A Unified Framework for IoT Privacy

Hossein Pishro-Nik (PI), Dennis L. Goeckel (Co-PI), Amir Houmansadr (Co-PI)

Univerisity of Massachusets Amherst

http://www.ecs.umass.edu/ece/pishro/privacy.html

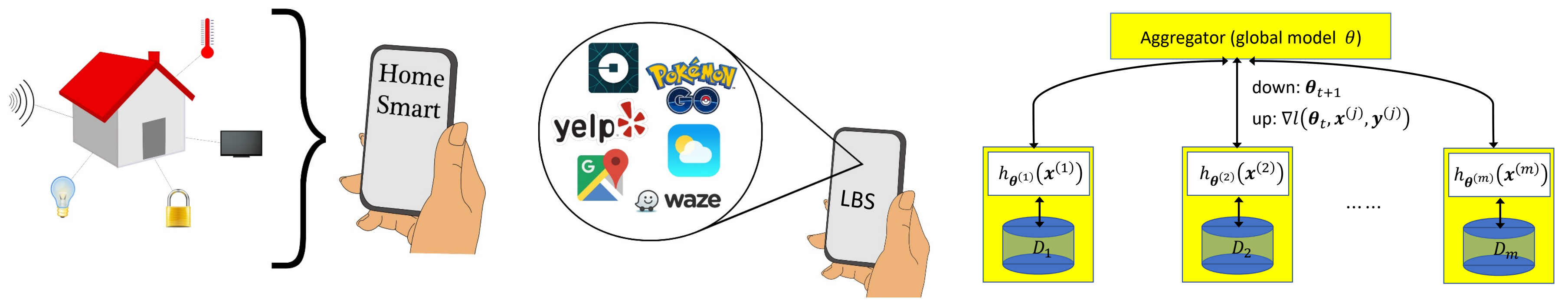
Challenge:

- IoT users gain significant *utility* by sharing data with applications
- Such sharing can compromise our *privacy*
- If we do not know the model of users' data

Solution:

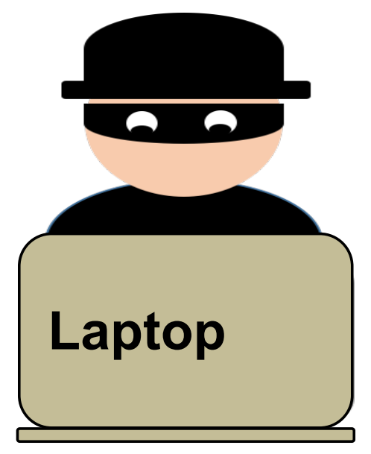
- Study methods and utility loss required for *perfect privacy* (no information leakage)
- Proposed:
  - – Degree of anonymization or obfuscation required
  - –*Randomized Remapping* for improving PUT
  - – Novel methods for thwarting pattern matching attacks

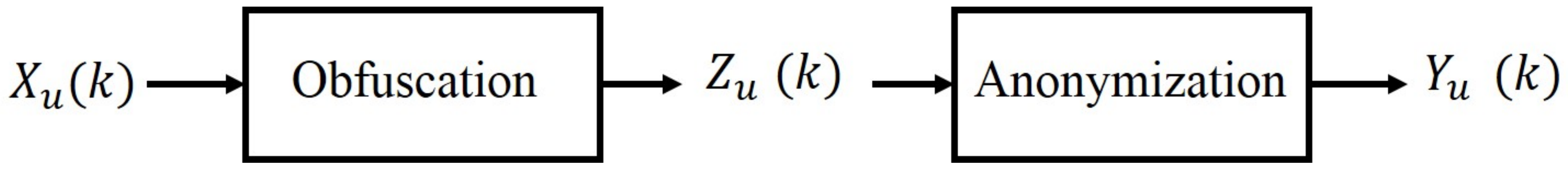
- **Internet of Things (IoT)** will revolutionize our lives.


Home
Smart
yelp
waze
LBS
Aggregator (global model θ)
down: $\boldsymbol{\theta}_{t+1}$
up: $\nabla l(\boldsymbol{\theta}_t, \boldsymbol{x}^{(j)}, \boldsymbol{y}^{(j)})$
$h_{\boldsymbol{\theta}^{(1)}}(\boldsymbol{x}^{(1)})$
$h_{\boldsymbol{\theta}^{(2)}}(\boldsymbol{x}^{(2)})$
$h_{\boldsymbol{\theta}^{(m)}}(\boldsymbol{x}^{(m)})$
D_1
D_2
D_m
……

1. Smart Homes 2. Location based services 3. Distributed Machine Learning

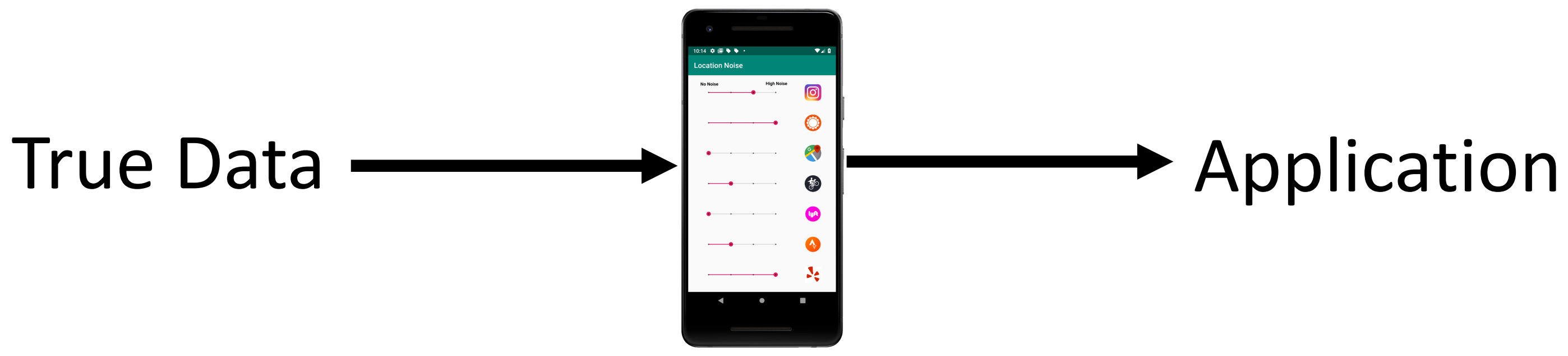
- Significant **privacy leakage** due to:
  - Large amount of data generated
  - Powerful **statistical inference** techniques





Scientific Impact:

- Provide a framework to protect against information leakage via statistical matching
- Demonstrate challenges of privacy, particularly for dependent users
- Establish a new framework for privacy against pattern-matching attacks



Tunable Obfuscation App

Broader Impact (impact on society who will care)

- Derive the fundamental limits of user privacy for IT society
- Provide potential solution for quantifying privacy leakage in distributed machine learning for ML society

Broader Impact (education and outreach)

- App developed by UMass undergrads for tunable obfuscation for different applications
- Supported multiple Ph.D. students, one now at QualComm, and undergraduate students in paper authorship
- PI Pishro-Nik a leader in supporting open access content (undergraduate probability text)

Broader Impact (quantify potential impact)

- The proposed project has the potential to produce theory to design and evaluate privacy preserving mechanism for real-world applications, impacting hundreds of million of users.

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: CNS-1739462