

PidLoc Issues in Edge Computing

Tuesday July 28, 2020 IETF 108

Side Meeting

Dirk von Hugo

Behcet Sarikaya

OUTLINE


- Current PS draft
<https://tools.ietf.org/html/draft-iannone-pidloc-privacy> based on Erik Nordmark's work
<https://tools.ietf.org/html/draft-nordmark-id-loc-privacy> requiring stronger relation to specific use case and application
- Main topic: Use of pidloc in Edge Computing
- Following considerations are based on "IoT Edge Challenges and Functions" draft:
<https://tools.ietf.org/html/draft-hong-t2trg-iot-edge-computing-05>

IoT Edge Challenges and Functions

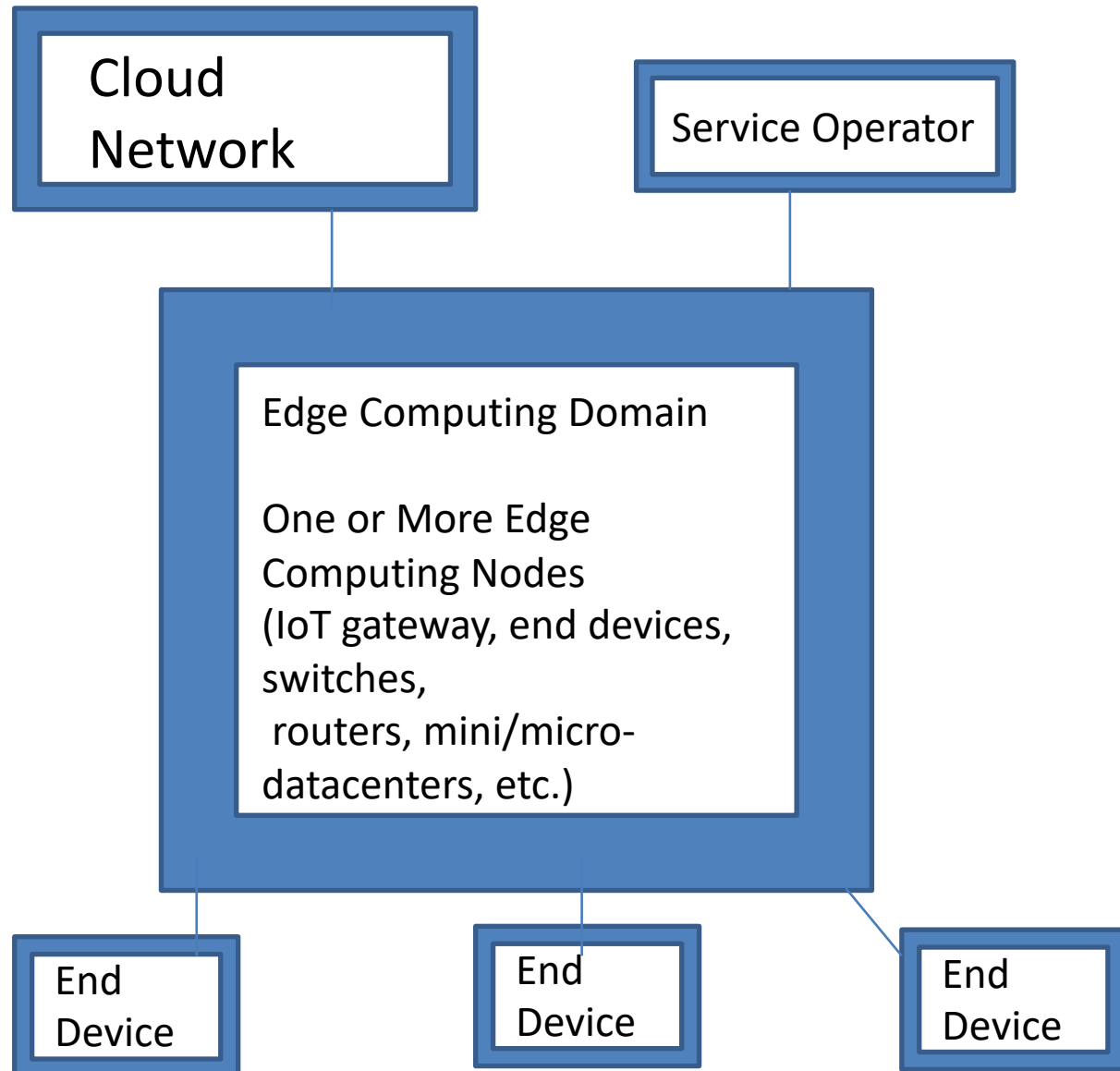
- challenges met by IoT that are motivating the adoption of edge computing for IoT
- **Time Sensitivity**
 - stringent end-to-end latency between the sensor and control node
- **Uplink Cost**
 - cost for high-bandwidth connectivity to upload all data to the Cloud is unjustifiable and impractical for most IoT applications
- **Resilience to Intermittent Services**
 - sensors, data collectors, actuators, controllers, etc. have very limited hardware resources and cannot rely solely on their limited resources to meet all their computing and/or storage needs. They require **reliable, uninterrupted or resilient services** to augment their capabilities in order to fulfill their application tasks
 - **hard to achieve with cloud services**

challenges of edge computing

(Cont'ed)

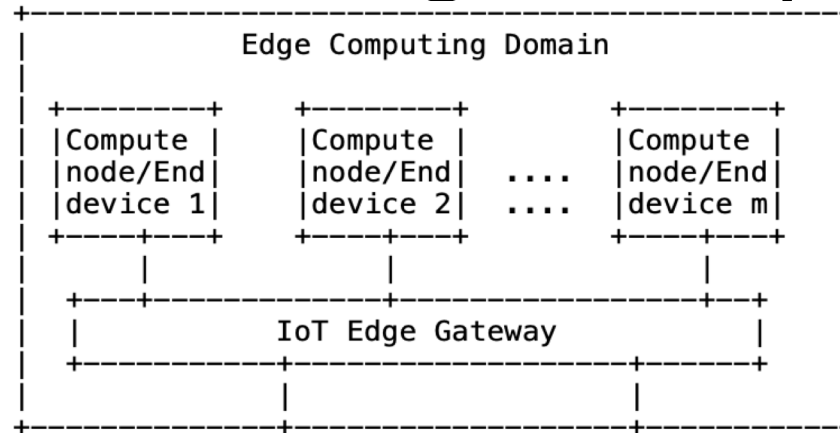
- **Edge cloud resources** distributed over multiple providers' domains (operators, data center providers, 3rd parties, verticals ...) raise privacy and security issues
- **Privacy and Security**
 - personal information can be learned from detected usage data from home IoT usage. For example, one can extract information about employment, family status, age, and income by analyzing smart meter data
- data from industrial IoT is often also highly sensitive, as one might be able to infer trade secrets such as the setup of production lines
- passive observers can perform traffic analysis on the device-to-cloud path. Hiding traffic patterns associated with sensor networks can therefore be another requirement for edge computing
-  Can we say that we definitely need pidloc?

Model of Edge Computing

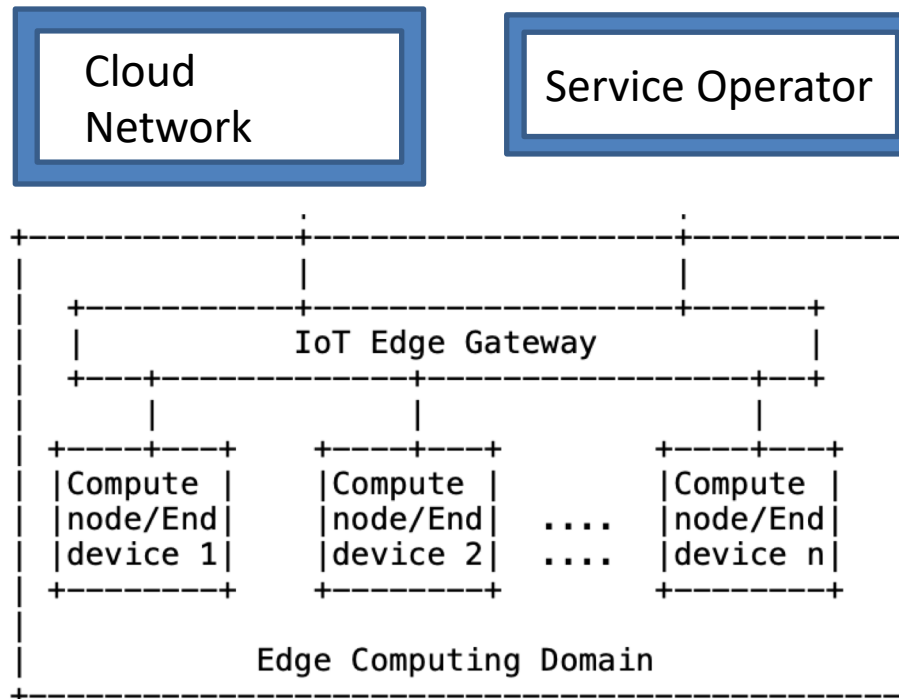


Distributed Edge Computing

a distributed
machine learning
application



the **training**
process for AI
services is executed
at **IoT edge**
gateways or cloud
networks and
the **prediction**
(inference) service
is executed in the
IoT end devices



Discussion

- Privacy and security issues in Edge Computing as a good background to justify IdLoc (LISP, ILA, ILNP, ...) systems?
- Detailed studies of course needed and drafts based on those
- One issue: which idloc system or systems to concentrate?
- Can we consider some **not** adequate?

Questions

- **Subscribe to pidloc ML**
- **<https://www.ietf.org/mailman/listinfo/pidloc>**
- **Questions?**