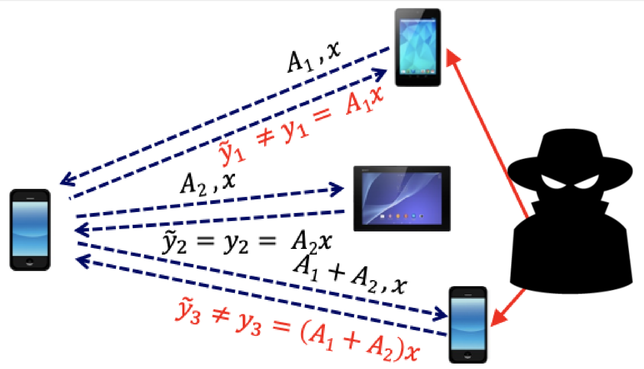
Secure Distributed Coded Computations for IoT

PIs: Yingying Chen[1], Salim El Rouayheb[2], Hulya Seferoglu[3]
[1,2]Rutgers University, [3]University of Illinois at Chicago

[1]http://www.winlab.rutgers.edu/~yychen/, [2]http://eceweb1.rutgers.edu/~csi/, [3]http://nrl.ece.uic.edu/

Distributed Learning in Mobile Internet-of-Things

- Coded computation algorithms have been proposed to securely distribute matrix operations to worker devices but have yet to be adapted for mobile platforms beyond theoretical means.
- We study existing distribution schemes from an operational complexity and security viewpoint in several mobile IoT networks, identifying performance bottlenecks regarding communication and computation costs.
- We propose new, scalable algorithms optimized to handle the unique constraints of mobile IoT.



Challenges

- Adapting computationally heavy cryptographic solutions for mobile IoT with limited or shared resources.
- Preservation of data privacy in potentially untrustworthy networks.
- Optimizing matrix multiplication energy efficiency for hardware with limited computing resources and smaller battery capacities.
- Scalability for heterogeneous mobile IoT devices.

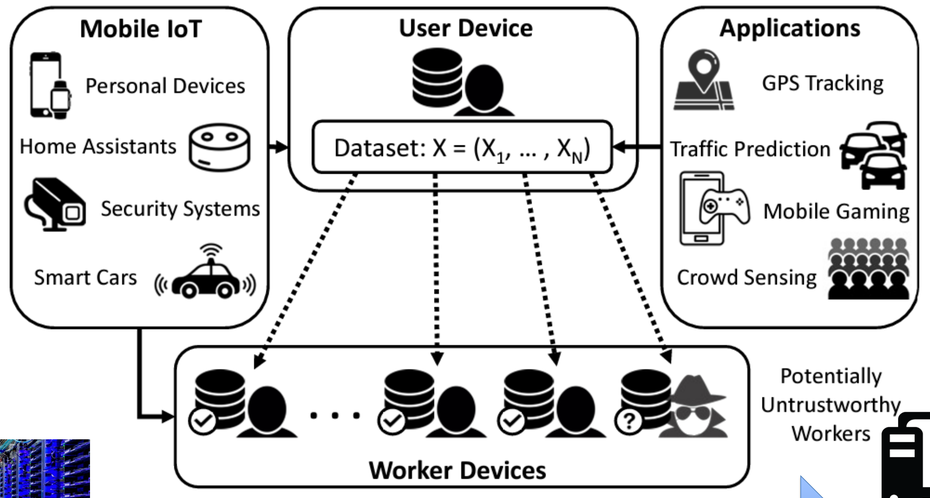
Scientific Impacts

- Data such as images, audio, and text can be represented as matrices to facilitate efficient computation, especially in the domains of distributed machine learning, computer vision, and signal processing.
- Secure distributed matrix multiplication (SDMM) can provide information theoretic security across a scalable and heterogenous IoT network.

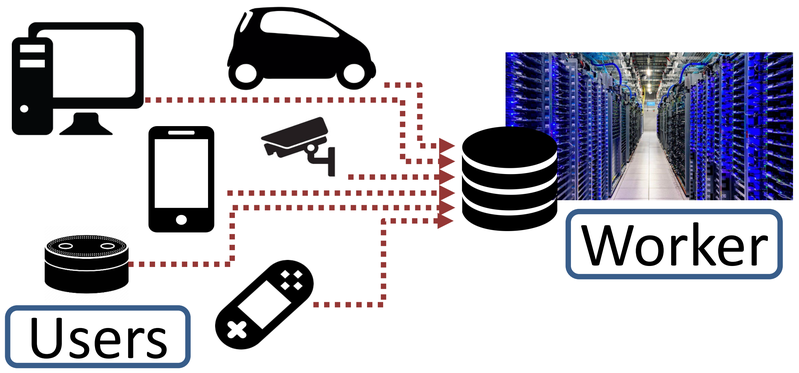
Approaches

Offloading Computational Burden to Third-Party Services vs. Shared Computational Burden in the Mobile IoT Through Coded Computation

- Dedicated data centers are powerful but difficult to scale and have full knowledge of user data, making them lucrative targets of multiple threat models.

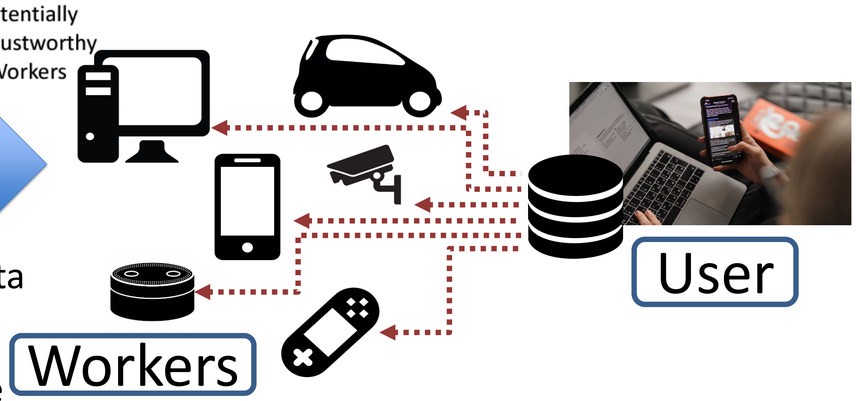


- Computational tasks can be distributed across multiple devices, leaving only the user in full control of their own data.
- Data can be partitioned such that curious or malicious worker devices cannot reverse-engineer the full user data.



4-Phase Distributed Learning

1. Quantize data and partition for workers
2. Generate random matrices to encode data
3. Send partition to worker for local SDMM
4. Return partial solution to user for update (repeat Phase 3 & 4 until convergence)



Broader Impacts

- Secure and optimize the handling of sensitive data shared in mobile IoT networks
- Include curriculum development, outreaching to K-12 students
- Improve mobile applications through safer, faster, energy-efficient mobile computing