Curriculum Vitae

Felice Antonio Merra

August 9, 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 Website: http://sisinflab.poliba.it/merra/
Personal Website: https://merrafelice.github.io/

Social Accounts:
Twitter: @merrafelice
LinkedIn: Felice Antonio Merra
GitHub: merrafelice
YouTube: Felice Antonio Merra, Ph.D. Student

Current Position

Ph.D. Candidate Polytechnic University of Bari. Graduation: October 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 adversarial training strategies on the beyond-accuracy effects of recommenders, i.e., bias disparity, fairness, novelty, and (iii) the proposal of adversarial attacks and defenses against multimedia retrieval models from image to music.

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 Awards

Best Paper Award at the 3rd Workshop on Adversarial Learning Methods for Machine Learning and Data Mining @ KDD 2021 sponsored by MIT-IBM Watson AI Lab for the [4] article.

3 Internship

Applied Science Intern at `Amazon.com`. July-September 2020. *Amazon Search and Personalization* research team.

4 Honors

- **Subject Expert**: Algorithms and Data Structure in Java *2020*
- **Poliba Ph.D. Fellowship**: Ph.D. supported by Politecnico di Bari *2018-2021*
- **Poliba Scholarship Award for Master Thesis Abroad**: Research Visiting Period at the Knowledge Media Institute (UK) supported by Politecnico di Bari *2018*

5 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 last-year Ph.D. Student under the supervision of Professor Tommaso Di Noia, technical manager of the laboratory.

5.1 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?"; "Which are the possible point of failure in the case of Multimedia Recommender Models?".

Furthermore, I have matured a deep interest in the direct impact of machine-learning models on humans. For instance, I am researching how much the perturbed product images [23, 13, 5] will affect the human evaluation trust on recommender models as well as varying convolutional neural architecture can have effects on the model performance [17]. 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 (customers) are in-the-loop. To this purpose, in [8], I have investigated the effects of adversarial training procedure on the amplification of biases and reduction of diversity and coverage in the generated recommendation lists.

6 International Collaboration

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

- Consorzio Interuniversitario per il Calcolo Automatico dell'Italia Nord Orientale (Cineca), Bologna, Italy Accepted Grant for the use of HPC Resources
- 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

7 International Activities

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

- Program Committee:
  - RecSys LBR, WDCS@NeurIPS, ECIR, JAIR, IEEE Signal Processing
- Summer Schools:
  - 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

8 GitHub Projects

An updated set of repositories related to my research activities and published papers is available at: `https://github.com/merrafelice`.
[**Elliot**] I have actively contributed in the development of an **open-source library** for the realization of extensive and reproducible experiments on recommendation models. In particular, the framework implements the complete pipeline form the data preparation, to the training and evaluation of state-of-the-art recommendation models (more than 50 models), passing through a set of possible optimization search strategies (e.g., Bayesian optimization). The public daily-maintained repository is available at `https://github.com/sisinflab/elliot`. In particular, I have actively contributed into the integration of deep learning, adversarial learning, and visual,-based recommendations models published into a RecSys 2021 demonstration paper [4].

9 Tools Experience

[**Programming Languages**] 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.
[**Large Scale Experiments**] During my Ph.D. activities, I have been matured experience in performing large-scale experiments on Super Computing resources. In particular, I have been performing experiments on `Marconi100` [1], a 32 PFlops accelerated cluster based on IBM Power9 architecture.
[**Multi-GPU Training for Feature Extraction on Music Content**] In the GitHub project, i.e., link to the project, I have implemented in TensorFlow v2, a convolutional neural network, with multi-gpu training, for the extraction of latent features from the mel-spectrogram generated from music tracks.

10 Teaching Activities

Data Structure and Algorithm in Java. I started my teaching activity in the academic year 2018/2019, 2019/20, 2020/2021 as Course Assistant for the bachelor degree course: *Data Structure and Algorithm in Java.*

11 Organized Workshops/Conference

- AdveRSe 2021: The 1st International Workshop on Adversarial Machine Learning for Recommendation and Search in conjunction with CIKM 2021, Australia

12 Publications

The authors of the papers are sorted in alphabetical order. I am the **main author** of all the listed publications related to the **adversarial machine learning** topic.

[1] Vito Walter Anelli, Alejandro Bellogin, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Msap: Multi-step adversarial perturbations on recommender

[1] https://www.hpc.cineca.it/hardware/marconi100

systems embeddings. In *The 34th International FLAIRS Conference*, pages 1–6. The Florida AI Research Society (FLAIRS), AAAI Press, May 2021.

[2] Vito Walter Anelli, Alejandro Bellogín, Antonio Ferrara, Daniele Malitesta, Felice Antonio Merra, Claudio Pomo, Francesco Maria Donini, and Tommaso Di Noia. Elliot: a comprehensive and rigorous framework for reproducible recommender systems evaluation. In *Proceedings of the 44th International ACM SIGIR conference on research and development in Information Retrieval, SIGIR 2021, Virtual Event, Canada*. ACM, July 2021.

[3] Vito Walter Anelli, Alejandro Bellogín, Antonio Ferrara, Daniele Malitesta, Felice Antonio Merra, Claudio Pomo, Francesco Maria Donini, and Tommaso Di Noia. How to perform reproducible experiments in the elliot recommendation framework: data processing, model selection, and performance evaluation. In *IIR*, CEUR Workshop Proceedings. CEUR-WS.org, 2021.

[4] Vito Walter Anelli, Alejandro Bellogín, Antonio Ferrara, Daniele Malitesta, Felice Antonio Merra, Claudio Pomo, Francesco Maria Donini, and Tommaso Di Noia. V-elliot: Design, evaluate and tune visual recommender systems. In *RecSys 2021: Fifteenth ACM Conference on Recommender Systems (RecSys '21), September 27-October 1, 2021, Amsterdam, Netherlands*. ACM, 2021.

[5] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Daniele Malitesta, and Felice Antonio Merra. A study of defensive methods to protect visual recommendation against adversarial manipulation of images. In *The 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*, page 10. ACM, July 2021.

[6] 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.

[7] 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.

[8] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Understanding the effects of adversarial personalized ranking optimization method on recommendation quality. In *3rd Workshop on Adversarial Learning Methods for Machine Learning and Data Mining @ KDD 2021 (virtual workshop)*. Online, 2021.

[9] 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 *RecSys 2020: Fourteenth ACM Conference on Recommender Systems, Virtual Event, Brazil, September 22-26, 2020*, pages 738–741. ACM, 2020.

[10] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Understanding the effects of adversarial personalized ranking optimization method on recommendation quality. *3rd Workshop on Adversarial Learning Methods for Machine Learning and Data Mining co-located with KDD 2021*, 2021.

[11] Vito Walter Anelli, Yashar Deldjoo, Tommaso Di Noia, Felice Antonio Merra, Giuseppe Acciani, and Eugenio Di Sciascio. Knowledge-enhanced shilling attacks

for recommendation. In *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.

[12] 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 *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.

[13] 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.

[14] Vito Walter Anelli, Tommaso Di Noia, Daniele Malitesta, and Felice Antonio Merra. Assessing perceptual and recommendation mutation of adversarially-poisoned visual recommenders (short paper). In *DP@AI*IA*, volume 2776 of *CEUR Workshop Proceedings*, pages 49–56. CEUR-WS.org, 2020.

[15] Vito Walter Anelli, Tommaso Di Noia, and Felice Antonio Merra. The idiosyncratic effects of adversarial training on bias in personalized recommendation learning. In *RecSys 2021: Fifteenth ACM Conference on Recommender Systems (RecSys '21), September 27-October 1, 2021, Amsterdam, Netherlands*. ACM, 2021.

[16] Giuseppe De Candia, Tommaso Di Noia, Eugenio Di Sciascio, and Felice Antonio Merra. Amflp: Adversarial matrix factorization-based link predictor in social graphs. In *SEBD 2021: The 29th Italian Symposium on Advanced Database Systems, September 5-9, 2021, Pizzo Calabro (VV), Italy*. CEUR Workshop Proceedings, sept 2021.

[17] Yashar Deldjoo, Tommaso Di Noia, Daniele Malitesta, and Felice Antonio Merra. A study on the relative importance of convolutional neural networks in visually-aware recommender systems. In *CVPRW-CVFAD 2021 :The 4th CVPR Workshop on Computer Vision for Fashion, Art, and Design*, pages 1–4. CVPR Proceedings, June 2021.

[18] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Assessing the impact of a user-item collaborative attack on class of users. In *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.

[19] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. Adversarial machine learning in recommender systems (aml-recsys). In *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.

[20] 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.

[21] Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Felice Antonio Merra. How dataset characteristics affect the robustness of collaborative recommendation models. In *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.

[22] Yashar Deldjoo, Tommaso Di Noia, Eugenio Di Sciascio, and Felice Antonio Merra. A regression framework to interpret the robustness of recommender systems against shilling attacks (discussion paper). In *IIR*, CEUR Workshop Proceedings. CEUR-WS.org, 2021.

[23] 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, August 9, 2021

Felice Antonio Merra