Curriculum Vitae

Felice Antonio Merra

September 13, 2019

Contents

Personal Data

Current Affiliation
Department of Electrical and Information Engineering (DEI)
Polytechnic University of Bari
via E.Orabona, 4 - 70125 Bari (Italy)

mobile: +39 340 421 3 560
e-mail: felice.merra@poliba.it
Institutional Web Site: http://sisinflab.poliba.it/merra/
Personal Web Site: https://merrafelice.github.io/

Social Accounts:
Twitter: @merrafelice
LinkedIn: Felice Antonio Merra
GitHub: merrafelice

Current Position

Since November 1, 2018 PhD Student at Polytechnic University of Bari Bari.

Brief Description of Scientific Activities

My research activities mainly focus on Artificial Intelligence. My investigation is devoted to novel approaches and application of Machine Learning algorithms, and in particular to Adversarial Machine Learning in the Recommender System domains. Particularly, I am pretty interested in the Security of Recommender Systems and the application of Adversarial Training to improve recommendations.

1 Education

Master's Degree in Computer Science Engineering. October 2018. Thesis title: *Privacy As A Service: automatic anoymization of microdataset for urban analytic.* In this work, a novel initial to data-quality preservation in Open Data has been proposed.

Bachelor's Degree in Computer Science and Automation Engineering. July 2016. Thesis title: *Information Flow Processing: Complex Event Processing in Healthcare Systems.*

2 Research Interests

My research activity starts in 2018 soon after my graduation at Politecnico di Bari with the Information Systems Laboratory group (`http://sisinflab.poliba.it/`). Currently, I am a PhD Student under the supervision of Professor Tommaso Di Noia, technical manager of the laboratory.

2.1 Research Topics

- **Adversarial Machine Learning** A core topic of my research is Adversarial Machine Learning and its application in Recommender Systems. Adversarial Machine Learning is a new hot area of research in a lot of application domain of Machine Learning techniques. Machine learning is an area of Artificial Intelligence that has had and is having a great impact in numerous application scenarios: the identification of objects and people, image processing, autonomous driving scenarios, support decision-making. The great diffusion of different machine learning models has been followed by the identification of security issues on their robustness to possible attacks. Indeed, when ML models are used in real-world scenarios, the presence of intelligent adversaries can manipulate the specific vulnerabilities of learning algorithms thus compromising the robustness of the machine learning system. Adversarial Machine Learning is a recent field of research whose aim is to identify limits and security issues of ML models and develop countermeasures. The focal points of my research interests are the application of Adversarial Attacks on Recommender Systems cases.

- **Deep Learning** I am particular interested on Deep Learning-based Recommender Systems. My interests are in analyzing, testing and proposing approaches able to improve the robustness and the accuracy of recommender models by applying AML techniques.

- **Recommender Systems** The core topic of my research interests is related to Recommender Systems. I focus my research on investigating novel approaches and algorithms to perturb data inputs of a recommender system with the goal to identify possible security issues in baseline recommender models. Another important interest on this topic is related to analysis and identification of possible application of Adversarial Machine Learning to improve or propose recommender model in the case of Cross-Domain and Social-aware Recommendations. I would like to exploit advances of AML in the Domain Adaptation and Knowledge Transfer for the Computer Vision domain, into Recommendation Scenarios.

- **Computer Vision** Computer Vision is another topic under my investigation. I work on this aspect with the purpose to investigate the AML-based models in

Domain Adaptation and Knowledge Transfer for the application in real world scenario.

- **Open Data** I studied how to design and implement novel approaches to protect privacy by preserving high quality of data. Firstly, I evaluated how it is possible to use Open Data to support healthcare services by extracting insights from the integration of heterogeneous Open Data. Then, I focused my research on the preservation of data quality with particular attention to the semantic of data. Finally, I designed and developed a probabilistic reasoner able to guess specific information of an individual only by combining Open Data from various public sources.

3 Developed Tools

An updated and shared version of all the tools developed during our research activities is available at *https://github.com/sisinflab*

- *Insights From Open Data* a tool for insight generation from Open Data;

4 Collaboration with national and international research institutes

Within my research activities, I have worked or currently work, with the following national and international research institutes:

- Knowledge Media institute - The Open University (prof. Enrico Motta, dr. A. Antonini);
- Istituto di Ricerca sulle Acque- Consiglio Nazionale delle Ricerche (IRSA-CNR) Bari (dr. R. Matarrese);

5 International Activities

- RecSys2019, The 13th ACM Recommender Systems Conference, September 16-20, 2019 Copenhagen, Denmark
- RecSys2019 Summer School, The ACM Summer School on Recommender Systems, September 9-13, 2019 Gothenburg, Sweden
- ESSIR 2019, The 12th European Summer School in Information Retrieval, July 15-19, 2019 Milan, Italy

6 Publications

[1] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Assessing the impact of a user-item collaborative attack on class of users. *arXiv preprint arXiv:1908.07968*, 2019.

In compliance with the Italian Legislative Decree no. 196 dated 30/06/2003, I hereby authorize the recipient of this document to use and process my personal details for the purpose of recruiting and selecting staff and I confirm to be informed of my rights in accordance to art. 7 of the above mentioned decree.

Bari, September 13, 2019

Felice Antonio Merra