Nan Yan | CS Ph.D. Applicant

✉ lunan0320@gmail.com • 🌐 lunan0320.github.io • lunan0320

Education

Wuhan University **School of CSE**
GPA: 90.07/100, National Scholarship (Top 0.2%), Advisor: Prof.Li Yuqing **M.Eng.***2023-Now*

Shandong University **School of CST**
GPA: 88.51/100, Graduated with Outstanding Honor **B.Eng.** *2019-2023*

Research Interests

Trustworthy AI (LLMs and Agent Security), Privacy-Preserving Machine Learning (FL, HE, DP)

Academic Experience

Publications

EmbedX: Embedding-Based Cross-Trigger Backdoor Attack Against Large Language Models
USENIX Security Symposium (acceptance rate: 17.1%) 2025
Nan Yan, Yuqing Li, Xiong Wang, Jing Chen, Kun He, Bo Li

FedPHE: A Secure and Efficient Federated Learning via Packed Homomorphic Encryption
IEEE Transactions on Dependable and Secure Computing (TDSC) 2025
Yuqing Li *(advisor)*, **Nan Yan**, Jing Chen, Xiong Wang, Jianan Hong, Kun He, Wei Wang, Bo Li

Efficient and straggler-resistant homomorphic encryption for heterogeneous federated learning
IEEE International Conference on Computer Communications (INFOCOM, acceptance rate: 19.6%) 2024
Nan Yan, Yuqing Li, Jing Chen, Xiong Wang, Jianan Hong, Kun He, Wei Wang

Manuscripts (Under Review)

TurboMINJA: Bidirectional Evolution of Cooperative Multi-Query Stealthy Memory Attack for LLM Agents
Nan Yan, Jiarong Xing *2025*

Towards Improved Differentially Private Federated Fine-tuning of Language Models on Heterogeneous Clients
Nan Yan, Yuqing Li, Jing Chen, Xiong Wang, Wei Wang, Shuhua Li *2025*

CoMoMark: Cross-Modal Collaborative Backdoor Watermarking for Vision-Language Models
Huiyi Tang, Yuqing Li, Yushi Yang, Xiong Wang, Haoran Wang, **Nan Yan**, Ruiying Du *2025*

Federated LoRA via Error-Free Aggregation and Matrix-Wise Freezing
Haoran Wang, Xiong Wang, Yuqing Li, Jing Chen, Junyi Zhang, **Nan Yan**, Kun He *2025*

FedP2P: Towards Accelerated Federated Learning with Peer-to-Peer Communication
Haoran Wang, Xiong Wang, Yuqing Li, Jing Chen, Yuntao Nie, **Nan Yan**, Meng Jin, Bo Li *2025*

Selected Projects

LLM and Agent Security

TurboMINJA: Bidirectional Set Evolution for Agent Memory Injection Attack *2025-Now*

- Built a bidirectional evolutionary attack that injects cooperative benign queries into LLM-agent memory, optimizing retrievability and reasoning bias to achieve highly stealthy and effective agent manipulation. (*Ongoing Project*)
- Rice University, working with Prof.Jiarong Xing and planing submit to ICML 2026.

EmbedX: Efficient and Stealthy Cross-Trigger Backdoor Attack on LLMs *2024–2025*

- Designed an embedding-level soft-trigger mechanism with latent frequency–gradient constraints, enabling multi-trigger activation with high stealthiness and robustness against fine-tuning.
- Delivered 100% ASR while reducing trigger-switching overhead from 4000s to 0.5s and lowering false-trigger rate to 1%, outperforming SOTA backdoor baselines on 5 datasets & 4 LLMs.
- 4.6 kloc in codebase, and accepted in the Proc. of USENIX Security 2025.

Federated Learning

FedPHE: Efficient Homomorphic Encryption for Heterogeneous Federated Learning *2023–2024*

- Proposed a contribution-aware encrypted weighted aggregation and sketching-based client selection algorithm for optimizing FL training efficiency with CKKS-based HE.
- Achieved a training speedup of 1.85–4.44×, cut the communication overhead by 1.24–22.62×, and reduce the straggler effect by up to 1.71–2.39×, outperforming 6 baselines on 4 datasets.
- 4.5 kloc in codebase, work earned 37 stars and accepted in the Proc. of IEEE INFOCOM 2024.

Federated Learning with Knowledge Distillation *2022–2023*

- Designed and implemented a federated learning framework with knowledge distillation and five baseline methods, earning 26 stars in codebase for facilitating efficient experimentation across diverse datasets and models.

Open Source Software

Pioneer: a low-cost Bluetooth-based virus tracking system *2022–2024*

- Built a cost-effective virus tracking system leveraging Bluetooth technology, secured with the national cryptographic algorithm SM3 for encryption and certification. 19.6 kloc, codebase released and work earned 153 stars, 86 forks.

Awards

Research Fundings

International Conference Support: Wuhan University	*2025*
Travel Support: USENIX Security'25 Student Grant	*2025*
Cyberspace Security Innovation Grant: TOPSEC'23 & Huawei'25	*2023, 2025*

Scholarship

National Scholarship **(Top 0.2%):** Ministry of Education, China	*2024, 2025*
BYD Scholarship **(Top 3):** Dept. CSE, Wuhan University	*2025*
First Class Scholarship **(Top 10%):** Wuhan University	*2024, 2025*
Second Class Scholarship **(Top 10%):** Shandong University	*2020, 2022*
Merit-Based Scholarship: Shandong University	*2020, 2022×4*

Honors

Metrit Student **(Ranking: Top 1%):** Wuhan University	*2024, 2025*
Excellent Student Cadre: Shandong University'22 & Wuhan University'25	*2022, 2025*
Outstanding Graduate Award **(Top 15%):** Shandong University	*2023*
Alumni Council Representative **(Top 6/101):** Dept. CST, Shandong University	*2023*
The Power of Role Models **(Top 1):** Dept. CST, Shandong University	*2023*

Competitions

Second Prize: National Open Source Award Program, China	*2025*
Second Prize: National College Cryptography Mathematics Contest, China	*2022*
Second Prize: National College Student Information Security Competition, China	*2022*
First Prize: National College Cryptography Mathematics Contest, North China Division	*2022*
First Prize: China Undergraduate Mathematical Contest in Modeling, Shandong Province	*2021*

Patents and Software Copyrights

Differential privacy-based heterogeneous federal fine tuning language model method and system
China Patent Application ZL 2024 1 1379992.3, PatentGrant *Sep 2025*

Cross-silo heterogeneous federated learning system based on homomorphic encryption V1.0
Software Copyrights License 2024SR1516588 *Oct 2024*

Technical Skills

Languages: Mandarin Chinese(native) and English (proficiency, IELTS: 7.0)

Technical Expertise: Adversarial Attacks & Defenses, LLM Fine-tuning(LoRA), Distributed Training