عنوان مقاله:

امنیت یادگیری فدرال و حفظ حریم خصوصی داده ها

محل انتشار:

اولین همایش ملی نوآوری در مهندسی: راهی به سوی توسعه (سال: 1402)

تعداد صفحات اصل مقاله: 8

نویسندگان:

پیمان بابائی – دانشگاه آزاد اسلامی واحد تهران غرب، دانشکده فنی و مهندسی، گروه مهندسی کامپیوتر

مهدیس ملامحمدی – دانشگاه آزاد اسلامی واحد تهران غرب، دانشکده فنی و مهندسی، گروه مهندسی کامپیوتر

خلاصه مقاله:

یادگیری فدرال به عنوان راه حلی برای حفظ حریم خصوصی داده ها، با تکیه بر آموزش مدل های محلی و بروزرسانییک مدل سراسری با استفاده از پارامترهای مدلهای محلی توسعه یافته است. از آنجائیکه طبق قانون، محدودیت هاییبرای استفاده و حفاظت از داده های محلی وجود دارد، لذا یادگیری فدرال با پیاده سازی غیرمتمرکز آموزش یک مدلسراسری، بعنوان جایگزین رویکردهای آموزش متمرکز در الگوریتم های یادگیری ماشین، ضرورت حفظ حریم خصوصیداده ها را برآورده می کند. با این حال، اخیرا دیده شده است که بازیابی داده های محلی از مدل های یادگیری همچنانامکان پذیر است. از طرفی به دلیل ماهیت توزیع شده ذاتی یادگیری فدرال، این تکنیک می تواند در برابر حملات آسیبپذیر باشد چراکه کاربران ممکن است داده های مخرب را برای تخریب مدل یادگیری محلی ارسال کنند و به طبع آنمدل سراسری نیز تخریب خواهد شد. از این رو، فضای تحقیقاتی زیادی برای بهبود چارچوب های یادگیری فدرال وجوددارد. در این مقاله، به بررسی تکنیکهای یادگیری فدرال میپردازیم و چالش ها و راه حل های موجود درخصوص امنیتآن را ارائه نموده و به جهت گیری های تحقیقاتی آینده یادگیری فدرال اشاره می کنیم.

کلمات کلیدی:

یادگیری فدرال، حریم خصوصی داده ها، آموزش غیرمتمرکز، امنیت مدل یادگیری

لینک ثابت مقاله در پایگاه سیویلیکا: