Belkhouja, Taha

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

Contact:

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 the robustness and reliability of deep learning models. My current work is focusing on studying and improving the robustness of deep learning models for the time-series domain for diverse applications including mobile health and finance. My research goal is to improve the reliability and safety of deep learning algorithms for diverse settings and data spaces.

Education

Washington State University, Pullman, WA 2019 – Current
Doctor of Philosophy in Computer Science - GPA 3.96
Advisor: Prof. Jana Doppa
- Research Topic: *Robust Machine Learning for Time-Series Data*

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 Assistant, Washington State University, USA, EECS Department May 2021 – Current
- Efficient learning and optimization algorithms to improve the robustness of deep learning models specific to time-series data.

Teaching Assistant, Washington State University, USA, EECS Department Aug 2019 – current
- 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, Washington State University, USA, EECS Department May 2019 – Aug 2019
- Investigation of security vulnerabilities in machine learning algorithms

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

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

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

Research Intern, Gres'Com, Tunis, Tunisia Jun 2015 – Aug 2015
• Study and analysis of end-to-end performances of Free Space Optical transmission systems

Software Engineering Intern, DisruptCK, Tunisia Oct 2014 – Apr 2015
• 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 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

Papers Under Review

1. T. Belkhouja, Y. Yan, and J. Doppa. **Detecting Out-of-Distribution Time-Seires data with Deep Generative Models**. 38th Conference on Uncertainty in Artificial Intelligence (UAI), 2022.

2. T. Belkhouja, Y. Yan, and J. Doppa. **Dynamic Time Warping based Adversarial Framework for Time-Series Data**. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021.

3. T. Belkhouja, D. Hussein, G. Bhat, and J. Doppa. **Reliable Machine Learning for Wearable Activity Monitoring: A Novel Statistical Optimization Approach**. International Conference on Computer-Aided Design (ICCAD), 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. 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.

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

3. 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.

4. 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.

5. 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.

6. 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

- 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

- **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

- 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