Secure distributed machine learning in healthcare: a study on FAIR, compliance and cybersecurity for federated learning

Plug, R.B.F.

Samenvatting

Kunstmatige intelligentie transformeert de gezondheidzorg: algoritmen voorspellen uitbraakcurves van epidemieën, diagnostische modellen beoordelen longfoto's in een fractie van een seconde en genetische databanken groeien met miljoenen virale genomen per jaar. Toch botsen deze technologische mogelijkheden op een weerbarstige realiteit van gefragmenteerde data, strenge privacywetgeving en toenemende cyberdreiging. Dit proefschrift onderzoekt hoe die kloof kan worden overbrugd door FAIR-dataprincipes te combineren met federatief leren en geavanceerde cryptografie.

In het eerste deel wordt het FAIR raamwerk onderzocht waaronder gezondheidsdata vindbaar, toegankelijk, interoperabel en herbruikbaar wordt gemaakt bij de bron. Door middel van FAIR Data Points en getrainde datastewards worden elektronische patiëntendossiers in acht Afrikaanse landen voorzien van semantische metadata. Zo ontstaat een netwerk waarin data vindbaar en continu herbruikbaar is voor epidemiologisch onderzoek.

Vervolgens toont het werk aan dat FAIR-datastewardship en de Europese GDPR niet alleen verenigbaar zijn, maar elkaar versterken. Een gefedereerde architectuur op basis van FAIR principes en getoetst op GDPR, waarin data eigendom blijft van de gezondheidszorginstelling, en bevraging van data verloopt via data visiting, maakt zowel juridische als ethische toetsing en toestemming transparant. De aanpak werd in 2020 voor het eerst continentaal ingezet tussen Oeganda en Nederland en bewees dat gevoelige klinische informatie inzetbaar is voor epidemiologisch onderzoek zonder fysieke dataoverdracht.

Het derde deel introduceert Secure Distributed Machine Learning (SDML), een variant van federatief leren die homomorfe encryptie en geheim-deling benut. Hiermee worden de gradiënten van het model versleuteld en verdeeld voordat ze door een aggregatieserver verwerkt

worden, zodat geen enkele partij individuele patiëntdata kan inzien of kan reconstrueren. Deze zero-trustarchitectuur maakt federatief leren geschikt voor omgevingen met beperkte infrastructuur en hoog risico op datalekken.

Tot slot valideert een simulatiestudie de praktische haalbaarheid van beveiligd federatief leren. Een versleutelde ResNet18 model voor röntgenfoto's bereikte in een tien-kliëntopstelling een ROC-AUC die nagenoeg identiek is aan de niet-beveiligde baseline, terwijl de reken-overhead voor de beveiligingsmaatregelen relatief beperkt bleef met gemiddeld één vijfde extra rekentijd. Daarmee laat het proefschrift zien dat privacy, beveiliging en diagnostische kwaliteit gelijktijdig haalbaar zijn in een federatieve opstelling.

Dit proefschrift levert een geïntegreerde onderzoek naar veilige, eerlijke en schaalbare AI-toepassingen in de detectie en diagnostiek van infectieziekte in de epidemiologie. Het biedt zowel theoretische inzichten als praktisch gereedschap voor onderzoekers, ingenieurs en clinici die willen bouwen aan een wereldwijd digitale gezondheidssysteem waarin ethiek, veiligheid én patiëntenrechten centraal staan.