

# Jiyuan SHEN

Tel: (+65) 87906052 | Personal Website: <https://shenjiyuan123.github.io/> | Email: jiyuan001@e.ntu.edu.sg

## EDUCATION

**Nanyang Technological University, Singapore**

08/2022 - 07/2024

M.Eng. in Computer Science and Engineering, supervised by Prof. LAM, Kwok Yan

GPA: 4.17/5.0

**Shanghai University, Shanghai, China**

09/2018 - 06/2022

B.Eng. in Intelligent Science and Technology

GPA: 3.54/4.0

## PUBLICATION

**Jiyuan Shen**, "Towards Efficient and Certified Recovery from Poisoning Attacks in Federated Learning ", *submitted to TIFS*

**Jiyuan Shen**, "A Survey on Federated Unlearning: Challenges, Methods, and Future Directions", *submitted to ACM Computing Survey*

**Jiyuan Shen**, "AST: Effective Dataset Distillation through Alignment with Smooth and High-Quality Expert Trajectories", *arxiv*

**Jiyuan Shen**, "Effective Intrusion Detection in Heterogeneous Internet-of-Things Networks via Ensemble Knowledge Distillation-based Federated Learning", *IEEE International Conference on Communications (ICC), 2024 (Oral)*

**Jiyuan Shen**, "An efficient training strategy for multi-agent reinforcement learning in card games", *International Conference on Artificial Intelligence, Automation, and High-Performance Computing (AIAHPC), 2022*

## PROJECT & RESEARCH EXPERIENCES

**LLM for Science: An Intelligent QA System;**

08/2023 – 01/2024

- We adapted the open-source LLAMA 7b model to suit the Chinese semantic environment. We use LoRA on a dataset comprising 60 billion tokens. We constructed an SFT instruction fine-tuning dataset, incorporating alpaca-zh and scientific QA data. Additionally, we expanded the scientific domain instruction fine-tuning dataset using GPT. We applied LoRA for supervised fine-tuning.
- We employed Retrieval Augmented Generation to obtain rich context-based answers. We built an encyclopedia database and used a multi-route recall strategy to find the knowledge content most relevant to the question. Our model offers a well-adapted experience for Chinese language environments, ensuring fluent scientific Q&A interactions.

**Fast Recovery from Attacks in Federated Learning;**

08/2023 – 01/2024

- We conducted a comprehensive survey in the promising field of Federated Unlearning, covering fundamental concepts and principles, unlearning and verification algorithms, and tailored optimizations for federated learning framework.
- We introduce an efficient and certified method designed for fast recovery of an accurate global model from poisoning attacks in federated learning. It can reduce huge memory consumption and computational cost with only a marginal trade-off in performance.
- We are the first to propose a privacy-preserving federated unlearning scheme that leverages sharing clients' historical information between two non-colluding servers and Two-Party Computation (2PC) techniques.

**Structures of Datasets in Learning (Synthetic Data Generation);**

11/2022 – 2023/5

- We distilled information from real-world datasets into compact synthetic datasets while maintaining their ability to train a well-performing model. Distilled datasets can be used for efficient parameters tuning, continual learning and model interpretability.
- We improved the efficacy, effectiveness, and robustness of DD, making it a practical data-efficient technique. We achieved the SOTA performance. Also, we applied DD to privacy-enhanced FL framework rely on the privacy for free and informative characteristic.

## WORK EXPERIENCES

**Bosch China Investment Co., Ltd. | Visual Algorithm Intern CR/RIX-AP**

01/2022 - 07/2022

- Explored and developed the Human Action Recognition project based on long time video (Know Your Motion), including document writing, cameras testing, dataset collection and labeling, feature engineering, algorithm comparison (ViT-based v.s. CNN-based), model training and evaluation. We also use Flask to deploy and apply the project's patent.

## COMPETITIONS REWARDS

*2<sup>nd</sup> National Prize of First Ocean Target Intelligent Perception International Challenge (Field: Detection, Top 3/200)*

12/2020

*3<sup>rd</sup> National Prize of Artificial Intelligence Application Competition (Field: Classification, Top 9/2100)*

11/2020

*2<sup>nd</sup> Prize of the East China Division of the WeChat Applet Application Development Competition*

06/2020

## SKILLS & QUALIFICATIONS

- **Programming Language:** Python(advanced for DS,ML), Pytorch/paddlepaddle(advanced for DL), MySQL,C++, Java, Matlab
- **Statistics:** Bayesian Learning, EM algorithm, PCA, regression, decision tree, clustering, ensemble learning, text analytics, etc.
- **ML/DL:** Transformer (bert, ViT), Federated Learning, VAE, GAN, YoloV5, Faster R-CNN, U-Net, Knowledge Distillation, etc.
- **Language:** Mandarin (native), English (TOEFL 100, GRE 319+3.5)