a broader spectrum of experiences and patterns, thereby promoting the creation of more resilient and adaptable algorithms. By incorporating insights from multiple fields and industries, MBFL enhances the models' capacity to identify intricate relationships and nuances that might not be apparent in standalone datasets. This cooperative learning process is essential for more precise predictions, improved decision-making abilities and improved overall performance across various tasks and applications.

B. Reduced data silos

Model-Based Federated Learning (MBFL) effectively addresses the challenge of data silos by enabling collaboration among various organizations and departments without necessitating the exchange of raw data. This approach dismantles traditional barriers that impede the sharing of valuable information, thereby fostering a more interconnected and knowledge-rich environment[10]. By allowing models to learn from diverse sources while maintaining data decentralization, MBFL promotes cross-domain insights and reduces redundancy in data collection and processing. This collaborative framework stimulates innovation and accelerates the development of artificial intelligence solutions by leveraging collective intelligence across sectors and industries.

C. Enhanced data privacy and security

One of the key benefits of Model-Based Federated Learning (MBFL) is its capacity to preserve data privacy and security while facilitating collaborative learning. By decentralizing data and sharing model updates, MBFL greatly reduces the risk of data breaches and unauthorized access to sensitive information. This approach is especially important in industries like healthcare, finance and defense, where safeguarding data

is critical. MBFL enables organizations to adhere to strict data regulations and privacy laws, while also benefiting from the collective intelligence of multiple AI models. Additionally, this method reduces the need for data transfer and centralized storage, thereby enhance security and protecting both data and organizational privacy.

4. Challenges and Limitations

A. Communication overhead

Federated learning systems face significant communication challenges due to the decentralized nature of their training processes. As models are developed across various devices and organizations, the frequent transmission of model updates can lead to substantial network congestion[11]. This issue is particularly pronounced in environments with limited bandwidth or unstable connections. To address this problem, researchers have explored methods such as gradient compression, quantization and selective parameter updates. Additionally, asynchronous communication protocols and adaptive update frequencies are being investigated to reduce the communication load while maintaining the model efficacy.

B. Model convergence issues

In federated learning environments, achieving model convergence presents greater challenges compared to centralized training scenarios. The decentralized nature of the training process, along with potential data heterogeneity among participants, can result in slower convergence rates or even divergence in some cases. Issues such as non-Independent and Identically Distributed (non-IID) data, varying data quality and increased data protection measures among participating entities further complicate these challenges[12]. To enhance the convergence properties in federated settings, researchers are developing advanced optimization algorithms, adaptive learning rates and personalized model architectures. Additionally, techniques such as federated averaging, client selection strategies and regularization methods are being explored to improve the model stability and convergence.

C. Heterogeneous data distributions

One of the main difficulties in federated learning is managing diverse data distribution among entities involved. In real-world scenarios, data from different sources often exhibit varying statistical characteristics, feature distributions and class imbalances. This diversity can lead to biased or less effective models when traditional federated learning techniques are used. To address this issue, researchers are developing methods such as federated transfer learning, domain adaptation strategies and personalized federated learning algorithms[13]. These approaches aim to manage data diversity while leveraging the shared knowledge of all participants. Additionally, robust aggregation techniques and fairness-aware federated learning strategies are being explored to mitigate the effects of data heterogeneity on model performance and ensure fair outcomes for all participants.

5. Implementation Framework

A. System architecture

The architecture for multi-brain federated learning is based on a decentralized network of autonomous artificial intelligence models, each residing on distinct devices or servers across various domains. A central aggregator orchestrates the learning process without direct access to local data. This architecture includes secure communication channels for model updates and parameter sharing, as well as systems for data preprocessing, model initialization and synchronization among participating nodes[14]. Privacy-preserving techniques, including differential privacy and secure multi-party computation, are incorporated to protect sensitive information. Scalability is achieved through efficient resource allocation and load balancing across the network. The architecture is compatible with diverse hardware and software environments, facilitating participation from various industries.

B. Protocol design

The protocol for multi-brain federated learning outlines a comprehensive procedure for collaboratively training models while preserving data privacy. It begins with the initialization phase, where participating nodes agree on a shared model architecture and hyperparameters. The protocol defines the frequency and method of communication between nodes and the central aggregator[15]. It details the computation, encryption and secure transmission of local model updates. The aggregation process at the central node is explained, including strategies for managing stragglers and ensuring fair contributions. The protocol also incorporates mechanisms to detect and counter potential attacks and malicious participants. Additionally, it specifies the procedure for transmitting global model updates back to local nodes and integrating them into local models. The design accounts for node failures, network disruptions and the dynamic participation of nodes throughout the training process.

C. Evaluation metrics

In the context of multi-brain federated learning, evaluation metrics assess both the model's effectiveness and the system's efficiency. To evaluate predictive performance, metrics like accuracy, precision, recall and F1-score are used on both local and global test datasets. The efficiency of the federated learning process is evaluated by analyzing the convergence rate and training duration. Privacy protection is quantified using metrics such as epsilon values in local-model privacy or indicators of information leakage. Communication overhead is assessed by monitoring the volume and frequency of data exchanged between nodes. Scalability is determined by analyzing system performance as the number of participating nodes increases. Fairness metrics ensure that the process provides equitable benefits to all participants. Robustness is evaluated through simulations of node failures. Resource utilization metrics track computational and storage demands in the network. Finally, domain-specific metrics are employed to assess model performance in sectors such as healthcare, finance and defense.

6. Applications in Various Industries

A. Healthcare

Federated learning, which involves collaboration between multiple institutions, shows significant potential in the healthcare industry, where safeguarding patient privacy and ensuring data security are critical. This approach allows different healthcare organizations to jointly train AI models on various patient datasets without the need to exchange raw data. For example, hospitals located in various regions can work together to create more accurate diagnostic models for rare diseases by pooling

their patient data. Federated learning supports the development of strong predictive models designed for personalized treatment plans, while maintaining patient confidentiality. Additionally, this technology can assist in creating AI-powered medical imaging analysis tools that draw from a wide range of imaging data s. By keeping sensitive medical information decentralized, healthcare providers can comply with strict data protection laws while also advancing medical research and improving patient care through collaborative AI efforts.

B. Finance

In the domain of finance, multi-brain federated learning offers a promising approach to developing advanced artificial intelligence models while ensuring data privacy and regulatory compliance. Financial institutions and banks can collaborate to enhance fraud detection systems by training models on diverse transaction data from various sources, all without disclosing sensitive customer information. This approach supports the creation of robust credit-scoring models that utilize a broader spectrum of financial data across multiple institutions. Federated learning also facilitates the development of more effective anti-money laundering (AML) systems by leveraging the collective expertise of numerous financial entities[16]. Furthermore, this technology aids in formulating AI-driven investment strategies that incorporate insights from multiple financial institutions without risking exposure to proprietary trading data. By maintaining the decentralization of financial data, institutions can preserve their competitive advantage while benefiting from collaborative AI model development.

C. Defense

In addition to defense, multi-brain federated learning presents a valuable opportunity to bolster national security while protecting the confidentiality of sensitive data. Military forces from allied countries can collaborate to develop advanced threat detection systems without the need to exchange classified information. This approach enables the creation of more resilient cybersecurity models that benefit from the diverse attack patterns observed across different defense networks. Federated learning also aids in developing AI-driven autonomous systems for reconnaissance and surveillance by leveraging the collective expertise of multiple military branches. Additionally, this technology supports the creation of more precise predictive maintenance models for military equipment by integrating data from various defense agencies. By decentralizing defense-related data, military organizations can maintain operational security while enhancing their AI capabilities through joint model development.

7. Conclusion

In conclusion, Multi-Brain Federated Learning (MBFL) represents a significant advancement in decentralized artificial intelligence, offering a comprehensive framework for collaborative model training across diverse domains while safeguarding data privacy and security. By leveraging data decentralization, model aggregation and privacy-preserving methodologies, MBFL addresses critical challenges in sectors such as healthcare, finance and defense. The benefits of enhanced model performance, reduced data silos and improved privacy make MBFL a promising solution for organizations seeking to harness collective intelligence without compromising sensitive data. Despite challenges such as communication overhead and model convergence issues, ongoing research and development continue to refine implementation frameworks and evaluation metrics.

As MBFL evolves, it has the potential to revolutionize AI development, fostering innovation and cross-industry collaboration while maintaining the highest standards of data protection and ethical AI practices.

8. References

1. Hu K, Li Y, Xia M, et al. Federated Learning: A Distributed Shared Machine Learning Method. Complexity, 2021: 1-20.
2. Ma X, Chen X, Wu Y, et al. Differentially Private Byzantine-Robust Federated Learning. IEEE Transactions on Parallel and Distributed Systems, 2022;33: 3690-3701.
3. Tahir M and Ali MI. On the Performance of Federated Learning Algorithms for IoT. IoT, 2022;3: 273-284.
4. Jiang D, Zhang Z and Shan C. Federated Learning Algorithm Based on Knowledge Distillation, 2020.
5. Bhuyan N and Moharir S. Multi-Model Federated Learning, 2022.
6. Jeon B, Rahman MR, Walid A and Ferdous SM. Privacy-Preserving Decentralized Aggregation for Federated Learning, 2021.
7. Zhao B, Jiang K, Sun P and Wang T. FedInv: Byzantine-Robust Federated Learning by Inversing Local Model Updates. Proceedings of the AAAI Conference on Artificial Intelligence, 2022;36: 9171-9179.
8. Fang W, Zhao D, Tan J, et al, Large-scale Secure XGB for Vertical Federated Learning, 2021: 443-452.
9. Yin X, Zhu Y and Hu J. A Comprehensive Survey of Privacy-preserving Federated Learning. ACM Computing Surveys, 2021;54: 1-36.
10. Li Q, Diao Y, Chen Q and He B. Federated Learning on Non-IID Data Silos: An Experimental Study. cornell university, 2021.
11. Kang J, et al. Communication-Efficient and Cross-Chain Empowered Federated Learning for Artificial Intelligence of Things. IEEE Transactions on Network Science and Engineering, 2022;9: 2966-2977.
12. Li Z, He Y, Yu H, et al. Data Heterogeneity-Robust Federated Learning via Group Client Selection in Industrial IoT. IEEE Internet of Things Journal, 2022;9: 17844-17857.
13. Mhaisen N, Abdellatif AA, Erbad A, et al. Optimal User-Edge Assignment in Hierarchical Federated Learning Based on Statistical Properties and Network Topology Constraints. IEEE Transactions on Network Science and Engineering, 2021;9: 55-66.
14. Wang T, Zheng X, Jia W, et al. Edge-Based Communication Optimization for Distributed Federated Learning. IEEE Transactions on Network Science and Engineering, 2022;9: 2015-2024.
15. Liu L, Zhang J, Letaief KB and Song SH. Client-Edge-Cloud Hierarchical Federated Learning, 2020.
16. Kute DV, Shukla N, Pradhan B, et al. Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering-A Critical Review. IEEE Access, 2021;9: 82300-82317.