Weijun Yin | Curriculum Vitae

github.com/SimonwYin simonwyin.github.io
yinweijun@buaa.edu.cn (+86) 18931532548

RESEARCH INTEREST

My research interests encompass a broad range of topics in big data and distributed machine learning technologies, including federated learning, privacy-enhancing technologies (PETs, such as differential privacy, homomorphic encryption, and secure multi-party computation), and privacy-preserving scenarios (including, but not limited to, federated learning/unlearning and privacy issues in LLMs).
Current Focus: ***Federated Learning***, ***Machine Unlearning***(Efficient and Provable Federated Unlearning based on stable retraining, LLM Unlearning, particularly Unlearning towards FedLora), Privacy-Enhancing Technologies(PETs, especially ***Differential Privacy***).

EDUCATION

Beihang University **Beijing, CHINA**
Master-PhD Direct Program in Cyberspace Security (Master's Stage) *September 2023 - June 2029 (expected)*
– GPA: 3.92/4.0
– Rank: 2/85
– Centesimal grade average: 93.95

Xidian University **Xi'an, CHINA**
B.E. in Infromation Security *September 2019 - June 2023*
– GPA: 3.8/4.0
– Rank: 8/146
– Centesimal grade average: 88.1

AWARDS & HONORS

- **The Second Prize Graduate Study Scholarship**, Beihang University, 2024
- **Outstanding Youth League Member**, Beihang University, 2024
- **The Second Prize Graduate Study Scholarship**, Beihang University, 2023
- **The Second Prize Graduate Scholarship**, Xidian University, 2023
- **Outstanding Youth League Member**, Xidian University, 2022
- **The National Encouragement Scholarship (Top 5%)**, Ministry of Education of P.R.C., 2021, 2022
- **The Second Prize Scholarship**, Xidian University, 2020

COMPETITIVE GRANTS

- **Cyber Security Academy Student Innovation Funding**, *Implementing a Comprehensive Federated Aggregation Algorithm Compatible with Poisoning Detection, Compression, Privacy Protection, and Non i.i.d. Based on MindSpore Federated*, Funded by Cyber Security Association of China (CSAC) and Huawei Technologies Co., Ltd (60 winners nationwide, total amount: 60,000 RMB), 2024.10-2025.04.

RESEARCH EXPERIENCE

Collision-Resistant Aggregation for Cross-Silo Federated Learning *2023 - 2024*

- It focuses on privacy-preserving mechanisms for cross-silo federated learning, especially addressing the issue of collusion between untrusted clients and servers while preserving privacy.
- It investigates the issue that the widely used single-key homomorphic encryption methods cannot resist collusion between untrusted clients and servers. By incorporating a multi-key homomorphic encryption scheme into the aggregation algorithm which supports dynamic weighted aggregation, it achieves high utility and security.
- It has promising prospects in cross-silo federated learning scenarios, especially when the participants are in a competitive relationship and it is difficult to find a fair and trusted third party.

Privacy-Preserving Federated Power Load Forecasting *2022 - 2023*

- It focuses on the privacy issues in scenarios where power departments collaboratively train load forecasting models.
- It introduces a distributed client-level differential privacy mechanism and encrypts the communication content using the Paillier homomorphic encryption scheme.
- It ensures security over the communication link, effectively preventing privacy leakage caused by untrusted third parties or a small number of malicious clients in federated learning, while maintaining prediction performance.

OTHER PUBLICATIONS (Under Review)

- **Heterogeneity-Robust Cross-Silo Federated Learning with Personalized Differential Privacy**
  Weijun Yin and Yanqing Yao*
  submitted to *Knowledge-Based Systems*, SCI. JCR Q1.
- **Collusion-Resistant and Dynamic Weighted Aggregation for Cross-Silo Federated Learning based on Multi-Key Homomorphic Encryption**
  Weijun Yin and Zhenglong Jia and Yanqing Yao*
  submitted to *Frontiers of Computer Science*, SCI. JCR Q1.

PROJECT EXPERIENCE

Behavior Analysis Research on Worm and Trojan Invasion in Intranet and Automated Construction of Experimental Cloud Platform *2021.09 – 2022.01*

- In the first phase, after thoroughly discussing the potential propagation paths of the worm, we built a local topology using virtual machines to simulate its lateral movement behavior. Through dynamic analysis and package capturing, we obtained the source code of the Trojan and the SSH password dictionary used for its lateral movement, thus determining the working mechanism and impact scope of the worm.
- In the second phase, we developed a Python script based on the Alibaba Cloud API and Jumpserver API, which can be used to set up a cloud experimental environment with personalized topologies and configurations at any time. The environment is managed centrally through a bastion host to ensure stability and security.

Anonymous Traffic Identification Based on Flow Multi-Level Filtering and Website Fingerprint Detection *2022.03 – 2022.06*

- It focuses on identifying anonymous traffic and resolving corresponding websites, which helps telecom regulatory authorities detect and analyze such traffic at a fine-grained level.
- We conduct preliminary filtering of traffic using metrics such as character entropy and length entropy of traffic packets. Subsequently, we train an XGBoost classifier to further identify anonymous traffic using flow-level features.

SELECTED COURSES

- **Postgraduate:**

  Machine Learning (91), Privacy and Security (94), Network Security (97), Modern Cryptography (94), Blockchain Principle and Technology (94), Cryptography Application and Security (97), Computational Complexity (92), Essential Mathematics For Cyber Security (96)

- **Undergraduate:**

  Advanced Mathematics A(I) (87), Advanced Mathematics A(II) (92), Linear Algebra (95), Security Programming with Python (95), Introduction of Computer and Program Design (98), Data Structure and Algorithm Analysis (92), Signals and Systems (95), Discrete Mathematics (98), Mathematics for Information Security (95), Principles of Modern Communications (94), Probability Theory and Mathematical

Statistics (90), Computer Networks Principle (95), Artificial Intelligence (93), Computer and Network Security (87), Information and Content Security (85), Digital Circuits and Logic Design (85), Principle of Computer Organization (84), Modern Cryptography (99), Software and System Security (95)

SKILLS

Programming	LaTex, Python, Pytorch
Languages	Chinese, English
Software	Office, Origin