

Friday, 8 November 2019 10:00 (20 minutes)

(Machine Learning) 本文提出了一种基于同态加密的机器学习框架，旨在保护用户数据隐私。该框架支持多种机器学习模型，包括线性回归、逻辑回归、决策树、神经网络等。通过引入同态加密技术，用户可以在加密状态下进行模型训练和推理，确保数据在传输和存储过程中不被窃取或篡改。

(Training) (Inference) 本文提出的框架支持两种操作模式：训练（Training）和推理（Inference）。在训练模式下，用户可以将加密数据输入模型，模型会在加密状态下进行参数更新。在推理模式下，用户可以将加密数据输入训练好的模型，模型会在加密状态下进行预测。两种模式均支持私有化（Private AI），确保用户数据在模型训练和推理过程中始终保持加密状态。

本文提出的同态加密机器学习框架，为保护用户数据隐私提供了一种有效的解决方案。通过引入同态加密技术，用户可以在加密状态下进行模型训练和推理，确保数据在传输和存储过程中不被窃取或篡改。该框架支持多种机器学习模型，包括线性回归、逻辑回归、决策树、神经网络等。通过引入同态加密技术，用户可以在加密状态下进行模型训练和推理，确保数据在传输和存储过程中不被窃取或篡改。

Presenter: Prof. CHEON, Jung Hee (Seoul National University)

Session Classification: Invited talks - Math & Stats 2