Dr. Mohammad Malekzadeh (Research Associate at Imperial College London)

- E-mail: m.malekzadeh@imperial.ac.uk
- Homepage: mmalekzadeh.github.io
- Code: http://github.com/mmalekzadeh
- Papers: https://scholar.google.co.uk/citations?user=xZr9WQMAAAAJ&hl=en

1. EDUCATION

2017 (JAN) – 2021 (JAN)

- **Ph.D. in Computer Science**
- School of Electronic Engineering and Computer Science
- Queen Mary University of London, UK
- Thesis Title**:** "Machine Learning Algorithms for Privacy-preserving Behavioral Data Analytics"
- Advisors: Prof. Andrea Cavallaro, Dr. Richard G. Clegg, and Dr. Hamed Haddadi

2009 (SEP) - 2011 (SEP)

- **M.Sc. in Computer Networks**
- Computer Engineering Department
- Sharif University of Technology, Tehran, Iran
- Thesis Title**:** "Link's Sign Prediction in Signed Social Networks"
- Thesis Grade: 19.8 / 20 | Overall GPA: 17.28 / 20

2004 (SEP) / 2008 (SEP)

- **B. Sc. in Software Engineering**
- Engineering Department
- Shahid Chamran University, Ahvaz, Iran
- Thesis Title: "Persian CAPTCHA"
- Thesis Grade: 20 / 20 | Overall GPA: 17.43 / 20

2. EMPLOYMENT

2020 (JUN) – Present	**Research Associate Information Processing and Communications Lab** *Imperial College London, UK*
2019 (JUN) – 2019 (SEP)	**PhD Intern in Machine Learning at Brave Research (Brave.com/Research)** *Brave Software, London, UK*
2018 (APR) – 2018 (NOV)	**Research Assistant in Databox Project (databoxproject.uk)** *Imperial College London, UK*
2017 (NOV) – 2020 (APR)	**Teacher Assistant** *Imperial College London & Queen Mary University of London, UK*
2014 (FEB) – 2016 (DEC)	**Head of Information and Communication Technology Institute (PGU)** *Persian Gulf University, Bushehr, Bushehr, Iran*
2016 (JUN) – 2016(SEP)	**Software Engineer at ChetorPro (ChetorPro)** *Business Engineering 360 (BE360.ir), Iran*
2014 (SEP) – 2016(FEB)	**Project Manager and Software Engineer at Shanab Project (Shanab)** *Persian Gulf University, Bushehr, Bushehr, Iran*
2012 (JAN) – 2016 (DEC)	**Lecturer in Computer Engineering (PGU)** *Persian Gulf University, Bushehr, Bushehr, Iran*

3. AREA OF INTERESTRS and EXPERTIES

My main focus is on privacy and machine learning. I have been working on machine learning systems and algorithms for privacy-preserving personal data analytics, particularly for data generated by the users at the edge. At the moment, I am working on privacy-preserving model training and inference with applications in distributed/federated learnings. I love coding, particularly for shaping new research ideas! Also, in my research career, I have had the opportunity to work on: *Deep Neural Networks, Complex Networks Modeling, Game Theory and its Applications, and Software Development.*

4. PUBLICATIONS

1. 2021: **M. Malekzadeh**, A. Borovykh, D. Gündüz. **Honest-but-Curious Nets: Sensitive Attributes of Private Inputs can be Secretly Coded into the Entropy of Classifiers' Outputs**, *ACM Conference on Computer and Communications Security (CCS).*
2. 2021: **M. Malekzadeh**, R. G. Clegg, A. Cavallaro, and H. Haddadi. **DANA: Dimension-Adaptive Neural Architecture for Multivariate Sensor Data**, *ACM Journal on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), and, ACM conference for Ubiquitous Computing (UbiComp).*
3. 2021: **M. Malekzadeh**, B. Hasircioglu, N. Mital, K. Katarya, M. E. Ozfatura, D. Gündüz. **Dopamine: Differentially Private Secure Federated Learning on Medical Data**. *AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI)*
4. 2021: F. Mo, A. Borovykh, **M. Malekzadeh**, H. Haddadi, S. Demetriou. **Layer-wise Characterization of Latent Information Leakage in Federated Learning**, *ICLR Workshop on Distributed and Private Machine Learning (DPML).*
5. 2020: **M. Malekzadeh**, D. Athanasakis, H. Haddadi, B. Livshits. **Privacy-Preserving Bandits.** *Conference on Machine Learning and Systems (MLSys)*
6. 2020: **M. Malekzadeh**, R. G. Clegg, A. Cavallaro, and Hamed Haddadi. **Privacy and Utility Preserving Sensor-Data Transformations**. Pervasive and Mobile Computing Journal, Elsevier.
7. 2020: E. Lisi, **M. Malekzadeh**, H. Haddadi, F. D. Lau, S. Flaxman. **Modeling and Forecasting Art Movements with CGANs.** Royal Society Open Science Journal, The Royal Society.
8. 2019: **M. Malekzadeh**, R. G. Clegg, A. Cavallaro, and H. Haddadi. **Mobile Sensor Data Anonymization**. ACM/IEEE Conference on Internet-of-Things Design and Implementation (IoTDI)
9. 2018: **M. Malekzadeh**, R.G. Clegg, A. Cavallaro, and H. Haddadi. **Protecting Sensory Data against Sensitive Inferences**. EuroSys Workshop on Privacy by Design in Distributed Systems, Porto, Portugal.
10. 2018: **M. Malekzadeh**, R. G. Clegg, and H. Haddadi. **Replacement AutoEncoder: A Privacy-Preserving Algorithm for Sensory Data Analysis**. ACM/IEEE Conference on Internet-of-Things Design and Implementation (IoTDI)
11. 2017: R. Gharibi, **M. Malekzadeh**. **Gamified Incentives: A Badge Recommendation Model to Improve User Engagement in Social Media Sites**, Journal of Advanced Computer Science and Applications 8(5), 2017.
12. 2014: Ma. Barghandan, **M. Malekzadeh**, A. Safdel and I. Mazloomzadeh. **A Multi-Generational Social Learning Model: the Effect of Information Cascade on Aggregate Welfare**, IEEE/ACM Conference on Advances in Social Networks Analysis and Mining (ASONAM)
13. 2011: **M. Malekzadeh**, M.A. Fazli, P. J. Khalilabadi, H. R. Rabiee, M.A. Safari. **Social Balance and Signed Network Formation Games**, KDD Social Network Mining and Analysis (SNA-KDD)
14. 2008: **M. Malekzadeh** and M. Bohlool. **Persian CAPTCHA System to Prevent Automatic Subscribing of Software Robots in Web Pages**, 13th National CSI Computer Science, Kish, Iran, 2008, (in Persian).

- ***Under Review / Preprints:***

15. 2021: G. Siracusano, S. Galea, D. Sanvit, **M. Malekzadeh**, H. Haddadi, G. Antichi, R. Bifulco. **Running Neural Network Inference on the NIC**, Under Review.
16. 2021: F. Mo, A. Borovykh, **M. Malekzadeh**, H. Haddadi, S. Demetriou. **Quantifying Information Leakage from Gradients**, Under Review.

- ***Tutorial:***

17. 2020: A. Cavallaro, **M. Malekzadeh**, and A. S. Shamsabadi, **Deep Learning for Privacy in Multimedia**, ACM International Conference on Multimedia, Seattle, United States, (tutorial's hompage).

- ***Dataset:***

18. 2018: **MotionSense Dataset:** Human Activity and Attribute Recognition from Smartphone's Motion Sensors.
   - https://github.com/mmalekzadeh/motion-sense
   - www.kaggle.com/malekzadeh/motionsense-dataset

- ***Technical Reports, Abstracts, Etc.:***

19. 2019: **"Fairness in Algorithmic Decision Making".**
20. 2018: **"Privacy-Preserving Sensor Data Analysis for Edge Computing".**
21. 2017: **"Towards Privacy-Preserving IoT Data Publishing"**

5. TEACHING EXPERIENCES

- Teacher Assistant of an undergraduate course (Sensing and IoT), 2018-2019 at Imperial College London.
- Teacher Assistant of a graduate course (Data Analytics), and two undergraduate courses (Software Engineering, and Computer Security), 2017-2019 at Queen Mary University of London.
- Teacher of "Fundamental Of Programming (C Language)", "Computer Architecture", "Operating Systems Concepts", "Software Engineering", "Advanced Programming (Java Language), "Numerical Analysis", "Technical and Scientific Presentation", "Complex and Dynamical Networks", and "Operating Systems Lab", 2011-2016, at Persian Gulf University

6. TECHNICAL SKILLS

- **Machine Learning:** Python, PyTorch, Tensorflow, Keras, NumPy, SciPy, Scikit-Learn, Pandas;
- **Software Engineering Experiences:** In the past, I have experienced HTML, CSS, JavaScript, AngularJS, NodeJS, PHP Laravel Framework; MySQL and MongoDB. I have designed small to mid-sized systems.

7. AWARDS, HONORS, GRANTS

- [2020] Our submission to the **ITU's global challenge** has been chosen as **the best solution for the sub-challenge: "Privacy-Preserving AI/ML for Healthcare"**.
- [2019] I was awarded a grant of **£290** covering registration to **Privacy Preserving Machine Learning workshop** at **CCS conference** in London.
- [2019] I was awarded a **$700** grant covering travel expenses to **IoTDI 2019** conference in Montreal, Canada.
- [2018] Our team earned **first place** in Imperial College AIHack 2018 for Brooklyn Housing Challenge. Nov2018.
- [2018] I was accepted on to the **Alan Turing Institute Data Study Group**, covering all the travelling and accommodation expenses, April 2018.
- [2018] I was awarded a grant covering registration to top-tier systems conference **EuroSys 2018** in Porto, Portugal.
- [2018] I was accepted on to the **2nd CommNet2 PhD Spring School**, covering all the travelling and accommodation expenses, March 2018.
- [2017] I was awarded a **$30000** grant of **Microsoft Azure** storage and compute for one year in 2018.
- [2017] I was awarded a grant of **$500** covering travel and lodging to top-tier systems conference **EuroSys 2017** in Belgrade, Serbia.
- [2017] I was awarded a **Ph.D. studentship**, to work on privacy-preserving personal data analytics, from **Queen Mary University of London, Life Sciences Initiative** in 2017.
- [2014] I was ranked **1th** among more than **30** faculty members of engineering department at Persian Gulf University as **the best teacher of the year**, 2014.
- [2009] I was ranked **10th** among more than **10,000** participants taking part in the **M.Sc. entrance exam of IT Engineering** in Iran, 2009.
- [2008] I was ranked **2th** among more than **50** computer engineering students **during the bachelor's degree** in Shahid Chamran University of Ahvaz, 2008.

8. SERVICE and EXPERIENCES

- Reviewer: Nature Communications, Privacy Enhancing Technologies Symposium, IEEE Transactions on Mobile Computing, World Wide Web Journal, The Web Conference, ACM Transactions on Internet of Things, Symposium on Experimental Algorithms, Privacy Preserving Machine Learning, Security and Privacy for Mobile AI, AMV2018.
- Shadow PC: EuroSys2018, IEEE S&P 2021.

9. LANGUAGES:

*** English** (fluent) * **Persian** (native)**.**

10. REFERENCES:

- Upon Request.