Mohamed Maouche, PhD.

Researcher – Data Science – Privacy

0 (+33) 6 29 12 03 14
https://mmaouche.github.io/
mohamed.maouche@inria.fr

Work experience

October 2021 – ongoing

Inria, Lyon, France.

Post-doc

Working on privacy preserving federated learning in the DSVD Chaire in partnership with Renault Group. Focusing on health data in the context of car fleets.

2021

Université Lille, France

Teacher Teaching Dimension Reduction for the 1st year students of the machine learning master.

November 2019 – September 2021

Inria, Lille, France.

Post-doc

On private machine learning for speech processing and anonymization in the Magnet Team.

October 2016 – October 2019

INSA-Lyon LIRIS Lab, France.

PhD Student

In the fields of Data Science, Security and Privacy. Working on Location Privacy. And more precisely on re-identification attacks and obfuscation techniques

October 2016 – August 2019

INSA-Lyon, France

Teacher Teaches computer science in the first cycle department (Dept PC) and in the computer science department of INSA-Lyon (Dept. IF).

January 2016 – June 2016

UTC - Heudyasic Lab, France

Research Intern

In the field of Optimization in Operations research. Working on the Vehicle Routing Problem (VRP).

Education

2016 –2019	**PhD in Computer Science** *INSA-Lyon, France.*
2011 –2016	**Engineer/Master degree In Computer Science** *Ecole Nationale Superieure d'Informatique - ESI, Algiers*
2008 – 2011	**Baccalaureat in Mathematics** High school diploma *Bouamama High school, Algiers*

Teachings

Dimensions Reduction	PCA, TSNE, Autoencoders
Computer Science	Algorithmic, OOP
Operating Systems	C, Concurrency, Memory
Web data	XML, XPath, MongoDB
Semantic Web	RDF, SPARQL
Human Computer Interaction	Android Project

Languages

French	Native speaker
Arabic	Native speaker
English	Oral: Good – Written: Good

</> Programming skills

Good level	Python, pytorch, scikit-learn, keras, git, Linux
Intermediate	Java, Scala, C/C++, MongoDB, XML

Review

Review for Computer Speech & Languages, IEEE TDSC, ACM IMWUT, MobiQuitous, Subreviewer for SRDS, Euro-Par, ICDCS, Shadow PC Eurosys.

Supervisions

Nada Ould Taleb – Master Student from ESI
Besma Khalfoun – Master Student from ESI
Jugurta Ikherbane – Master Student from ESI
Dorian Lefeuvre – Ph.D. Track Student project from INSA-Lyon

Responsibilities

Co-webmaster and member of the local organization committee of IEEE SRDS 2019
www.srds-conference.org.

Server administrator of DRIM Reasearch Team (2018-2019).

Manager of DRIM's twitter account (2017-2019).

Publications Summary

Preprints (3)

Enhancing Speech Privacy with Slicing. M. Maouche, B. Srivastava, N. Vauquier, A. Bellet, M. Tommasi, E. Vincent. https://hal.inria.fr/hal-03369137/document

Privacy and utility of x-vector based speaker anonymization. B. Srivastava, M. Maouche, Md. Sahidullah, E. Vincent, A. Bellet, M. Tommasi, N. Tomashenko, X. Wang, E. Vincent, J. Yamagishi. [Submitted to Transactions on Audio, Speech and Language Processing] https://hal.inria.fr/hal-03197376/file/design_choices_informed.pdf

Differentially Private Speaker Anonymization. A. Shamsabadi, B. Srivastava, A. Bellet, N. Vauquier, E. Vincent, M. Maouche, M. Tommasi, N. Papernot. [Submitted to USENIX Security'22]

International Journals (2)

HMC: Robust Privacy Protection of Mobility Data against Multiple Re-Identification Attacks. M. Maouche, S. Ben Mokhtar, S. Bouchenak. IMWUT/Ubicomp 2018 https://hal.archives-ouvertes.fr/hal-01954041

The VoicePrivacy 2020 Challenge: Results and findings. N. Tomashenko, X. Wang, E. Vincent, J. Patino, B. Srivastava, PG. Noé, A. Nautsch, N. Evans, J. Yamagishi, B. O'Brien, A. Chanclu, JF. Bonastre, M. Todisco, M. Maouche. [Accepted in Computer Speech and Language] https://arxiv.org/pdf/2109.00648.pdf

International Conferences (5)

A comparative study of speech anonymization metrics. M. Maouche, B. Srivastava, N. Vauquier, A. Bellet, M. Tommasi, E. Vincent. INTERSPEECH 2020. https://hal.inria.fr/hal-02907918/document

Design Choices for X-vector Based Speaker Anonymization. B. Srivastava, N. Tomashenko, X. Wang, E. Vincent, J. Yamagishi, M. Maouche, A. Bellet, M. Tommasi. INTERSPEECH 2020. https://hal.archives-ouvertes.fr/hal-02610447v2/document

MooD: MObility Data Privacy as Orphan Disease. B. Khalfoun, M. Maouche, S. Ben Mokhtar, S. Bouchenak. Middleware 2019. https://hal.archives-ouvertes.fr/hal-02355325/document

ACCIO: How to Make Location Privacy Experimentation Open and Easy. V. Primault, M. Maouche, A. Boutet, S. Ben Mokhtar, S. Bouchenak, L. Brunie. ICDCS 2018. https://hal.archives-ouvertes.fr/hal-01784557

AP-Attack: A Novel User Re-identification Attack On Mobility Datasets. M. Maouche, S. Ben Mokhtar, S. Bouchenak. MobiQuitous 2017. https://hal.archives-ouvertes.fr/hal-01785155

Software Development

Anonymization Metrics: This toolkit encapsulates multiple python implementations of anonymization metrics. https://gitlab.inria.fr/magnet/anonymization_metrics

SFERA: A toolkit to experiment on re-identification attacks on mobility traces https://github.com/mmaouche-insa/SFERA

HMC: A toolkit to test the Location Privacy Protection Mechanism HMC (Heat-Map Confusion) https://github.com/mmaouche-insa/HMC

Participation in **Accio** (main contributer is Vincent Primault: A scientific workflow management tool, used to study location privacy https://privamov.github.io/accio/