Mohamed Maouche, PhD.

Research Scientist – Data Science – Privacy

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

Work experience

December 2022 (permanent)
Research Scientist (ISFP) – Inria, Lyon, France.

I'm a permanent researcher at Inria Lyon with Privatics team. My main topic of interest is privacy, especially in machine learning.

October 2022 - November 2022
Post-doc – Inria, Lyon, France.

Continuing the work on preserving privacy in federated learning setting with Privatics Team

October 2021 – October 2022
Post-doc – ENTPE/Inria, Lyon, France.

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.

January 2021 – July 2021
Teacher – Université Lille, France

Course on Dimension Reduction for the 1st year students of the machine learning master.

November 2019 – September 2021
Post-doc – Inria, Lille, France.

Working on anonymization and private machine learning for speech processing within COMPRISE (H2020) and Deep-privacy (ANR) projects of Magnet team and close collaboration with Multispeech team.

October 2016 – October 2019
PhD Student – INSA-Lyon LIRIS Lab, France.

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

October 2016 – August 2019
Teacher – INSA-Lyon, France

Teaching in the first cycle department and the computer science department of INSA-Lyon (+200h).

Languages

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

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

</> Programming skills

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

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 @lirisDRIM twitter account (2017-2019).

Software Development

Anonymization Metrics: Toolkit for anonymization metrics. Integrated to Voice Privacy Challenge 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 for 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/

Review

Review for Computer Speech & Languages 2021, IEEE TDSC 2020-2022, ACM IMWUT 2019, ICDCS 2022, DSN 2020,MobiQuitous 2020, ICAC 2019 Euro-Par 2019, Shadow PC Eurosys 2018.

Publications Summary

International Journals (4)

Differentially Private Speaker Anonymization. A. Shamsabadi, B. Srivastava, A. Bellet, N. Vauquier, E. Vincent, M. Maouche, M. Tommasi, N. Papernot. [Accepted to PETS'22] https://arxiv.org/pdf/2202.11823.pdf

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. Transactions on Audio, Speech and Language Processing 2022 https://hal.inria.fr/hal-03197376/file/design_choices_informed.pdf

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. Computer Speech and Language 2021 https://arxiv.org/pdf/2109.00648.pdf

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

International Conferences (7)

Enhancing Speech Privacy with Slicing. M. Maouche, B. Srivastava, N. Vauquier, A. Bellet, M. Tommasi, E. Vincent. INTERSPEECH 2022. https://hal.inria.fr/hal-03369137/document

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. Computer Speech and Language 2021 https://arxiv.org/pdf/2109.00648.pdf

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