Curriculum Vitae

Felice Antonio Merra

February 11, 2021

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
YouTube: Felice Antonio Merra, Ph.D. Student

Current Position

Since November 1, 2018 Third-year Ph.D. Student at Polytechnic University of Bari.
[Graduation]: Winter 2021

Brief Description of Scientific Activities

My research activities mainly focus on artificial intelligence (AI). My investigation is devoted to novel approaches and applying machine learning (ML) algorithms, particularly to Trustworthy AI. In particular, I devote my attention to recommender system (RS) applications to study the robustness of modern ML recommender models affected by adversarial threats. After having assessed the state-of-the-art of AML techniques in RS, I have investigated three main areas of study: (i) the robustness of recommender models when affected by hand-engineered shilling attacks, (ii) the formal study of the effects of AML training strategies on the beyond-accuracy effects of recommenders, i.e., bias disparity, fairness, novelty, and (iii) the proposal of adversarial attacks against multimedia retrieval models. In the future, I plan to extend the previous line of study and continue to investigate AML approaches on other ML tasks, e.g., computer vision and reinforcement learning, with the aim to bridge the final users' at the core of my research to verify how much they can Trust an ML system.

1 Education

Ph.D. in Computer Science and Automation Engineering. Winter 2021. Thesis Topic: *Adversarial Machine Learning in Recommender Systems.*.

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. **Final Score**: Full marks with honors.

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

2 Internship

Applied Science Intern at `Amazon.com`. July-September 2020. *Amazon Search and Personalization* research team. Project: Query to Refinement Recommendation. Manager: Lange Dustin, Ph.D.

3 Research Interests

My research activity starts in 2018, soon after my graduation at Polytechnic University of Bari with the Information Systems Laboratory (SisInfLab) group (`http://sisinflab.poliba.it/`). Currently, I am a second-year Ph.D. Student (moving to third in November 2020) under the supervision of Professor Tommaso Di Noia, technical manager of the laboratory.

3.1 Description of PhD Dissertation

Nowadays, recommender systems are part of our everyday life and one of the most impactful Machine Learning (ML) applications in the real world. They mainly estimate users' utility on a catalog of items, news, health training programs, and recommend those a user might be interested in buying. This has a severe influence not only on the business of many services and product providers but also on users' actual life. Unfortunately, we are well aware that ML systems are vulnerable to adversaries able to invalid the predicted output of a recommendation model. For instance, the top music-services provider has been recently hacked by adversaries in recommending tracks of non-existent bands. Driven by theoretical and industrial use cases, Adversarial Machine Learning then emerged as a sub-field of machine learning devoted to studying the vulnerabilities of ML models.

I am focusing on the robustness of machine-learning models with a deep interest in recommendation models. Robustness of recommenders refers here to the consistency of the produced recommendations concerning the expected ones. Low robustness implies that the recommendation system can be maliciously altered with enormous risks for the customers, companies, and actors of a multi-stakeholder scenario.

I plan to explore different attacks, with a deep focus on the exposure of ML recommender systems to sophisticated ML-based attacks. Indeed, the core of my research is the study and evaluation of ML-based adversarial attacks to recommender systems and the study of attackers' effectiveness and limitations in different scenarios. The assessment of the analyzed algorithms under adversarial settings is the foundation for addressing these security shortcomings. To this end, the overarching questions to my research are: “How robust are ML models concerning adversarial attacks?”; “How is it possible to protect recommender systems against malicious adversaries?”.

Furthermore, I have matured a novel interest in the direct impact of machine-learning models on humans. For instance, I am researching how much the perturbed product images [11, 6] will affect the human evaluation trust on recommender models. This side of my research interest grown during the Summer Internship at Amazon.com, where I learned how to do research and be effective in real-world problems when humans are in-the-loop.

4 International Collaboration

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

- Escuela Politécnica Superior, Universidad Autónoma de Madrid (dr. Alejandro Bellogín), Madrid, Spain
- Università del Salento and Politecnico di Torino for the project *FLET4.0 – FLEet managemenT optimization through I4.0 enabled smart maintenance*, as Project Research Scientist
- Knowledge Media institute - The Open University (prof. Enrico Motta, dr. A. Antonini), Milton Keynes, United Kingdom

5 International Activities

In the follow, I present the attended conferences, the activities as reviewer/sub-reviewer, and attended summer schools schools [1].

- Attended Conferences:

  2020 : **NeurIPS**, **SIGIR**, **RecSys**, **WSDM**, ESWC, **SEBD**, SIGMOD+POD, CIRCLE, **DSN-DSML-W**

  2019 : **RecSys**, **FDIA**, **SMFC**

- Program Committee:

  2020 : RecSys, WDCS@NeurIPS

- Summer Schools:

  2019
  - ∗ RecSys 2019 Summer School, The ACM Summer School on Recommender Systems, September 9-13, 2019 Goteborg, Sweden
  - ∗ ESSIR 2019, The 12th European Summer School in Information Retrieval, July 15-19, 2019 Milan, Italy

6 Teaching Activities

Data Structure and Algorithm in Java. I started my teaching activity in the academic year 2019/20 as Course Assistant for the bachelor degree course: *Data Structure and Algorithm in Java.*

[1] **Bold**: Presenter of at least one publication.

7 GitHub Projects

An updated set of repositories related to my research activities and published papers is available at: `https://github.com/merrafelice`.

8 Tools Experience

Within my research activities, I currently work with different frameworks for the implementation and evaluations of research activities. Particularly, I have strong experience in *Python* programming, with a daily use of *TensorFlow*. I have also worked on projects with other program languages such as *C++*, *C#*, *Java* and *JavaScript*. I consider my coding skills really important for my research path and career. During my internship, I matured experience with Apache-Spark tools.

9 Publications

I am the **main author** of all the listed publications. The authors are sorted in alphabetical order.

[1] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial learning for recommendation. In *Advances in Information Retrieval - 43rd European Conference on IR Research, ECIR 2021*, Lecture Notes in Computer Science. Springer, 2021.

[2] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. *Adversarial Recommender Systems: Attack, Defense, and Advances.* to appear in the Third Edition of Recommender Systems Handbook, Springer, third edition, 2021. to appear in the Third Edition of Recommender Systems Handbook.

[3] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial learning for recommendation: Applications for security and generative tasks - concept to code. In Rodrygo L. T. Santos, Leandro Balby Marinho, Elizabeth M. Daly, Li Chen, Kim Falk, Noam Koenigstein, and Edleno Silva de Moura, editors, *RecSys 2020: Fourteenth ACM Conference on Recommender Systems, Virtual Event, Brazil, September 22-26, 2020*, pages 738–741. ACM, 2020.

[4] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Felice Antonio Merra, Giuseppe Acciani, and Eugenio Di Sciascio. Knowledge-enhanced shilling attacks for recommendation. In Maristella Agosti, Maurizio Atzori, Paolo Ciaccia, and Letizia Tanca, editors, *Proceedings of the 28th Italian Symposium on Advanced Database Systems, Villasimius, Sud Sardegna, Italy (virtual due to Covid-19 pandemic), June 21-24, 2020*, volume 2646 of *CEUR Workshop Proceedings*, pages 310–317. CEUR-WS.org, 2020.

[5] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Felice Antonio Merra. Sasha: Semantic-aware shilling attacks on recommender systems exploiting knowledge graphs. In Andreas Harth, Sabrina Kirrane, Axel-Cyrille Ngonga Ngomo, Heiko Paulheim, Anisa Rula, Anna Lisa Gentile, Peter Haase, and Michael Cochez, editors, *The Semantic Web - 17th International Conference, ESWC 2020, Heraklion, Crete, Greece, May 31-June 4, 2020, Proceedings*, volume 12123 of *Lecture Notes in Computer Science*, pages 307–323. Springer, 2020.

[6] Vito Walter Anelli, Tommaso Di Noia, Daniele Malitesta, and Felice Antonio Merra. Assessing perceptual and recommendation mutation of adversarially-poisoned visual recommenders. *The 1st Workshop on Dataset Curation and Security co-located with the 34th Conference on Neural Information Processing Systems (NeurIPS 2020), Vancouver, Canada (Virtual Event).*, 2020.

[7] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Assessing the impact of a user-item collaborative attack on class of users. In Oren Sar Shalom, Dietmar Jannach, and Ido Guy, editors, *Proceedings of the 1st Workshop on the Impact of Recommender Systems co-located with 13th ACM Conference on Recommender Systems, ImpactRS@RecSys 2019), Copenhagen, Denmark, September 19, 2019*, volume 2462 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2019.

[8] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial machine learning in recommender systems (aml-recsys). In James Caverlee, Xia (Ben) Hu, Mounia Lalmas, and Wei Wang, editors, *WSDM '20: The Thirteenth ACM International Conference on Web Search and Data Mining, Houston, TX, USA, February 3-7, 2020*, pages 869–872. ACM, 2020.

[9] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. A survey on adversarial recommender systems: from attack/defense strategies to generative adversarial networks. *ACM Computing Surveys*, March 2021.

[10] Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Felice Antonio Merra. How dataset characteristics affect the robustness of collaborative recommendation models. In Jimmy Huang, Yi Chang, Xueqi Cheng, Jaap Kamps, Vanessa Murdock, Ji-Rong Wen, and Yiqun Liu, editors, *Proceedings of the 43rd International ACM SIGIR conference on research and development in Information Retrieval, SIGIR 2020, Virtual Event, China, July 25-30, 2020*, pages 951–960. ACM, 2020.

[11] Tommaso Di Noia, Daniele Malitesta, and Felice Antonio Merra. Taamr: Targeted adversarial attack against multimedia recommender systems. In *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN Workshops 2020, Valencia, Spain, June 29 - July 2, 2020*, pages 1–8. IEEE, 2020.

Bari, February 11, 2021

Felice Antonio Merra