Yuchen Zhou

Portfolio Website

+86 13212168838 | erwinzhou021227@126.com | GitHub Profile

Education

College of Cyber Security, Nankai University, Tianjin, China Sep.2021 - July.2025

- **Bachelor of Engineering in Information Security**
- **Core Modules:** *Calculus, Linear Algebra, Probability and Mathematical Statistics, Algorithm Design and Analysis, Machine Learning and Application, Database System, Data Structure, Data Security; etc.*
- **GPA**: 88.7/100; **WES**: 3.75/4.0 ***Rank****:1/53 (2024 Spring, GPA: 91.29)*

Publication

- **Published:** Xiaoyang Ji, **Yuchen Zhou**, Haofu Yang, Shiyue Xu, Jiahao Li, "Self-Supervised Contrastive Graph Clustering Network via Structural Information Fusion," *2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD).*

Academic Experience

FedMoLLM: The first federated learning framework for End-to-End MM-LLM Training

School of Information Science and Technology, Tsinghua University

Research Assistant, Advisor: Dr. Sicheng Zhao (Research Associate Professor at Tsinghua University)

Jul.2024 - Now

- Proposed FedMoLLM, the first federated learning framework for End-to-End MM-LLM pre-training, offering a decentralized training solution to address privacy issues for the true industrialization of AGI.
- Expanded multimodal federated learning from classification to reasoning and generation by scaling models to billions of parameters; leveraged LLM backbones to enhance reasoning capabilities across tasks; applied meta-learning methods to mitigate performance decrease in imbalanced data distribution.
- Contributed to the design and integration of the three-stage training into a decentralized framework and will be the first author of an academic paper to be submitted to ICML or IJCV early next year.
- FedMoLLM achieved state-of-the-art performance in several multimodal tasks, with a Fréchet inception distance (FID) score of 13.74 for text-to-video on the MSR-VTT dataset while ensuring data privacy.

Defending Against Backdoor Attacks on Deep Neural Networks by Meta Backdoor Analysis

Advisor: Professor Zheli Liu (Associate Dean of College of Cyber Security at Nankai University)

Sep.2023 - Aug.2024

- Proposed a Meta Backdoor Defense System (MBDS) to detect and defend against backdoor attacks in deep neural networks (DNNs) without assumptions about the attacker's strategies.
- Employed a meta-classifier trained on shadow datasets created through Jumbo Contamination, aiming to identify and filter malicious samples. Implemented related experiments on image classification, trained and optimized the meta-classifier simulating various backdoor attack scenarios for better generalization.
- Contributed to the experimental design and drafting of project proposals, focusing on building CNNs identical to the victim models to extract representations and selection strategies specific to different types of backdoor attacks to enhance the classifier's performance, and writing of an academic paper.
- The MBDS method achieved an F2 Score of 94.73% on BadNets attacks and accuracy (ACC) of 80.01% on Jumbo attacks, which simulate various backdoors. This work was summarized in a paper.

MIT Project-Based Learning | Deep Learning for Computer Vision - Microsoft Project

Research Track: Image Synthesis, Advisor: Dr. Shashvat Shukla (University College London)

Apr.2024 - Jun.2024

- Enhance the capabilities of AI4Sci models to effectively convey complex scientific and mathematical concepts through multimedia (e.g., videos), assisting researchers in various scientific fields.
- Leveraged large models with billions of parameters, particularly state-of-the-art LLMs proficient in Chain of Thought (CofT) 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 that the LLMs are not trained on before.
- Contributed to building the training pipeline and integration of various data modalities; summarized our research findings by making the codes open-source on GitHub and writing a research poster.

Self-Supervised Contrastive Graph Clustering Network via Structural Information Fusion
Advisor: Dr. Biao Yi (Nankai University) May.2023 - Nov.2023

- Enhance model accuracy and reliability of the prior clustering distribution in graph clustering tasks.
- Developed a novel deep graph clustering method named CGCN; integrated contrastive learning mechanism and structural information to boost interoperability and adaptability.
- Contributed to the development and optimization of the model's self-adjustment for information aggregation across different order structures by infusing information from AE (structural) and GAE (attribute) to learn more accurate representation; designed and implemented ablation studies to further validate our effectiveness; played a key role in writing an academic paper summarizing our work.
- CGCN consistently outperforms other clustering techniques on various real-world datasets. For example, on the DBLP dataset, CGCN achieves a 1.71% improvement (77.3±0.2) in accuracy (ACC), a 3.43% improvement in normalized mutual information (NMI), a 4.46% improvement in adjusted Rand index (ARI), and a 1.58% improvement (76.9±0.6) in F1 score compared to state-of-the-art methods.

Internship Experience

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

- Contributed to analyzing pandemic-related population migration data (4 million records), focusing on data processing and storage using MapReduce, Hive, and HDFS for secure and efficient data handling.
- Assisted in integrating Sqoop, Kafka, and Zookeeper to streamline data processing and analysis; collaborated with the front-end team for Spring Boot development to implement interactive features.

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 abilities; helped in implementing monitoring and alerting mechanisms.
- Optimized deployment processes by implementing CI/CD practices with Jenkins, Docker, and Kubernetes (K8S), enhancing overall system performance and reliability by decreasing error rates.

Honors and Awards

- **2024:** Nankai University College of Cyber Security Academic Excellence Scholarship, 2023-2024 (Top 5%); Second Prize (Top 20%) in Tianjin Division, China Undergraduate Mathematical Contest in Modeling (CUMCM);
- **2023:** Nankai University College of Cyber Security Academic Excellence Scholarship, 2022-2023 (Top 5%); Silver Award (Top 1.5%) in Nankai University, Undergraduate Mathematical Contest in Modeling; Outstanding Internship Individual (Top 10%), Chinasoft International;
- **2022:** Selected for the provincial-level project (Top 33.3%), 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 the 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.

Professional Skills

- Programming Languages: PYTHON, C++, JAVA, C, MATLAB, Web Dev & Database (e.g., SQL)
- Technical Tools & Platforms: Pytorch, TensorFlow, DeepSpeed, Accelerate, Git, Shell, Hadoop, Docker, FastAPI, MySQL, Hive, MapReduce, Jenkins, Kubernetes (K8S)
- Language Proficiency: TOEFL 104(*MyBest*™ Scores 108, R29+L28+S24+W26), GRE 323(AW: 3.5)

Detailed Information

- For more detailed information regarding my project experiences and others, please visit my GitHub and personal website, where I documented and listed the corresponding descriptions, demos, and outcomes.