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

Plug, R.B.F.

Stellingen behorende bij het proefschrift getiteld

Secure Distributed Machine Learning in Healthcare:
A Study on FAIR, Compliance and Cybersecurity for
Federated Learning

1. Data sovereignty is a necessity for regulatory compliance in the medical domain. **(this thesis)**

2. The FAIR principles are viable guidelines for the machine-interoperability of clinical data across distributed, heterogeneous health systems. **(this thesis)**

3. Combining data locality and cryptographic guarantees enables secure distributed machine learning in regulated environments on medical data. **(this thesis)**

4. Incorporating homomorphic encryption and secret sharing into federated aggregation achieves state-of-the-art security and privacy-preservation for clinical model training, without degrading model convergence under constrained edge environments. **(this thesis)**

5. Data curation redefines the economics of data: what is costly to generate becomes valuable to share.

6. Data quality is the new gold standard: higher quality data yields better results than simply investing in more compute or bigger models.

7. In medical machine learning, accuracy without transparency and accountability is a clinical risk. Model performance is meaningful only when its provenance and limitations are known to those affected by its decisions.

8. The defining test of any medical AI is not whether it outperforms humans, but whether it preserves human agency in decisions that concern health and dignity.

9. We measure progress by what we automate, yet progress is better measured by what we choose not to.

10. Research is less about finding answers and more about learning which questions are worth asking.