2025 年　04　月　09　日

2024 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 2 年生 【修了者】 所属・職種：
	指導教員（所属・職・氏名）：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：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。

From June 2024 to March 2025, the proposed research plan targeting the enhancement of fault tolerance, robust aggregation, and parameter privacy in Federated Learning (FL) systems has been effectively implemented. The plan was executed across three core aspects—theoretical research, experimental design, and data analysis—and yielded substantial results that align well with the original objectives.

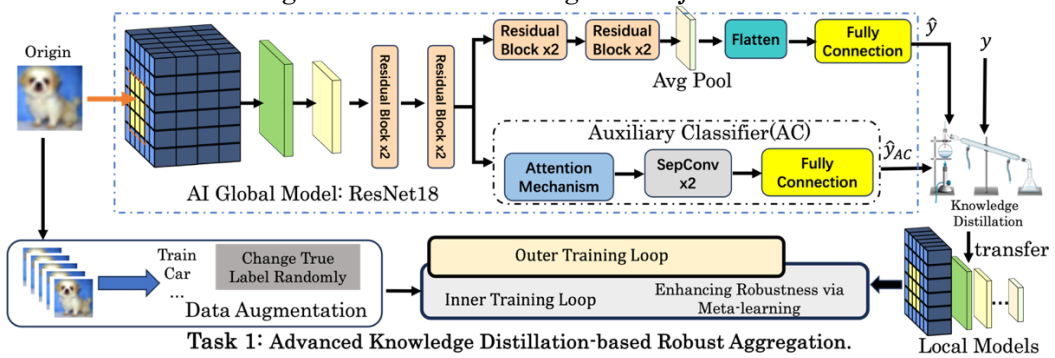

Fig 1 Combining knowledge distillation with meta-learning to defend FL

1. Theoretical Research Achievements

1.1 Knowledge Distillation and Meta-Learning Integration:

As shown in Fig. 1, this study developed novel strategies combining knowledge distillation with meta-learning to defend FL models against poisoning attacks. In the publication "Blockchain-Empowered Resilient Attack Defense in Federated Learning for Consumer Electronics" (IEEE CEM), a robust decentralized trust mechanism was proposed. It integrates teacher-student distillation under adversarial settings, enabling the system to maintain over 80% accuracy even with 50% of clients being malicious.

年間の研究実施概要

1.2 Blockchain and Tree-Based Decentralized Trust:

The above work also introduced a TreeChainFL architecture, where blockchain and tree-structured communication pathways enable tamper-resilient parameter exchange and verification. This contributes to system robustness against parameter pollution and Byzantine failures.

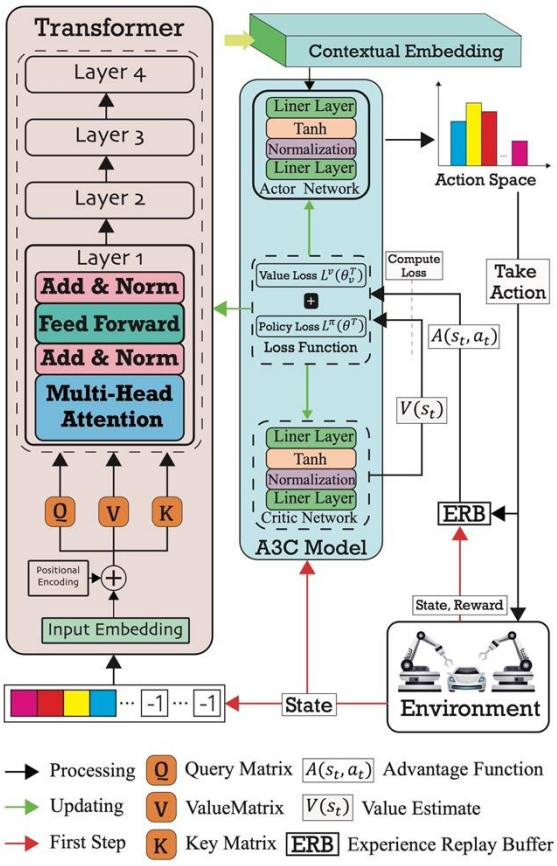

Fig. 2 Transformer-based Production Planning Unit

1.3 Privacy via Encryption during Training:

As shown in Fig.3, in "Dynamic Optimization of Vehicle Production Planning Using Federated Reinforcement Learning" (IEEE T-ITS), a CKKS-based homomorphic encryption scheme was implemented for protecting model parameters in collaborative reinforcement learning settings. This ensures privacy without compromising optimization performance

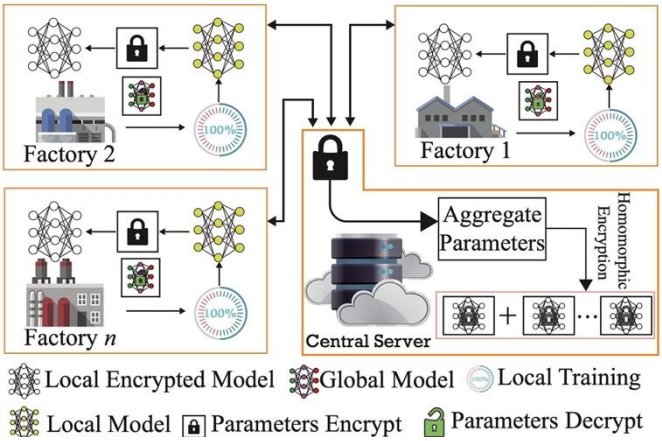

Fig. 3 Federated Reinforcement Learning with Privacy-Preserving for Vehicle Production Planning

2. Experimental Design and Simulation

Federated Learning systems were simulated on real-world tasks: In the consumer electronics domain, Byzantine attack scenarios were simulated using standard image classification datasets to evaluate defensive strategies.

In the transportation manufacturing domain, a novel federated reinforcement learning system was developed to optimize vehicle production planning. Two modules—DOPM (GRU-based) and HQPM (Transformer-based, as shown in Fig. 2)—were built to dynamically and efficiently schedule 1000 vehicles in less than 5 seconds, with over 95% fewer constraint violations compared to traditional methods.

The FL environments employed public datasets (e.g., CIFAR-10, CIFAR-100) and real-world vehicle production planning dataset, aligning with the initial plan. These were tested under both non-IID and Byzantine attack settings.

3. Comparative Data Analysis and Evaluation

The effectiveness of the proposed methods was quantitatively evaluated against multiple baselines: In the attack defense study, proposed methods outperformed FedAvg and Krum under poisoning conditions. In the scheduling task, HQPM under FL achieved 93.18% improvement in constraint satisfaction and 95.11% speed enhancement compared to NSGA-II. Evaluation metrics included accuracy, recall, reward values, and violation scores, thoroughly supporting the claims of robustness, scalability, and privacy-preservation.

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
IEEE Transactions on Intelligent Transportation Systems	Dynamic Optimization of Vehicle Production Planning in Transportation Networks Using Federated Reinforcement Learning	January 2025
IEEE Consumer Electronics Magazine	Blockchain-Empowered Resilient Attack Defense in Federated Learning for Consumer Electronics	October 2024
2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)	A Byzantine-Fault-Tolerant Federated Learning Method Using Tree-Decentralized Network and Knowledge Distillation for Internet of Vehicles	November 2024
2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)	Enhancing Production Planning in the Internet of Vehicles: A Transformer-based Federated Reinforcement Learning Approach	September 2024
2025 IEEE Consumer Communications and Networking Conference (CCNC)	Enhancing Federated Learning in Consumer Electronics with Decoupled Knowledge Distillation against Data Poisoning	January 2025

その他（アピールすることがあればご記入ください。）