2026 年 3 月 28 日

2025 年度若手研究者共同研究プロジェクト実施報告書

法政大学総長　殿

以下のとおり研究実施報告書を提出します。

基本情報	研究課題名：ビザンチン耐故障連合学習：ツリートポロジーの分散化と知識蒸留による防御アルゴリズム
	研究代表者氏名：陳　錦華（CHEN Jinhua）
	【在籍者】 研究科・専攻・学年：理工学研究科　応用情報工学専攻　博士後期課程 3 年 【修了者】 所属・職種：
	指導教員（所属・職・氏名）：理工学研究科　准教授　余　恪平 （※在籍者のみ記入）
	共同研究者（所属・職・氏名）： （※指導教員と同人の場合は記入不要）
	その他 研究分担者：理工学研究科応用情報工学専攻　修士修了　趙子涵（ZHAO Zihan）
	研究期間：　　２０２４年度　～　２０２６年度（※研究終了年度を記載）
年間の研究実施概要	※研究計画の進捗状況を中心に今年度の研究実施状況を記載してください。 During this academic year, the research project has made steady, systematic, and well-structured progress toward its overarching objective of developing **robust, secure, and scalable federated learning frameworks for multimodal large-scale models**. At the initial stage, the study conducted a comprehensive analysis of the fundamental challenges inherent in multimodal federated learning systems. In particular, three critical issues were identified: **severe data heterogeneity across clients**, **weak and unstable aggregation performance under non-IID data distributions**, and the **increasing risk of parameter leakage and privacy exposure** when training large language and vision models in distributed environments. These challenges were further analyzed from both theoretical and practical perspectives, providing a clear problem formulation and guiding subsequent research directions. To address these challenges, the first phase of the research focused on the design and development of **robust aggregation mechanisms**. A novel **privacy-preserving aggregation framework** was proposed by integrating **relative distance-based similarity metrics with CKKS homomorphic encryption**. This approach enables **secure aggregation of model updates while preserving structural relationships among client models**. Compared with conventional aggregation methods such as FedAvg, the proposed method demonstrates **stronger robustness against malicious or unreliable client updates**, including poisoning and noisy contributions. At the same time, it ensures **confidentiality during parameter transmission**, thereby enhancing both security and reliability in federated learning systems. This stage of work established a **solid methodological foundation for trustworthy and scalable federated learning**.

年間の研究実施概要

Building upon the aggregation-level improvements, the research then progressed to a more fine-grained investigation of data heterogeneity from a sample-level perspective. Recognizing that client-level aggregation alone is insufficient to fully address heterogeneity, a novel **uncertainty-aware federated learning framework** was proposed. This framework leverages **Monte Carlo Dropout-based uncertainty estimation** to identify hard or informative samples within local datasets. Based on the estimated uncertainty, **adaptive weighting and optimization strategies** were introduced to dynamically emphasize difficult samples during training. This mechanism allows the model to focus on more informative data points, thereby **improving generalization performance under highly heterogeneous data distributions**. In this context, several methods, including **MCMFL and MC-Agg**, were designed, implemented, and systematically validated, demonstrating their effectiveness in **balancing robustness and accuracy**.

In addition to methodological development, **extensive experimental evaluations** were conducted to verify the effectiveness and generalizability of the proposed approaches. Experiments were performed on benchmark datasets including CIFAR-10, CIFAR-100, and TinyImageNet under various **non-IID and adversarial settings**. The results consistently show that the proposed methods achieve **superior performance over baseline federated learning algorithms in both robustness and accuracy**. Notably, improvements are particularly significant in scenarios with **high data heterogeneity and partial client unreliability**, confirming the **practical applicability of the proposed frameworks**. Furthermore, ablation studies and comparative analyses were carried out to provide **deeper insights into component-level contributions and performance gains**.

Overall, the research conducted during this academic year demonstrates a clear and logical progression from **system-level robustness enhancement** to **data-level adaptive optimization**. The work successfully integrates **secure aggregation mechanisms with uncertainty-driven learning strategies**, forming a **comprehensive and scalable solution** to key challenges in federated learning for giant models. This progression not only advances the **theoretical understanding of federated learning under heterogeneous conditions** but also provides **practical and deployable methodologies**. The results achieved provide a **solid and reliable foundation for future research**, including federated large language models and retrieval-augmented generation systems.

Next Plan

In the next stage of this research, the focus will shift toward advancing **federated training techniques for large language models (LLMs)**. A key direction is to develop **adaptive and parameter-efficient fine-tuning methods** tailored for federated environments. In particular, this includes designing **client-specific optimization strategies**, where the rank of **Low-Rank Adaptation (LoRA) modules can be dynamically adjusted** according to the complexity and distribution of local data. Such an adaptive mechanism is expected to **significantly improve training efficiency while maintaining model performance under highly heterogeneous client conditions**. In addition, **more robust aggregation strategies** will be further explored to address inconsistencies and potential biases introduced by diverse client updates.

Another important direction is the development of **federated Retrieval-Augmented Generation (RAG) systems**. This research aims to enable **collaborative knowledge utilization across distributed data sources while preserving privacy**. Specifically, a federated RAG framework will be designed to support **privacy-preserving retrieval over decentralized knowledge bases**, allowing multiple clients to jointly contribute to and benefit from shared knowledge **without exposing their raw data**. Efficient knowledge sharing mechanisms will be investigated to balance **communication cost, retrieval accuracy, and privacy constraints**. Furthermore, practical deployment will also be considered, including **implementing LLM-based AI agents (e.g., OpenClaw-like systems) on local devices such as personal computers (MacBook, Windows)**, enabling **real-world usability and scalability**.

As a next step, the research will aim to integrate **federated LLM training and federated RAG into a unified framework**. This integrated system will combine **adaptive client-side rank selection with collaborative knowledge retrieval**, forming a **more efficient and robust learning paradigm**. By jointly optimizing **model training and knowledge augmentation under federated settings**, the proposed framework is expected to **better handle data heterogeneity, improve generalization performance, and enhance privacy protection**. This direction represents a **natural extension of the current work with strong practical application potential in distributed intelligent systems**.

研究業績

成果発表（学会・論文・研究会等）

学会・論文・研究会等の別	タイトル	発行または発表年月
国際論文誌	**Jinhua Chen** et al.,"A Robust Aggregation of Federated Large Language Models for Multimodal Knowledge Discovery in Computational Social Systems," IEEE Transactions on Computational Social Systems	2025 年 7 月
国際論文誌	**Jinhua Chen** et al., "MCMFL: Monte-Carlo-Dropout-Based Multimodal Federated Learning for Giant Models in 6G Symbiotic Internet of Things," IEEE Internet of Things Journal	2025 年 7 月
国際論文誌	T. Liu, S. Zhang, **Jinhua Chen** et al., "Intent-Driven DRL-Based Resource Allocation for RIS-Assisted Wireless-Powered IoT Edge Networks," IEEE Internet of Things Journal	2025 年 11 月
国際会議	**Jinhua Chen** et al., "Federated Fine-Tuning of Large Language Models for Intelligent Automotive Systems with Low-Rank Adaptation," IEEE VTC 2025 Spring	2025 年 6 月
国際論文誌	T. Liu, S. Zhang, **Jinhua Chen** et al.,"Joint Resource Allocation and RIS Beamforming for Enhanced Computational Efficiency in Multi-RIS Assisted MEC Networks,"IEEE Transactions on Vehicular Technology	2025 年 12 月

その他（アピールすることがあればご記入ください。）

- ✓ 1--F. J. A. Messou, **Jinhua Chen** et al.,"TAPformer: A Transformer with Adaptive Attention and Temporal Projection Encoding for Long-Term Electricity Load Forecasting in IoT Systems," Internet of Things, 2026. 02. **国際論文誌**
- ✓ 2--Franck Junior Aboya Messou, **Jinhua Chen**, Yu Tao, Keping Yu, Osama Alfarraj, Amr Tolba,"Spec2Llama: A Spectral-Aware Forecasting Approach for Versatile Time Series Analysis,"Expert Systems with Applications, 2026.03. **国際論文誌**
- ✓ 3--**J. Chen** *et al*., "Distance-Aware Secure Federated Learning against Model Theft and Heterogeneous Data for Communication and Information Systems," *GLOBECOM 2025 - 2025 IEEE Global Communications Conference*, Taipei, Taiwan, 2025.12, **国際会議**
- ✓ 4--S. Zhang, T. Liu, **J. Chen**, F. J. Aboya Messou, K. Yu and M. Guizani,"Dynamic IoT Resource Allocation Using Graph Reinforcement Learning with Hypergraph Convolutions," IEEE VTC2025-Spring, Oslo, Norway, 2025.06 **国際会議**
- ✓ 5--F. J. A. Messou, **J. Chen**, T. Liu, S. Zhang and K. Yu,"TSFormer: Temporal-Aware Transformer for Multi-Horizon Forecasting with Learnable Positional Encodings and Attention Mechanisms,"Sixteenth International Conference on Ubiquitous and Future Networks (ICUFN), Lisbon, Portugal, 2025. 07 **国際会議**