

# 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 field of the robustness of machine learning systems. My current research focuses on developing efficient learning and optimization algorithms to improve reliability and safety of deep learning algorithms for diverse settings and data spaces. My current work includes:

- Robust deep learning for the time-series domain with diverse applications including human activity recognition and mobile health.
- Trustworthy machine learning for sequential data with a focus on Out-Of-Distribution detection.
- Uncertainty quantification for reliable machine-learning using conformal prediction.

## EDUCATION

**Washington State University**, Pullman, WA 2019 – Current

Doctor of Philosophy in Computer Science - GPA 3.96

Advisor: Prof. Jana Doppa

- Research Topic: *Novel Computational Tools for Reliable and Safe Machine Learning: Algorithms, Theory, and Applications*

**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 (SUPCOM)**, 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

**Research Intern**

June 2022 – Aug 2022

Computer Science Lab - SRI International, USA

- Trustworthy machine learning with a focus on sequential data.

**Research Assistant**

May 2021 – Current

EECS Department - Washington State University, USA,

- Novel Computational Tools for Reliable and Safe Machine Learning: Algorithms, Theory, and Applications.

- Teaching Assistant** Aug 2019 – current  
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

- VCEA Outstanding Teaching Assistant within the School of EECS 2021
- Best Graduate Student Teaching Assistant in Computer Science 2021
- Mahmoud M. Dillsi Family Graduate Fellowship 2020
- Alfred Suksdorf Fellowship 2019
- Third Prize in UIIdaho 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

### PAPERS UNDER REVIEW

1. S. Ghosh, T. Belkhouja, 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.
2. T. Belkhouja, Y. Yan, and J. Doppa. **Detecting Out-of-Distribution Time-Series data with Deep Generative Models.** Transactions on Intelligent Systems and Technology (TIST), 2022.
3. T. Belkhouja, Y. Yan, and J. Doppa. **Dynamic Time Warping based Adversarial Framework for Time-Series Data.** Revision of IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022.

## JOURNAL PAPERS

1. T. Belkhouja and J. Doppa. **Adversarial Framework with Certified Robustness for Time-Series Data via Statistical Features**. Journal of Artificial Intelligence Research (JAIR), 2022.
2. 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), 2020.
3. 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, 2019.
4. 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, 2018.

## CONFERENCE PAPERS

1. D. Hussein\*, T. Belkhouja\*, 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)
2. 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.
3. T. Belkhouja, S. Sorour, M. Hefaida. **Role-based Hierarchical Medical Data Encryption for Implantable Medical Devices**. IEEE Global Communications Conference (GlobeCom), 2019.
4. 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.
5. 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.
6. 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.
7. 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

### REVIEW ACTIVITIES

- PC Member for the 37th AAAI Conference on Artificial Intelligence - Safe and Robust AI Track, 2023
- Elsevier: Future Generation Computer Systems, 2019
- IEEE Communications Letters, 2019
- Next Generation Systems and Networks Symposium-IWCMC, 2019
- Next Generation Systems and Networks Symposium-IWCMC, 2018
- IEEE Access, 2017

## MENTORSHIP

- Have mentored Tyler Cleveland, an undergraduate student pursuing a Computer Science degree at WSU during Summer and Fall 2020. Tyler aims to pursue graduate school in the field of Machine Learning. I started with Tyler as a mentor for the Research Experiences for Undergraduates (REU) program and continued mentoring him in the Fall session as he has extended his work in the research project.

## ORGANIZATIONS

- **TEDxUIIdaho:** 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 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
- German: Basic