

ADRIAN SHUAI LI

305 N University S, West Lafayette, IN 47907

765-775-3121

li3944@purdue.edu

[linkedin.com/in/adrian-shuai-li-616487107](https://www.linkedin.com/in/adrian-shuai-li-616487107)

[homepage](#)

EDUCATION

Purdue University

Ph.D. in Computer Science, Advisor: Elisa Bertino, GPA: 4.0/4.0

Expected Graduation Date: May 2026

West Lafayette, IN

University of Calgary

M.Sc. in Computer Science, Advisor: Rei Safavi-Naini, GPA: 4.0/4.0

Jan 2020

Master Thesis: A Capability-based System to Enforce Context-aware Permission Sequences

Calgary, Canada

Wuhan University

BSc. in Computer Science, GPA: 3.7/4.0

Jul 2017

Wuhan, China

RESEARCH POSITIONS

Purdue University

May 2021 – Present

Graduate Research Assistant

West Lafayette, IN

- Engineered an LLM-based malware transformation framework that generated 600+ functional variants across 10 families, reducing AV detection rates by up to 31% and achieving up to 91% attack success against ML-based classifiers (Best Paper Award [C3])
- Developed adaptation methods using adversarial training and KL-divergence to maintain accuracy under distribution shifts (image classification + intrusion detection), enabling models to generalize without additional labels (Best Paper Award [C2])
- Built a CNN-based malware classifier with transfer learning capability, reusing knowledge from fully labeled datasets to new datasets with limited labels, maintaining high detection performance while reducing labeling costs (Computer & Security [J1])
- Developed a label-free drift adaptation framework that automatically adapts malware classifiers to evolving threats using unsupervised domain adaptation with high-confidence pseudo-labeling, eliminating labeling and enabling continuous deployment on real-world malware streams
- Investigated robust malware classifiers resilient against Control-Flow-Graph (CFG)-based adversarial attacks, strengthening ML detectors against evasion techniques
- Mentored a junior PhD student on malware research, coordinating experiments and guiding publications

Cisco Research

May 2023 – Aug 2023

Research Intern III

San Jose, CA

- Built an end-to-end malware detection pipeline by disassembling binaries with IDA Pro, extracting CFGs, and generating instruction embeddings with a pre-trained BERT model, enabling scalable training and evaluation on large malware corpora
- Developed and optimized a graph neural network-based malware classifier that achieved high accuracy on evolving variants under limited-label settings, demonstrating robustness and applicability for enterprise security products (NDSS'25 [C1])
- Automated malware feature extraction, retraining, and evaluation workflows, reducing manual overhead and accelerating the transition from research prototype to enterprise-ready systems
- Presented findings at Cisco Open Mic Talks (Nov 2023), engaging both research and product teams

Aviatrix Systems

May 2022 – Aug 2022

Software Developer Intern

Champaign, IL

- Implemented an ETL pipeline to extract, transform, and load large-scale network telemetry data from Elasticsearch into Spark dataframes, supporting ML analytics and real-time anomaly detection at production scale
- Designed and replayed realistic network attack traces across AWS VPCs to generate high-fidelity training data, integrating seamlessly into the company's security monitoring systems
- Delivered a network intrusion detection system using Spark MLlib that achieved 97% detection accuracy, demonstrating feasibility for scalable deployment in cloud-native environments

University of Calgary

Sep 2017 – Jan 2020

Graduate Research Assistant

Calgary, Canada

- Conducted research on distributed authorization and resilient IoT systems, resulting in publications at SAC-MAT'22 ([C6]) and IoT S&P'18 (Best Paper Award [C8])

PUBLICATIONS

Peer-Reviewed Journal Articles

- [J1] [Computers & Security] Bhardwaj, S., **Li, A. S.**, Dave, M., & Bertino, E. (2024). Overcoming the Lack of Labeled Data: Training Malware Detection Models Using Adversarial Domain Adaptation. *Computers & Security*. doi: [10.1016/j.cose.2024.103769](https://doi.org/10.1016/j.cose.2024.103769)

Peer-Reviewed Conference Papers

- [C1] [NDSS'25] **Li, A. S.**, Iyengar, A., Kundu, A. and Bertino, E. (2025). Revisiting Concept Drift in Windows Malware Detection: Adaptation to Real Drifted Malware with Minimal Samples. *Network and Distributed System Security Symposium 2025*. doi: [10.14722/ndss.2025.240830](https://doi.org/10.14722/ndss.2025.240830)
- [C2] [CIC'25][Best paper award] **Li, A. S.**, Bertino, E., Dang, X. H., Singla, A., Tu, Y., & Wegman, M. N. (2025). Maximizing Information in Domain-Invariant Representation Improves Transfer Learning. *The 11th IEEE International Conference on Collaboration and Internet Computing*. URL <https://arxiv.org/abs/2306.00262>. To Appear
- [C3] [TPS'25][Best paper award] Ajwad Akil, M., **Li, A. S.**, Karim, I., Iyengar, A., Kundu, A., Parla, V. and Bertino, E. (2025). LLMalMorph: On The Feasibility of Generating Variant Malware using Large-Language-Models. *The 7th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*. URL <https://arxiv.org/abs/2507.09411>. To Appear
- [C4] [INDIN'24] Imtiaz Mostafiz, M., Kim, E., **Li, A. S.**, Bertino, E., Jun, M. B. G., & Shakouri, A. (2024). Adversarial Domain Adaptation for Metal Cutting Sound Detection: Leveraging Abundant Lab Data for Scarce Industry Data. *IEEE International Conference on Industrial Informatics*. doi: [10.1109/INDIN58382.2024.10774310](https://doi.org/10.1109/INDIN58382.2024.10774310)
- [C5] [ICIT'23] **Li, A. S.**, Bertino, E., Wu, R. T., & Wu, T. Y. (2023). Building Manufacturing Deep Learning Models with Minimal and Imbalanced Training Data Using Domain Adaptation and Data Augmentation. In *2023 IEEE International Conference on Industrial Technology*. doi: [10.1109/ICIT58465.2023.10143099](https://doi.org/10.1109/ICIT58465.2023.10143099)
- [C6] [SACMAT'22] **Li, A. S.**, Safavi-Naini, R., & Fong, P. W. (2022). A Capability-based Distributed Authorization System to Enforce Context-aware Permission Sequences. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*. doi: [10.1145/3532105.3535014](https://doi.org/10.1145/3532105.3535014)
- [C7] [FPS'19] Avizheh, S., Safavi-Naini, R., & **Li, S.** (2020). Secure Logging with Security Against Adaptive Crash Attack. In *Foundations and Practice of Security: 12th International Symposium*. Springer International Publishing. doi: [10.1007/978-3-030-45371-8_9](https://doi.org/10.1007/978-3-030-45371-8_9)
- [C8] [IoT S & P'18][Best paper award] Doan, T. T., Safavi-Naini, R., **Li, S.**, Avizheh, S., K, M. V., & Fong, P. W. (2018). Towards a resilient smart home. In *Proceedings of the ACM SIGCOMM 2018 Workshop on IoT Security and Privacy*. doi: [10.1145/3229565.3229570](https://doi.org/10.1145/3229565.3229570)

Book

- [B1] Bertino, E., Bhardwaj, S., Cicala, F., Gong, S., Karim, I., Katsis, C., Lee, H., **Li, A.S.** and Mahgoub, A.Y. (2023). *Machine Learning Techniques for Cybersecurity*. Springer Nature. doi: [10.1007/978-3-031-28259-1](https://doi.org/10.1007/978-3-031-28259-1)

Patent

- [U1] Wegman, M., Tu, Y., Dang, X. H., Singla, A., **Li, A.S.** (2024). Autoencoder with Generative Adversarial Networks for Transfer Learning Between Domains. U.S. Patent Application No. 18/129,540

Preprints Under Review

- [P1] **Li, A. S.**, Iyengar, A., Kundu, A., & Bertino, E. (2024). Transfer Learning for Security: Challenges and Future Directions. URL <https://arxiv.org/abs/2403.00935>

Technical Blog Posts (Full list at: <https://gloryer.github.io/blog/>)

- [B1] **Li, A. S.** (2021). A Technical Look into Flotera Ransomware. URL [flotera-ransomware](https://gloryer.github.io/blog/flotera-ransomware)

- [B2] **Li, A. S.** (2021). An Analysis of the Recent Ransomware Families. URL [ransomware-families](https://gloryer.github.io/blog/ransomware-families)

- [B3] **Li, A. S.** (2019). Understanding Linux Random Number Generator. URL [lrng](https://gloryer.github.io/blog/lrng)

AWARDS AND HONORS

Internet Society NDSS Fellowship
Academic and Research Achievement Recognition
Best paper awards
Mitacs Globalink Graduate Fellowship
Academic Excellence Scholarship

Internet Society
Purdue University Computer Science Department
IoT S&P'18, IEEE CIC'25, IEEE TPS'25
Mitacs
Wuhan University

SERVICE

Reviewer: WIRES Data Mining and Knowledge Discovery; Digital Threats: Research and Practice; ICDE'24; ESORICS'24; ACSAC'23–24; SACMAT'22 & '24; IJCNN'25
Committee Roles: Vice President — University of Calgary CS Graduate Society (2018–2019); Program Committee — Security Researchers and Industry Experts Talks (2018)
Volunteer: Student Volunteer — Selected Areas in Cryptography (2018)

TEACHING

Purdue University

Graduate Teaching Assistant: CS 242 Introduction to Data Science

Fall 2025

West Lafayette, IN

Purdue University

Guest Lecturer: CS 59000-DSP Data Security And Privacy

Spring 2023 and 2024

West Lafayette, IN

Purdue University

Graduate Teaching Assistant: CS 182 Foundations of Computer Science

Spring 2021

West Lafayette, IN

INVITED TALKS

Cisco Open Mic Talks

Nov 2023

Domain Adaptation for Malware Classification Using Control Flow Graphs

Virtual

TECHNICAL SKILLS

Programming & ML: Python, PyTorch, TensorFlow, Spark MLlib, SQL

Infrastructure & Cloud: Docker, AWS EC2/S3/security groups, Azure, GCP, Ansible, Elasticsearch, MongoDB

Security Tools & Frameworks: IDA Pro, Wireshark, Snort, Suricata, Kali Linux, MITRE ATT&CK, VMware

Other Tools: Node.js, Django, Git, Apache JMeter, Postman

REFERENCES

Prof. Elisa Bertino

Samuel Conte Professor of Computer Science

Purdue University

Email: bertino@purdue.edu

Dr. Ashish Kundu

Head of cybersecurity research

Cisco Research

Email: ashkundu@cisco.com

Dr. Arun Iyengar

Co-Founder and Partner

Intelligent Data Management and Analytics, LLC

Email: aki@akiyengar.com