YUANYUAN ZHOU

yuanyuan.zhou.23@ucl.ac.uk | London, UK

EDUCATION

UNIVERSITY COLLEGE LONDON, PhD in Electronic and Electrical Engineering (First Year); Feb 2025– present

Focus: Internet of Things, Security & Privacy, Network, Machine Learning

Supervisor: Dr. Anna Maria Mandalari, funded by industry-academia scholarship

UNIVERSITY COLLEGE LONDON, MEng Machine Learning; Sep 2023 – Sep 2024

Grade: Distinction

Modules: Applied Machine Learning, Internet Protocol Networks, Security and Privacy, Cloud Computing, Data Acquisition and Processing, Natural Language Processing

Thesis: Machine Learning, Distributed Systems, Data Engineering, Security, Federated Learning

SICHUAN UNIVERSITY, BSc Telecommunications Engineering; Sep 2019 – Jun 2023

Grade: 3.7/4.0

3rd & 4th year: Signal Processing & Information Theory, Computer Networks, Machine Learning, Embedded Systems

1st & 2nd year: General Engineering, Advanced Mathematics, Basic Programming

*Award*s: Outstanding Graduate, Comprehensive Scholarship, Gold Medal of Mathematical Modeling Contest, Gold Medal of Internet+ Innovation and Entrepreneurship Competition

EXPERIENCE

Siemens Healthineers, IT Cloud Intern; Sep 2024 – Dec 2024

- Designed and implemented a document intelligence solution using Azure services, enabling API function
- Automated tasks with PowerShell scripts and resource graph explorer for FinOps and SQL server optimization

Bosch Automotive Products, Data Analyst Intern; Feb 2023 – May 2023

- Developed interactive data logging, visualization, and analysis, and actively participated in project management

PROJECT

TwinGuard: An Adaptive Digital Twin for Real-Time HTTP(S) Intrusion Detection and Threat Intelligence

- Developed a lightweight digital twin system combining machine learning and probabilistic trie models, achieving over 90% detection accuracy across 3.3M+ HTTP(S) honeypot sessions.
- Designed a sliding window retraining strategy to adapt to emerging behavioral patterns, successfully validated on an additional 800K-session honeypot dataset.
- Implemented attacker fingerprinting and hierarchical taxonomy mapping, enabling fine-grained behavioral insights across 7+ user-agent groups and 4 major cloud providers.

Distributed AI Intrusion Detection System with Enhanced Privacy

- Developed feature extraction pipelines from raw network data, addressing data heterogeneity for attack detection.
- Built and optimized deep learning and autoencoder models, improving network traffic classification accuracy.
- Deployed a federated learning system with gradient separation, ensemble methods, and local differential privacy, enhancing resilience against Byzantine attacks and strengthening privacy guarantees.

PRESENTATION

Speaker, RIPE 90 (May 2025): Presented collaborative research on IoT security and intrusion detection, in partnership with Global Cyber Alliance and Yokohama National University. Link: https://ripe90.ripe.net/programme/meeting-plan/iot-wg/