MOHAMMAD MALEKZADEH (CV)

Email: m.malekzadeh@imperial.ac.uk Homepage: mmalekzadeh.github.io

1. EDUCATION:

- **PhD in Computer Science | Queen Mary University of London, UK | 2017–2020**
  - *Awarded a full PhD studentship, to work on privacy-preserving personal data analytics, from Queen Mary University of London, Life Sciences Initiative*
  - *Thesis: "Machine Learning Algorithms for Privacy-preserving Behavioural Data Analytics"*
- **M.Sc. in Information Technology | Sharif University of Technology, Iran | 2009–2011**
  - *Ranked 10th among more than 10,000 participants taking part in the national M.Sc. entrance exam for information technology in Iran, 2009*
  - *Thesis: "Link's Sign Prediction in Signed Social Networks"*
- **B. Sc. in Software Engineering | Shahid Chamran University, Iran | 2004–2008**
  - *Ranked 2nd among more than 50 students in the bachelor's degree, class 2004.*
  - *Final project: "Persian CAPTCHA System to Prevent Automatic Subscribing of Software Robots"*

2. CURRENT POSITION:

- From JUN-2020: **Research Associate (PostDoc)** at Information Processing and Communications Lab, Department of Electrical & Electronic Engineering, **Imperial College London**: working on *privacy-preserving and robust machine learning*.

3. PAST POSITIONS:

- 2017–2020: **PhD Student** | School of EE&CS, Queen Mary University of London, UK
- 2019 JUN–SEP: **PhD Intern** | Research Team, Brave Software, London, UK
- 2018 APR–NOV: **Research Assistant** | Faculty of Engineering, Imperial College, UK
- 2018–2020: **Demonstrator** (Teacher Assistant) | QMUL and Imperial College, UK
- 2014–2016: **Co-Founder & Director** | ICT Institute, Persian Gulf University, Iran
- 2012–2016: **Lecturer in Computer Engineering** | Persian Gulf University, Iran

4. TEACHING:

- 2021: **Lecturer** of **Machine Learning Course,** EEE department, Imperial College London.
- 2020: Presenting parts of a **Tutorial on Deep Learning for Privacy in Multimedia**, for ACM International Conference on Multimedia.
- 2018 & 2019: **GTA** of **Sensing and IoT** course at Imperial College London.
- 2018, 2019, & 2020: **GTA** of **Computer Security**, **Data Analytics**, and **Software Engineering** modules, at Queen Mary University of London.
- 2012 to 2016: **Lecturer** of **Fundamental of Programming**, **Computer Architecture, Operating Systems Concepts**, **Software Engineering**, **Advanced Programming**, **Numerical Analysis**, **Technical and Scientific Presentation**, **Complex and Dynamical Networks**, and **Operating Systems Lab**, at Persian Gulf University in Iran.
- Ranked **1st** among **30** faculty members of the Engineering Department at Persian Gulf University as **the best teacher of the year** in 2014 (official university evaluation).

5. RESEARCH:

- The complete list of my publications is attached at the end of this CV. A selected list:
  - **NSDI'22 |** Top in Networked Systems | acceptance rate ~16%
  - **ACM CCS'21** | Top in Computer Security and Privacy | acceptance rate ~17%
  - **ACM UbiComp'21** | Top in Human-Computer Interaction | acceptance rate ~22%
  - **MLSYS'20** | Top in Machine Learning and Systems | acceptance rate ~20%
  - **IEEE/ACM IoTDI'19** & **IoTDI'18** | Top in Internet-of-Things | acceptance rate ~25%
  - **Pervasive and Mobile Computing** Journal'20 | impact factor 3.45
- Collected and published **"MotionSense Dataset"** in 2018, a dataset for Human Activity and Attribute Recognition from Smartphone's Motion Sensors, which has become a benchmark dataset in the field and have been used by many other researchers.
- Awarded a **$30000** grant of **Microsoft Azure** storage and compute for one year in 2018.
- Led a project chosen as **the best solution** for the **"Privacy-Preserving AI/ML for Healthcare"** in the International Telecommunication Union Global Competition.
- Our team was ranked **First** in Imperial College **AIHack 2018**.
- Participant in **Alan Turing Institute Data Study Group** in 2018.

6. PROGRAMMING:

- **Please visit my GitHub homepage: https://github.com/mmalekzadeh**
- **Machine Learning:** Python, PyTorch, Tensorflow, Keras, NumPy, SciPy, Scikit-Learn, Pandas (2017 – to this date)
  - Code and instructions for reproducing all of my published papers (since 2017) are publicly available and being used by other researchers.
- **Software Engineering:** HTML, CSS, JavaScript, AngularJS, NodeJS, PHP Laravel Framework; MySQL and MongoDB. (2008 – 2016). Designed and developed small to mid-sized software systems.

7. SERVICE and EXPERIENCES:

- **Reviewer:** Nature Communications, Privacy Enhancing Technologies Symposium (PETS), International Conference on Learning Representations (ICLR), IEEE Transactions on Mobile Computing, World Wide Web Journal, The Web Conference (WWW), ACM Transactions on Internet of Things, Symposium on Experimental Algorithms, NeurIPS Workshop on Privacy Preserving Machine Learning.
- **PC:** CoNEXT Workshop on Distributed Machine Learning (2021), ICLR workshop on Distributed and Private Machine Learning (2021), MobiSys Workshop on Security and Privacy for Mobile AI (2021), Workshop on Advanced Machine Vision Workshop (2018).
- **Shadow PC:** EuroSys2018, IEEE S&P 2021.

8. REFERENCES:

- **Prof. Deniz Gunduz.** Professor in Information Processing at Imperial College London.
- **Prof. Andrea Cavallaro.** Professor of Multimedia Signal Processing at QMUL.
- **Dr. Hamed Haddadi.** Reader in Human-Centred Systems at Imperial College London.
- **Dr. Richard G. Clegg.** Lecturer in the Networks Group at QMUL.

PUBLICATIONS (in chronological order)

Please visit my Google Scholar homepage: https://scholar.google.co.uk/citations?user=xZr9WQMAAAAJ&hl=en

My peer-reviewed publications are **16 papers** (7 conferences, 4 journals, and 5 workshops) including ACM CCS, USENIX NSDI, MLSYS, ACM UbiComp/IMWUT, IEEE/ACM IoTDI, RSOS, and PMC Journal. My current focus is on **Data Privacy and Robust Machine Learning**. I have been mainly working on machine learning systems and algorithms for **privacy-preserving personal data analytics**, particularly for data generated by the **users at the edge**, and privacy-preserving model training and inference with applications in **distributed/federated settings**. 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.

1. 2022: G. Siracusano, S. Galea, D. Sanvito, **M. Malekzadeh**, G. Antichi, P. Costa, H. Haddadi, R. Bifulco. **Re-architecting Traffic Analysis with Neural Network Interface Cards**, *USENIX Symposium on Networked Systems Design and Implementation (**USENIX NSDI**)* [Top venue in Networked Systems]
2. 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 (**ACM CCS**).* [acceptance rate: 17%] [Top venue in Computer Security and Privacy]
3. 2021: A. Priyanshu, R. Naidu, F. Mireshghallah, **M. Malekzadeh. Efficient Hyperparameter Optimization for Differentially Private Deep Learning.** *Workshop on Privacy Preserving Machine Learning (**ACM CCS**)*

4. 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**).* [acceptance rate: 22%] [Top venue in Human Computer Interaction]

5. 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**)*

6. 2021: F. Mo, A. Borovykh, **M. Malekzadeh**, H. Haddadi, S. Demetriou. **Layer-wise Characterization of Latent Information Leakage in Federated Learning,** *Workshop on Distributed and Private Machine Learning (**ICLR**).*

7. 2020: **M. Malekzadeh**, D. Athanasakis, H. Haddadi, B. Livshits. **Privacy-Preserving Bandits.** *Conference on Machine Learning and Systems (**MLSys**)* [acceptance rate: 20%][Top venue in Machine Learning]

8. 2020: **M. Malekzadeh**, R. G. Clegg, A. Cavallaro, and Hamed Haddadi. **Privacy and Utility Preserving Sensor-Data Transformations**. *Pervasive and Mobile Computing Journal, Elsevier (**PMC**).* [impact factor: 3.45]

9. 2020: E. Lisi, **M. Malekzadeh**, H. Haddadi, F. D. Lau, S. Flaxman. **Modeling and Forecasting Art Movements with CGANs.** *Royal Society Open Science Journal (**RSOS**).* [impact factor: 2.96]

10. 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**)* [acceptance rate: 34%][Top venue in Internet-of-Things]

11. 2018: **M. Malekzadeh**, R.G. Clegg, A. Cavallaro, and H. Haddadi. **Protecting Sensory Data against Sensitive Inferences**. *Workshop on Privacy by Design in Distributed Systems, Porto, Portugal (**EuroSys**).*

12. 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**)* [acceptance rate: 23%][Top venue in Internet-of-Things]

13. 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 (**IJACSA**) 8(5).* [impact factor: 1.32]

14. 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**)* [acceptance rate: 18%]

15. 2011: **M. Malekzadeh**, M.A. Fazli, P. J. Khalilabadi, H. R. Rabiee, M.A. Safari. **Social Balance and Signed Network Formation Games**, *Workshop on Social Network Mining and Analysis (**KDD**)*

16. 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:**

17. 2021: F. Mo, A. Borovykh, **M. Malekzadeh**, H. Haddadi, S. Demetriou. **Quantifying Information Leakage from Gradients**, Under Review.

- **Tutorial:**

18. 2020: A. Cavallaro, **M. Malekzadeh**, and A. S. Shamsabadi, **Deep Learning for Privacy in Multimedia**, ACM International Conference on Multimedia (**ACM MM**), Seattle, United States, (tutorial's hompage).

- **Dataset:**

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