Edge-enabled Utility-Preserving Privacy for Data-driven CPS Systems

Prashant Shenoy

University of Massachusetts, Amherst

Data-driven CPS Systems

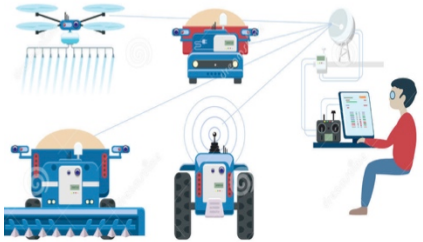
- Emergence of the Internet of Things: Network of Physical Devices
  - Low-cost embedded hardware, ubiquitous wireless connectivity
  - Sensing and computing "everywhere"
- Data-driven CPS systems: sense-analyze-respond applications

Smart Health

Smart Buildings

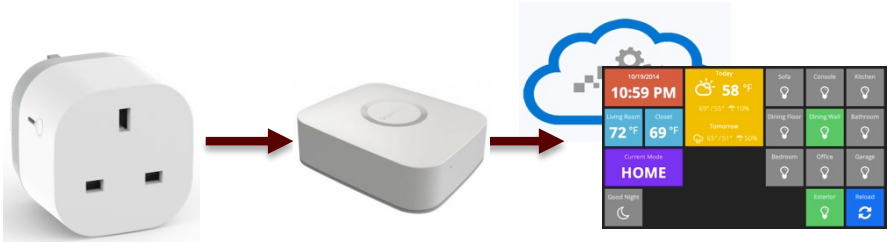
Smart Transportation

Smart Agriculture



Three-tier Model for Data-driven CPS Systems

Examples

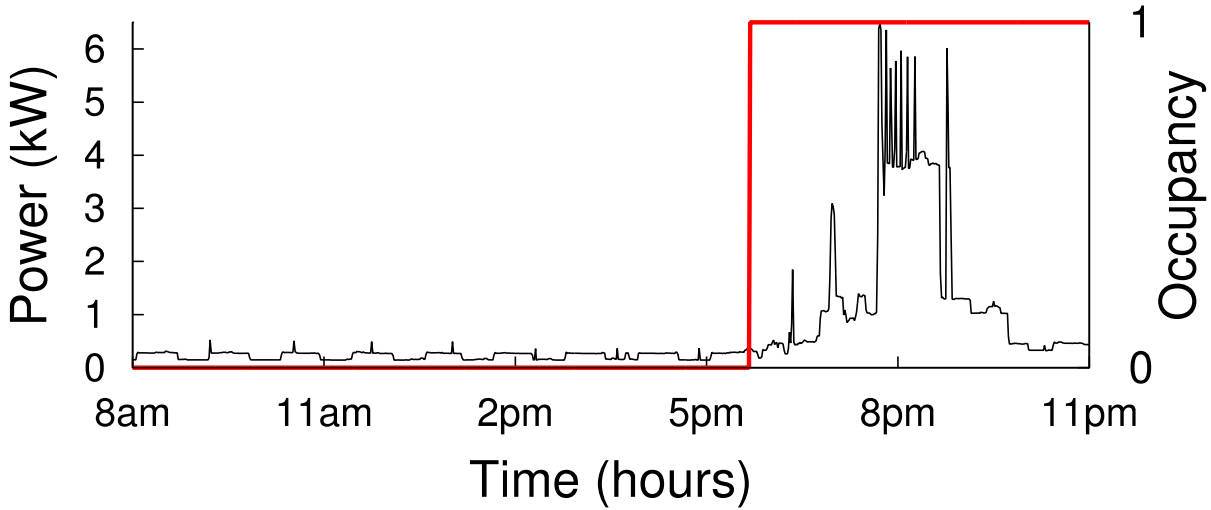


CPS Data Embeds Private Information

- Data from CPS devices embeds private information
- Monitored data may be private/sensitive
  - Apple watch heart rate sensor:
- CPS data often reveals host of other information
  - Susceptible to side-channel attacks
- Data sent to cloud subjected to sophisticated ML analysis
  - May reveal unintended information beyond the actual data

Building CPS Systems

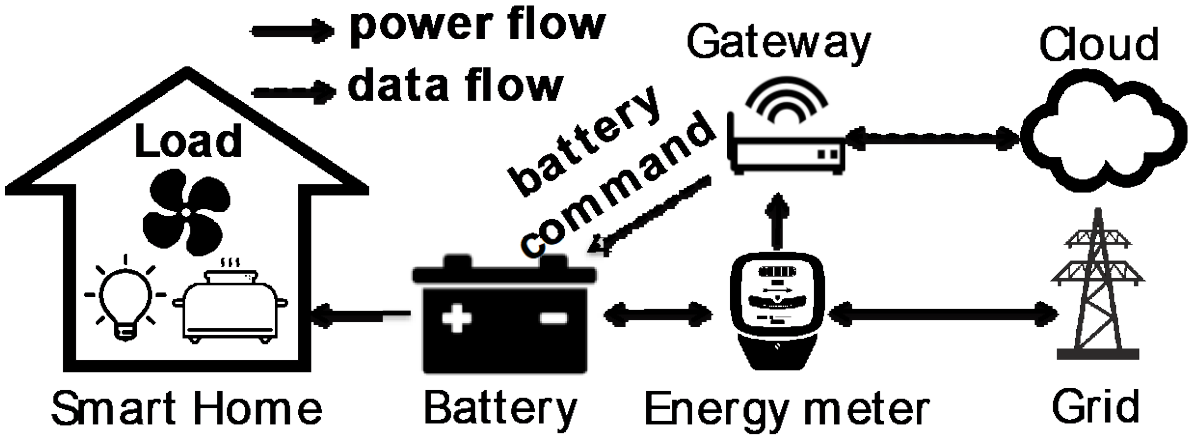
- Electricity usage in your home reveals when you are home or away (occupancy)
- Papers report up to 90% accuracy



Utility-Preserving Privacy

- Data obfuscation removes ”all” information
  - Both private and non-private information gets obfuscated
- Utility-preserving transformations: suppress private information embedded in data but reveal non-private information
- Enables useful analytics but prevents privacy attacks

Role of Edge in Utility-Preserving Privacy



Concluding Remarks

- Data-driven CPS systems becoming common
  - Side-channel information leakage common
- Need methods to preserve privacy while retaining data utility
- Edge architectures can enable user privacy