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 defendable, and have been approved as such by the promotors Em. prof. dr. ir. D.H.J. Epema, Prof. dr. S. Roos, and the copromotor Prof. dr. Y. Chen.