TANJA ŠARČEVIĆ

PhD candidate @ TU Wien | Researcher @ SBA Research

ta.sarcevic@gmail.com · linkedin.com/in/tanjasarcevic

RESEARCH EXPERIENCE

1ST FEBUARY – CURRENT

RESEARCHER, SBA RESEARCH

Privacy and security-related topics such as anonymity, digital intellectual property protection via techniques of watermarking and fingerprinting, privacy-preserving computation… Impact of privacy- and security-preserving techniques on Machine Learning.

AUGUST 1ST 2018 – 1ST FEBUARY

RESEARCH INTERN, SBA RESEARCH

Data anonymity and the effects that anonymity protection methods have on Machine Learning; how well the predictive Machine Learning models trained on anonymized sensitive and/or personal data perform.

EDUCATION

OCTOBER 2019 - CURRENT

PHD STUDIES

FACULTY OF INFORMATICS, VIENNA UNIVERSITY OF TECHNOLOGY, AUSTRIA

THESIS: INTELLECTUAL PROPERTY PROTECTION OF MACHINE LEARNING PROCESSES

OCTOBER 2016 - OCTOBER 2019.

MASTERS IN LOGIC AND COMPUTATION

FACULTY OF INFORMATICS, VIENNA UNIVERSITY OF TECHNOLOGY, AUSTRIA

THESIS: FINGERPRINTING RELATIONAL DATABASES; QUALITY EVALUATION AND IMPACT ON LEARNING TASKS

OCTOBER 2017 - FEBUARY 2018

ERASMUS STUDENT EXCHANGE PROGRAMME

FACULTY OF ENGINEERING, UNIVERSITY OF PORTO, PORTUGAL

OCTOBER 2013 - JULY 2016

B.SC. IN COMPUTER SCIENCE

FACULTY OF ENGINEERING AND COMPUTING, ZAGREB UNIVERSITY, CROATIA

THESIS: SIMULATION AND VISUALIZATION OF PARTICLE SWARM OPTIMIZATION FOR PROBLEMS IN TWO-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.

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

TEACHING EXPERIENCE

LECTURER

SEPTEMBER 2022 – CURRENT
Course: Security & Privacy in AI @ FH Technikum Wien

SEPTEMBER 2022 – FEBRUARY 2024
Seminar: Scientific Writing @ FH Technikum Wien

FEBRUARY 2022 – JULY 2023
Course: Security, Privacy & Explainability in ML @ TU Wien

TEACHING ASSISTANT

FEBRUARY 2019 – JANUARY 2022
Course: Security, Privacy & Explainability in ML @ TU Wien

OCTOBER 2020 – JULY 2023
Course: Machine Learning @ TU Wien