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

Plug, R.B.F.

Appendix A

Summary

Artificial intelligence is reshaping health care: algorithms forecast epidemic outbreak curves, diagnostic models interpret chest radiographs within a fraction of a second and genomic repositories expand by millions of viral sequences each year. Despite these advanced technological capabilities, we face a reality of fragmented data, stringent privacy regulation and ever escalating cybersecurity threats. This dissertation explores how that gap can be bridged by combining the FAIR data principles with federated learning and advanced cryptography.

The first part of this dissertation analyses the FAIR framework, through which healthcare data are defined to be Findable, Accessible, Interoperable and Reusable at their source. By deploying FAIR Data Points and training dedicated data stewards, electronic medical records in eight African nations were enriched with semantic metadata, creating a network in which data remain findable within the network, interoperable through machine-readable format, accessible under well-defined conditions and continuously reusable for epidemiological research.

The work then demonstrates that FAIR data stewardship and the European General Data Protection Regulation are not merely compatible but mutually reinforcing and beneficial to each other. A federated architecture grounded in FAIR principles and audited against GDPR, where ownership stays with the healthcare institution and data are queried via data visiting, renders both legal and ethical audit and consent fully transparent. This method was first piloted in a cross-continent setting in 2020 between Uganda and the Netherlands, in

which the approach showed that pre-defined aggregates over sensitive clinical information can enable epidemiological studies without any physical data transfer.

The third section introduces Secure Distributed Machine Learning (SDML), a variant of federated learning that combines homomorphic encryption with secret sharing. Model gradients are encrypted and partitioned before reaching the aggregation server, preventing any party from reading or reconstructing individual patient data. This zero-trust design makes federated learning viable in settings with limited infrastructure and a high risk of data leakage to a malicious actor.

A simulation study finally validates the practical feasibility of secure federated learning. An encrypted ResNet-18 vision model for x-ray analysis achieved, in a ten-client configuration, a ROC-AUC virtually indistinguishable from the unsecured baseline, while the security measures introduced only about twenty per cent additional computation time. The dissertation thus shows that privacy, security and diagnostic performance can coexist within a federated learning framework.

Overall, the thesis provides an integrated investigation of secure, equitable and scalable AI for the detection and diagnosis of infectious diseases. It offers both theoretical insight and practical guidance for researchers, engineers and clinicians committed to building a global digital health ecosystem in which ethics, security and patient rights take centre stage.