Belkhouja, Taha

School of Electrical Engineering and Computer Science
Washington State University
Pullman, WA

tahabelkhouja.github.io
taha.belkhouja@gmail.com

Research Interests

My general research interests are in the area of robust, secure, and trustworthy machine learning. My current research focuses on developing efficient algorithms and theory to improve reliability and security of deep learning algorithms for diverse problem settings and data domains. Specific research thrusts include:

- Robust deep learning for the time-series domain with diverse applications including mobile health, smart grid management, human activity monitoring, and agriculture automation.
- Uncertainty quantification for robust and effective Human-ML collaborative systems using conformal prediction.
- Trustworthy machine learning for sequential data with a focus on out-of-distribution detection.

Education

Washington State University, Pullman, WA 2019 – May 2024
Doctor of Philosophy in Computer Science - GPA 3.96
Advisor: Prof. Jana Doppa
- Thesis: *Novel Directions for Robust and Secure Machine Learning: Algorithms and Theory*

University of Idaho, Moscow, ID
Master of Science in Electrical Engineering - GPA: 4.0 2017 – 2019
Advisor: Prof. Sameh Sorour
- Thesis Title: *Efficient Security Schemes for Wireless Implantable Medical Devices*

University of Padova, Padova, Italy
Exchange Program in Information Technology Engineering Program 2015 – 2016
- Focus Area: *Optical Communication.*

Higher School of Communications of Tunis (SUP'COM), Ariana, Tunisia
Engineering degree in Telecommunication - *Graduated with Excellence* 2013 – 2016
- Thesis Title: *Experimental Characterization of Distributed Fiber Optic Pressure Sensors*

Preparatory School For Engineering Studies of Tunis (IPEIT), Tunis, Tunisia
University first cycle studies 2011 – 2013
- Major: Mathematics-Physics

Professional Appointments

Software Engineer Intern June 2023 – Aug 2023
Google Geo, Google, USA
- Developing Machine Learning technologies for Google Maps.

Research Intern June 2022 – Aug 2022
Computer Science Lab - Stanford Research Institute (SRI) International, USA
- Trustworthy machine learning with a focus on sequential data: Out-of-distribution detection for sequential traffic data with multiple driving agents using deep learning and neuro-symbolic regularization.

Research Assistant May 2021 – Current
EECS Department - Washington State University, USA,
- Novel Directions for Reliable and Safe Machine Learning: Algorithms and Theory.

Teaching Assistant Aug 2019 – May 2021
EECS Department - Washington State University, USA
- CptS 315 - Introduction to Data Mining (Spring-2020, Spring-2021)
- CptS 570 - Machine Learning (Fall-2020)
- CptS 223 - Advanced Data Structures in C++ (Fall-2020)
- CptS 451 - Introduction to Database Systems (Spring-2020)
- CptS 440/540 - Artificial Intelligence (Fall-2019)

Summer Research Appointment May 2019 – Aug 2019
EECS Department - Washington State University, USA
- Investigation of security vulnerabilities in machine learning algorithms

Teaching Assistant Jan 2017 – May 2019
ECE Department - University of Idaho, USA
- ECE 241 - Digital Logic Circuit Lab
- ECE 311 - Microelectronics I Lab

Research Assistant Jan 2017 – May 2019
ECE Department - University of Idaho, USA
- Light-weight security schemes for wireless Implantable Medical Devices

Graduation Project Internship Mar 2016 – Aug 2016
University of Padova, Padova, Italy
- Design and experimental characterization of distributed fiber optic pressure sensors based on a novel structure

Research Intern Jun 2015 – Aug 2015
GresCom Research Lab, Tunis, Tunisia
- Study and analysis of end-to-end performances of Free Space Optical transmission systems

Software Engineering Intern Oct 2014 – Apr 2015
DisruptCK, Tunisia
- Design and implementation of a desktop application for detecting, identifying and recognition of humans in video streams

Awards and Honors

- Voiland College of Engineering, Outstanding Graduate Research Assistant Award 2023
- School of EECS, Outstanding Graduate Research Assistant Award 2023
- Voiland College of Engineering, Outstanding EECS Graduate Teaching Assistant from Award 2021
- School of EECS, Outstanding Graduate Teaching Assistant in Computer Science Award 2021
- Mahmoud M. Dillsi Family Graduate Fellowship 2020
- Alfred Suksdorf Fellowship 2019
- Third Prize in UIdaho 3-Minute Thesis Competition 2019
- Best Graduate Research Presentation Award, ECE Spring Colloquium 2018
- Distinctive Entrepreneurial Project Prize for Sustainable Development 2014
- Top 5% in the National Qualification Exam for Engineering Schools Entrance 2013

Publications

Journal Papers

1. T. Belkhouja, Y. Yan, and J. Doppa. **Out-of-Distribution Detection in Time-Series Domain: A Novel Seasonal Ratio Scoring Approach**. To appear in *ACM Transactions on Intelligent Systems and Technology (TIST), 15(1): 9:1-9:24*, 2023.

2. T. Belkhouja, Y. Yan, and J. Doppa. **Dynamic Time Warping based Adversarial Framework for Time-Series Domain**. *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 45(6): 7353-7366*, 2022.

3. T. Belkhouja and J. Doppa. **Adversarial Framework with Certified Robustness for Time-Series Data via Statistical Features**. *Journal of Artificial Intelligence Research (JAIR), 73: 1435-1471*, 2022.

4. T. Belkhouja, J. Doppa. **Analyzing Deep Learning for Time-Series Data through Adversarial Lens in Mobile and IoT Applications.** *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 39(11): 3190-3201*, 2020.

5. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani. **Biometric-based Authentication Scheme for Implantable Medical Devices during Emergency Situations**. *Future Generation Computer Systems - Elsevier, 98, 109-119,* 2019.

6. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani. **Symmetric Encryption Relying on Chaotic Henon System for Secure Hardware-Friendly Wireless Communication of Implantable Medical Systems**. *Journal of Sensor and Actuator Networks, 7(2):21*, 2018.

Conference Papers

1. T. Belkhouja*, D. Hussein*, G. Bhat, and J. Doppa. **Energy-Efficient Missing Data Recovery in Wearable Devices: A Novel Search-based Approach**. ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED), 2023. (* denotes equal contribution)

2. S. Ghosh, Y. Shi, T. Belkhouja, Y. Yan, J. Doppa, and B. Jones. **Probabilistically Robust Conformal Prediction**. Uncertainty in Artificial Intelligence (UAI), 2023.

3. T. Belkhouja and J. Doppa. **Adversarial Framework with Certified Robustness for Time-Series Data via Statistical Features**. International Joint Conference on Artificial Intelligence (IJCAI), 2023.

4. T. Belkhouja*, S. Ghosh*, Y. Yan, and J. Doppa. **Improving Uncertainty Quantification of Deep Classifiers via Neighborhood Conformal Prediction: Novel Algorithm and Theoretical Analysis**. 37th AAAI Conference on Artificial Intelligence, 2023. (* denotes equal contribution)

5. T. Belkhouja, Y. Yan, and J. Doppa. **Training Robust Deep Models for Time-Series Domain: Novel Algorithms and Theoretical Analysis**. 36th AAAI Conference on Artificial Intelligence, 2022.

6. T. Belkhouja*, D. Hussein*, G. Bhat, and J. Doppa. **Reliable Machine Learning for Wearable Activity Monitoring: Novel Algorithms and Theoretical Guarantees**. International Conference on Computer-Aided Design (ICCAD), 2022. (* denotes equal contribution)

7. T. Belkhouja, S. Sorour, M. Hefeida. **Role-based Hierarchical Medical Data Encryption for Implantable Medical Devices**. IEEE Global Communications Conference (GlobeCom), 2019.

8. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani. **Light-Weight Solution to Defend Implantable Medical Devices Against Man-In-The-Middle Attack**. IEEE Global Communications Conference (GlobeCom), 2018.

9. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani. **Salt Generation for Hashing Schemes based on ECG readings for Emergency Access to Implantable Medical Devices**. International Symposium on Networks, Computers and Communications (ISNCC), 2018.

10. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani. **Light-weight encryption of wireless communication for implantable medical devices using henon chaotic system**. Wireless Networks and Mobile Communications International Conference (WINCOM), 2017.

11. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani. **New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control**. IEEE Global Communications Conference (GlobeCom), 2017.

Professional and Outreach Activities

Conference Tutorials Organization

- Lead Organizer of the Tutorial on *Recent Advances in Robust Time-Series ML* at AAAI Conference, 2024.

Program Committee

- International Conference of Machine Learning (ICML), 2024
- AAAI Conference on Artificial Intelligence (AAAI), 2024
- AAAI Conference on Artificial Intelligence (AAAI) - Student Program, 2023
- AAAI Conference on Artificial Intelligence (AAAI) - Safe and Robust AI Track, 2024
- Conference on Neural Information Processing Systems (NeurIPS), 2023
- International Conference of Machine Learning (ICML), 2023
- International Conference on Artificial Intelligence and Statistics (AISTATS), 2023
- AAAI Conference on Artificial Intelligence (AAAI), 2023

Graduate and Undergraduate Mentoring

- Subhankar Ghosh, CS PhD Student
  Project: Advances in conformal prediction based uncertainty quantification for effective human-ML collaborative systems.
- Chibuike Ugwu, CS PhD Student
  Project: Conformal prediction based uncertainty quantification for clinical health assessment in the small-data setting.
- Yuanjie Shi, CS PhD Student
  Project: Advances in conformal prediction based uncertainty quantification for effective human-ML collaborative systems.
- Dheeraj Vurukuti, MS Thesis Student
  Project: Robust classifiers for malware detection on mobile platforms.
- Nithyashree Senguttuvan, MS Thesis Student)
  Project: Time-series anomaly detection in healthcare applications
- Tyler Cleveland, Undergraduate Researcher
  Project: Adversarial robustness for audio classifiers

Organizations

- **TEDxUIdaho:** Team member, Volunteer coordinator and Speaker curator, Moscow, ID. 2019
- **TEDxSupCom:** Team leader, Webmaster and Community builder, Tunisia. 2014
- **IT Innovation organization (NetLinks):** Technical manager, Tunisia. 2015-2016

Technical/Professional Events

- Volunteer for AAAI Conference on Artificial Intelligence 2023
- Mentor and Judge for Digital AgAthon (AgAID Institute) 2023
- Volunteer for AAAI Conference on Artificial Intelligence 2020
- Volunteer for Conference on Neural Information Processing Systems (NeurIPS) 2019
- TEDxSupCom second edition 2015
- IONS Tunisia: First North African International OSA (The Optical Society) Network of Students conference 2015
- OpenUp: Cultural event supporting diversity and underrepresented students minorities 2015
- LUPA: Lighting Up Africa Tunisia, Optics and Photonics conference 2015
- National Engineering School Forum: Higher School of Communications of Tunis representative 2014
- ACM ICPC: Tunisian Collegiate Programming Contest 2013

Languages

- Arabic: Native
- French: Bilingual
- English: Professional