Kaleel Mahmood

82 Fairlane Dr, Shelton, CT, 06484 | kaleel.mahmood@uconn.edu |https://kaleel-mahmood.scholar.uconn.edu

Education

University of Connecticut, Storrs, CT

- **Assistant Professor in Residence**, Dept. of Computer Science and Engineering, January 2022-Present
- **Assistant Research Professor,** Dept. of Electrical and Computer Engineering, July 2022-Present (joint appointment)
- **PhD in Computer Science and Engineering**, January 2018-December 2021
  Dissertation*: Designing Deep Networks for Adversarial Robustness and Security*
  Major Advisor: Marten van Dijk
  Associate Advisors: Shengli Zhou, Jinbo Bi, Caiwen Ding
- **M.S. in Computer Science and Engineering**, August 2017
- **M.S. in Electrical Engineering**, August 2016
  Major Advisor: Marten van Dijk
- **B.S. in Electrical Engineering**, May 2013
  Senior Project Advisor: Shengli Zhou

Research Areas

- Adversarial Machine Learning, AI, Deep Learning, Computer Vision and Hardware Security.

Research Work

- *Adversarial Machine Learning*: Design and research of robust machine learning algorithms for classification and recognition tasks. Code implementations in PyTorch and TensorFlow/Keras. Six accepted publications in the field. Ongoing work focusing on the attack, defense and transferability theories of adversarial examples in the image domain.

- *Applied Secure Machine Learning*: Analysis and application of adversarial attacks to new machine learning domains including Spiking Neural Networks (SNNs), Multi-Task Learning (MTL) and game theory. Four papers currently in submission.

- *Systems Security*: Evaluation and design of the security of hardware (physically uncloneable functions) and real imaging systems (ballot marking devices for U.S. elections). Two accepted publications in the field, with one more in submission.

Experience

ASSISTANT PROFESSOR IN RESIDENCE| UCONN | JANUARY 2022 - PRESENT

- Conducted research in adversarial machine learning. Worked on interdisciplinary research projects within the department and with the University of Massachusetts at Amherst, North Carolina State University and CWI Amsterdam.
- Advised PhD, M.S. and undergraduate students in machine learning research.
- Developed and taught courses in computer science including principles of programming (CSE 1729), discrete mathematics (CSE 2500) and C programming (CSE 3100).

SECURE COMPUTING LABORATORY GRADUATE RESEARCHER | UCONN | DECEMBER 2015-DECEMBER 2021

- Designed and developed adversarial machine learning attacks on Convolutional Neural Networks and Vision Transformers. Coded defenses to evasion attacks in PyTorch and TensorFlow/Keras.
- Programmed machine learning attacks on physically unclonable functions (PUFs).
- Mentored M.S. students and undergraduates on research projects.

CYBER SECURITY INTERNSHIP| UNITED TECHNOLOGIES RESEARCH CENTER | MAY 2016-AUGUST 2016

- Developed a cyber security defense for IoT and embedded devices based on code partitioning.
- Implemented moving target defense based security measures on unmanned aerial vehicles.

OPTICAL IMAGING LABORATORY GRADUATE RESEARCHER | UCONN | APRIL 2013-DECEMBER 2015

- Worked on image processing and computer vision research projects including 3D integral imaging with unknown sensor poses and counterfeit integrated circuit detection using x-ray imaging and deep neural networks.

UNDERWATER SENSOR NETWORK LABORATORY RESEARCHER | UCONN | MAY 2012-AUGUST 2013

- Implemented asynchronous localization algorithms in C language.
- Conducted real time testing and analysis of algorithms in aquatic environments using digital signal processing boards and acoustic modems.

Publications (Google Scholar Link)

1. **K. Mahmood**, R. Mahmood and M. van Dijk, "On the Robustness of Vision Transformers to Adversarial Examples", Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV) 2021, paper available here.

2. H. Peng, S. Huang, T. Zhou, Y. Luo, C. Wang, Z. Wang, J. Zhao, X. Xie, A. Li, T. Geng, **K. Mahmood**, W. Wen, X. Xu, C. Ding, "AutoReP: Automatic ReLU Replacement for Fast Private Network Inference", (in submission) arXiv preprint, arXiv:2308.10134, 2023, E-print available here.

3. L. Zhang, X. Liu, **K. Mahmood**, C. Ding and H. Guan. "Dynamic Gradient Balancing for Enhanced Adversarial Attacks on Multi-Task Models", (in submission) arXiv preprint, arXiv:2305.12066, 2023, E-print available here.

4. S. Huang, H. Fang, **K. Mahmood**, et al., "Neurogenesis Dynamics-inspired Spiking Neural Network Training Acceleration", (in submission) arXiv preprint, arXiv:2304.12214, 2023, E-print available here.

5. B. Kivilcim, D. Zhou, Z. Shi, and **K. Mahmood**, "An Efficient Approach to Wireless Firmware Update Based on Erasure Correction Coding", International Conference on Information Technology-New Generations, pp. 431-435, paper available here.

6. Y. Wang, N. Xu, S. Huang, **K. Mahmood**, D. Guo, C. Ding, W. Wen, and S. Rajasekaran, "Analyzing and Defending against Membership Inference Attacks in Natural Language Processing Classification", in 2022 IEEE International Conference on Big Data, pp. 5823-5832, 2022, paper available here.

7. E. Rathbun, **K. Mahmood**, S. Ahmad, C. Ding and M. van Dijk, "Game Theoretic Mixed Experts for Combinational Adversarial Machine Learning", (in submission) arXiv preprint arXiv:2211.14669, 2022, E-print available here.

8. S. Ahmad, B. Fuller and **K. Mahmood**, "Inverting Biometric Models with Fewer Samples: Incorporating the Output of Multiple Models", IEEE International Joint Conference on Biometrics (IJCB), 2022, paper available here.

9. N. Xu, **K. Mahmood**, H. Fang, E. Rathbun, C. Ding and W. Wen, "Securing the Spike: On the Transferability and Security of Spiking Neural Networks to Adversarial Examples", (in submission) arXiv preprint, arXiv:2209.03358, 2022, E-print available here.

10. **K. Mahmood**, P. H. Nguyen, L. M. Nguyen, T. Nguyen and M. Van Dijk, "Besting the Black-Box: Barrier Zones for Adversarial Example Defense," in IEEE Access, vol. 10, pp. 1451-1474, 2022, paper available here.

11. **K. Mahmood**, R. Mahmood, E. Rathbun and M. van Dijk, "Back in Black: A Comparative Evaluation of Recent State-Of-The-Art Black-Box Attacks", IEEE Access, vol. 10, pp. 998-1019, 2022, paper available here.

12. **K. Mahmood**, D. Gurevin, M. van Dijk and P. Nguyen, "Beware the Black-Box: On the Robustness of Recent Defenses to Adversarial Examples", Entropy, 23, 1359, 2021, paper available here.

13. P. Nguyen, D. Sahoo, C. Jin, **K. Mahmood** and M. van Dijk, "The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks", Conference on Cryptographic Hardware and Embedded Systems, Volume 4, 2019.

14. **K. Mahmood** and D. M. Shila, "Moving target defense for Internet of Things using context aware code partitioning and code diversification", 2016 IEEE 3rd World Forum on Internet of Things, pp. 329-330, 2016.

15. **K. Mahmood**, P. Carmona, S. Shahbazmohamadi, F. Pla, and B. Javidi, "Real-time automated counterfeit integrated circuit detection using x-ray microscopy", in *Applied Optics*, vol. 54, D25-D32, 2015.

16. **K. Mahmood**, K. Domrese, P. Carroll, H. Zhou, X. Xu and S. Zhou, "Implementation and Field Testing of On-Demand Asynchronous Localization", in *Asilomar Conference on Signals, Systems and Computers,* Pacific Grove, California, Nov. 3-6, 2013.

17. P. Carroll, **K. Mahmood**, S. Zhou, H. Zhou, X. Xu and J.-H. Cui, "On-Demand Asynchronous Localization for Underwater Sensor Networks", in *IEEE Transactions on Signal Processing*, vol.62, no.13, pp.3337-3348, July 1, 2014.

18. X. Xu, S. Zhou, **K. Mahmood**, L. Wei, and J.-H. Cui, "Study of Class-D Power Amplifiers for Underwater Acoustic OFDM Transmissions", in *Oceans/IEEE,* San Diego, Sept. 23-27, 2013.

19. P. Carroll, S. Zhou, **K. Mahmood**, H. Zhou, X. Xu, and J.-H. Cui, "On-Demand Asynchronous Localization for Underwater Sensor Networks", in *Proc. of IEEE/MTS OCEANS conference*, Hampton Roads, Virginia, Oct. 14-19, 2012.

Proposals and Funding

- *Machine Learning Systems for Mitigating Microgrid Cyber-Physical Attacks* –Submitted to Eversource Energy, March 2023.
- *Authentication and Verification of 3D Printed Components through Speckle Patterns and Machine Learning* – Submitted to National Institute for Undersea Vehicle Technology (NIUVT), June 2022.

- *Stealthy Underwater Communication, Detection and Localization* - Submitted to National Institute for Undersea Vehicle Technology (NIUVT), June 2022.
- *Machine Learning for Integrated Sensing and Communication Design* - In progress, to be submitted to National Science Foundation (NSF), 2024.

Teaching and Mentorship

- Systems Programming (CSE 3100: 137 students, spring 2023, fall 2023)
- Introduction to Discrete Systems (CSE 2500: 99 students, spring 2022, fall 2022, fall 2023)
- Introduction to Principles of Programming (CSE 1729: 143 students, spring 2022)
- Introduction to Computing for Engineers (CSE 1010: 236 students, fall 2022)
- Deep Learning and Neural Networks (CSE 5099: 8 students, summer 2019, spring 2022, fall 2022)
- Major advisor for 1 PhD student, co-advisor for 2 M.S. students and research mentor for 3 undergraduate students.
- *NSF REU Trustable Embedded Systems Security Research Mentor 2022, 2023* – Mentored undergraduate and high school students in the National Science Foundation Research Experience for Undergraduates (NSF REU) for the Trustable Embedded Systems Security research program. Mentorship resulted in one publication.
- *NSF REU Cyber Aquatic Systems Research Mentor* - Taught C#, Java and C, as well as basic research techniques to undergraduate researchers in the NSF REU 2013 for the Cyber Aquatic Systems research program.

Leadership/Service

- *Reviewer for IEEE Transactions on Dependable and Secure Computing*
- *Reviewer for IEEE Transactions on Neural Networks and Learning Systems*
- *Reviewer for IEEE Military Communications Conference (MILCOM)*
- *Graduate Assistance in Areas of National Need* (GAANN) Fellowship- Awarded funding from August 2013 to December 2016 and from August 2019 to May 2021 to work at the University of Connecticut in a U.S. department of education designated area of national need (computer security).
- *Team Leader Underwater Network Localization Senior Design* - Leader of senior design team to create hardware solutions for localization algorithms. Took 3rd place in the University of Connecticut Senior Design Competition.

Personal

- United States Citizen (Born in the U.S), Native English Speaker

  Other Activities:
  UConn Badminton Club Captain (2021- 2022)
  UConn Badminton Club Vice President (2014-2017)
  UConn Racquetball Graduate Student Group Organizer (2014-2020)
  Tennis Instructor (2010-Present)