Zitao Chen

zitaoc@ece.ubc.ca | https://zitaoc.github.io

Professional Experience

Assistant Professor, Department of EECS, **University of Kansas** — Oct 2025 - present

Research Technician, University of British Columbia — Jul 2020 - Feb 2021

Education

University of British Columbia

Ph.D. in Electrical and Computer Engineering — Jan 2022 - Oct 2025

M.A.Sc. in Electrical and Computer Engineering — Sep 2018 - Jun 2020

Advisor: Karthik Pattabiraman

China University of Geosciences (Wuhan)

B.Eng. in Information Security — Sep 2014 - Jun 2018

Research Interests

Trustworthy machine learning; Responsible AI; Cybersecurity

Publications [Google Scholar]

[CCS’25] **Zitao Chen**, Karthik Pattabiraman **“Anonymity Unveiled: A Practical Framework for Auditing Data Use in Deep Learning Models”** *In Proceedings of the 2025 ACM Conference on Computer and Communications Security*. *Acceptance rate: 13.9%* [Paper] [Code]

Earned all Artifact Badges: *Artifact Available, Functional and Results Reproduced*

[NDSS’25] **Zitao Chen**, Karthik Pattabiraman **“A Method to Facilitate Membership Inference Attacks in Deep Learning Models”** *The ISOC Network and Distributed Systems Security Symposium*, 2025. *Acceptance rate: 16.1%* [Paper] [Code]

Earned all Artifact Badges: *Artifact Available, Functional and Results Reproduced*

[NDSS’24] **Zitao Chen**, Karthik Pattabiraman **“Overconfidence is a Dangerous Thing: Mitigating Membership Inference Attacks by Enforcing Less Confident Prediction ”** *The ISOC Network and Distributed Systems Security Symposium*, 2024. *Acceptance rate: 15%* [Paper] [Code]

Earned all Artifact Badges: *Artifact Available, Functional and Results Reproduced*

[AsiaCCS’23] **Zitao Chen**, Pritam Dash, Karthik Pattabiraman **“ Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on Deep Neural Networks ”** *The 18th ACM ASIA Conference on Computer and Communications Security*, 2023. *Acceptance rate: 16%* [Paper] [Code]

[DSN’21] **Zitao Chen**, Guanpeng Li, Karthik Pattabiraman **“A Low-cost Fault Corrector for Deep Neural Networks through Range Restriction”** *The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2021. *Acceptance rate: 16.3%* [Paper] [Code]

Best paper award runner up (2 out of 295 submissions)
Selected for IEEE Top Picks in Test and Reliability (1 of 7 papers)
Invited for submission to the IEEE Design & Test (DnT) journal
Our algorithm (called Ranger) was adopted by Intel’s OpenVINO [Details]

[DSN'21] Pritam Dash, Guanpeng Li, **Zitao Chen**, Mehdi Karimi, Karthik Pattabiraman **"PID-Piper: A Framework for Recovering Robotic Vehicles From Physical Attacks"** *The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2021. *Acceptance rate: 16.3%* [Paper] [Code]

Best paper award (1 out of 295 submissions)

[ISSRE'20] **Zitao Chen***, Niranjhana Narayanan*, Bo Fang, Guanpeng Li, Karthik Pattabiraman, Nathan DeBardeleben, **"TensorFI: A Flexible Fault Injection Framework for TensorFlow Applications"** *The 31st IEEE International Symposium on Software Reliability Engineering*, 2020. *Acceptance rate: 25.7%* [Paper] [Code]

[SC'19] **Zitao Chen**, Guanpeng Li, Karthik Pattabiraman, Nathan DeBardeleben **"BinFI: An Efficient Fault Injector for Safety-Critical Machine Learning Systems"** *In Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, 2019. *Acceptance rate: 20.9%* [Paper] [Code]

Finalist for SC Reproducibility Initiative (3 out of 344 submissions)

Journal papers -

[TDSC] Pritam Dash, Guanpeng Li, **Zitao Chen**, Mehdi Karimi, Karthik Pattabiraman **"Feed-Forward Controller-Based Recovery for Robotic Vehicles from Physical Attacks"** *IEEE Transactions on Dependable and Secure Computing*, 2025

[DnT] **Zitao Chen**, Guanpeng Li, Karthik Pattabiraman **"A Low-cost Fault Corrector for Deep Neural Networks through Range Restriction"** *IEEE Design & Test*, 2025 (Invited submission to IEEE DnT based on our DSN'21 paper)

[TDSC] Niranjhana Narayanan, **Zitao Chen**, Bo Fang, Guanpeng Li, Karthik Pattabiraman, and Nathan DeBardeleben **"Fault Injection for TensorFlow Applications"** *IEEE Transactions on Dependable and Secure Computing*, 2022 [Code]

[FGCS] **Zitao Chen**, Wei Ren, Yi Ren and Kim-Kwang Raymond Choo **"LiReK: A Lightweight and Real-time Key Establishment Scheme for Wearable Embedded Devices by Gestures or Motions"** *Future Generation Computer Systems*, 2018

Short papers -

[CCS'24 Doctoral Symposium] **Zitao Chen "Catch Me if You Can: Detecting Unauthorized Data Use in Training Deep Learning Models"** *In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS'24)*. 3 pages. 2024

[IOLTS'20] Karthik Pattabiraman, Guanpeng Li, **Zitao Chen**, **"Error Resilient Machine Learning for Safety-Critical Systems: Position Paper"** *IEEE 26th International Symposium on On-Line Testing and Robust System Design*, 4 pages, 2020. *Invited paper*

Honors and Awards

- **ACM CCS Young Scholars Development Travel Grant** 2025
- **ACM CCS Student Travel Grant** 2025
- **IEEE Top Picks in Test and Reliability** (1 of 7 papers) 2024
  - Recognizing the most impactful publications in Computer Systems Reliability from 2018-2024
  - Selected in the final list of Top Picks and invited for submission to the IEEE Design & Test journal
- **DAAD AInet Fellowship** (50 awardees worldwide) 2024
- **Brandwajn Graduate Fellowship (twice)** (given to the top-ranked student in the ECE dept) 2023, 2024
- **ACM CCS Doctoral Symposium Travel Grant** 2024

- **UBC Public Scholar Award** (45 awardees university-wide) 2022
- **UBC Four Year Doctoral Fellowship** (awarded to the top PhD applicants) 2022
- **Best paper award at DSN** (DSN is the flagship venue in Dependable Computing) 2021
- **Best paper award runner up at DSN** (DSN is the flagship venue in Dependable Computing) 2021
- **Finalist for SC Reproducibility Initiative** (SC is the flagship venue in High Perf. Computing) 2019
- **UBC Faculty of Applied Science Graduate Award** 2019-2024

Teaching Experience

Instructor	Introduction to Aritficial Intelligence (University of Kansas)	2026
Teaching assistant	Building Modern Web Applications (University of British Columbia)	2019
Guest lecturer	Adversarial Machine Learning (Texas State University)	2024

Invited Talks

Technical University of Berlin, Germany	Host: Prof. Konrad Rieck	October 2024
Technical University of Darmstadt, Germany	Host: Prof. Thomas Schneider	October 2024

Services

Conference organization

- Co-chair of the IEEE Workshop on Dependable and Secure Machine Learning @ DSN'26 2026

Program committee

- ACM Conference on Computer and Communications Security (CCS) 2026
- The ISOC Network and Distributed System Security Symposium (NDSS) 2026
- The Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2026
- The IEEE European Symposium on Security and Privacy (EuroS&P) 2026
- ACM/SIGAPP Symposium On Applied Computing (SAC) 2026
- The European Dependable Computing Conference (EDCC) 2026
- ACM Workshop on Large AI Systems and Models with Privacy and Security Analysis @ CCS'25 2025
- IEEE Workshop on Reliable and Secure AI for Software Engineering @ ISSRE'25 2025

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC) 2025
- IEEE Transactions on Parallel and Distributed Systems (TPDS) 2025
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) 2023, 2024
- Elsevier Neural Networks 2025
- Elsevier Computer & Security 2024, 2025