Jingwen Shi

Personal Website | Google Scholar | Linkedin | shijingwen9@gmail.com | (517) 974-8921 | East Lansing, MI 48823

EDUCATION

Research Areas: Mobile Systems & Network Security, AI + Systems/Networks, Cloud Computing

- **College of Engineering, Michigan State University** Michigan, USA
  Ph.D. Candidate, Computer Science - GPA:4.0 Aug. 2019 - Flexible, anytime in 2025
  Award Highlight: AT&T Security Award, Google Bug Bounty for High-Severity and High-Quality Reports, Freshgogo Website Bug Bounty Reward, ACM MobiCom Best Community Paper, MSU 2020/2022 Fellowship
- **SIAT, University of Chinese Academy of Sciences** Beijing, China
  M.S.E, Computer Applied Technology Sept. 2016 - May 2019
  Award Highlight: Google Girl Hackathon Best Practical Award, First-Class Scholarship
- **College of Computer Science and Electronic Engineering, Hunan University** Hunan, China
  B.E., Information Security Sept. 2012 - May 2016
  Award Highlight: Graduated with Honor (summa eq.), 2013/2014 First-Class Scholarships, 2015 National Encouragement Scholarship, First Prize of National Student Innovation Program, First Prize of Robocup

SKILLS

Python, C/C++, Java, Android, iOS, Tensorflow, Keras, PyTorch, scikit-learn, Linux, Matlab, Wireshark, srsRAN, USRP, 3GPP/GSMA/IETF standards, QXDM, QPST, ADB, Hadoop, MongoDB, PostgreSQL, OpenSSL, MySQL

INTERNSHIP

AT&T Lab – *Senior Associate Student Intern* Jun. 2024 - Aug. 2024, USA

- Designed an **AI-based traffic monitoring platform for 5G/4G IoT networks** to analyze unknown IP traffic, supporting time-series extraction, application clustering, traffic mapping, and anomaly detection
- Built an **interactive visualization website** using *Plotly* to display temporal and geographic IoT/IoV results
- Enhanced robustness by leveraging clustered application features and applying *machine learning (One-class SVM, DBSCAN, LSTM)*, *statistical analysis (Normal distribution, KDE)*, and *signal processing (FFT, STL)*
- Presented to three market teams and a research team, collaborating to advance the project **online**
- Submitted **one patent** application filed with the U.S. Patent Office
- Submitted 5G IoV research **proposal as Co-PI** for long-term collaboration between AT&T Lab and MSU

Los Alamos National Lab – *Research Intern* Jun. 2021 - Aug. 2021, USA

- Built a *Cyber-Physical System (CPS)* simulation testbed for a HVAC system, integrating a complex Finite State Machine and differential equations using programming language *Julia*
- Investigated the reconstruction problem of Cyber-Physical Systems from measurement data and developed a *machine learning* (*Ordinary Least Squares*, *SVD*) framework achieving an accuracy of **97%**

Alibaba Group – *Research and Development Intern* Jan. 2019 - Jun. 2019, China

Project 1. Robust Cloud Resource Allocation with Uncertainty Prediction

- Collaborated with R&D teams to analyze a real-time cloud platform and define an AI-driven research focus on *dynamic uncertainty prediction* for worst-case QPS to optimize resource allocation
- Deployed deep learning algorithms on *Hadoop* and *Alibaba EagleEye*, a distributed tracing and monitoring system to conduct large-scale evaluations
- Designed and developed *deep learning* models (*Bayesian Neural Networks*, *CNN*, *LSTM*) to enhance QPS prediction at Taobao, achieving an accuracy of **99.8%**

Project 2. Swift and Intelligent Anomaly Detection for Large-Scale Cloud Systems

- Collaborated closely with a production team to improve the anomaly detection algorithm for identifying abnormal containers
- Developed a ML framework (*Isolation Forest, Joint probability, 3-Sigma*) optimized for low-latency responses on high-volume system footprints (e.g., CPU, memory)
- Evaluated on clusters of 1,000+ virtual machines, reducing false alarms by **95%** with **one publication** [JST'19]

PROJECT EXPERIENCE

Project 1. LLM for Security Cross-Analysis of Standards [Participant] Oct. 2024 - Jan. 2025, USA

- Utilized *LLM* (*Gemini*, *GPT 3.5*, *LLaMA Embedding*, *RAG*, *Prompt Engineering*) to assist in retrieving, comparing, and analyzing information across standards
- Identified **three vulnerabilities** enabling *Rich Communication Services* hijacking, as ground truth for *LLM*

Project 2. Mobile Operating System Security [Lead] Aug. 2023 - Oct. 2024, USA

- Discovered **two vulnerabilities** in mobile operating systems, specifically in the *Android*'s *Linux* kernel
- Developed and validated **two attacks**: (1) a **DoS-ALL** attack blocking network access over *Wi-Fi*, *4G LTE*, and *5G NR*, and (2) an **SMS Name-Spoofing** attack fabricating messages with arbitrary sender names
- Discovered **two modem vulnerabilities** enabling media traffic hijacking (via *H.264* codecs) during video calls by analyzing the *baseband architecture*, including *DSP* and *RTOS*
- Test vulnerabilities on *iOS* by implementing proposed attacks in *Swift* and analyzing *Darwin* source code
- Implemented all proposed attacks by developing *malware* for *Android*, *VPN* services, and *Wi-Fi* routers
- Reported vulnerabilities were identified as **high severity and high quality** by **Google Bug Bounty and Vulnerability Reward Programs**
- Invited to submit a 2023 Google ASPIRE proposal as Co-PI and authored two research papers [ACM Mobicom'24, ACM TON'24 Reviewing]

Project 3. Security and Spoofing Attacks on Emergency 911 [Co-Lead] Aug. 2022 - Jan. 2025, USA

- Constructed the cellular network simulation testbed of Emergency 911 from device to *5G/4G* core network using *USRP*, *srsRAN*, *Open IMS Core*, and *Linphone VoIP Client*
- Successfully defended DoS and free-data attacks against 911 services using *TLS encryption*
- Authored three research papers [ACM Mobicom'22 (SIGMOBILE Highlight, MobiCom Best Community Paper, AT&T Security Award), ACM GetMobile'23, IEEE TON'24]

Project 4. Deep Learning-based Inference on Wireless Network [Lead] Jun. 2019 - May. 2022, USA

- Applied *machine learning* (*DBSCAN*, *Moving Average*) and *computer vision* (*Mask RCNN*, *DSFD*, *ResNet50*) algorithms to reveal user call behaviors and speaking patterns with time errors are below **9%**
- Identified **two vulnerabilities** in *5G/4G radio protocols* (*PHY*, *MAC*, *RLC*, *PDCP*), enabling the association of radio identities with user identities, achieving accuracy rates of **89% to 98%**
- Designed and implemented a **DoS attack against wireless channel** that stealthily mutes a user's voice during cellular phone calls, utilizing *USRP*, *FPGA*, *UHD*, *srsRAN*, *signal booster antennas*, and *C/C++*
- Proposed a defense against side-channel attacks by enhancing radio protocols, achieving a success rate of **100%**
- Analyzed PDCP-layer radio packets using *deep learning* models (*LSTM*, *ResNet50*, *Siamese Neural Networks*) to identify the company in an Interactive Voice Response call, achieving an accuracy of **93%**
- Authored two research papers and one poster presentation [CERIAS'24 Poster, IEEE CNS'23, Preprint]

Project 5. Cloud Systems [Participant/Lead] Aug. 2020 - Oct. 2021, China

Project. Distributed Spatial Index for Large-Scale IoT and Vehicle Data

- Collaboratively designed a distributed spatial index for storing large-scale mobility IoT and vehicle GPS data
- Assisted in implementing the spatial index on *HBase* and *MongoDB*, reducing I/O traffic by **70%**
- Authored one research papers [IEEE IPCCC'18]

Project. Distributed Storage and Computing System for Satellite Images

- Designed and implemented the data pipeline connecting *HDFS* to *PostgreSQL* for satellite images
- Authored two patents [CN 110147353 A, CN 110147904 B]

Project 6. Visual Search Engine with Crawler System [Sole Contributor] Feb. 2016 - Apr. 2016, China

- Designed and implemented a crawler system to collect Chinese laws, cases, regulations, and news related to information security using *Python*, *SQLite3*, and *Scrapy*
- Developed a search engine with interactive visualization features using *Django*, *Ajax*, *PageRank*, and *D3.js*
- Optimized the *PageRank* algorithm using *linear algebra* to function efficiently with limited CPU and memory
- Awarded the **Outstanding Undergraduate Graduation Project**