PRIMAL

Privacy Preserving Machine Learning for Industrial Applications

Programm / Ausschreibung	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - 7. Ausschreibung (2018)	**Status**	abgeschlossen
Projektstart	01.01.2020	**Projektende**	30.09.2023
Zeitraum	2020 - 2023	**Projektlaufzeit**	45 Monate
Keywords	Trustworthy Industrial IoT; Privacy Preserving; Deep Learning; Transfer Learning; Collaborative Predictive Analytics		

Projektbeschreibung

Ausgangssituation: Google und Facebook haben bewiesen, dass die Erfassung großer Datenmengen und die Anwendung von Deep Learning prädiktive Dienste mit erstaunlicher Genauigkeit ermöglichen. Ähnliche Chancen bestehen in vielen anderen Branchen.

Problem und Motivation für das F&E-Projekt: Für industrielle Anwendungen sind jedoch große homogene Datensätze, wie sie für Deep Learning benötigt werden, oft nicht vorhanden. Transfer Learning lindert dieses Problem, da es erlaubt, Modelle auf verschiedenen (aber verwandten) Datensätzen aufzubauen. Ein weiterer vielversprechender Ansatz ist die gemeinsame Nutzung von verteilten Daten (z.B. verschiedener Abteilungen und Unternehmen), um Modelle gemeinsam zu erstellen, was allerdings datenschutzrechtliche Bedenken aufwirft. Zwei indikative Anwendungen sind: A1) Maschinenhersteller könnten die Daten ihrer Kunden nutzen, um maschinenbezogene Prognosemodelle zu erstellen; Kunden befürchten jedoch, dass sensible Informationen preisgegeben werden. A2) Materialhersteller wollen gemeinsam ein Modell zur Repräsentation von Molekülstrukturen erarbeiten, das eine effizientere Erstellung von individuellen Modellen für funktionelle Eigenschaften ermöglicht. Sie sind jedoch nicht gewillt, detaillierte experimentelle Daten zu teilen.

Ziele und Innovationsgrad: PRIMAL adressiert diese Probleme, indem privatsphärenerhaltende Verfahren für Deep Learning entwickelt werden, um gemeinsame globale Modelle unter Verwendung verteilter Datensätze so aufzubauen, dass jeder Datensatz im Privatbesitz jedes Einzelnen bleibt. Ziel ist es, private Daten jedes Einzelnen zu schützen und gleichzeitig eine maschinelle, lernbasierte Analyse der Gesamtdaten aller Beteiligten als Ganzes zu ermöglichen. Über den Stand der Technik hinaus gibt es viele offene Fragen zu klären: Schutz vor neu entwickelten Angriffen auf die Privatsphäre; Evaluierung von Methoden jenseits einfacher Bildklassifikationsaufgaben, d.h. Eignung von Ansätzen für industrielle Anwendungen; Unterstützung von Transfer- und Multitasking-Learning sowie rekurrenten Netzwerken; Schnittstellen zur Integration in Datenanalyse-Infrastrukturen einschließlich Authentifizierungskonzepten.

Erwartete Ergebnisse: Das Hauptergebnis des Projekts wird ein Software-Framework sein, das Algorithmen und Schnittstellen für die Erstellung von privatsphärenerhaltende Predictive Analytics Anwendungen für eine Vielzahl von

(industriellen) Anwendungen bereitstellt. Es wird Mechanismen bereitstellen, um (zumindest) Anwendungen zu unterstützen, die homomorph zu A1 und A2 sind. Darüber hinaus werden Transfer Learning und Multi-Task-Lernmethoden eingesetzt, um die Integration inhomogener Datenquellen in den Modellierungsprozess zu unterstützen. Um die Allgemeingültigkeit des Ansatzes zu gewährleisten, wird das Framework unter Verwendung von Daten mit unterschiedlichen Modalitäten aus verschiedenen Anwendungsbereichen entwickelt: Intralogistik, Schweißtechnologie und Bioinformatik.

Konsortium: PRIMAL bündelt alle erforderlichen wissenschaftlichen & technologischen Kompetenzen durch die Partner SCCH (privatsphärenerhaltendes maschinelles Lernen, Software-Architektur, Big Data Technologien, Deep- & Transfer Learning), Institut für Machine Learning der JKU Linz (Deep Learning, Bioinformatik), SBA Research (Security, Privacy), TGW Logistics (Intralogistik, Connected Warehouse Infrastructure) und Fronius International (Schweißtechnik, Datenanalyse-Infrastruktur).

Abstract

Initial situation: It has been demonstrated by companies like Google and Facebook that the collection of vast amounts of data and the application of deep learning enables predictive services with astonishing accuracy. Similar opportunities exist in many other industries.

Problem and motivation for the R&D project: However, for industrial applications the homogeneous sets of data required for building high quality deep (predictive) models are often scarce. Transfer learning alleviates this problem to a certain degree as it allows building models on different (but related) sets of data. Sharing data between departments and companies to collaboratively build models is another promising approach, which however raises data privacy issues. Two indicative applications are: A1) Machine and plant manufacturers may want to use their clients' data in order to build machine related prediction models; clients are concerned that process specific information is leaked. A2) Material producers may want to join efforts in developing a model for a molecule structure representation which allow more efficient training of classifiers for functional properties. However, they are not willing to share detailed experimental results.

Goals and level of innovation compared to the state-of-the-art: This project proposal addresses the aforementioned problems by using privacy preserving deep learning methods for collaboratively building global models using distributed datasets such that each dataset is privately owned by a party. The goal is to simultaneously protect private data of an individual party while permitting a machine deep learning based analysis of total data of all parties as a whole.
There are many open issues beyond the state-of-the-art to be solved: protection against recently devised privacy attacks; evaluation of methods beyond simple image classification tasks, i.e. suitability of approaches for industrial applications; support for transfer and multi-task learning as well as recurrent networks; interfaces for integration into data analysis infrastructures including authentication concepts.

Expected results and findings: The main result of the project will be a software framework providing algorithms and interfaces to build privacy preserving predictive analytics applications for a wide range of (industrial) applications. It will (at least) provide privacy mechanisms to support applications homomorphic to A1 and A2. In addition, it will employ transfer learning and multi-task learning methods to support the integration of inhomogeneous data sources into the modelling process. To ensure the general validity of the approach, the framework will be developed by using data with different modalities from different application domains: intralogistics, welding technologies and bioinformatics.

Consortium: PRIMAL combines all the required scientific & technological competences through its partners, the SCCH (privacy preserving machine learning, software architecture, big data technologies, deep and transfer learning), the Institute for Machine Learning of the JKU Linz (deep learning, bioinformatics), SBA Research (security, privacy), TGW Logistics (intralogistics, connected warehouse infrastructure) and Fronius International (welding technology, data analytics infrastructure).

Projektkoordinator

- Software Competence Center Hagenberg GmbH

Projektpartner

- SBA Research gemeinnützige GmbH
- FRONIUS INTERNATIONAL GmbH
- TGW Logistics Group GmbH
- Universität Linz