IPP 4 ML

Intellectual Property Protection of Machine Learning Processes

Programm / Ausschreibung	FORPA, Forschungspartnerschaften NATS/Ö-Fonds, FORPA NFTE2018	**Status**	abgeschlossen
Projektstart	01.03.2020	**Projektende**	31.07.2023
Zeitraum	2020 - 2023	**Projektlaufzeit**	41 Monate
Keywords	Watermarking, Fingerprinting, Intellectual Property Protection, Machine Learning		

Projektbeschreibung

Digital data sharing is as old as digital data itself. Data creators are sharing data for commercial reasons, for increasing their reputation for valuable creations or information, for research reasons, to support the preservation of data long-term, etc. And over the last decades, the trend of sharing and processing digital data has vastly increased. Since data is a valuable asset to its owner, any type of unauthorised usage of shared data should be detected and sanctioned. With the advances in the area of Machine Learning (ML), outsourcing data and processing thereof became an increasingly popular trend among businesses. In this scope, the data is given to data management professionals that are involved in data mining, data classification etc., to make more use of the data more. This can foster business growth by additional services (recommendation systems) or customer behaviour understanding. In healthcare, for example, medical data are shared with researchers for help in medical diagnosis or other types of services that ML may provide. Furthermore, online services like Machine-Learning-as-a-Service (MLaaS) have an increasing popularity. Companies like Microsoft, Amazon and Google provide their own platforms (MS Azure, AWS, Google Cloud AI; respectively) for users to build and deploy their own Machine Learning models. Since available online, the ML models on such platforms became the target of the attackers who want to claim or use models as their own property. Protecting intellectual property (IP) is an area of study that has long been pursued both in research and real-world applications. With new types of properties, such as ML models, new ways of distributing the IP and thus new types of attacks on the schemes protecting the property, the research of IP protection must push forward with new approaches of protecting it.

The proposed research project seeks to advance the research in the area of IP protection, with the focus on the property that is a part of Machine Learning processes. Firstly, this includes the input data, which can be of various types (images, text, relational data, gene sequences, etc.). Novel aspects of research to be conducted include innovative techniques for ownership protection of mixed-type databases, applicable to real-world data bases and preserving coherence in the data. The project further addresses techniques of emergent types of data, and their effects on the result of Machine Learning processes. Secondly, novel schemes for IP protection addressing machine learning models themselves will be investigated, with the aim of protecting models from false ownership claim and model stealing attacks.

Projektpartner

- SBA Research gemeinnützige GmbH