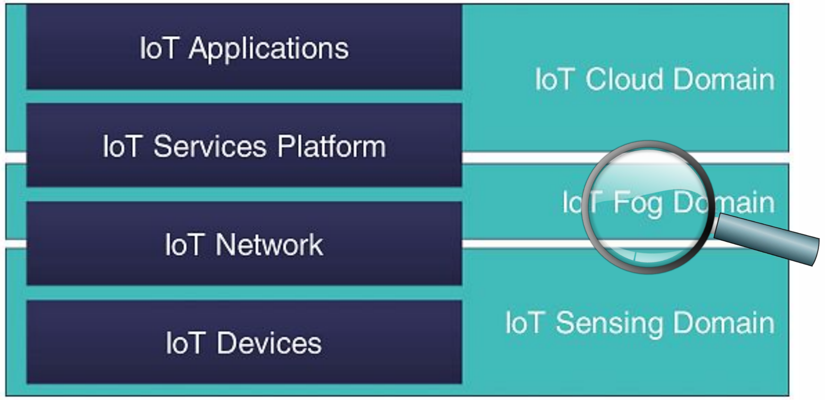
Ch. 14 - IoT Security and Privacy

Sec 3 – Fog Domain

COMPSCI 244p
Internet-of-Things; Software and Systems

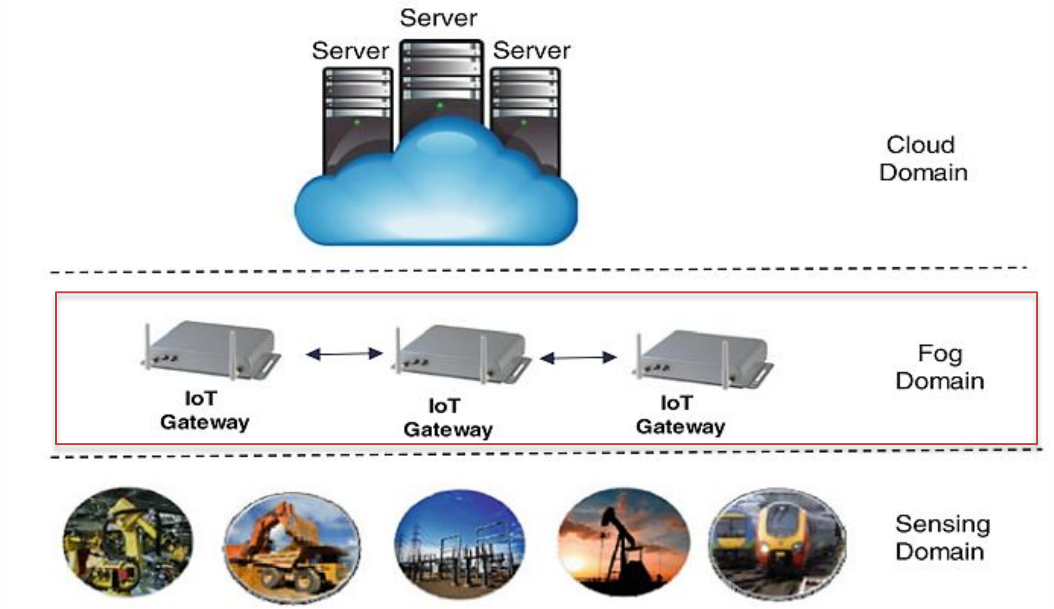


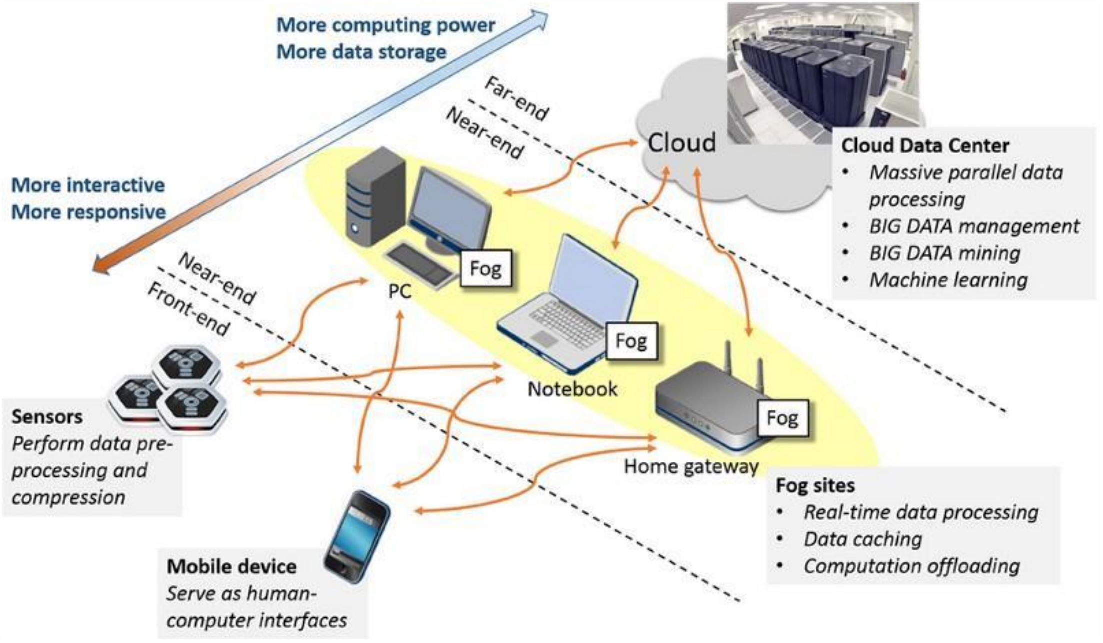
Fog Domain Attacks and Countermeasures

- Fog device provide computing resources for IoT smart objects close to them.
  - These computing resources are **virtualized**
  - Allowing the connected objects to **share** the computing resources

- Virtualized environments provided by fog devices are very **similar** to servers.

- **Fog domain can be susceptible to all the cloud domain attacks.**





Fog Domain Attacks and Countermeasures
Cloud vs fog - key differences

- **Location**
  - Quick response
  - Location-aware services

- **Mobility**
  - VMs handling smart objects must be moved for mobile objects
  - Keeping the processing close to objects

- **Lower Computing Capacity**
  - A lower computing capacity compared to cloud data center

Fog Domain Attacks and Countermeasures threats specific to the fog domain

1. **Authentication and Trust Issues.**
   - Fog devices are expected to be owned by multiple and **less-known entities.**
   - **Mobility** may cause **switching** between fog devices with different owners.
   - To authenticate first the **identity of the owner** of the fog device.
   - To decide whether the **owner** of the fog device can be **trusted.**

- **Countermeasure**:
  - **Reputation** systems can be used to select a trustworthy fog device.
    - E.g.: Proposed in peer-to-peer networks or to rank cloud providers.

Fog Domain Attacks and Countermeasures threats specific to the fog domain

2. Higher Migration Security Risks

- VM migration in the cloud mostly happens over the cloud' s **internal** network or VPN
- The migrations in the fog layer are carried over the **Internet**!

- **Countermeasure**
  - Vital to **encrypt** the migrated VM and to **authenticate** the VM migration messages exchanged among the fog devices

3. Higher vulnerability to DoS Attacks

- Lower computing capacities => easier to overwhelm

Fog Domain Attacks and Countermeasures threats specific to the fog domain

4. Privacy Issues

- Fog device can **infer the location** of all the connected objects.
- Fog devices can track users or to know their commuting habits.
- Capturing and analyzing the wireless signals that are exchanged between the sensing objects and the fog domain.
  - identify the presence of humans, track their location, even their heartbeats.

- **Countermeasure**
  - Using **obfuscator** that emit signals that make it hard for an unauthorized receiver to infer : the amplitude, frequency and the time shift of the originally exchanged signals.

Fog Domain Attacks and Countermeasures threats specific to the fog domain

5. Additional Security Threats due to Container Usage

- Using **container-based** virtualization over **full-virtualization** due to its lower overhead.
- Containers share not only the same **hardware** but also the same **operating system.**
- More opportunities for data leakage and for hijacking the fog device.

Countermeasure

- The industry needs to address these gaps in container security to enable IoT applications at scale.