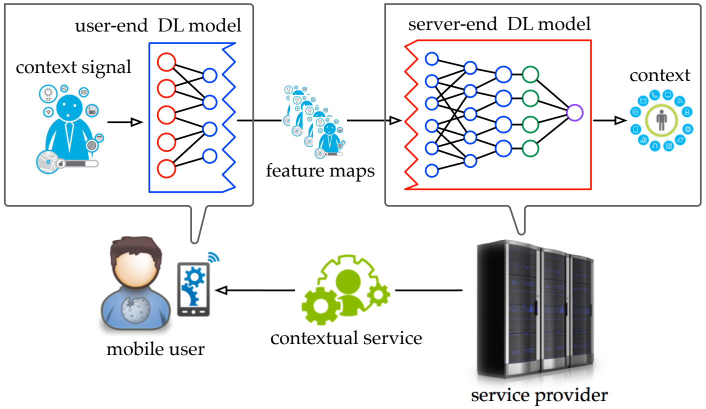
Re-Envisioning Contextual Services and Mobile Privacy in the Era of Deep Learning

National Science Foundation

LEHIGH UNIVERSITY.

Challenges:

- Immense privacy threat of DL-powered mobile contextual services
- Array of semantic-rich context data (e.g., image, audio, sensory, text)
- Multiple desiderata for privacy protection solutions (e.g., system overhead, communication cost, service quality, attack resilience)
- Support for current and future DL-powered mobile contextual services



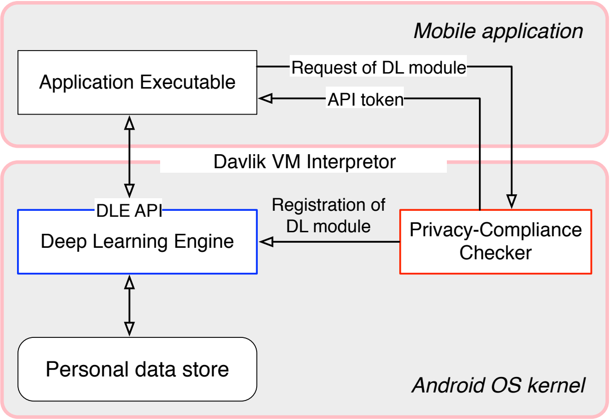
Privacy-Aware Deep Learning of Contextual Knowledge (PADLOCK)

Scientific Impact:

- Understanding of the fundamental tradeoff between privacy protection, communication cost, system overhead, and service quality
- Theoretical advances in optimizing multiple objectives under the setting of DL computation
- Innovation of enforcing protection against malicious service providers following varied attack models
- Development of a testbed to enable automated investigation of privacy leakage in mobile applications

Solutions:

- New privacy definitions tailored to DL-powered contextual services
- Analytical formulation of tradeoff among privacy protection, computational and communication costs, and service quality
- Divisive execution of DL computation that allows users to flexibly control such tradeoff
- Lightweight static and runtime privacy policy compliance checking



Mobile application

Application Executable

Request of DL module

API token

Davlik VM Interpretor

DLE API

Deep Learning Engine

Registration of DL module

Privacy-Compliance Checker

Personal data store

Android OS kernel

System design of PADLOCK

Broader Impact:

- Re-thinking how to build a healthy ecosystem for data-driven business so that every member (e.g., user, service provider, app developer) is benefited
- Facilitating the adoption of DL-powered mobile contextual services
- Deepening our understanding on developing privacy-aware personalized services
- Developing new course on “privacy-aware data analytics”

Award #: CNS-1566526 Investigator: Ting Wang (tiw315@lehigh.edu) Start date: 07/01/2016 Sponser: Lehigh University