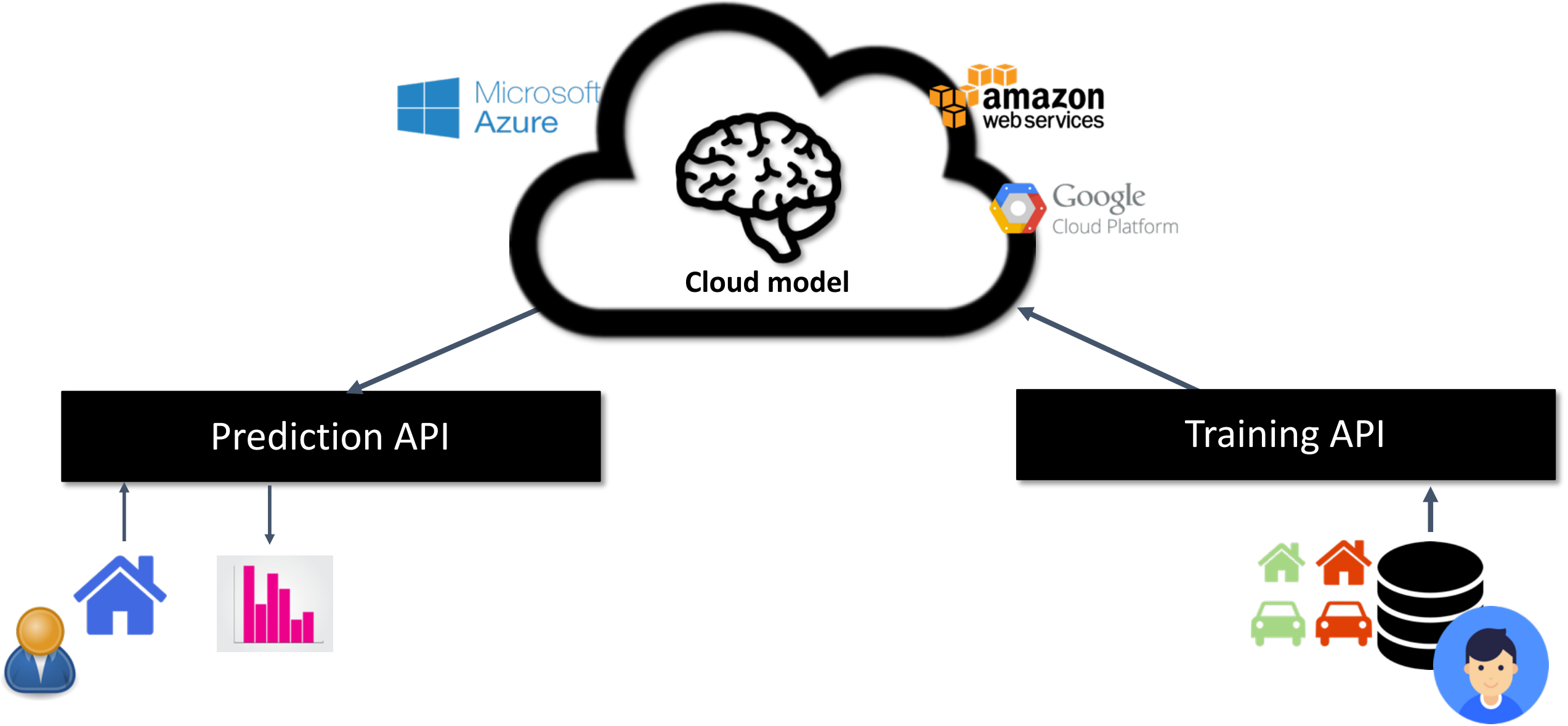
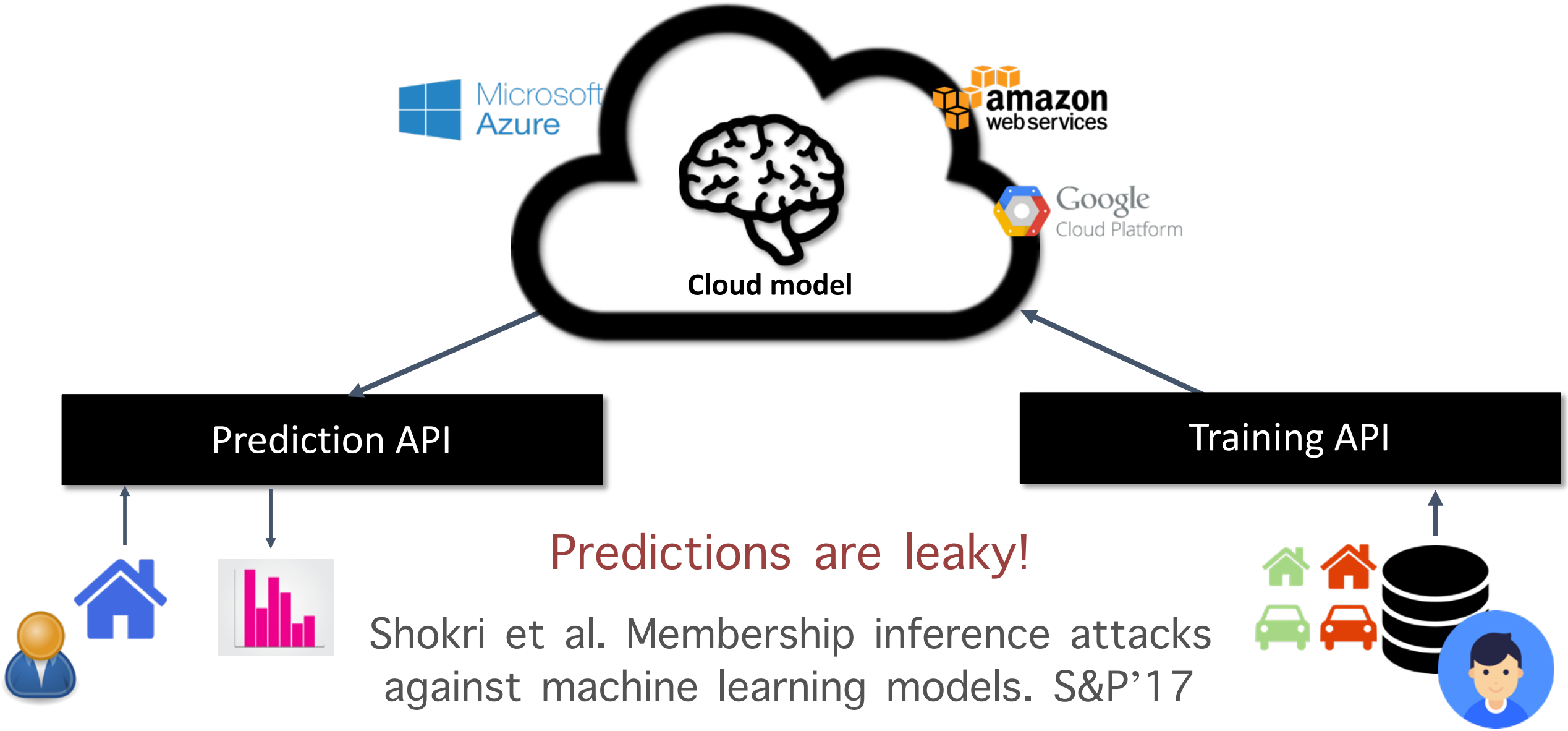
Machine Learning as a Service

Predictions are leaky!

Shokri et al. Membership inference attacks against machine learning models. S&P'17


Microsoft Azure
amazon web services
Google Cloud Platform
Cloud model
Prediction API
Training API

Machine Learning as a Service



Predictions are leaky!

Shokri et al. Membership inference attacks against machine learning models. S&P'17

Membership Inference in Generative Models