TANJA ŠARČEVIĆ

ML SECURITY AND PRIVACY RESEARCHER

Vienna, Austria | ta.sarcevic@gmail.com | tanjascats.github.io | linkedin.com/in/tanjasarcevic

SUMMARY

Experienced researcher specializing in privacy and security in AI, with a PhD focus on data watermarking and fingerprinting. Published in leading venues and developed open-source tools. Skilled in machine learning, data science, and collaborative industry-academic projects, including privacy-preserving healthcare analytics. Passionate about transitioning to industry to apply advanced AI expertise to real-world challenges.

Technical skills

Python	Privacy-preserving Methods	Version Control and Collaboration
ML Development and Training	Adversarial ML	Public Speaking
Scikit-learn, PyTorch, TensoFlow	Scientific Writing and Publishing	Teaching & Mentoring

Professional experience

ML Security and Privacy Researcher, SBA Research **Feb 2019 - Current**

- Collaboration on national (Austrian) and international scientific projects with academic and industry partners, across multiple disciplines such as health and legal.
- Developed innovative methods for data ownership protection; an open-source toolbox for data fingerprinting and a novel method improving the state-of-the art.
- Designed a trusted analysis environment for executing data analytics in a PoC platform for privacy-preserving data analysis, WellFort.
- Published 6 peer-reviewed research papers, multiple posters, short papers and magazine articles.
- Demnonstrated strong technical communication, presenting complex research findings effectively to both technical and non-technical audiences, fostering collaboration and knowledge sharing.

Lecturer, FH Technikum Wien **Sep 2022 - Current**

- Course: Security & Privacy in AI (WS2022, WS2024)
- Course: Scientific Writing (WS2022, WS2023)

Lecturer, TU Wien **Feb 2022 - Sep 2023**

- Course: Security, Privacy & Explainability in ML (SS2022, SS2023)

Research Intern, SBA Research **Aug 2018 - Feb 2019**

- Evaluated the impact of data anonymisation methods on predictive ML tasks.
- Published a peer-reviewed paper at an international cross-domain conference for ML & Knowledge Extraction (CD-MAKE 2019)

Education

Faculty of Informatics, TU Wien - PhD **Oct 2019 - Current**

- Information Hiding - Advances in Data Ownership Protection

Faculty of Informatics, TU Wien - Master (Dipl.-Ing.) **Oct 2016 - Oct 2019**

- Focus: Logic and Computation
- Thesis: Fingerprinting Relational Databases; Quality Evaluation and Impact on Learning Tasks

Faculty of Engineering and Computing, Zagreb University - Bachelor **Oct 2013 - Jul 2016**

- Focus: Computer Science
- Thesis: Simulation and Visualisation of Particle Swarm Optimisation for Problems in 2-dimensional space

Publications

- Šarčević, T., Karlowicz, A., Mayer, R., Baeza-Yates, R. and Rauber, A., 2024. U Can't Gen This? A Survey of Intellectual Property Protection Methods for Data in Generative AI. arXiv preprint arXiv:2406.15386.
- Šarčević, T., Mayer, R. and Adler, P., 2023, December. Achieving Privacy and Tracing Unauthorised Usage: Anonymisation-based Fingerprinting of Private Data. In 2023 IEEE International Conference on Big Data (BigData) (pp. 5578-5587). IEEE.
- Šarčević, T., Mayer, R. and Rauber, A., 2022, December. Adaptive attacks and targeted fingerprinting of relational data. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 5792-5801). IEEE.
- Ekaputra, F.J., Ekelhart, A., Mayer, R., Miksa, T., Šarčević, T., Tsepelakis, S. and Waltersdorfer, L., 2021. Semantic-enabled architecture for auditable privacy-preserving data analysis. Semantic Web, pp.1-34.
- Šarčević, T., Molnar, D. and Mayer, R., 2020, September. An Analysis of Different Notions of Effectiveness in k-Anonymity. In International Conference on Privacy in Statistical Databases (pp. 121-135). Springer, Cham.
- Šarčević, T. and Mayer, R., 2020, September. A Correlation-Preserving Fingerprinting Technique for Categorical Data in Relational Databases. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 401-415). Springer, Cham.
- Šarčević, T. and Mayer, R., 2019, August. An Evaluation on Robustness and Utility of Fingerprinting Schemes. In International Cross-Domain Conference for Machine Learning and Knowledge Extraction (pp. 209-228). Springer, Cham.
- Šarčević, T., Rocha, A.P. and Castro, A.J., 2018, June. Artificial Bee Colony Algorithm for Solving the Flight Disruption Problem. In International Conference on Practical Applications of Agents and Multi-Agent Systems (pp. 72-81). Springer, Cham.

Talks

- WellFort: Auditable Privacy-Preserving Data Analysis Platform for SMEs. Šarčević, T. At DataSHIELD conference 2021. November 11, 2021. Online.
- Fingerprinting Relational Data. Šarčević, T. At Expert Meeting on Statistical Data Confidentiality. December 3, 2021. Poznan, Poland. https://unece.org/statistics/events/SDC2021
- Ownership protection of data and machine learning models. Šarčević, T. At Social Artificial Intelligence Night (SAINT). April 1, 2022. FH St. Pölten. https://www.fhstp.ac.at/de/onepager/social-artificial-intelligence-night-saint
- Ownership protection in Machine Learning: How to protect your neural network? Šarčević, T. At Women in Privacy & Security Vienna. October 18, 2022. Vienna, Austria. https://www.meetup.com/secwomenvienna/
- Anonymisation and Fingerprinting of Microdata: A Genetic Algorithm for Finding the Optimal Set for Data Distribution. Šarčević, T. At Privacy in Statistical Databases. November 21, 2022. Paris, France. https://crises-deim.urv.cat/psd2022/
- IP Protection in Machine Learning/AI. Šarčević, T. and Mayer R. At sec4dev2022. September 6, 2022. Vienna, Austria. https://sec4dev.io/2022/
- Poster: Ownership Protection of Federated Machine Learning. Strauß D. and Šarčević, T. At Social Artificial Intelligence Night (SAINT), March 24, 2023. FH St. Pölten. Austria. https://www.fhstp.ac.at/de/newsroom/events/saint-2023

Projects & Grants

- FemTech grant 2019: Internship for female students in research, technology and innovation sector.
- Industry-related dissertations 2020 by The Austrian Research Promotion Agency (FFG) for project Intellectual Property Protection for Machine Learning (IPP4ML).
- WellFort: A Platform for Privacy-preserving Data Analysis. Grant no. 871267 by the Austrian Research Promotion Agency (FFG). https://www.sba-research.org/research/projects/wellfort/
- FeatureCloud: Privacy-preserving Federated Machine Learning for Healthcare. Grant no. 826078 by the European Union's Horizon2020 research and innovation programme. https://featurecloud.eu/
- Beyond Coding: Coaching programme for efficient, agile and secure software development. https://www.sba-research.org/research/projects/beyond-coding/
- Monitaur: Monitoring system for copy protection through malicious client detection. Grant by ”Netidee Internet Stiftung” 2024. https://www.netidee.at/monitaur