Attacking and Protecting Data Privacy inEdge-Cloud Collaborative Inference Systems

ABSTRACT:

Benefiting from the advance of Deep Learning technology, IOT devices and systems are becoming more intelligentand multi-functional. They are expected to run various DeepLearning inference tasks with high efficiency and performance.This requirement is challenged by the mismatch between thelimited computing capability of edge devices and large-scaleDeep Neural Networks. Edge-cloud collaborative systems are thenintroduced to mitigate this conflict, enabling resource-constrained IoT devices to host arbitrary Deep Learning applications.However, the introduction of third-party clouds can bringpotential privacy issues to edge computing. In this paper, weconduct a systematic study about the opportunities of attackingand protecting the privacy of edge-cloud collaborative systems.Our contributions are twofold: (1) we first devise a set of newattacks for an untrusted cloud to recover arbitrary inputs fed intothe system, even if the attacker has no access to the edge device'sdata or computations, or permissions to query this system. (2)We empirically demonstrate that solutions that add noise fail todefeat our proposed attacks, and then propose two more effectivedefense methods. This provides insights and guidelines to developmore privacy-preserving collaborative systems and algorithms.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15’’ LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 10.
- Coding Language : Java
- Web Framework : Flask

REFERENCE:

Z. He, T. Zhang and R. B. Lee, "Attacking and Protecting Data Privacy in Edge–Cloud Collaborative Inference Systems," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9706-9716, 15 June15, 2021, doi: 10.1109/JIOT.2020.3022358.