

# Moustafa F. Alzantot

---

## CONTACT INFORMATION

1310 Barry Ave.,  
Apt. 205,  
Los Angeles, CA 90025,  
USA.

Voice: +1 (310) 948-6252  
Web: <http://cs.ucla.edu/~malzantot>  
E-mail: [malzantot@ucla.edu](mailto:malzantot@ucla.edu)

## RESEARCH INTERESTS

Machine Learning, Deep Learning, Pervasive Sensing, Internet of Things.

## EDUCATION

**University of California, Los Angeles (UCLA)**, Los Angeles, CA.  
*Ph.D. Student, Computer Science Department* **Oct. 2014 - Present**  
• Advisor : Prof. Mani Srivastava

**University of California, Los Angeles (UCLA)**, Los Angeles, CA.  
*M.Sc., Computer Science Department* **Oct. 2014 - Mar. 2017**  
GPA: 3.80/4.0  
• Completed Courses:  
- Introduction to Pattern Recognition - Embedded Systems  
- Machine Learning Algorithms - Energy Aware Systems  
- Big Data: Modeling and Mining Social Media - Reasoning with Partial Beliefs  
- Advanced Computer Networks - Graphs and Network Flows

**Faculty of Engineering, Tanta University**, Tanta, Egypt **Jul. 2008**  
*B.Sc., Computer Engineering and Automatic Control*  
• Cumulative Grade: **Distinction with Honor** (Percentage : **90%**, Equivalent GPA: **3.84/4.0**).  
• Cumulatively ranked **the 1<sup>st</sup>** in the Department of Computer Engineering and Automatic Control Systems among 150 students.  
• Graduation Project: "City Guide: a Mobile Phone Application for LBS"

## WORK EXPERIENCE

**University of California, Los Angeles (UCLA)** **Oct. 2014 - Present**  
*Graduate Student Researcher and Teaching Assistant*  
• Advisor: Prof. Mani Srivastava  
• Conducting research on privacy-aware mobile sensing. Modified the Android OS sensing stack to enhance the mobile phones users privacy.

**Facebook**, Menlo Park, USA **June 2018 - Sep. 2018**  
*Machine Learning Software Engineering Intern*  
• I am working with the Ads ranking team to improve the personalized selection of ads for Facebook users.

**Google**, Mountain View, USA **June 2016 - Sep. 2016**  
*Software Engineering Intern*  
• I worked with Android location and context-awareness team on implementing algorithms that increase the reliability and quality of WiFi based localization in Android.

**Qualcomm Research Center**, San Diego **June 2015 - Sep. 2015**  
*Research Intern*  
• Designed and implemented a machine learning health monitoring application using low-power sensors of a wearable device.

**Thirdwayv, Inc.** **March 2014 - Sep. 2014**  
*Part-time Software Consultant*

- Contributed to the design and implementation of an SDK for Internet of Things devices.

**Alcatel-Lucent Bell Laboratories**, Antwerp, Belgium. **May 2013 - Aug. 2013**  
*Research Intern, Scalable Systems Research Department*

- Contributed to the Travel-Dashboard project. Developed programs to visualize and model travel patterns of passengers in London underground.

**Google Switzerland GmbH**, Zurich, Switzerland. **Sep. 2011 - Nov. 2011**  
*Software Engineer Intern*

- Worked with Gmail team to implement settings in the widely used email service.

**Egypt-Japan University for Science and Technology**, Egypt. **Sep. 2010 - Nov. 2013**  
*Research Assistant*

Working on a number of research projects including: CrowdInside, UPTIME, and UnLoc.

**Faculty of Engineering, Tanta University**, Egypt. **Mar. 2009 - Sep. 2014**  
*Teaching Assistant*

- Preparing and delivering lab experiments and tutorials.
- Discussing and grading homework assignments.

**FuoEg Solutions and Consultancy**, Egypt. **Jan. 2009 - July, 2010**  
*Consultant*

- Offering help for the design and implementation of mobile Android and iOS applications.
- Delivering training for junior developers on Android development.

**Fujitsu Services**, Egypt. **Summer 2006**  
*Software Developer Intern*

- Designing and implementing a retail management system.

HONORS AND AWARDS

- 4<sup>th</sup> place award in the NSF 2018 Differential Privacy Synthetic Data Challenge.
- Google Cloud Award for achieving the 1<sup>st</sup> place in the 2<sup>nd</sup> round *NIPS 2017 targeted adversarial attacks* competition.
- UCLA Graduate Division Award, 2017-2018.
- Recipient of the UCLA Graduate Division Award, 2016-2017.
- Listed in the Marquis Who's Who in the World (32nd Edition), 2015.
- UCLA Graduate Division Award, Fall 2014.
- The Common Market for Eastern and Southern Africa (COMESA) 2013 innovation award.
- Invited for Microsoft Research Cambridge Ph.D. Summer School 2013.
- MIT Technology Review Magazine: "Smartphone App Crowdsources Indoor Floorplans", CrowdInside work cited, Sep. 2012.
- Scientific American Magazine: "Mixed Signals: Smart Phone Sensors Recruited to Deliver Indoor GPS", UnLoc work cited, July 2012.
- Microsoft Research (Project Hawaii) best mobile computing project award in E-JUST, Spring 2011.
- Excellence scholarship for graduate studies at Egypt-Japan University of Science and Technology, Fall 2010.
- Distinction award with the degree of honor for graduation from the department of Computer Engineering, Tanta University, July 2008.
- Bronze medal in the nation-wide programming contest held as part of annual week of Egyptian universities, March 2007.

INVENTIONS AND PATENTS

- Value-Based Information Flow Tracking in Software Packages. Saman Zonous, Gabriel Salles-Loustau, **Moustafa Alzantot**, Mani Srivastava.

US Patent Application No: 62/567,498.

- Unsupervised Indoor Localization and Heading Direction Estimation.  
R. R. Choudhury, H. Wang, N. Roy, S. Sen, Moustafa Youssef, A. Elgohary, and **Moustafa Farid**.  
Patent Application No: 2013/ 069178, USA.

#### RESEARCH PAPERS

- Generating Natural Language Adversarial Examples.  
**Moustafa alzantot**, Yash Sharma, Ahmed Elgohary, BoJhang Ho, Mani Srivastava, Kai-wei Chang.  
EMNLP 2018 : Conference on Empirical Methods in Natural Language Processing. (**Acceptance Rate ~ 23.2%**)
- GenAttack: Practical Black-box Attacks with Gradient-Free Optimization.  
**Moustafa Alzantot**, Yash Sharma, Huan Zhang, Supriyo Chakraborty, Cho-Jui Hsieh, Mani Srivastava.  
*Accepted in GECCO 2019, The Genetic and Evolutionary Computation Conference.*
- JustWalk: A Crowdsourcing Approach for the Automatic Construction of Indoor Floorplans.  
Moustafa El-Hamshaary, **Moustafa Alzantot**, Moustafa Youssef.  
*IEEE Transactions on Mobile Computing.*
- Did you hear that? Adversarial Examples Against Automatic Speech Recognition Model.  
**Moustafa Alzantot**, Bharathan Balaji, Mani Srivastava.  
Machine Deception Workshop, NIPS 2017.
- RSTensorFlow: GPU Enabled TensorFlow for Deep Learning on Commodity Android Devices.  
**Moustafa Alzantot**, Yingnan Wang, Zhengshuang Ren, Mani Srivastava.  
Embedded and Mobile Deep Learning (EMDL 2017) workshop (with ACM MobiySys 2017).
- SenseGen: A Deep Learning Architecture for Synthetic Sensor Data Generation.  
**Moustafa Alzantot** , Supriyo Chakraborty, Mani B. Srivastava  
IEEE BICA'17 (co-located with IEEE Percom 2017).
- SeleCon: Scalable IoT Device Selection and Control Using Hand Gestures.  
Amr Alanwar, **Moustafa Alzantot**, Bo-Jhang Ho, Paul Martin, Mani Srivastava  
IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI 2017).
- CryptoImg: Privacy Preserving Processing Over Encrypted Images  
M Tarek Ibn Ziad, Amr Alanwar, **Moustafa Alzantot** , Mani Srivastava  
IEEE Security and Privacy in the Cloud (SPC) 2016 (co-located with IEEE CNS 2016).
- SemanticSLAM: Using Environment Landmarks for Unsupervised Indoor Localization.  
Heba Abdelnasser, Reham Mohamed, Ahmed Elgohary, **Moustafa Farid**, He Wang, Souvik Sen, Romit Choudhury, Moustafa Youssef.  
IEEE Transactions on Mobile Computing (TMC), 2016.
- CrowdInside: Automatic Construction of Indoor Floorplans.  
**Moustafa Alzantot**, Moustafa Youssef  
The 20th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL GIS) 2012, Redondo Beach, USA. (**Acceptance Rate ~ 15.4%**)
- No Need to War-Drive: Unsupervised Indoor Localization.  
H. Wang, S. Sen, Ahmed Elgohary, **Moustafa Farid**, Moustafa Youssef, Romit R. Choudhury  
ACM Tenth International Conference on Mobile Systems, Applications, and Services (ACM Mo-

biSys) 2012.(**Acceptance Rate** ~ **17%**)

- UPTIME: Ubiquitous Pedestrian Tracking using Mobile Phones.  
**Moustafa Alzantot**, Moustafa Youssef  
IEEE Wireless Communications and Networking Conference (IEEE WCNC) 2012, Paris, France.

RESEARCH DEMOS  
AND POSTERS

- (Demo) **Moustafa Alzantot**, Moustafa Youssef. Demonstrating CrowdInside : A System for the Automatic Construction of Indoor Floor-plans. IEEE PerCom 2013.
- (Demo) H. Wang, S. Sen, A. Mariakakis, Romit R. Choudhury, Ahmed Elgohary, **Moustafa Farid**, Moustafa Youssef, Unsupervised indoor localization. ACM MobiSys 2012.
- (Poster) **Moustafa Alzantot**, Reem elkholly, Amal Lotfy, Moustafa Youssef. IPS: Ubiquitous Indoor Positioning System. MobiQuitous 2011.
- (Demo) **Moustafa Alzantot**, Muhammed Hataba, Moustafa Youssef. Classroom7: Please Make Sure Your Phones are Switched On!. MobiQuitous 2011.

PROFESSIONAL  
ACTIVITIES

- Reviewer: IEEE Communications Magazine 2019.
- Reviewer: IEEE Transactions on Mobile Computing 2018.
- Reviewer: ACM Proceedings on Interactive, Multimedia, Wearable and Ubiquitous Technologies (IMWUT 2019).
- Reviewer: ACM Proceedings on Interactive, Multimedia, Wearable and Ubiquitous Technologies (IMWUT 2017).
- Reviewer: IEEE Transactions on Mobile Computing 2016.
- Reviewer: International Conference on the Internet of Things 2015.
- Reviewer: IEEE Journal on Selected Areas in Communications - 2014 Special Issue on Location-Awareness for Radios and Networks.
- Reviewer: The Fifth International Conference on Mobile Computing, Applications and Services (MobiCASE 2013).
- Reviewer: IEEE International Wireless Communications and Mobile Computing Conference, 2013.
- Reviewer: IEEE Wireless Communications Magazine Special Issue on Cloud Computing.

INVITED TALKS

- DEFCON 26, CAAD Village. **Las Vegas, USA, Aug 2018**  
*Title: Practical adversarial attacks against challenging models environments.*
- Distributed Analytics and Information Science International Technology Alliance (DAIS-ITA) Annual Meeting, **London, UK. Sep, 2017**  
*Title: Adversarial Attacks on Machine Learning.*
- SoCal Data Science Conference **Los Angeles, CA, USA. Oct, 2017**  
*Title: Introduction to Deep Reinforcement Learning.*

TEACHING  
EXPERIENCE

- **CS35L Software Construction Labartory**, CS Dept, UCLA **Fall 2017**
- **CS112 Modeling Uncertainty in Information Systems**, CS Dept., UCLA. **Winter 2017**
- **CS188 Scalable Internet Services**, Computer Science Department, UCLA. **Fall 2016**
- **Computer Networks Security** Course, Faculty of Engineering, Tanta University. **2014**
- **Software Engineering** Course, Faculty of Engineering, Tanta University. **2009**
- **Introduction to E-Commerce** Course, Faculty of Engineering, Tanta University. **2009**
- **Android Development** Course, FuoEg Solutions and Consultancy, Tanta, Egypt. **2009**

COMPUTER SKILLS

- **Programming:** C++, C, Java, Python, JavaScript.

- **Mobile Apps Development:** iOS, Android, NDK.
- **Machine Learning Frameworks:** TensorFlow, PyTorch, Caffe2, Scikit-Learn, Theano, Keras, Pandas, R, Weka.
- **Others:** AOSP,  $\LaTeX 2_{\epsilon}$ , Gnuplot, vim, MatLab, NS2.

LANGUAGES            Arabic, and English.

- PROFESSIONAL  
MEMBERSHIPS
- Student member of ACM.
  - Student member of IEEE, IEEE Communication Society.
  - Member of the Egyptian Engineering Syndicate.

- EXTRACURRICULAR  
ACTIVITIES
- Volunteer in Egypt-Scholars NGO.
  - Volunteered for organizing Imagine Cup 2009 international finals, and Google days (gegypt 2012) events held in Cairo, Egypt.
  - Microsoft Student Partner in Tanta university during the academic year 2008/2009.
  - Enjoys reading novels and history books, listening to music, and playing intellectual games.