

WENWEN HE

✉ wenddd@whu.edu.cn · ☎ (+86) 15986957320 · 🏠 My Homepage

🏠 School of National Cybersecurity, Wuhan University

🎓 EDUCATION

Wuhan University, Wuhan, Hubei

2024 - 2026

Cybersecurity. M.S.

Advisor Mang Ye

Guangdong University of Technology, Guangzhou, Guangdong

2020 – 2024

GPA 88.96/100

Computer Science and Technology. B.S.

🔧 EXPERIENCE

IDEA Lab, Shenzhen, Guangdong

2025.9 - 2026.3

Visiting Student

Responsibilities Responsible for algorithm design and prototype implementation, focusing on distributed personalized learning scenarios (such as federated learning and personalized fine-tuning), and conducting model optimization and system coordination.

📖 PUBLICATION

†: equal contribution

[1] **Wenwen He**†, Wenke Huang†, Bin Yang, Shukan Liu, Mang Ye, "SPMC: Self-Purifying Federated Backdoor Defense via Margin Contribution", ICML 2025. [CCF A](#)

[2] **Wenwen He**, Wenke Huang, Yiyang Fang, Wenjie Qu, Jiaheng Zhang, Mang Ye, "Batman: Benign Knowledge Alignment Through Malicious Null Space in Federated Backdoor Attack", CVPR 2026 **Highlight**. [CCF A](#)

[3] **Wenwen He**, Wenke Huang, Jian Liang, Yi Liu, Xirui Li, Guansong Pang, Mang Ye, "FedPissa: Federated Personalized LoRA Matrix and Subspace Adaptation", ICML 2026 **Spotlight**. [CCF A](#)

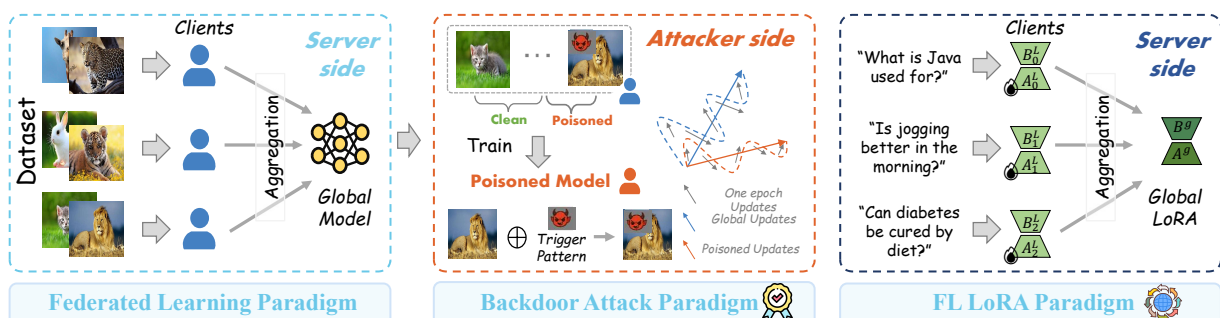
[4] Zhiqiang Kou, Junxiang Wu, **Wenwen He**, Ming-Kun Xie, Changwei Wang, Yuheng Jia, Di Jiang, Yang Liu, Xin Geng, Qiang Yang, "FedHarmony: Harmonizing Heterogeneous Label Correlations in Federated Multi-Label Learning", CVPR 2026 **Highlight**. [CCF A](#)

[5] Xingyue Zhao, Wenke Huang, **Wenwen He**, Linghao Zhuang, Haoran Wu, Anwen Jiang, Zhifeng Wang, Ming Feng, Mang Ye, Bo XU, "Shift-Dependent Asymmetry: Orthogonal Inverse Low-Rank Adaptation for Federated Medical Segmentation", ICML 2026. [CCF A](#)

[6] **Wenwen He**, ..., Guansong Pang, "FLoRA-Chef: Making A Good LoRA Recipe in Federated Generalization", Under review ([Submitted to AAAI 2026](#)).

[7] Wenke Huang, ..., **Wenwen He**, Mingjun Li, Mang Ye, Bo Du, Dacheng Tao, "MAPO: MIXED ADVANTAGE POLICY OPTIMIZATION", Under review ([Submitted to AAAI 2026](#)).

📚 RESEARCH



Federated Learning

2024 – now

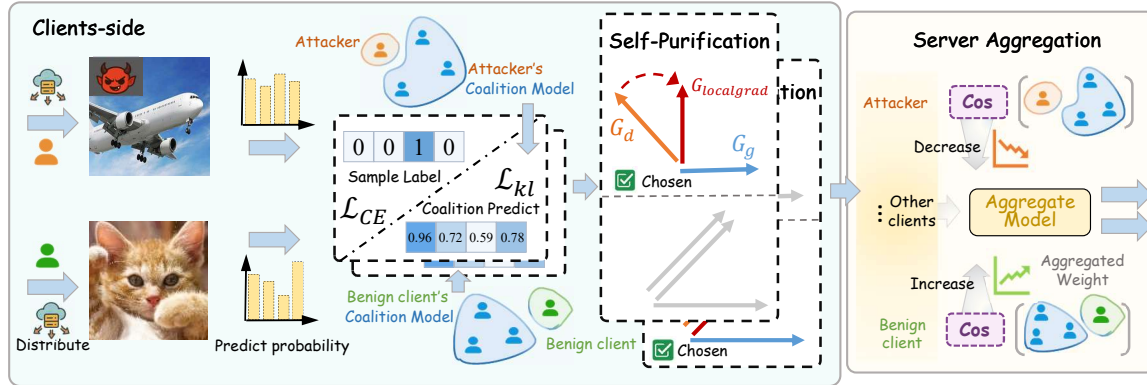
Federated Learning (FL) does not require the exchange of raw data. It achieves collaborative model training solely through the exchange of intermediate model parameters or feedback. However, the server cannot easily discern participants collaborative intentions, making it vulnerable to malicious attacks and hindering the model ability to achieve strong generalization. Therefore, our primary goal is to pursue **trustworthy multi-party security** and ensure strong **generalization** under heterogeneous FL.

Trustworthy Security

2024 – 2025.06

Contributed to the development of a privacy-preserving heterogeneous federated learning framework aimed at multi-source collaboration. Develop a robust defense mechanism and a novel federated backdoor attack method.

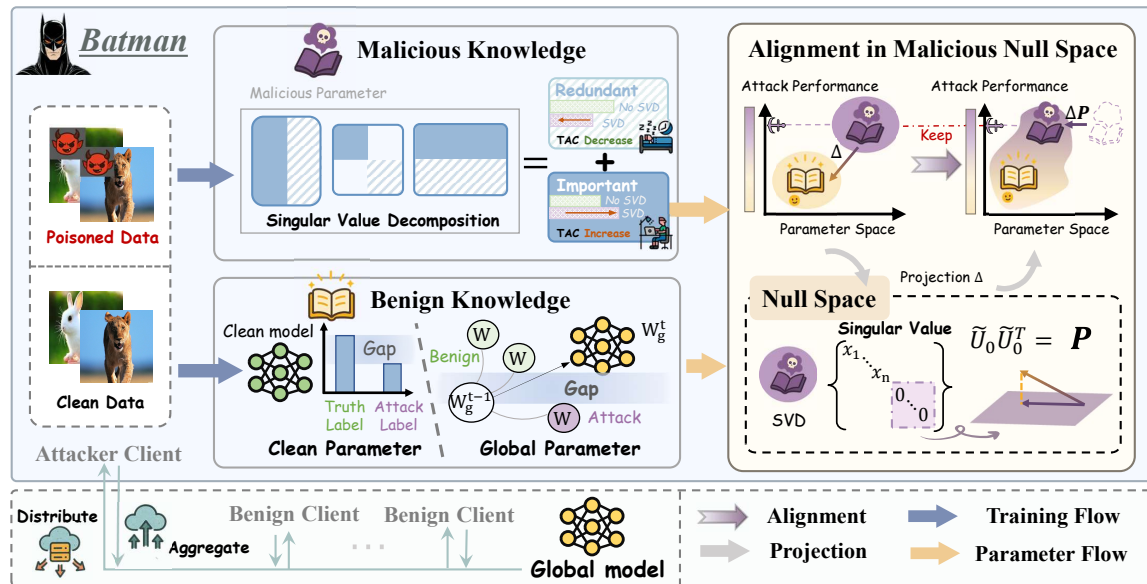
• SPMC: Self-Purifying Federated Backdoor Defense via Margin Contribution



Contribution: SPMC proposes a self-purifying defense that reweights aggregation via margin contributions and aligns local gradients with coalition knowledge to mitigate backdoor effects without proxy data.

Highlight: SPMC departs from prior defenses by eliminating reliance on predefined scales or proxy datasets, enabling adaptive and flexible purification against adaptive attackers.

• Batman: Benign Knowledge Alignment Through Malicious Null Space in Federated Backdoor Attack



Contribution: Batman introduces a FL backdoor attack that constructs a malicious null space via truncated SVD and aligns benign knowledge in this orthogonal space, ensuring both attack effectiveness and stealthiness.

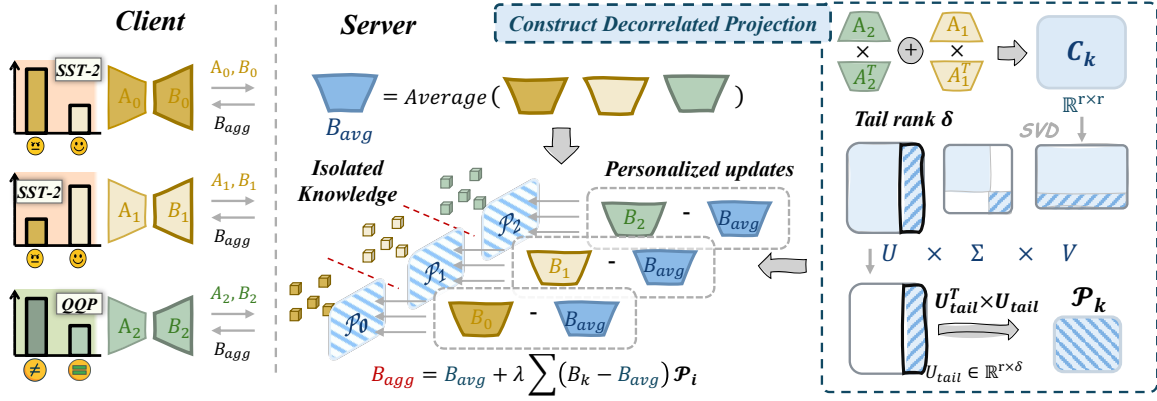
Highlight: Batman is the first work to discuss parameter space conflicts and departs from prior attacks by decoupling benign and malicious knowledge through a malicious null space.

FedLLMs Generalization

2025.06 – now

Federated Learning combined with Low-Rank Adaptation (LoRA) offers an efficient and privacy-preserving solution for fine-tuning large language models across distributed clients. However, challenges like non-IID data and biased aggregation of shared LoRA components often compromise performance.

- **FedPissa: Federated Personalized LoRA Matrix and Subspace Adaptation**



Contribution: FedPissa proposes a selective aggregation strategy and adopts a decorrelated projection matrix to map the client-specific updates into a decorrelated subspace, which maximizes misalignment between each client and protects the personalized knowledge.

Highlight: Unlike prior dual-LoRA methods with heavy overhead and bias, FedPissa introduces a compact design that resolves inter-client conflicts while safeguarding personalization.

EXPERIENCE

- As the primary investigator for a provincial-level innovation project under the **National Undergraduate Training Program for Innovation and Entrepreneurship 2024**.
- Publish a conference paper as the first author at **ICML 2025** and **CVPR 2026**.
- Invited reviewer member by **TIPS** and **TKDE**.

AWARDS

First Prize, China "Internet+" Innovation and Entrepreneurship Competition	2023
Third Prize, National University Statistic Mathematical Modeling Competition	2023
Second Prize, National University Mathematical Modeling Competition	2022