Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems

Glen Cathey[1], James Benson[2], Maanak Gupta[1], and Ravi Sandhu[2]

**[1]Dept. of Computer Science, Tennessee Technological University,
Cookeville, Tennessee 38505, USA
[2]Dept. of Computer Science and Institute for Cyber Security
University of Texas at San Antonio, TX 78249, USA**

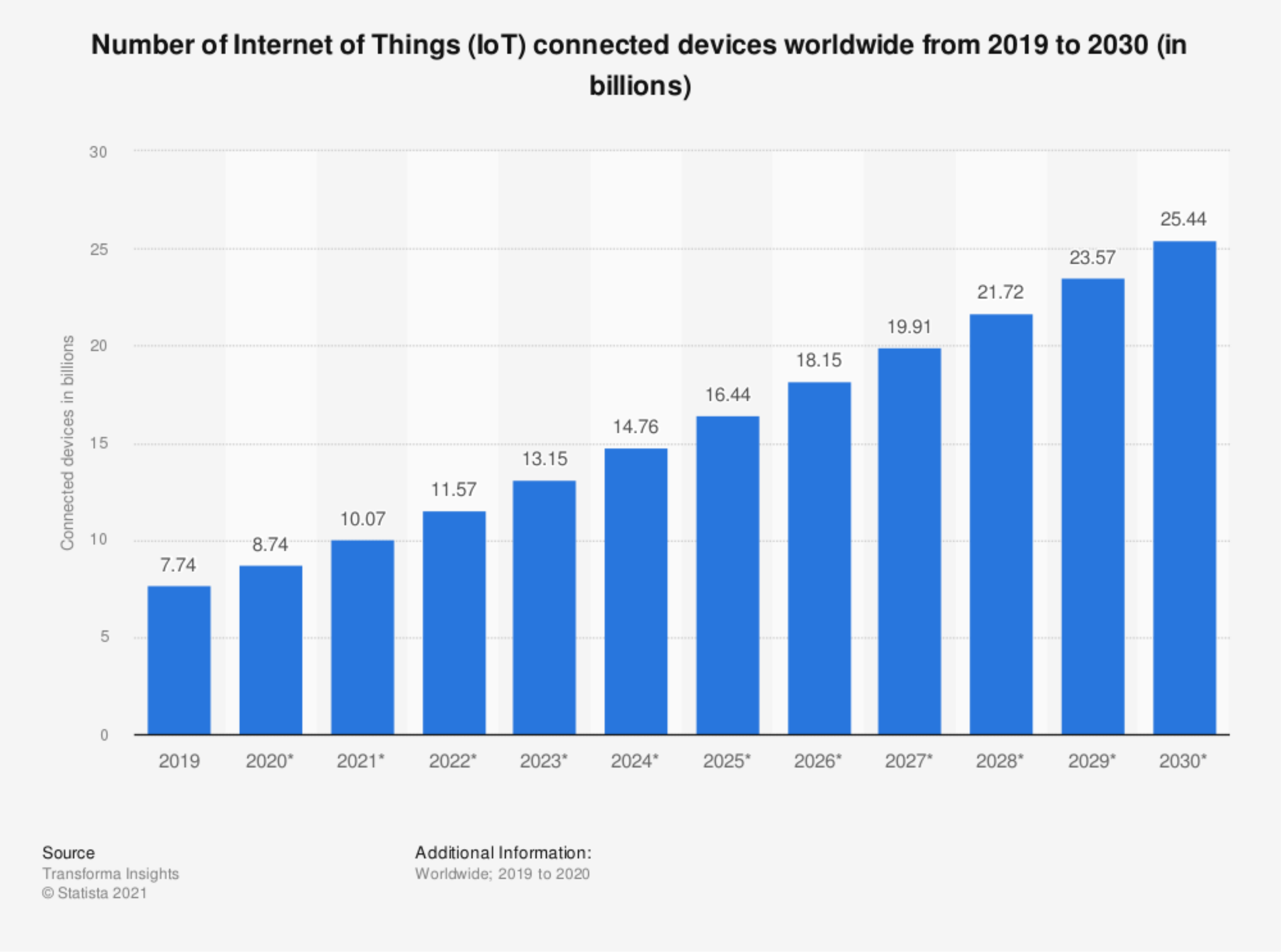
TPS 2021, Dec. 13, 2021

Outline

- IoT Background
- ACO Architecture
- Clustered Objects
- Digital Twins and Current State of the Market
- TBAC and our implementation
- Results
- Future Direction

A. Holst, "IoT connected devices worldwide 2019-2030," Jan 2021. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected- devices-worldwide/

IoT Devices Prediction



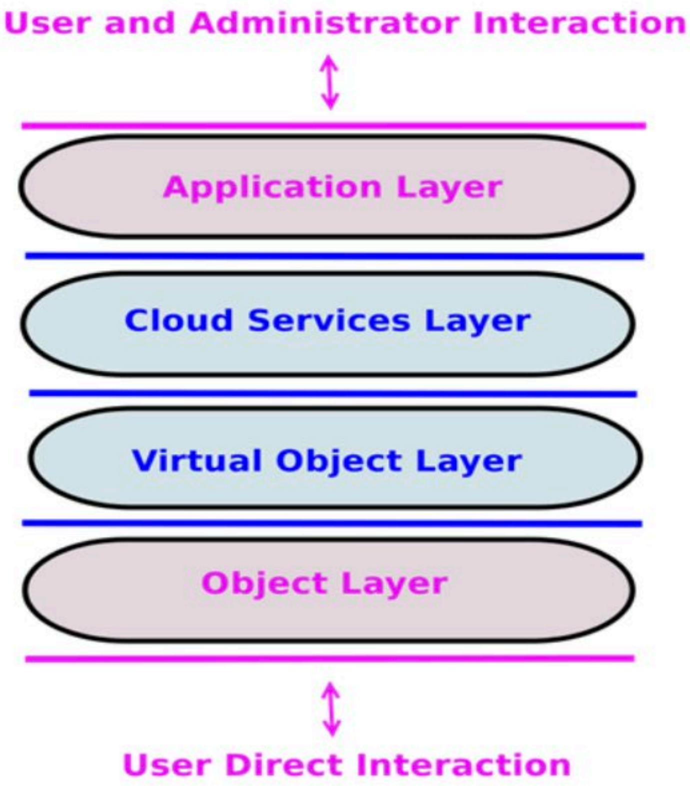
Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030 (in billions)

Source
Transforma Insights
© Statista 2021

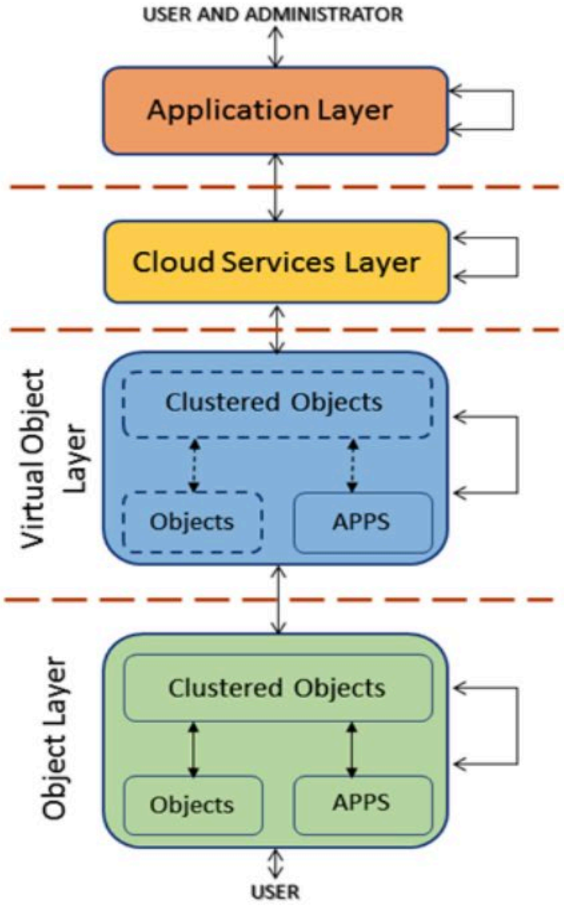
Additional Information:
Worldwide; 2019 to 2020

A. Holst, “IoT connected devices worldwide 2019-2030,” Jan 2021. [Online].
Available: https://www.statista.com/statistics/1183457/iot-connected- devices-worldwide/

ACO Architecture

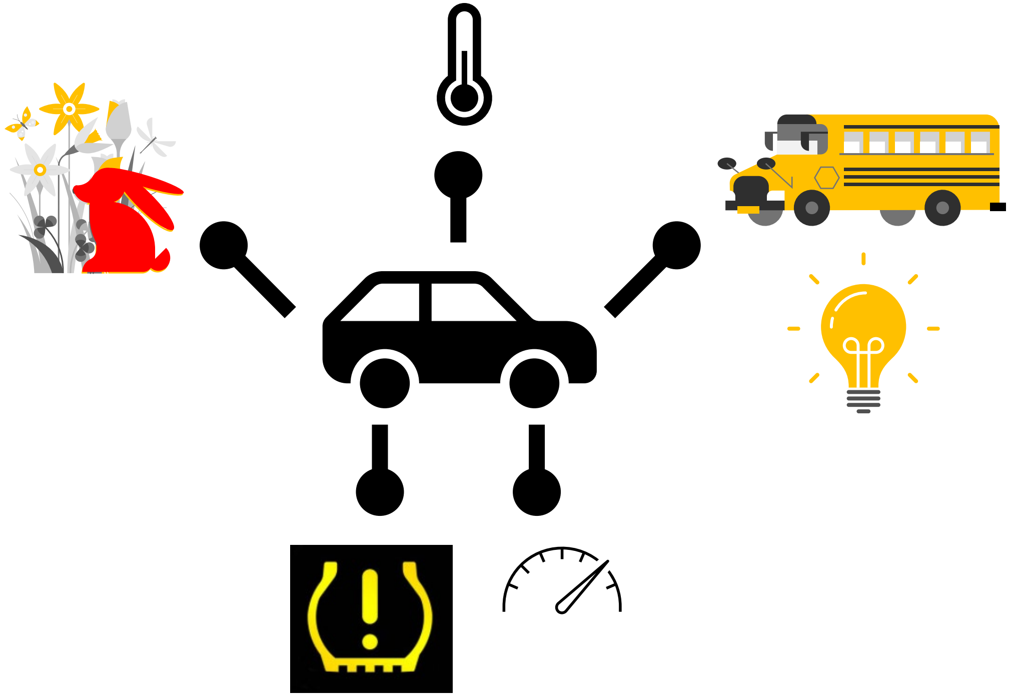


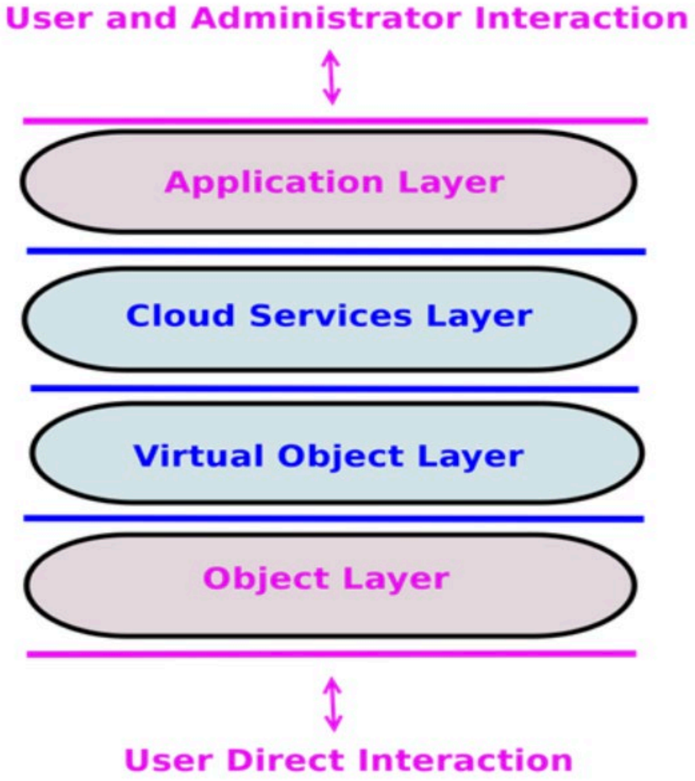
a) Access Control Oriented Architecture



b) Extended Access Control Oriented Architecture

Example of Clustered Obj.





User and Administrator Interaction

Application Layer

Cloud Services Layer

Virtual Object Layer

Object Layer

User Direct Interaction

Current Security Measures

Two main common methods consist of:

- ❖ Encryption security measures
- ❖ Multifactor Authorization

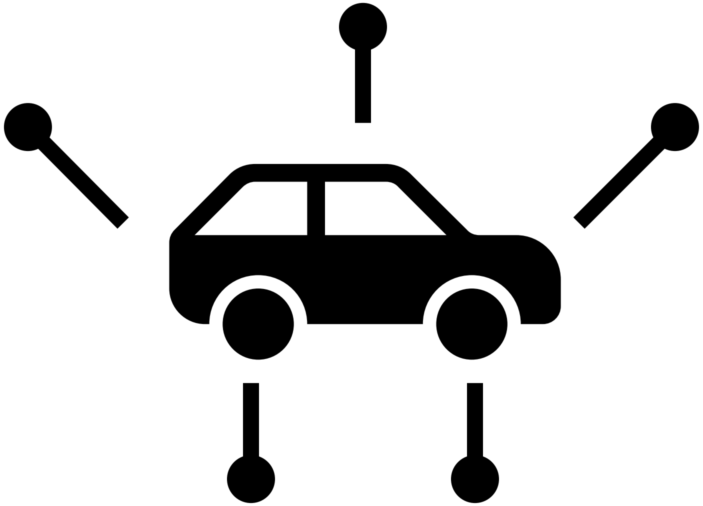
Limits:

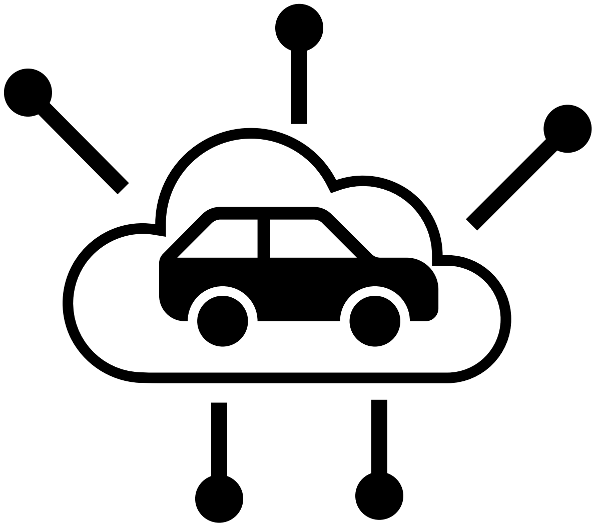
- ❖ Encryption requires more powerful IoT devices
- ❖ Multifactor only grants access, it does not limit how data is shared.

Digital Twins

Digital twins are virtual counterparts to physical devices.

These twins help facilitate separation between objects and cloud services layer.





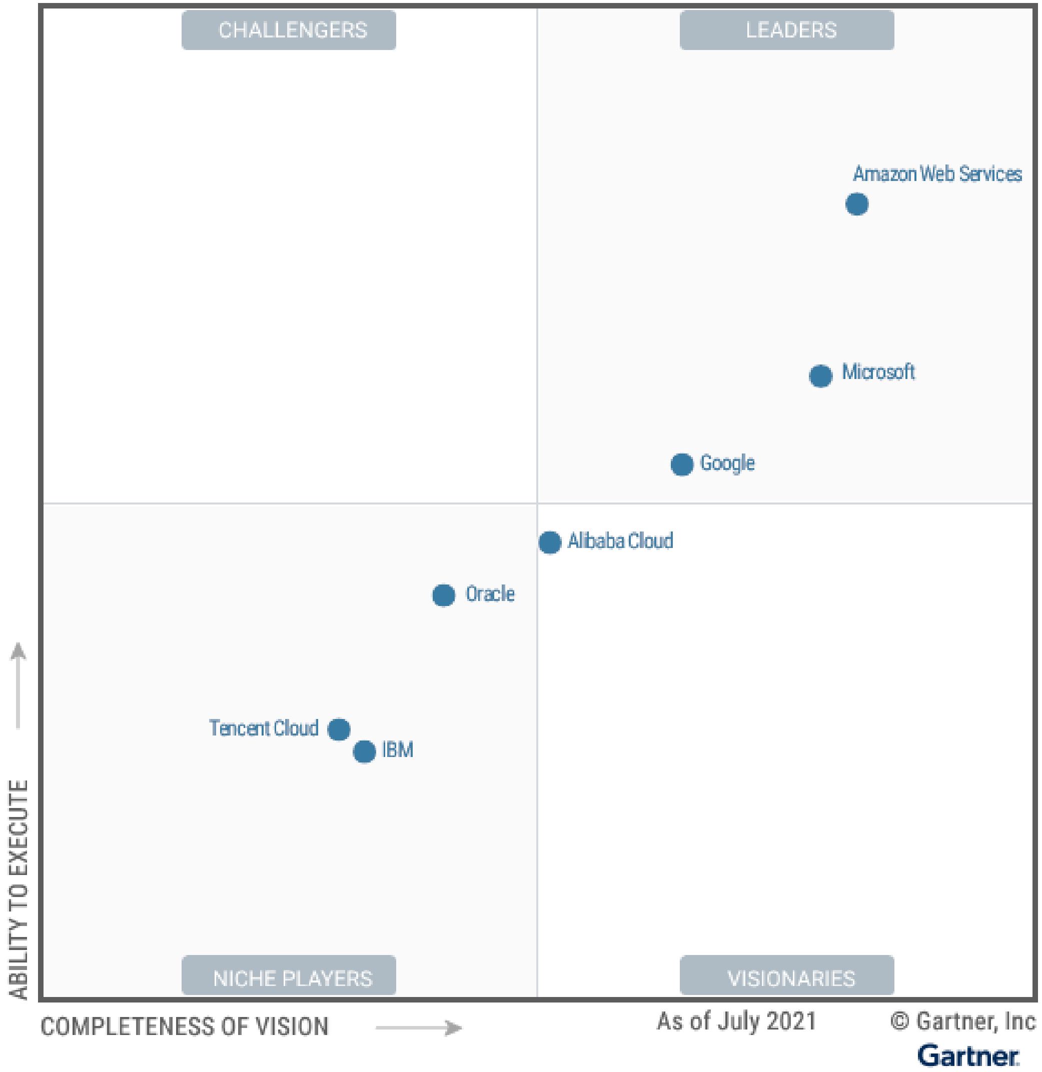
Current State

Often, there is a one-to-one mapping between physical devices and virtual devices.

Limitations:

- All users have access to the entire shadow
- All users can read and update the state data.
- All data may be exposed to unauthorized users/objects

Cloud Providers



As of July 2021

© Gartner, Inc

Gartner.

World-Leading Research with Real-World Impact!

Industry access control approaches

AWS supports a many-to-many digital twin-to-physical device relationship to a base unnamed shadow. Users can publish to named shadows for subsets of physical device data in order to minimize data exposure.

Azure offers tags which operate more as static attributes

Google offers tags which are more like device identifiers

Oracle offers tags which are more descriptive and have no security/access control features.

Proposed Solution

- ❖ The use of multiple shadows or digital twins for one physical object with the intent of separating data among different virtual objects based on tags assigned on the fly.

- ❖ Attach tags directly to the device state information in order to reduce the “distance” between access control mechanisms and device itself.

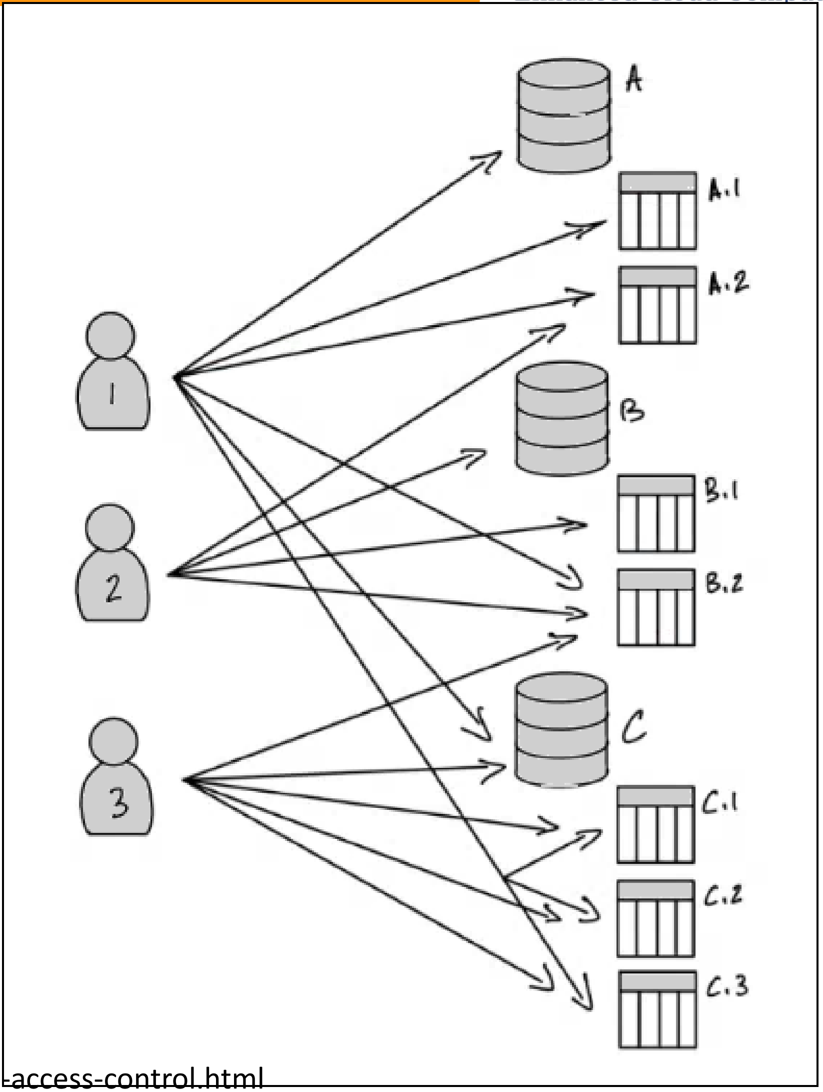
- ❖ Dynamic and on-to-fly subdivision of device state at the local edge according to attached tags.

- ❖ Limit data exposure to authorized entities via subdivision of data in a many-to-one relationship between digital and physics devices.

TBAC vs others

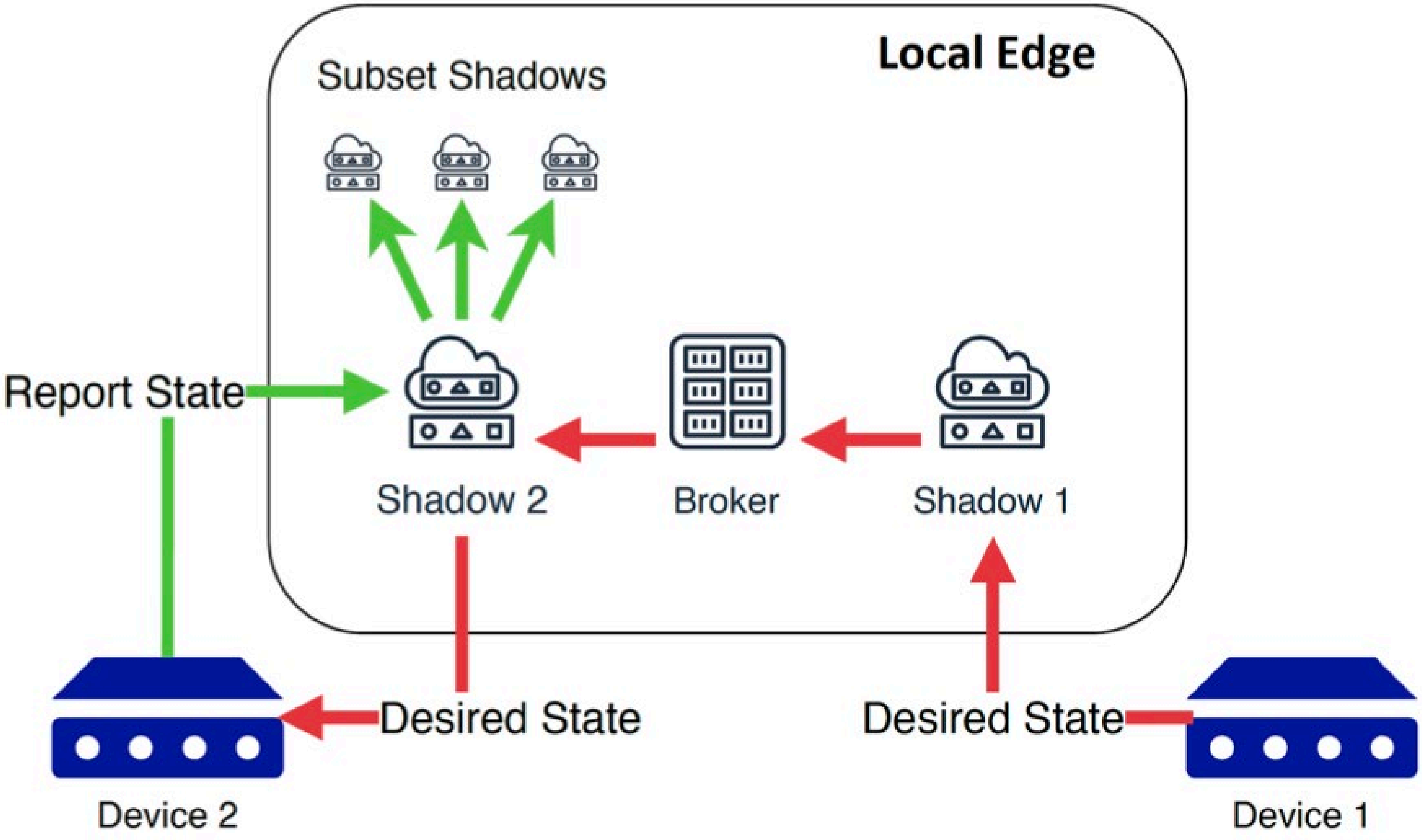
- Tag Based Access Control is popular and coincides well with data lakes as well. Imagine streaming data into various DB's and their corresponding Tables.

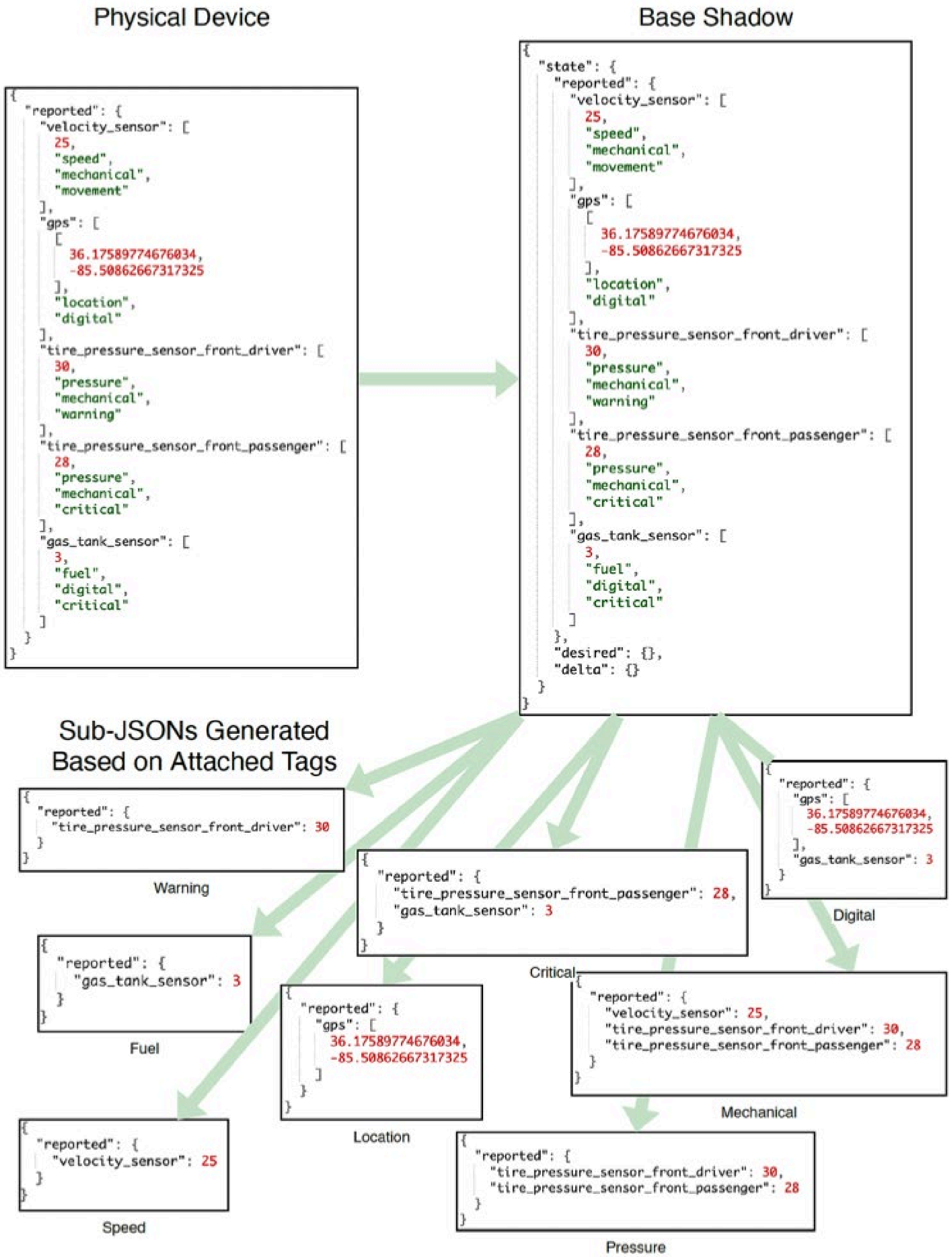
- With TBAC, using five assignment operations and eight grant operations, the data lake administrator can specify 17 permissions.



https://docs.aws.amazon.com/lake-formation/latest/dg/tag-based-access-control.html

Proposed system architecture





Physical Device

```
{
  "reported": {
    "velocity_sensor": [
      25,
      "speed",
      "mechanical",
      "movement"
    ],
    "gps": [
      [
        36.17589774676034,
        -85.50862667317325
      ],
      "location",
      "digital"
    ],
    "tire_pressure_sensor_front_driver": [
      30,
      "pressure",
      "mechanical",
      "warning"
    ],
    "tire_pressure_sensor_front_passenger": [
      28,
      "pressure",
      "mechanical",
      "critical"
    ],
    "gas_tank_sensor": [
      3,
      "fuel",
      "digital",
      "critical"
    ]
  }
}
```

Base Shadow

```
{
  "state": {
    "reported": {
      "velocity_sensor": [
        25,
        "speed",
        "mechanical",
        "movement"
      ],
      "gps": [
        [
          36.17589774676034,
          -85.50862667317325
        ],
        "location",
        "digital"
      ],
      "tire_pressure_sensor_front_driver": [
        30,
        "pressure",
        "mechanical",
        "warning"
      ],
      "tire_pressure_sensor_front_passenger": [
        28,
        "pressure",
        "mechanical",
        "critical"
      ],
      "gas_tank_sensor": [
        3,
        "fuel",
        "digital",
        "critical"
      ]
    },
    "desired": {},
    "delta": {}
  }
}
```

Sub-JSONs Generated Based on Attached Tags

```
{
  "reported": {
    "tire_pressure_sensor_front_driver": 30
  }
}
```

Warning

```
{
  "reported": {
    "tire_pressure_sensor_front_passenger": 28,
    "gas_tank_sensor": 3
  }
}
```

Critical

```
{
  "reported": {
    "gps": [
      36.17589774676034,
      -85.50862667317325
    ],
    "gas_tank_sensor": 3
  }
}
```

Digital

```
{
  "reported": {
    "gas_tank_sensor": 3
  }
}
```

Fuel

```
{
  "reported": {
    "gps": [
      36.17589774676034,
      -85.50862667317325
    ]
  }
}
```

Location

```
{
  "reported": {
    "velocity_sensor": 25,
    "tire_pressure_sensor_front_driver": 30,
    "tire_pressure_sensor_front_passenger": 28
  }
}
```

Mechanical

```
{
  "reported": {
    "velocity_sensor": 25
  }
}
```

Speed

```
{
  "reported": {
    "tire_pressure_sensor_front_driver": 30,
    "tire_pressure_sensor_front_passenger": 28
  }
}
```

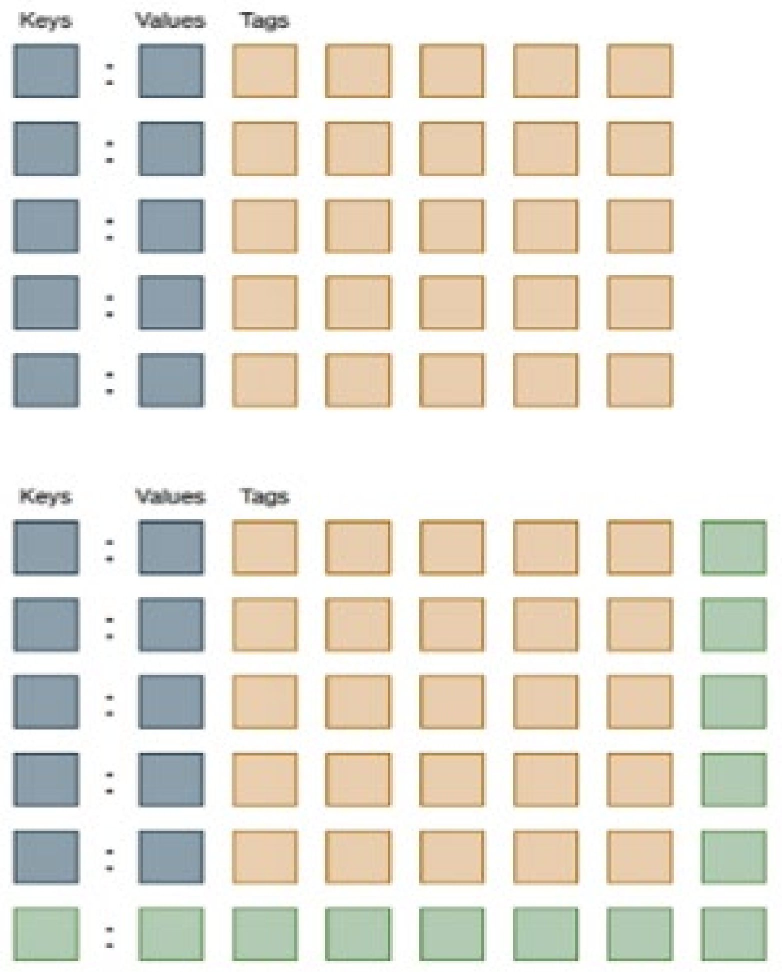
Pressure

Transformation from 5 to 6 Key-Value Pairs

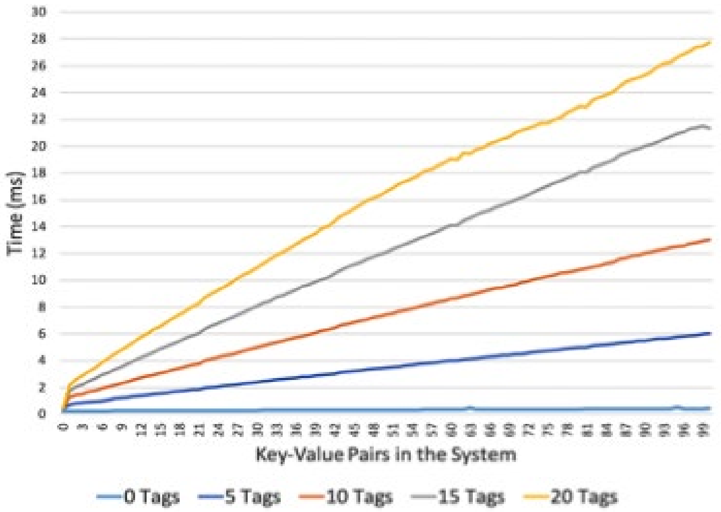
When there are five KV pairs in the system, there are 5 tags (upper diagram).

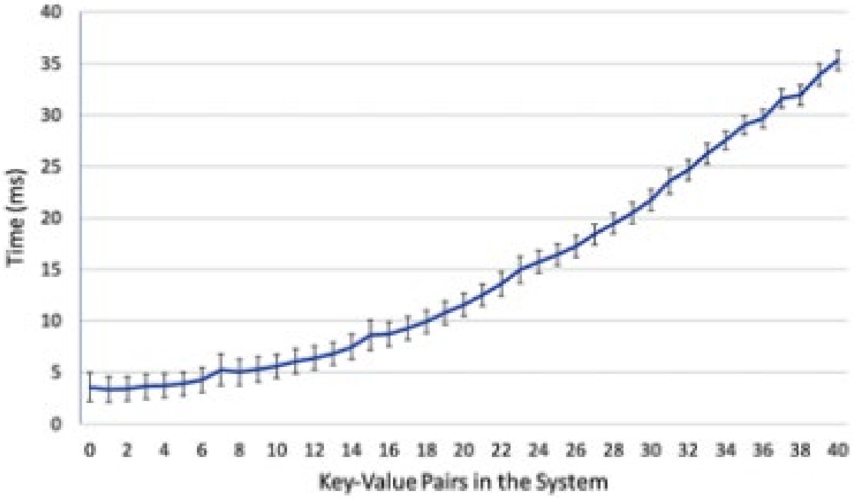
When we expand the testing to 6 KV pairs, we add additional tags (lower diagram).

Upon reception of a reported state from a simulated device, the shadow introduces a new k-v pair as well as increment the number of tags attached to all other pairs previously present.



Results


Time (ms)
30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
0
3
6
9
12
15
18
21
24
27
30
33
36
39
42
45
48
51
54
57
60
63
66
69
72
75
78
81
84
87
90
93
96
99
Key-Value Pairs in the System
0 Tags
5 Tags
10 Tags
15 Tags
20 Tags


Time (ms)
40
35
30
25
20
15
10
5
0
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
Key-Value Pairs in the System

Future Directions

Investigate additional ways of separating one shadow into multiple shadows

Potentially with the adoption for cloud scalability

How this could be applied to other smart environments

✓ Evaluating the overhead of existing schemes without TBAC as a type of benchmark.

Combination of TBAC with ABAC or other forms of access control on the tagged shadows of creation of shadows and tags

Acknowledgements

- This work is partially supported by:
  - NSF CREST Grant HRD-1736209 at UTSA &
  - Grant 2025682 at TTU

- Question/ Feedback