



Delft University of Technology

Document Version

Final published version

Citation (APA)

Huang, J. (2026). *Detecting Vulnerabilities of Heterogeneous Federated Learning Systems*. [Dissertation (TU Delft), Delft University of Technology]. <https://doi.org/10.4233/uuid:4c0ba115-3376-48a9-9071-91adfbcbd044>

Important note

To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright

In case the licence states "Dutch Copyright Act (Article 25fa)", this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership. Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Propositions

accompanying the dissertation

DETECTING VULNERABILITIES OF HETEROGENEOUS FEDERATED LEARNING SYSTEMS

by

Jiyue HUANG

1. Owning real data, as oppose to having no data at all, does not necessarily enable an attacker to launch stronger attacks on federated learning systems. [This thesis]
2. A good strategy to enhance privacy against data reconstruction in a federated learning system is to increase the local training batch size. [This thesis]
3. The interpretability of diffusion models lies in more than the inference output: knowledge is also hidden in the input noise, as the model can generate better samples by tailoring the input. [This thesis]
4. Although enhancing privacy and security are important motivations for distributed machine learning systems, they are the killers of early-phase research of such systems.
5. In distributed systems, there has to be a trade-off between the importance of knowing the contribution of each party and the overhead of measuring the contributions.
6. Complex training algorithms are more effective in centralized machine learning, but simple strategies are more effective in distributed machine learning.
7. Privacy in distributed machine learning systems can be enhanced by local data generation, turning crowdsourcing data into crowdsourcing computation.
8. Agreement is the heart and the soul of distributed systems.
9. Future hot distributed Artificial Intelligence applications will be based on multi-modal data integration.
10. The start of designing a game is to create a world-view.

These propositions are regarded as opposable and defensible, and have been approved as such by the promotors Em. prof. dr. ir. D.H.J. Epema, Prof. dr. S. Roos, and the promotor Prof. dr. Y. Chen.