Yuchen Zhou

https://erwinzhou.github.io/
+86(0)22 13212168838 | erwinzhou021227@126.com | GitHub: ErwinZhou

Education

Nankai University, Tianjin, China Sep.2021 - July.2025

- **Bachelor of Engineering in Information Security**
- **Core Modules:** *Algorithm Design and Analysis (92), Probability and Mathematical Statistic (93), Introduction to Artificial Intelligence (91), Machine Learning and Application (98), Database System (94), Software Engineering (99), Big Data Analytics and Application (95), Data Security (97)*
- **GPA**: 88.7/100; **WES**: 3.75/4.0
  Year1: 86.94(3.63), Year2: 88.60(3.69), Year3: 91.29;2023-2024 Fall Rank:1/53

Academic Experience

FedMoLLM: The first federated learning framework for End-to-End MM-LLM Training
TsingHua University; Beijing National Research Center for Information Science and Technology (BNRist)
Research Assistant, Advisor: Dr. Sicheng Zhao (Research Associate Professor at TsingHua University)
Jul.2024 - Now

- **Research Focus:** Proposed the first federated learning framework for MM-LMM training, FedMoLLM. It is a promising decentralized training pipeline aiming to address the privacy concerns when training an End-to-End MM-LLM.
- **Methodology:** FedMoLLM expanded the traditional tasks of multimodal federated learning from classification to multimodal reasoning and generation by increasing the model scale to billion-parameter level and using the LLM backbone such as Vicuna-13B as an agent. It also adapts meta-learning to tackle the performance decrease while facing imbalanced and missing modalities in federated learning scenarios.
- **Expected Results:** FedMoLLM will reach SOTA MM-LLM performance in multimodal tasks (e.g. VQA) without compromising data privacy, offering a promising solution for the future deployment of AGI.
- **Research Significance:** Innovatively incorporated End-to-End MM-LLM training pipeline with federated learning framework to ensure data privacy for true industrialization of AGI.

MIT Project-Based Learning | Deep Learning for Computer Vision - Microsoft Project
Advisor: Dr. Shashvat Shukla (University College London) Apr.2024 - Jun.2024

- **Research Track:** Image Synthesis
- **Research Focus:** Enhance the capabilities of AI4Sci models to effectively convey complex scientific and mathematical concepts through multimedia (e.g. video), assisting researchers in various scientific fields.
- **Methodology:** Leveraged large models with billions of parameters, particularly SOTA LLMs proficient in Chain of Thought (CoT) reasoning and mathematical problem-solving for describing complex concepts with diffusion models for video generation; utilized existing 3D models for concrete examples and developed a specialized interface for visualizing abstract ones.

Self-Supervised Contrastive Graph Clustering Network via Structural Information Fusion
May.2023 - Nov.2023

- **Published:** International Conference on Computer Supported Cooperative Work in Design, January 31, 2024. (Second Author)
- **Research Focus:** Enhance model accuracy and reliability of the prior clustering distribution in graph clustering tasks.
- **Methodology:** Developed a novel deep graph clustering method named CGCN; integrated contrastive learning mechanism and structural information to boost interoperability and adaptability; facilitated model's self-adjustment for information aggregation across different order structures.

- **Results:** Our proposed method CGCN consistently outperforms other clustering techniques on various real-world datasets, with a 77.3±0.2 accuracy and 1.71% improvement on DBLP dataset.
- **Research Significance:** Innovatively applied contrastive learning and structural information fusion in graph clustering tasks to enhance model accuracy and reliability of the priori clustering distribution.

Deep Neural Network Backdoor Attack Sample Detection Method Based on Meta Backdoor Analysis
Advisor: Professor Zheli Liu, Associate Dean of College of Cyber Security at Nankai University
Sep.2023 - Aug.2024

- **Research Focus:** Proposed a Meta Backdoor Defense System (MBDS) to detect and defend against backdoor attacks in deep neural networks (DNNs) by utilizing a meta-classifier trained on shadow datasets created through Jumbo Contamination, aiming to identify and filter malicious samples without assumptions about the attacker's strategies.
- **Methodology:** Implemented related experiments, trained and optimized the meta-classifier, simulated various backdoor attack scenarios. Contributed to the experimental design, drafting, and defense of project proposals, focusing on feature extraction and selection strategies to enhance the classifier's performance.
- **Results:** The MBDS method demonstrated effectiveness in detecting and preventing malicious backdoor samples, improving the model's robustness and security against a wide range of backdoor attacks, with F2 Score of 94.73% on BadNets attacks.

Internship Experience

Longshine Tlogy Croup Co., Ltd
Assistant of Operations and Maintenance Engineer, Mar. 2023- May. 2023

- Automated daily system maintenance tasks using Shell and Python scripts, improving system response times and transaction processing capabilities.
- Optimized deployment processes by implementing CI/CD practices with Jenkins, Docker, and Kubernetes (K8S), enhancing overall system performance and reliability.

Chinasoft International
Data Analyst Intern, Jul. 2023 - Aug. 2023

- Contributed to the analysis of pandemic-related population migration data (4 million records), focusing on data processing and storage using Hive and HDFS.
- Assisted in the integration of Sqoop, Kafka, and Zookeeper to optimize data flow and ensure secure, efficient handling.

Honors and Awards

- **2024:** Nankai University College of Cyber Security Academic Excellence Scholarship, 2023-2024; Second Prize in Tianjin Division, China Undergraduate Mathematical Contest in Modeling (CUMCM);
- **2023:** Nankai University College of Cyber Security Academic Excellence Scholarship, 2022-2023; Outstanding Internship Individual, Chinasoft International; Silver Award (Second Prize) in Nankai University, Undergraduate Mathematical Contest in Modeling;
- **2022:** Innovation and Entrepreneurship Training Program for College Students, Ministry of Education;

Extracurricular and Club Activities

- Nankai University AI Association (2021-2022): Core member, organized competitions and tech talks, enhancing organizational and communication skills.
- Nankai University Freshmen Football Cup (2021 & 2022): Key player (Right back defender), leading the team to championship, fostering teamwork and athletic spirit.
- Nankai University Community Service: Volunteered for COVID-19 screening, developing community service consciousness, patience, and a sense of responsibility.

Software Skills

- Programming Languages: PYTHON, C, C++, JAVA, MATLAB, SQL
- Software skills: Pytorch, TensorFlow, DeepSpeed, Git, Shell, Hadoop, Docker, FastAPI, MySQL
- Language Proficiency: TOEFL 104(*MyBest*™ Scores 108, S24+W26), GRE 323(3.5)