UNIVERSITÀ DEGLI STUDI FIRENZE

DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

www.disit.org

Course: Cybersecurity and Data Privacy

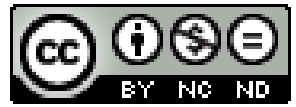
Part on Privacy by Paolo Nesi

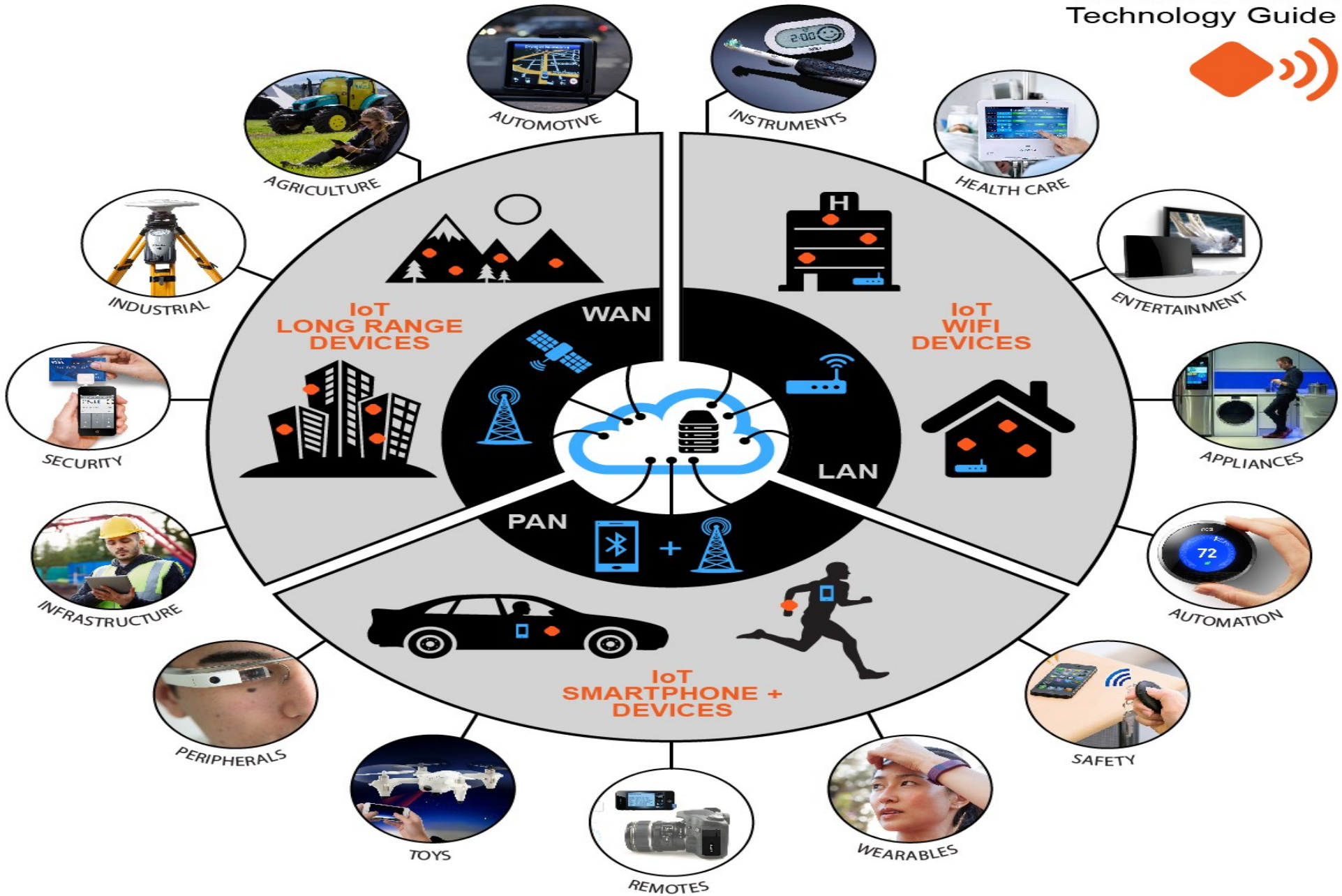
Topic: IoT Networks Security

University of Florence, DISIT lab, Https://www.disit.org

Https://www.snap4city.org

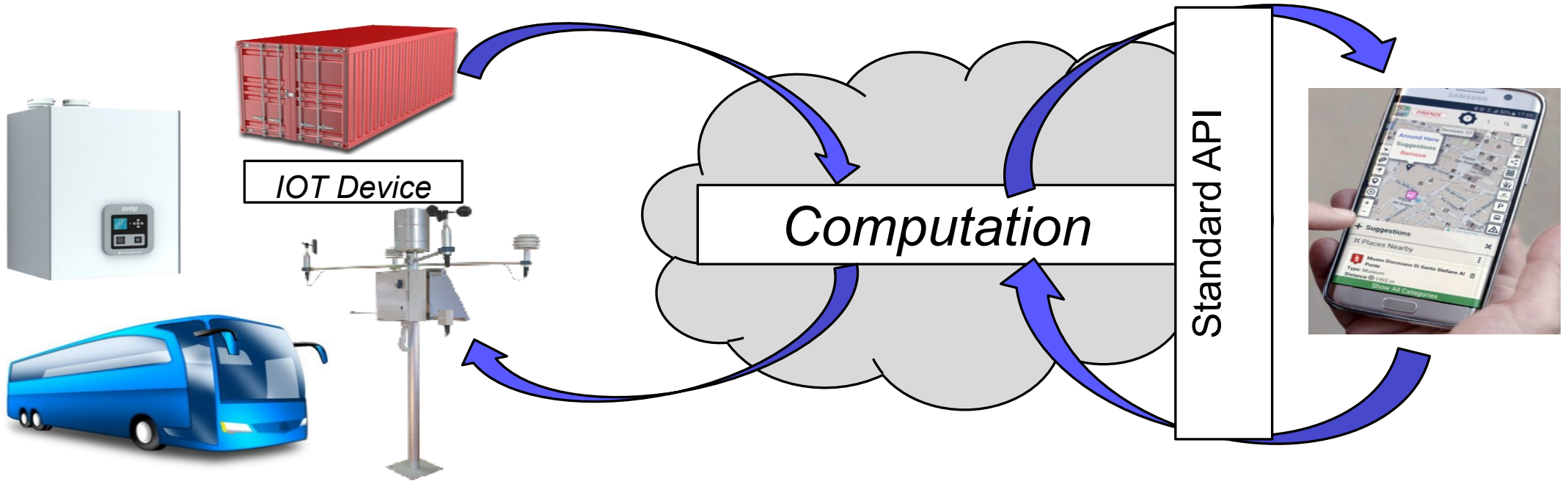
Paolo.nesi@unifi.it




IoT HARDWARE
Technology Guide
AUTOMOTIVE
INSTRUMENTS
AGRICULTURE
HEALTH CARE
INDUSTRIAL
ENTERTAINMENT
IoT
LONG RANGE
DEVICES
WAN
IoT
WIFI
DEVICES
LAN
SECURITY
APPLIANCES
PAN
INFRASTRUCTURE
AUTOMATION
IoT
SMARTPHONE +
DEVICES
PERIPHERALS
SAFETY
TOYS
REMOTES
WEARABLES

IOT Main Concept

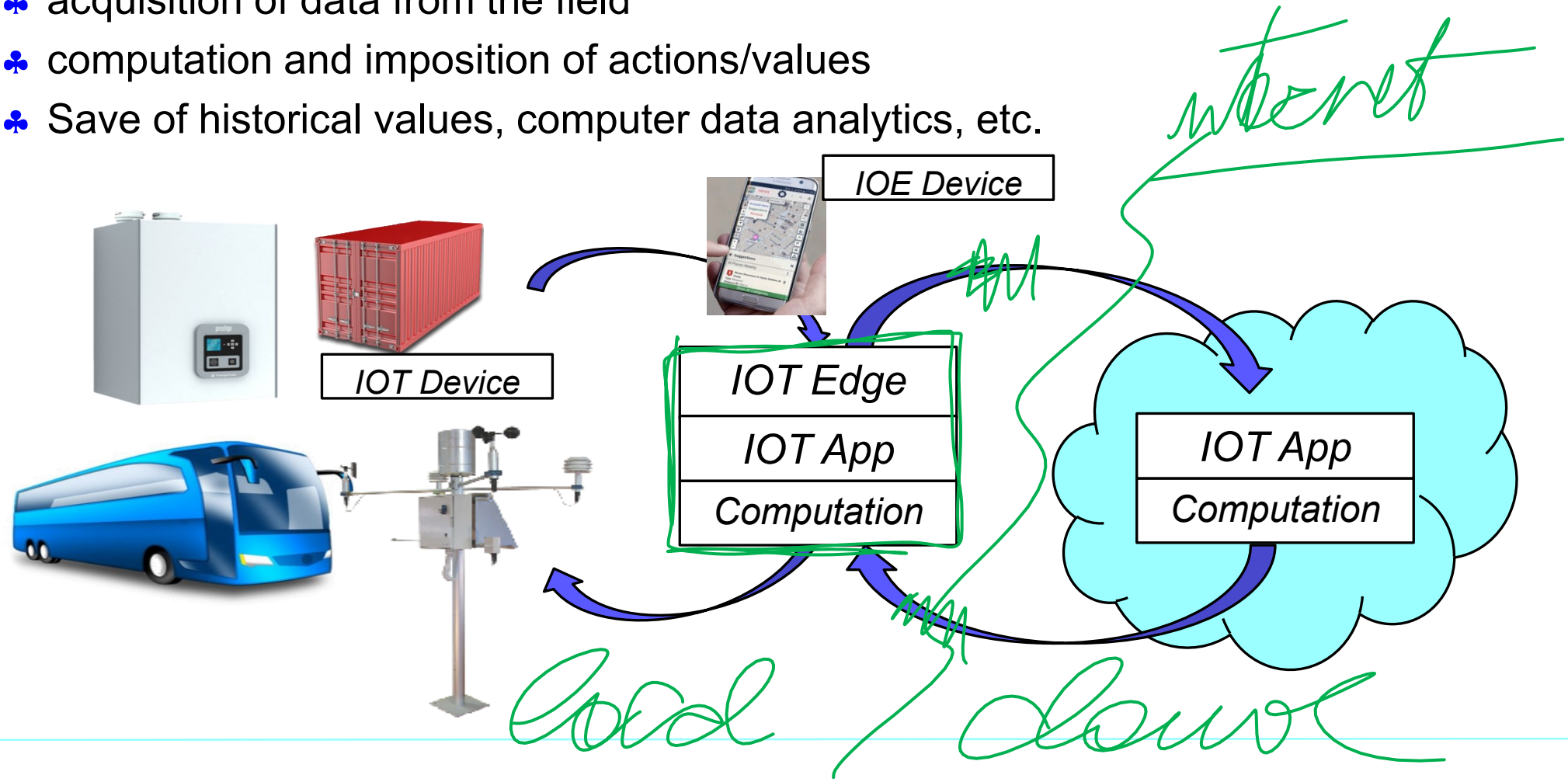
- The implementation of smart services may implies the:
  - acquisition of data from the field
  - computation and imposition of actions/values
  - Save of historical values, computer data analytics, etc.



IOT Main Concept

The implementation of smart services may implies the:

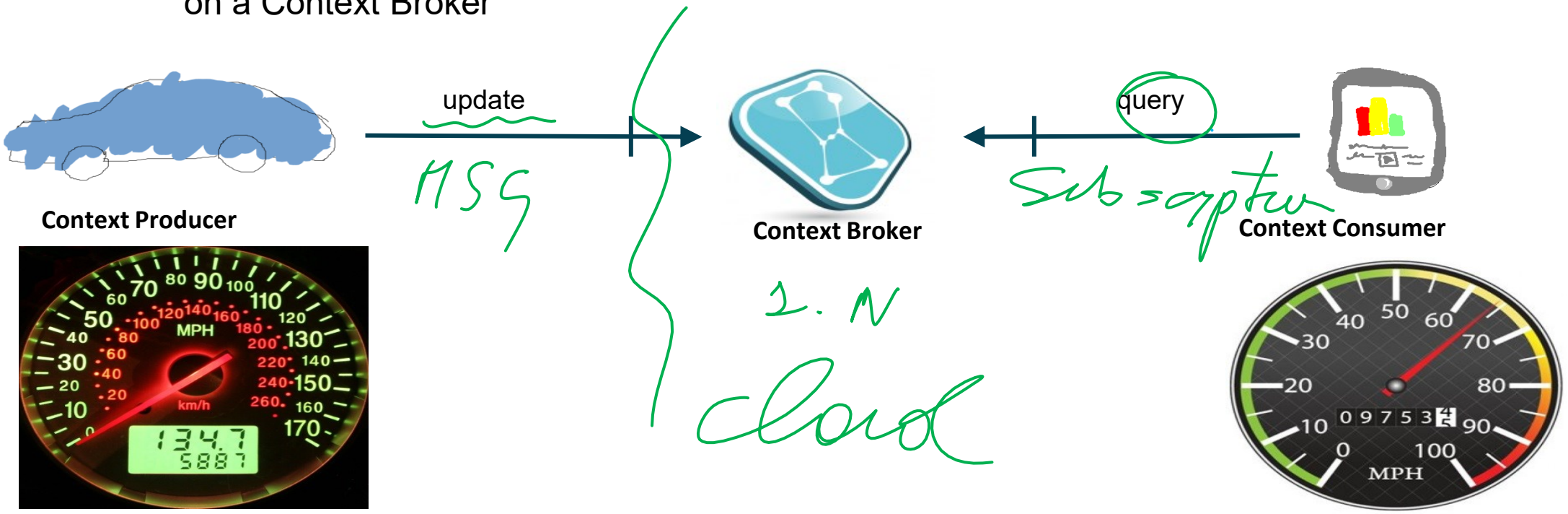
- acquisition of data from the field
- computation and imposition of actions/values
- Save of historical values, computer data analytics, etc.



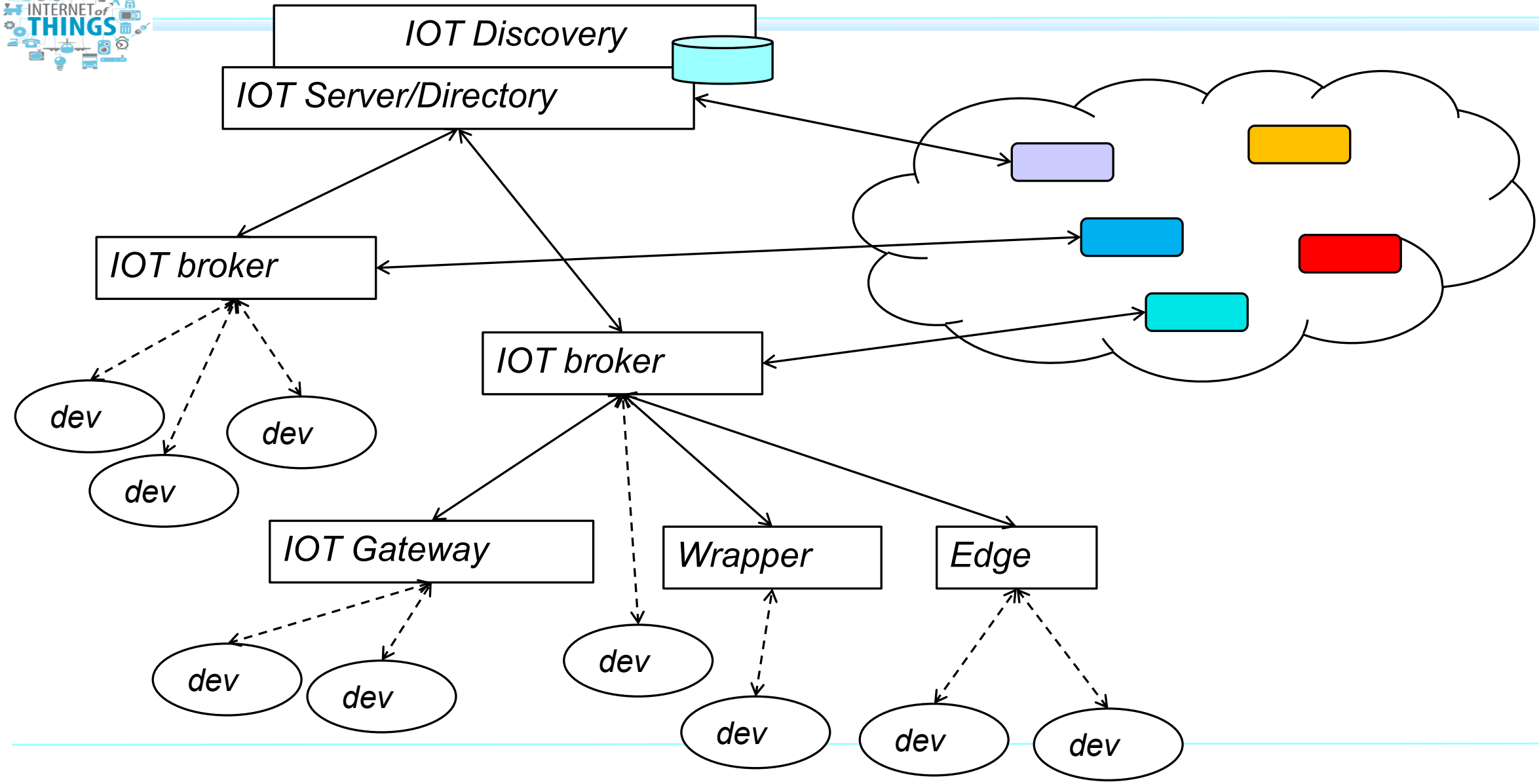
IOT Context Broker

Context Broker operations: create & pull data

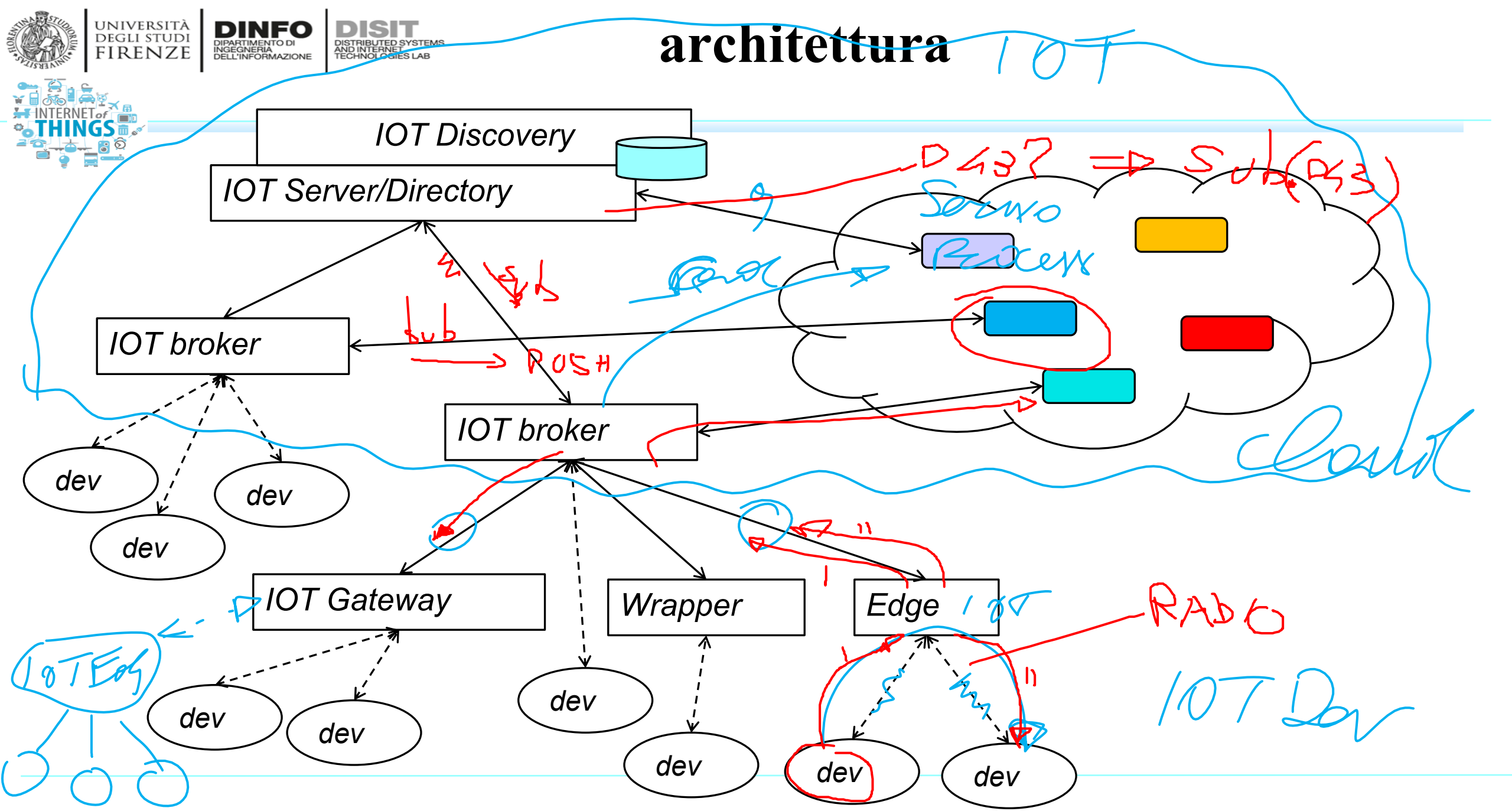
- **Context Producers** publish data/context elements by invoking the **update** operations on a Context Broker.
- **Context Consumers** can retrieve data/context elements by invoking the **query** operations on a Context Broker



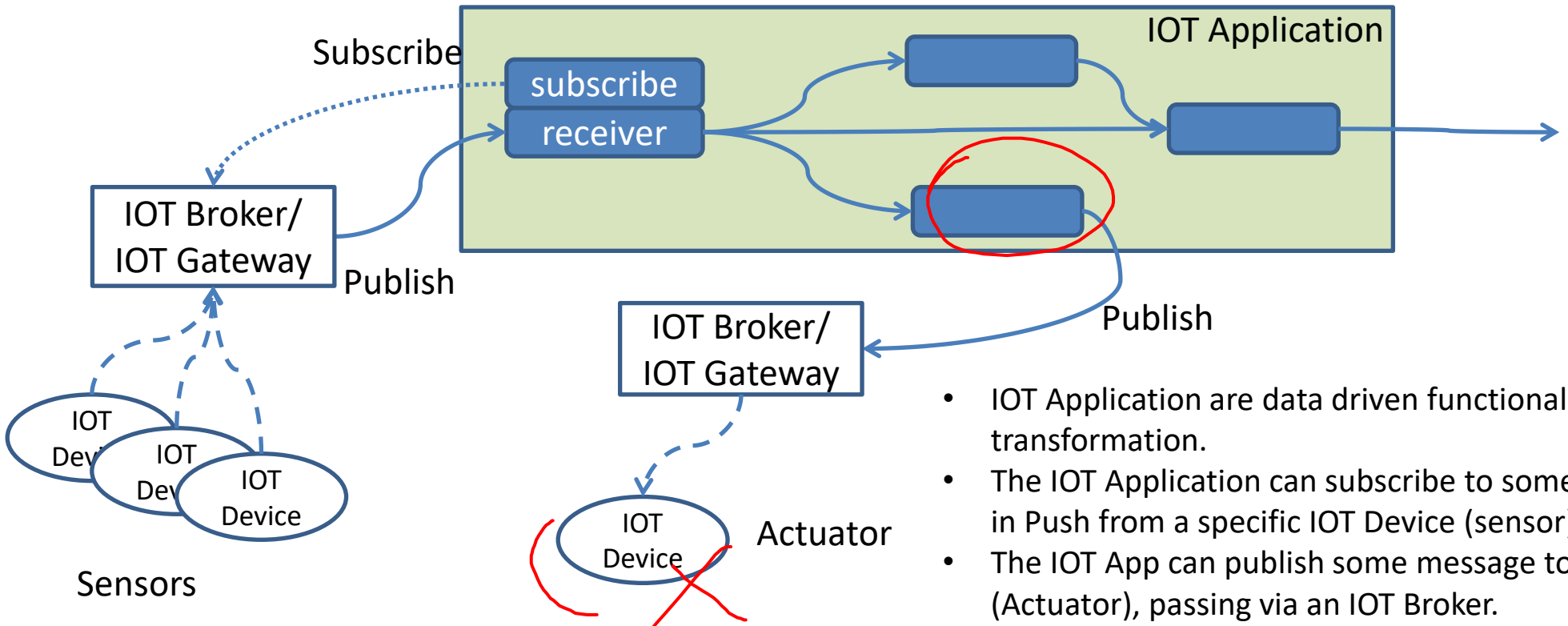
architettura



architettura



IOT Basic

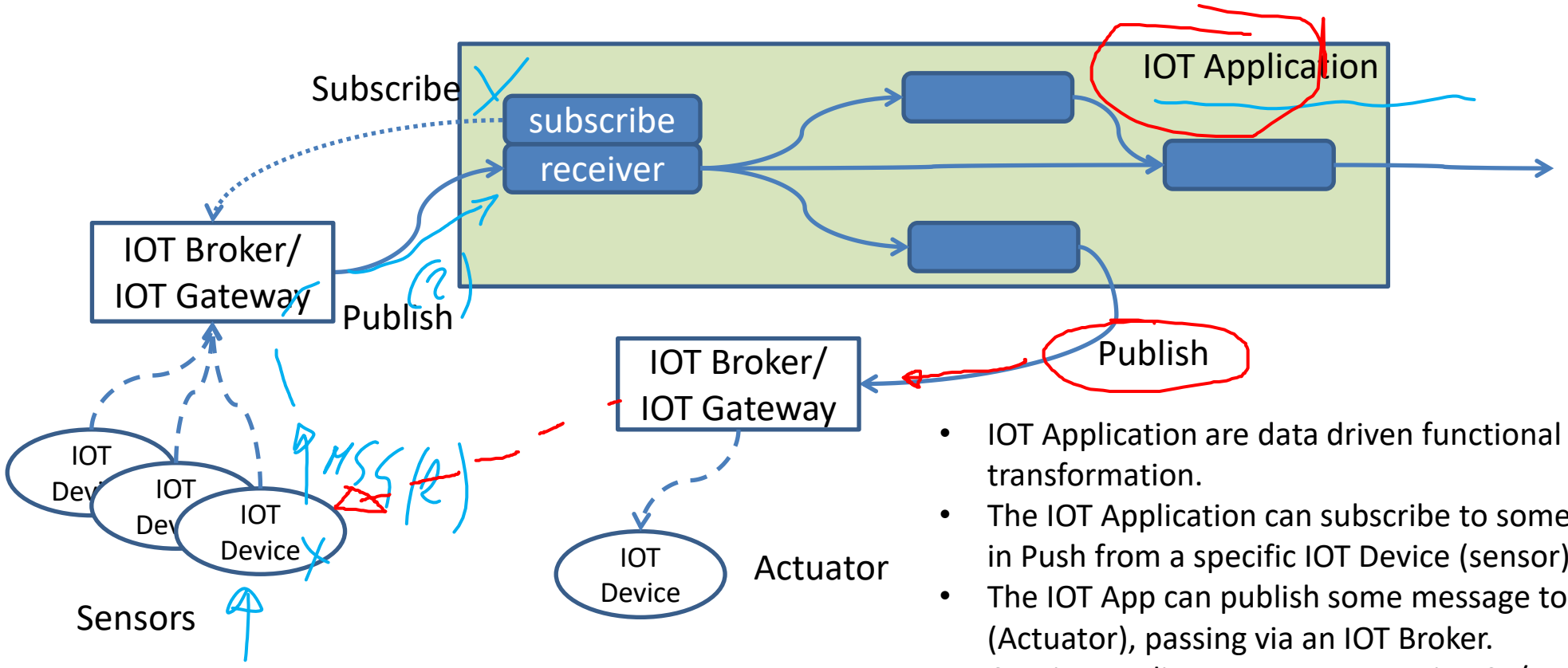


Sensors

- Sensors are programmed to send data (i) periodically, or (ii) when a relevant change occurs in the sensor value, or (iii) when events occur (for example a change of status of something), etc.
- Actuator perform some action on the field: change of status, reset, turn on something, change setting value, etc.

- IOT Application are data driven functional programs for data transformation.
- The IOT Application can subscribe to some IOT Brokers to receive data in Push from a specific IOT Device (sensor)
- The IOT App can publish some message toward some IOT Device (Actuator), passing via an IOT Broker.
- Continuous lines are messages via TCP/IP
- Dashed lines are message via some radio channel (Lora, BT, Wi-Fi, …)
- IOT Brokers and IOT Gateway can be distinct servers
- IOT Brokers can be on cloud
- IOT Gateway performs the SW update, the business management, access in Push and Pull

IOT Basic

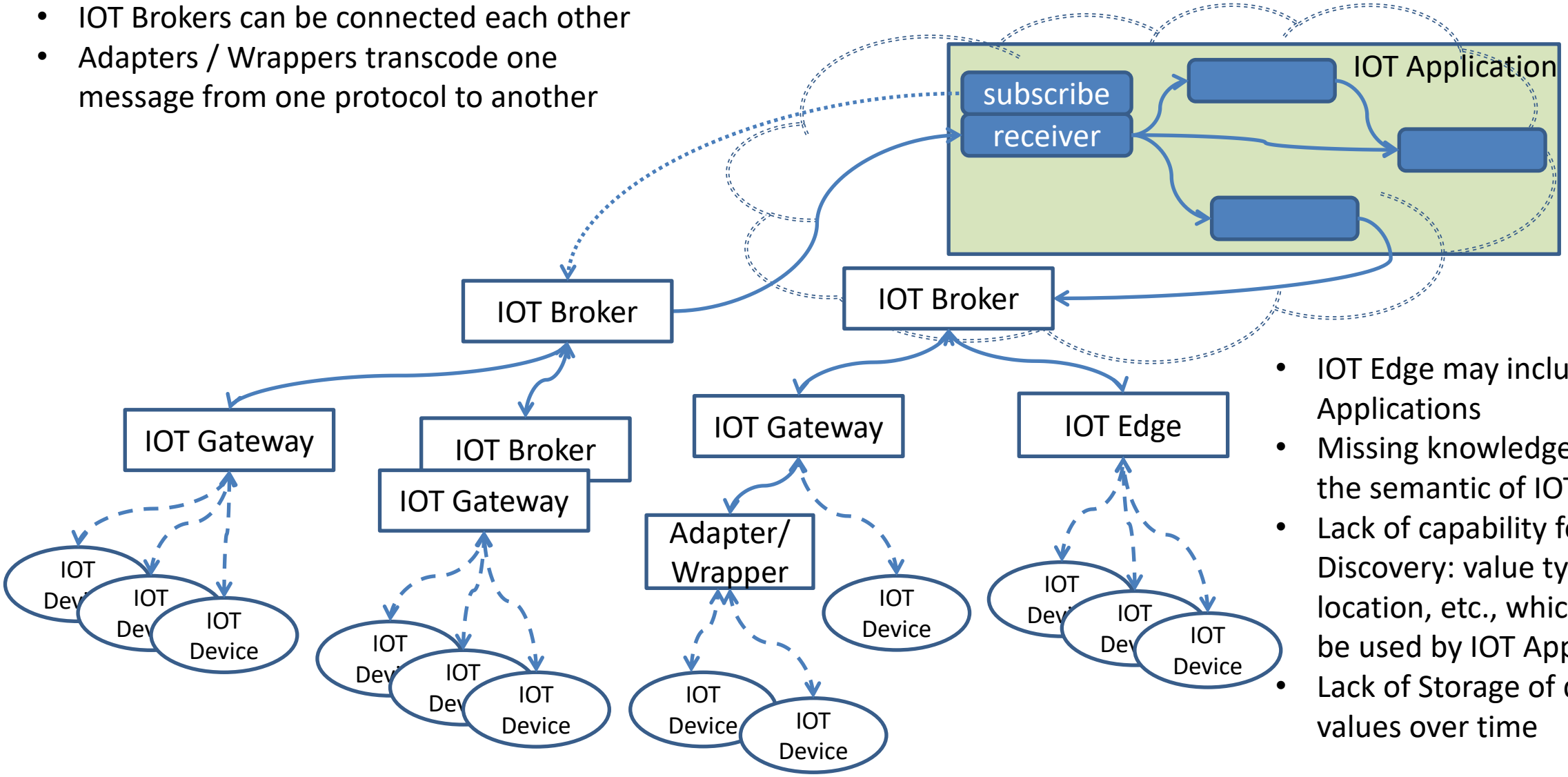


- Sensors are programmed to send data (i) periodically, or (ii) when a relevant change occurs in the sensor value, or (iii) when events occur (for example a change of status of something), etc.
- Actuator perform some action on the field: change of status, reset, turn on something, change setting value, etc.

- IOT Application are data driven functional programs for data transformation.
- The IOT Application can subscribe to some IOT Brokers to receive data in Push from a specific IOT Device (sensor)
- The IOT App can publish some message toward some IOT Device (Actuator), passing via an IOT Broker.
- Continuous lines are messages via TCP/IP
- Dashed lines are message via some radio channel (Lora, BT, Wi-Fi, …)
- IOT Brokers and IOT Gateway can be distinct servers
- IOT Brokers can be on cloud
- IOT Gateway performs the SW update, the business management, access in Push and Pull

Definitions

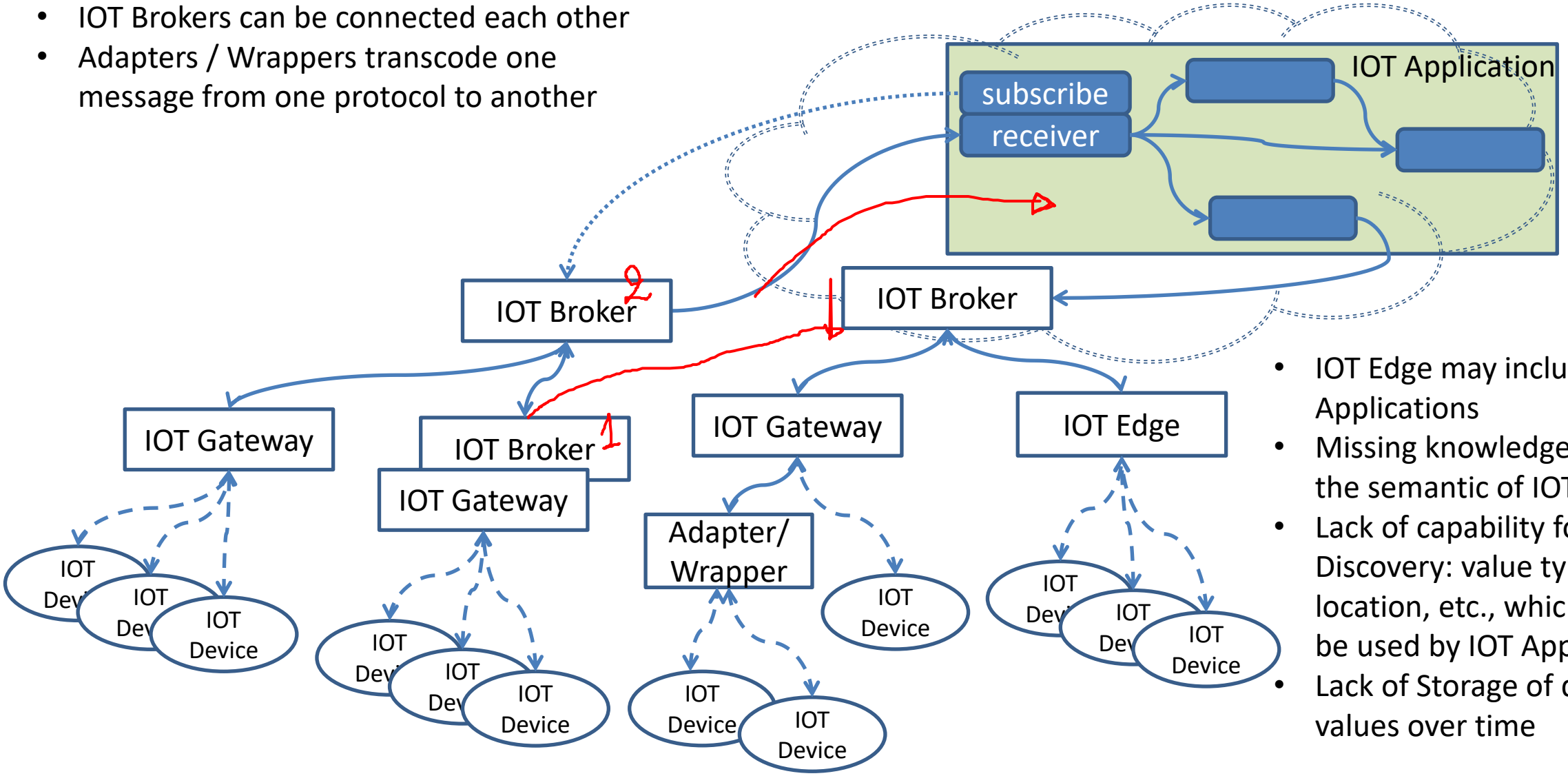
- IOT Brokers can be connected each other
- Adapters / Wrappers transcode one message from one protocol to another



- IOT Edge may include IOT Applications
- Missing knowledge about the semantic of IOT devices
- Lack of capability for IOT Discovery: value type, location, etc., which could be used by IOT App
- Lack of Storage of data values over time

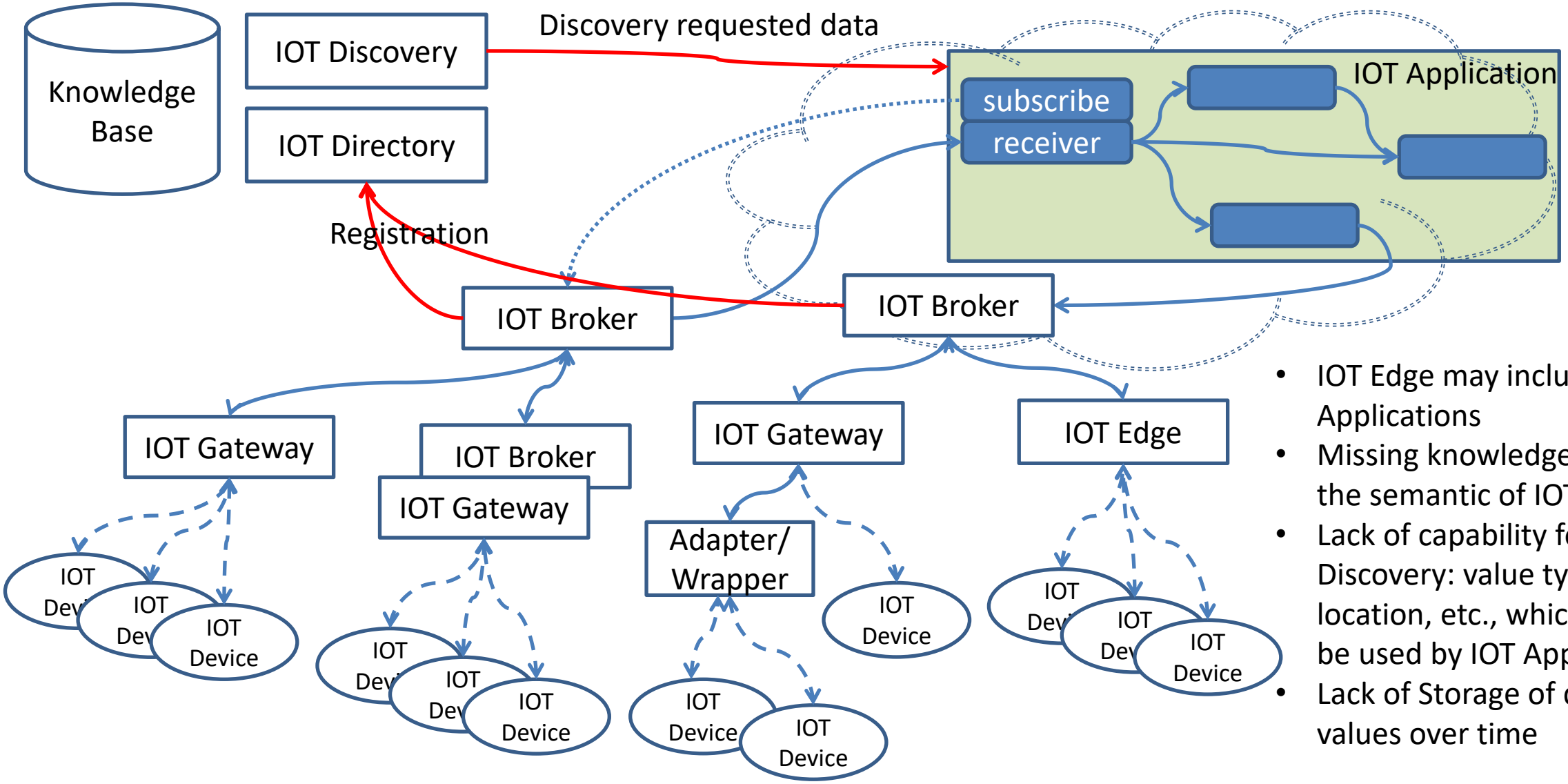
Definitions

- IOT Brokers can be connected each other
- Adapters / Wrappers transcode one message from one protocol to another



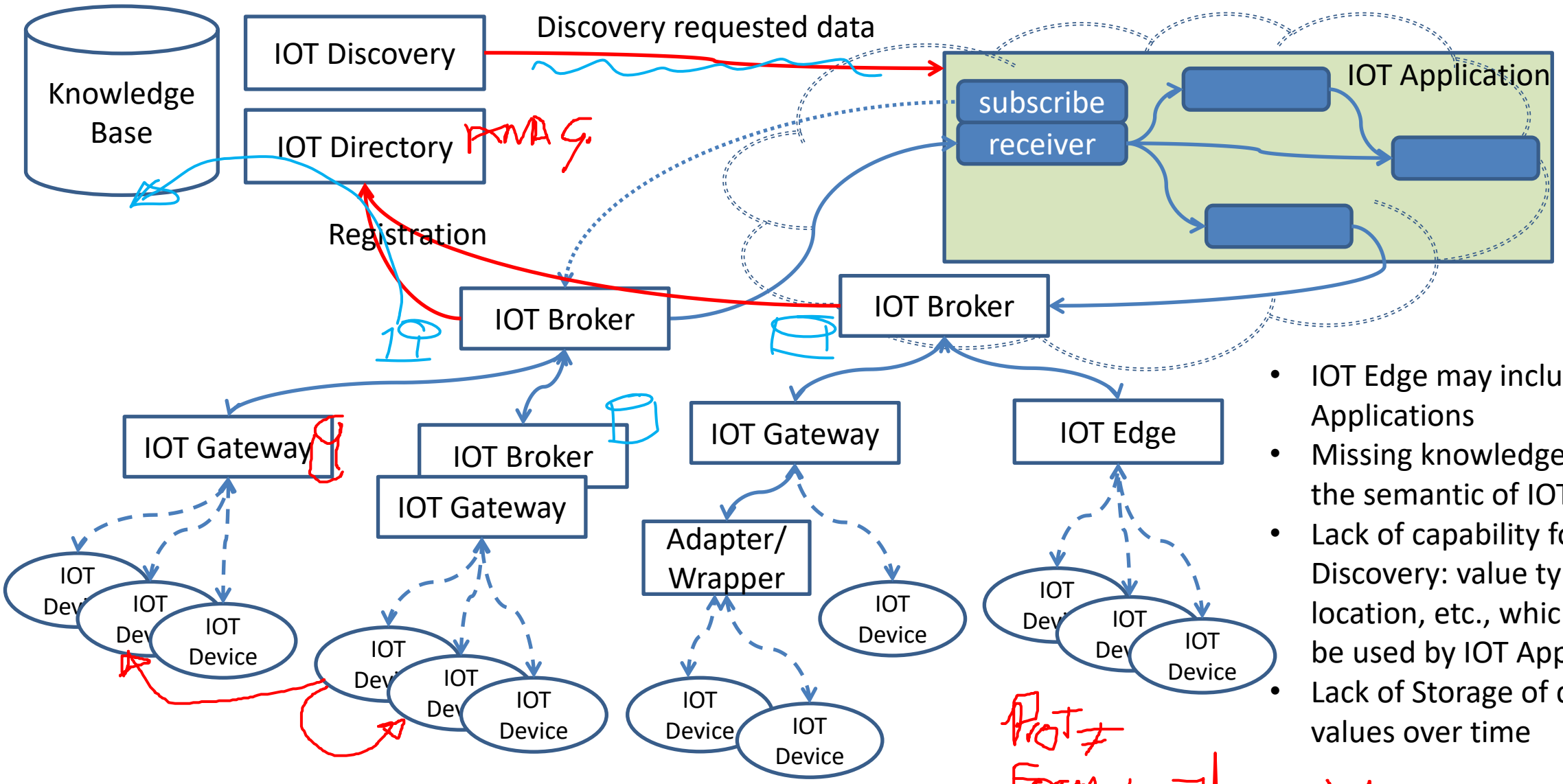
- IOT Edge may include IOT Applications
- Missing knowledge about the semantic of IOT devices
- Lack of capability for IOT Discovery: value type, location, etc., which could be used by IOT App
- Lack of Storage of data values over time

Definitions



- IOT Edge may include IOT Applications
- Missing knowledge about the semantic of IOT devices
- Lack of capability for IOT Discovery: value type, location, etc., which could be used by IOT App
- Lack of Storage of data values over time

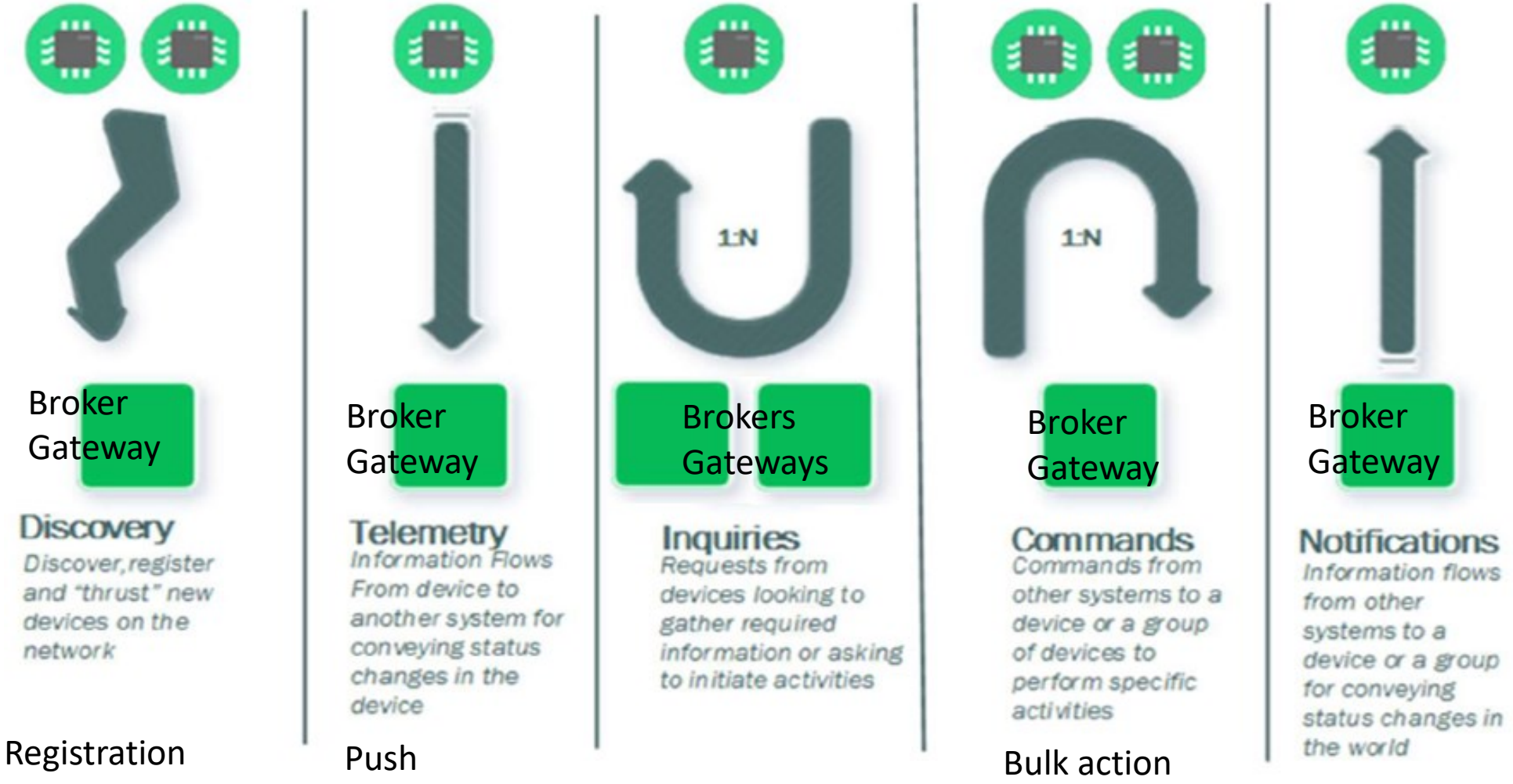
Definitions



- IOT Edge may include IOT Applications
- Missing knowledge about the semantic of IOT devices
- Lack of capability for IOT Discovery: value type, location, etc., which could be used by IOT App
- Lack of Storage of data values over time

IOT/IOE Protocols

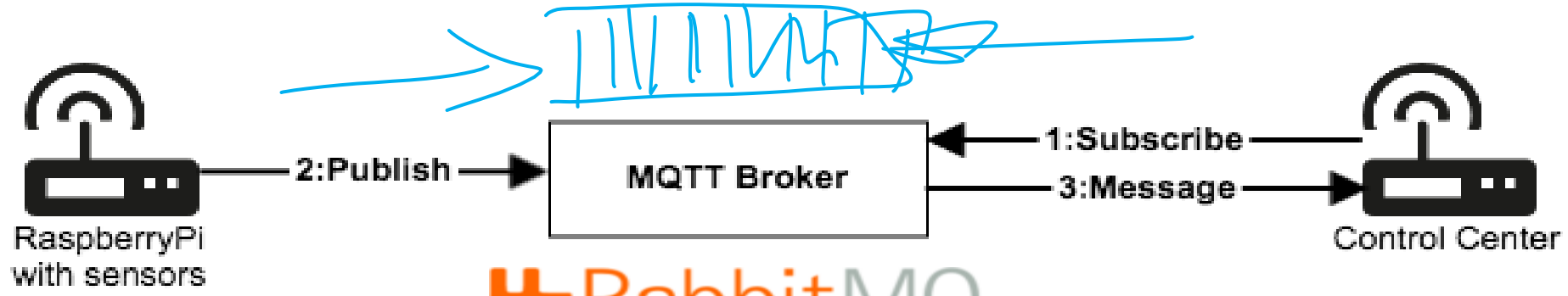
Communication Patterns



- MQTT
- HTTP(s)
- AMQP
- COAP
- NGSI
- OneM2M
- WebSockets
- ……..
- Etc.

IOT Brokers

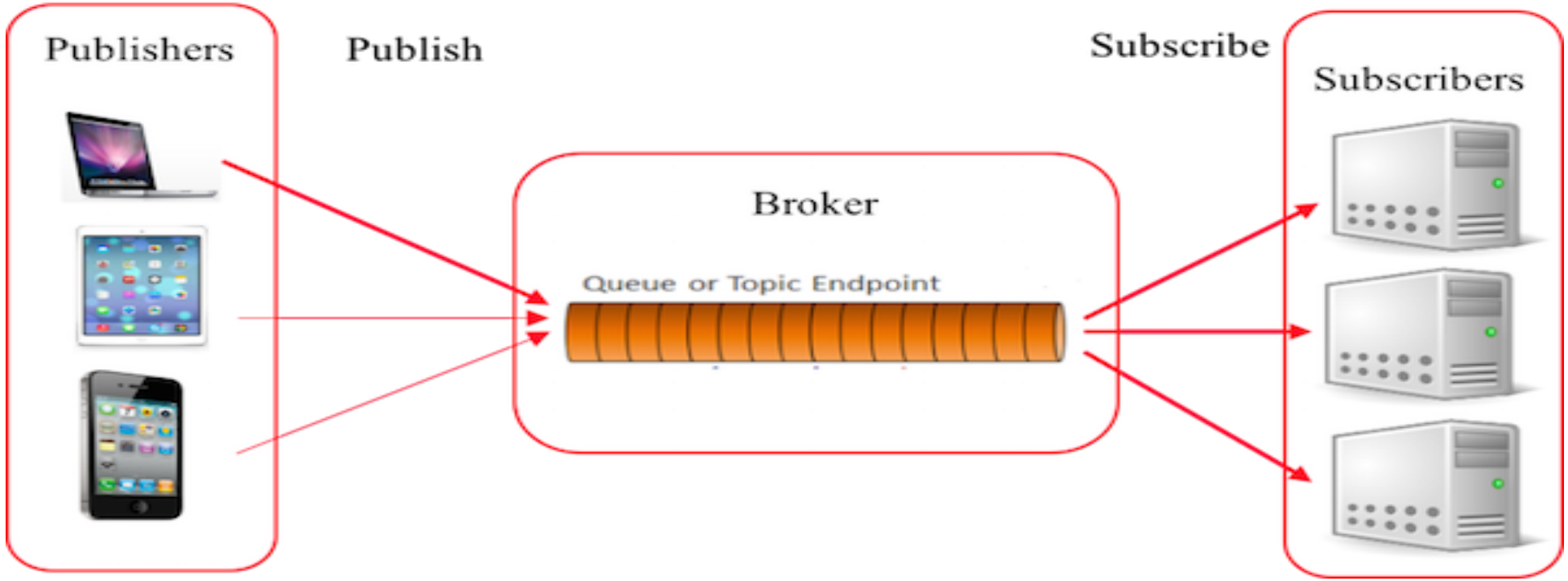
	AMQP	STOMP	JMS	COAP	NGSI	MQTT OASIS
RabbitMQ	X	X	X	X		X
Mosquitto						X
ActiveMQ	X	X	X			X
StormMQ	X					
HIVEMQ			X			X
ORION BROKER				X	X	X



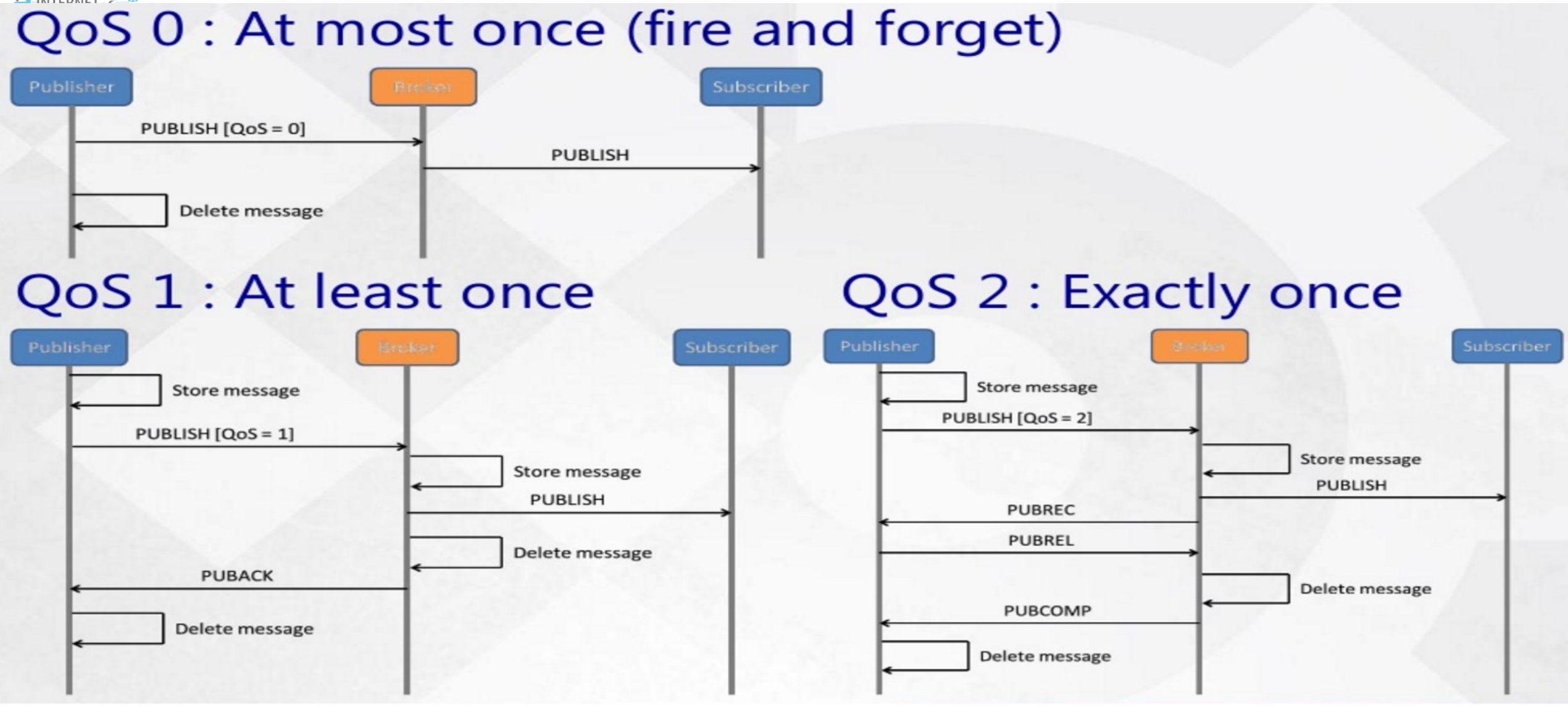
RabbitMQ
Open Source Enterprise Messaging

MQTT: Message Queue Telemetry Transport

- security obtained with SSL/TLS since it is over TCP
- ISO/IEC PRF 20922
- Over TCP/IP, Async, pub/subscribe,
- payload agnostic (can be encrypted)

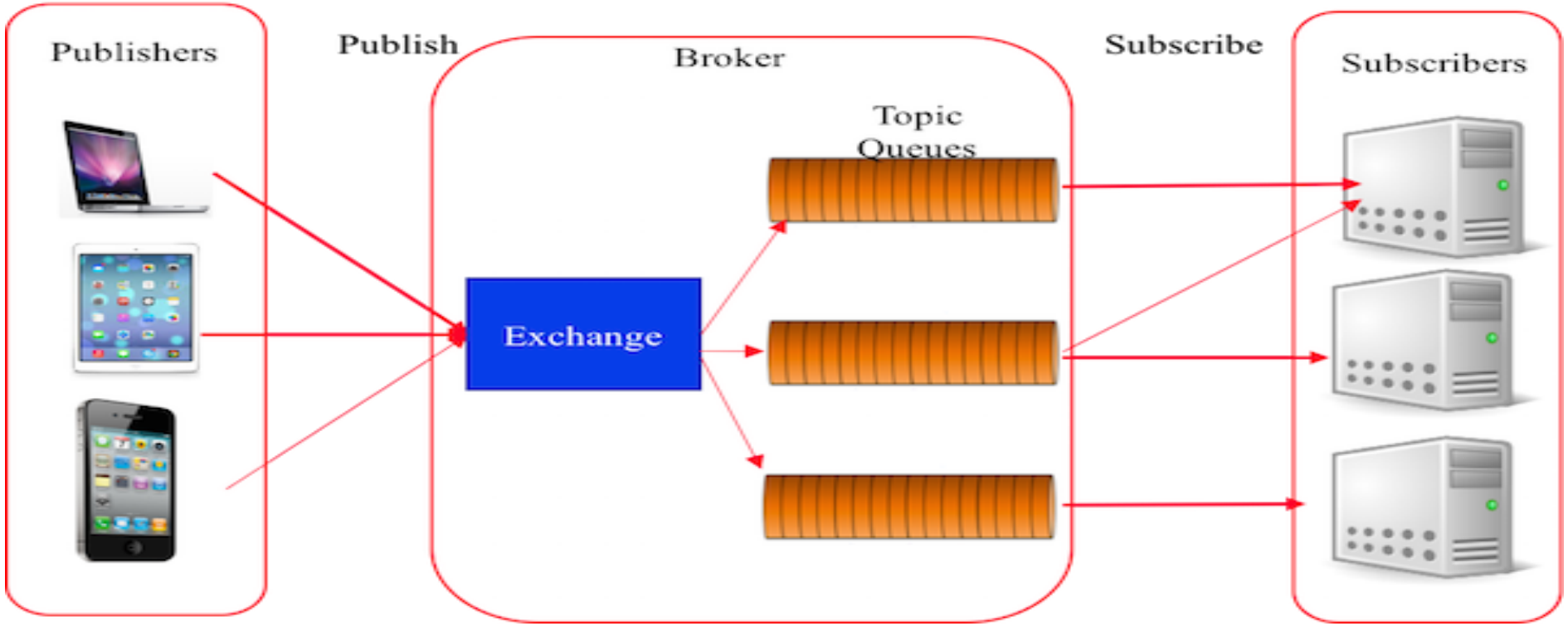


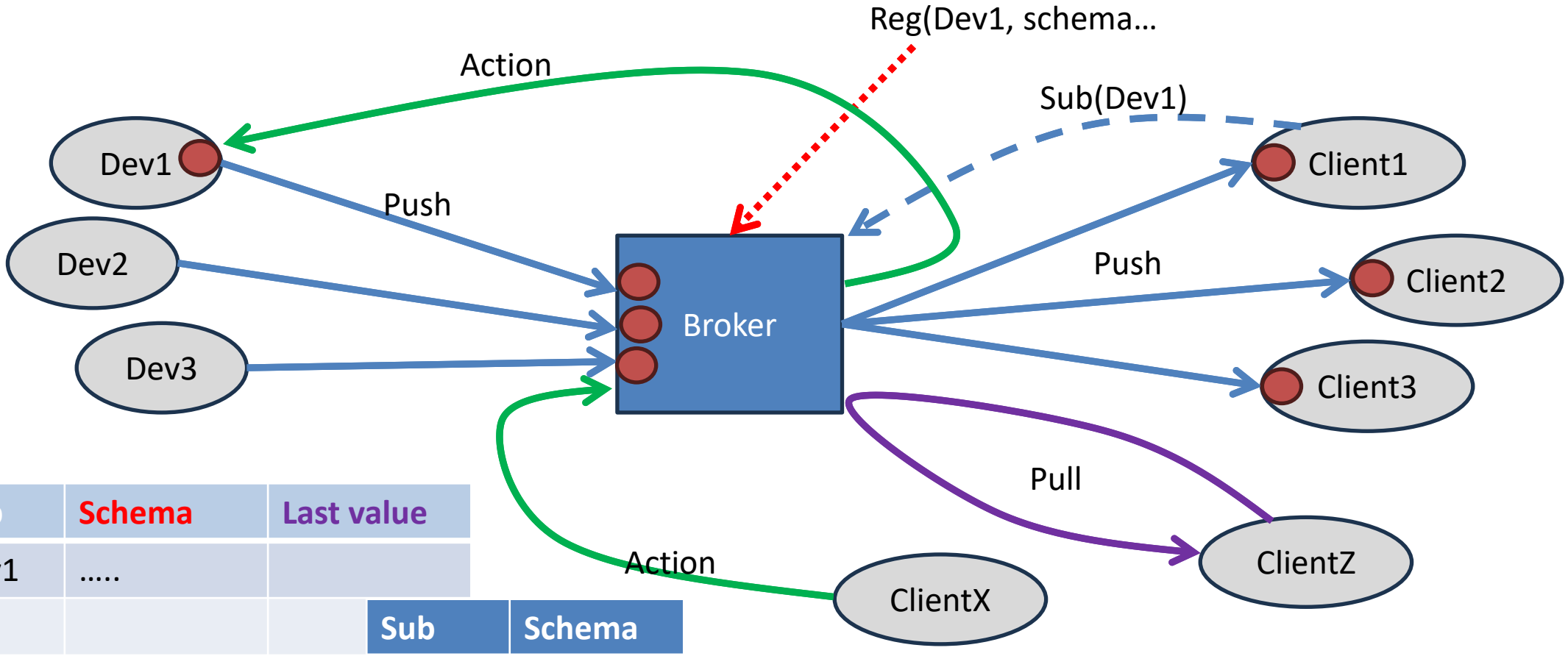
MQTT QoS


QoS 0 : At most once (fire and forget)
Publisher
Broker
Subscriber
PUBLISH [QoS = 0]
PUBLISH
Delete message
QoS 1 : At least once
Publisher
Broker
Subscriber
Store message
PUBLISH [QoS = 1]
Store message
PUBLISH
Delete message
PUBACK
Delete message
QoS 2 : Exactly once
Publisher
Broker
Subscriber
Store message
PUBLISH [QoS = 2]
Store message
PUBLISH
PUBREC
PUBREL
Delete message
PUBCOMP
Delete message

AMQP Advanced Message Queuing Protocol

- Over TCP, binary wire protocol
- Exchange decoupling





Pub	Schema	Last value
Dev1	…..	

Sub	Schema
Client1	Dev1
Client1	Dev2

IoT ecosystem

- *"a **dynamic global network infrastructure** with self-configuring capabilities based on standard and interoperable communication protocols where **physical and virtual 'Things'** have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"* Institute of Network Cultures

- *"a global infrastructure for the information society enabling **advanced services by interconnecting** (physical and virtual) things based on, existing and evolving, interoperable information and communication technology"* ITU-T (2012) Next Generation Networks

IoT architecture

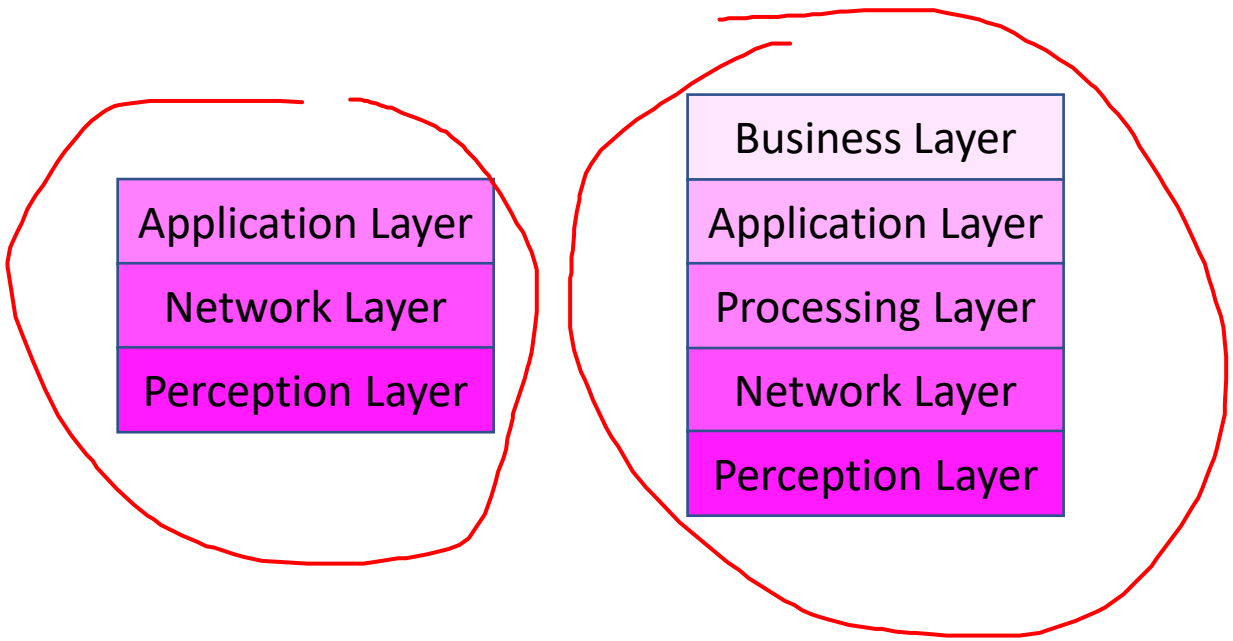
- Independent **IoT ecosystems** that can be
  - physical
  - virtual
  - hybrid mix of the two

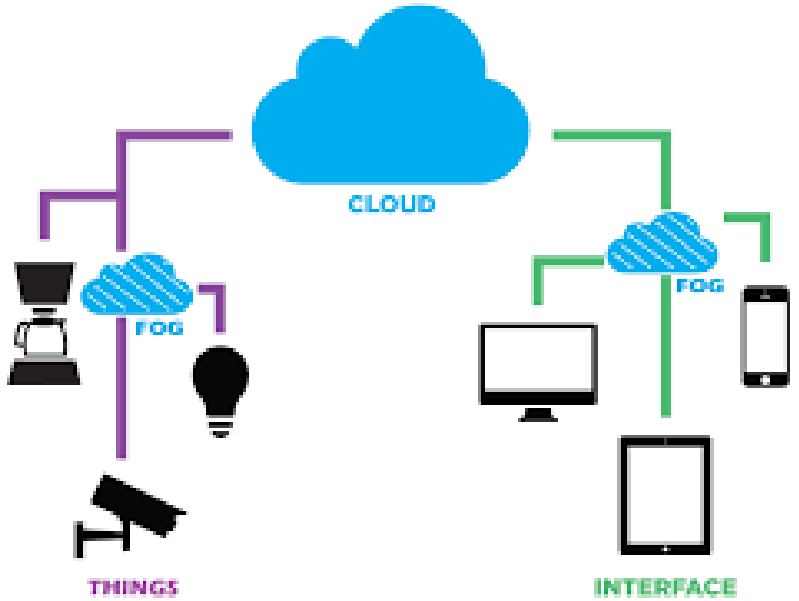
- consist of a list of **active** physical devices, sensors, actuators, services, communication protocols and layers, final users, developers and interface layers

IoT architecture

- Several functional blocks are defined in an IoT system, even if a **common conceptualization is not found**, but several different approaches are usual considered: 3-layer, 5-layer, cloud and fog systems, social IoT paradigms.

3 — BL — UI





UNIVERSITÀ DEGLI STUDI FIRENZE

DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

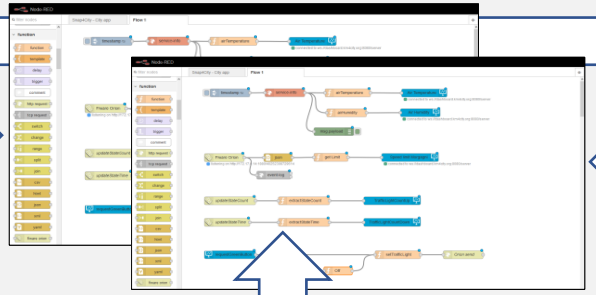
www.disit.org

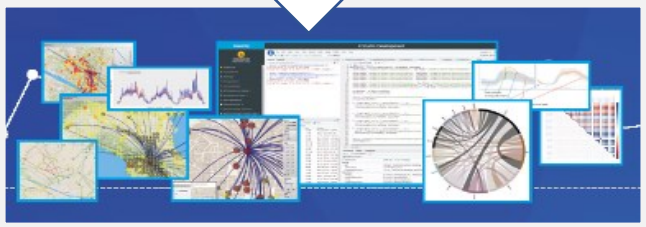
IoT Sentient solutions

IoT and City data World

My IoT Devices

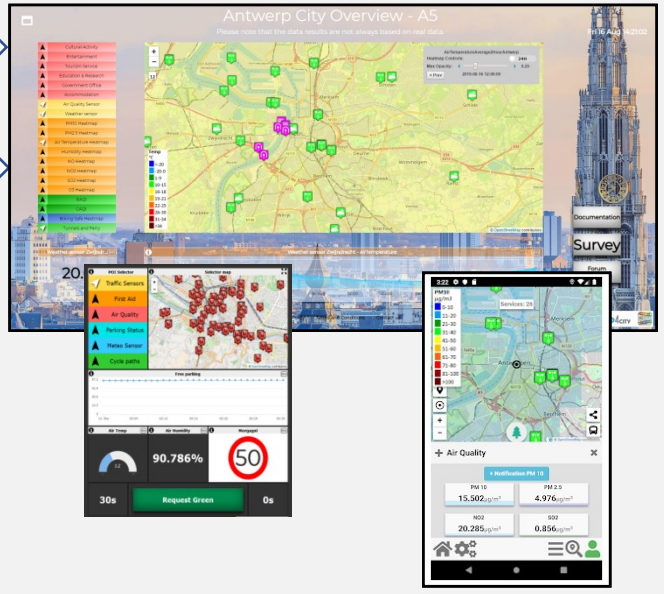
IoT Applications



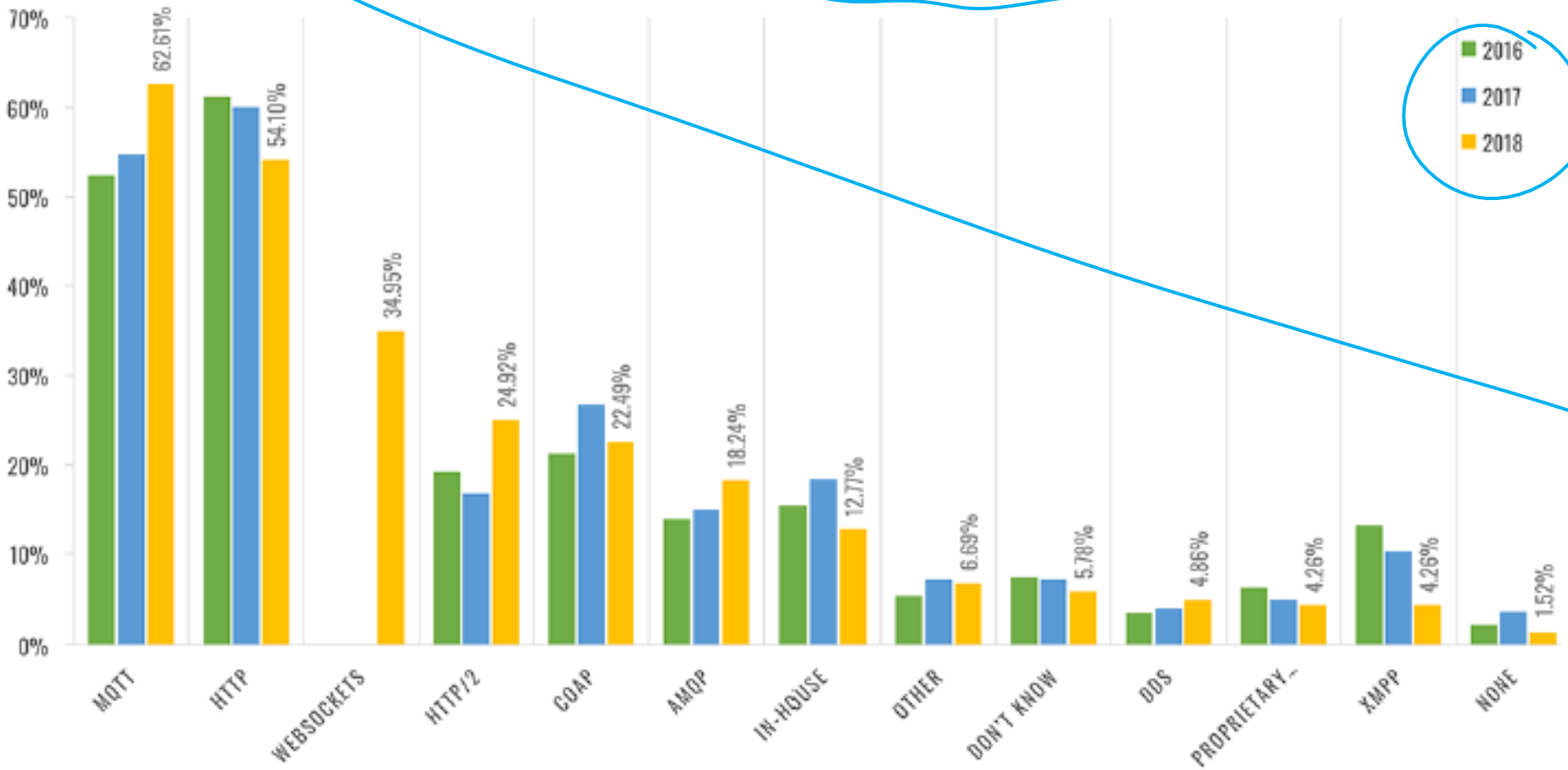


Big Data Analytics, Artificial Intelligence

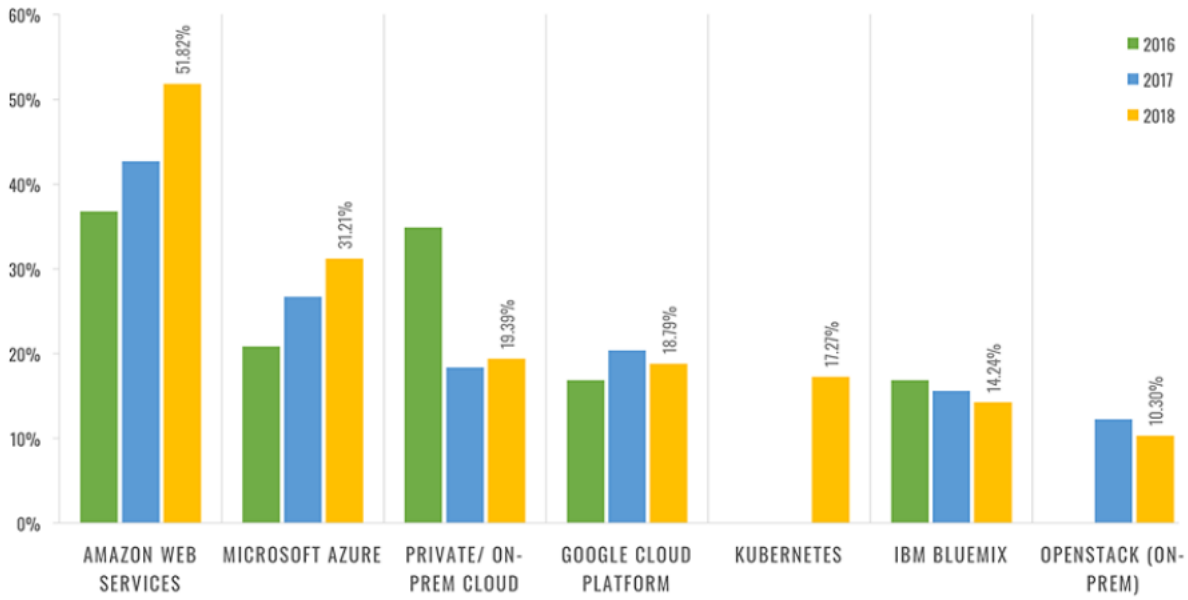
Dashboards and Apps

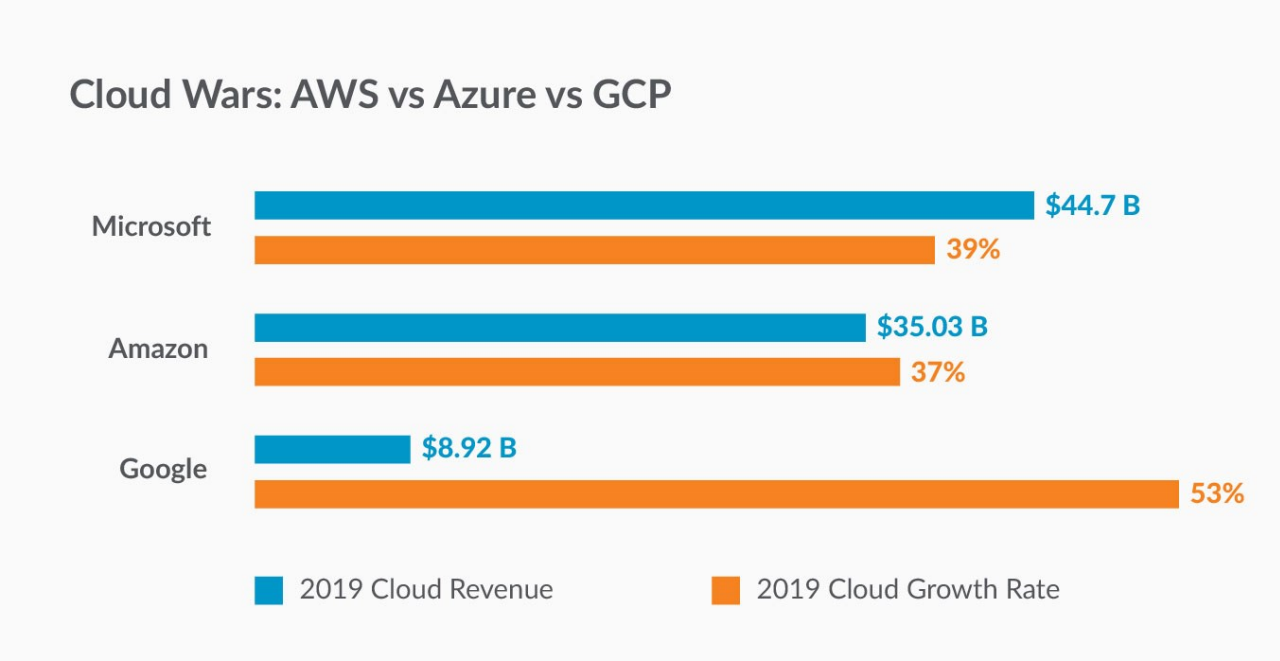


	Azure IoT	AWS	Google IoT
Data di rilascio (Out of beta)	Febbraio 2016	Dicembre 2015	Febbraio 2018
Quota di mercato	31.21%	51.82%	18.79%



State-of-the-art IoT architecture





	Azure IoT	AWS	Google IoT
Data di Rilascio (Out of Beta)	Febbraio 2016	Dicembre 2015	Febbraio 2018
Documentazione	Ottima	Molto Buona	Sufficiente
Certificazione	Ottenibile inviando l'applicazione sviluppata	Ottenibile sostenendo esami relativi a specifici ambiti	Ottenibile sostenendo esami relativi a specifici ambiti
Tipologia Certificazione	Non definita	Per specializzazione (Big Data, Security ecc) oppure per ruolo (Architect, Developer ecc)	Cloud Architect, Data Engineer, Suite Administrator
Vantaggi	Logo, crediti, sottoscrizioni, consulenze, accesso alla community ed eventi	Accesso alla community, logo, merchandise, accesso ad eventi	Non previsti

	Azure IoT	AWS	Google IoT
Architettura	Hub che comunica con tutti gli altri servizi.	I dati vengono raccolti dal Rules Engine e dal Device Shadows. A partire da questi si attivano i vari servizi	Core che comunica con Funzioni, Pub/Sub e Dataflow. Questo si interfaccia agli altri servizi
API	REST	REST	REST
Protocolli	MQTT, AMQP, MQTT on WebSocket, AMQP on WebSocket, HTTPS, (1)	MQTT, MQTT on WebSocket, HTTPS	MQTT, HTTP
Sicurezza	TLS	TLS (mutual)	TLS
Autenticazione	SAS Token, IAM, x.509	x.509, IAM, Amazon Cognito, Federated, (2)	JSON Token, IAM, x.509
SDK	.NET, Java, Node.js, C, Python, (3)	C, Javascript, Java, Python, IOS, Android, Arduino Yun	Go, Java, .NET, Javascript, IOS, Android, PHP, Ruby, Python
Starter Kit	Intel. Raspberry Pi, Freescale, Texas Instruments, Seeed, resin.io, MinnowBoard, BeagleBoard	Broadcome, Marvell, Renesas, Texas Instruments, Intel, Microchip, Seeed, Mediatek, Qualcomm, BeagleBoard	Microchip, Adafruit, Marvell, TechNexion, Grove, Realtek, Allwinner, MangOH.

	Azure IoT	AWS	Google IoT
Edge			
Storage	Blob, CosmosDB, SQL		
Big Data			
Data Visualization	Power Bi		
Artificial Intelligence			
Intelligence API	Language, Speech, Vision, Knowledge		

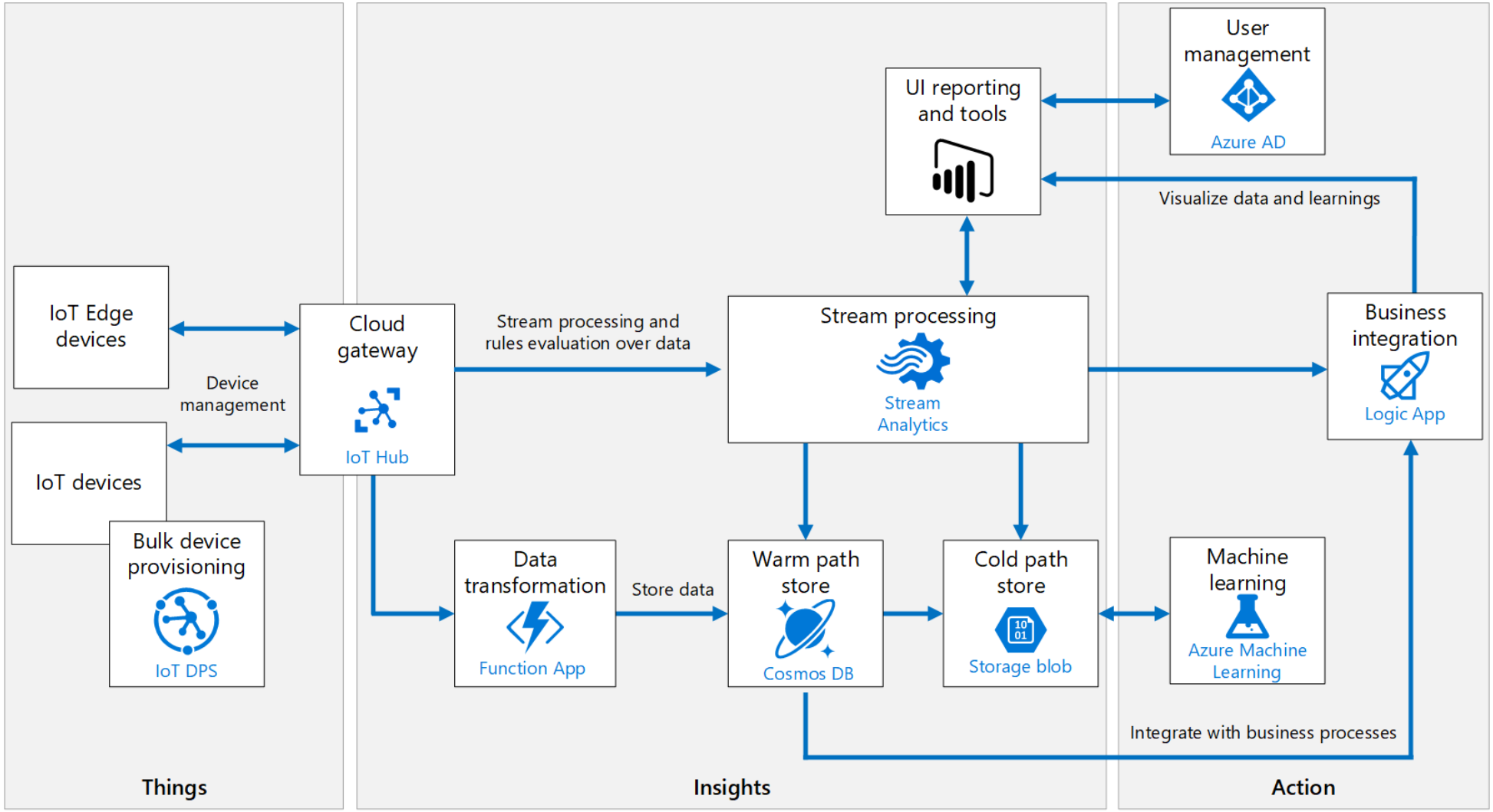
	Azure IoT	AWS	Google IoT
Prezzo	Diverse fasce di prezzo in base al numero di messaggi scambiati	Costo unitario per messaggio e per tempo di connessione del dispositivo	Costo basato sul volume di dati scambiati

	Azure IoT	AWS	Google IoT
Sicurezza	TLS	TLS (mutual)	TLS
Autenticazione	SAS Token, IAM, x.509	x.509, IAM, Amazon Cognito, Federated Identities	JSON Token, IAM, x.509

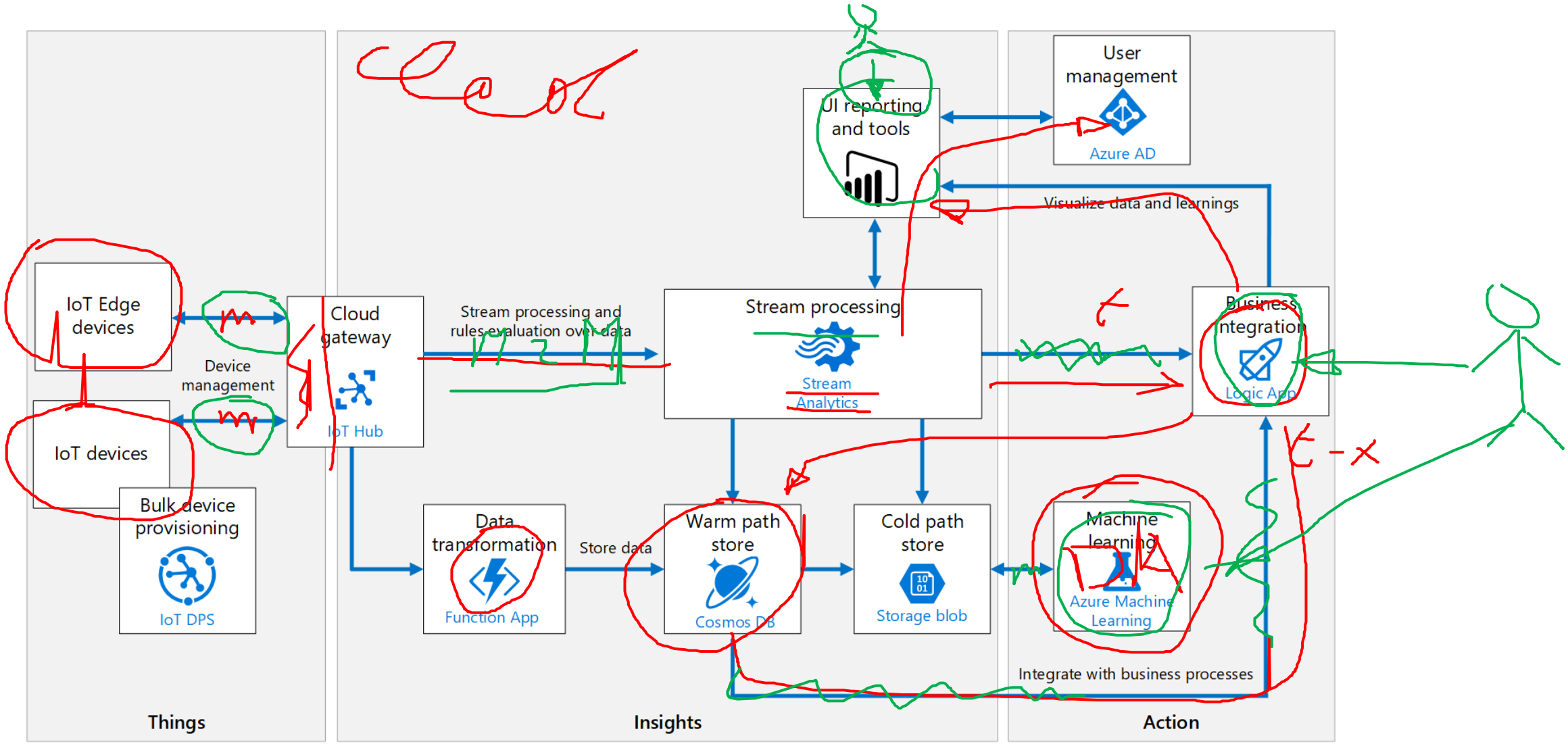
	Azure IoT	AWS	Google IoT
Protocolli	MQTT, AMQP, MQTT on WebSocket, HTTPS, AMQP on WebSocket	MQTT, MQTT on WebSocket, HTTPS	MQTT, HTTP
Communication Patterns	Telemetry, Query, Notification, Command	Telemetry, Query, Notification, Command	Telemetry, Query, Notification, Command

	Azure IoT	AWS	Google IoT
Scalability	Scaling da configurare mediante funzione	Servizio di scaling automatico	Servizio di scaling automatico
Rimborsi	10% di rimborso fino al 99%, al di sotto viene rimborsato il 25%	10% di rimborso fino al 99%, al di sotto viene rimborsato il 30%	10% di rimborso fino al 99%, nella fascia fino al 95% viene restituito il 25% e al di sotto di questa il 50%

Azure Microsoft IoT (1)



Azure Microsoft IoT (1)



Azure Microsoft IoT (2)

- IoT Hub / Cloud Gateway that communicate with the internal ecosystem
- Supported languages in Azure Functions:
  - C# (Full . NET Framework), Java, Node.js, Python
- communication protocols: MQTT, MQTT over WebSockets, AMQP, AMQP over WebSockets, HTTPS
- Azure Security Center: TLS, SAS Token, IAM, x.509, Role-Based Access Control, Shared Access Signature, ….

Azure Microsoft IoT (3)

Secure Score

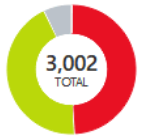
58% (~35 of 60 points)

Recommendations status

1 completed control 17 Total

38 completed recommendations 229 Total

Resource health



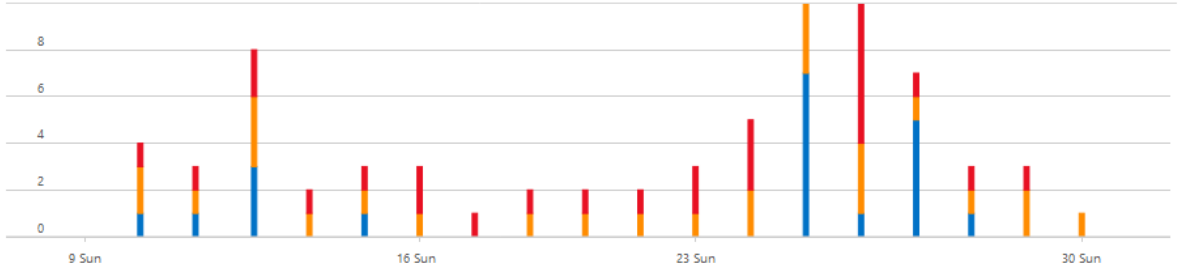
Unhealthy 1.5K
Healthy 1.3K
Not applicable 215

Controls	Potential score increase	Unhealthy resources	Resource Health
Remediate vulnerabilities	+ **10%** (6 points)	171 of 219 resources	
Enable encryption at rest	+ **5%** (3 points)	147 of 231 resources	
Manage access and permissions	+ **5%** (3 points)	20 of 36 resources	
Remediate security configurations	+ **4%** (3 points)	134 of 212 resources	
Protect applications against DDoS attacks	+ **3%** (2 points)	14 of 156 resources	
Encrypt data in transit	+ **3%** (2 points)	135 of 331 resources	
Apply system updates	+ **3%** (2 points)	57 of 212 resources	
Apply adaptive application control	+ **2%** (1 point)	75 of 165 resources	
Secure management ports	+ **2%** (1 point)	14 of 151 resources	
Apply data classification	+ **2%** (1 point)	16 of 53 resources	
Restrict unauthorized network access	+ **1%** (1 point)	48 of 241 resources	
Enable endpoint protection	+ **1%** (1 point)	75 of 192 resources	
Enable auditing and logging	+ **1%** (1 point)	134 of 180 resources	
Implement security best practices	+ **0%** (0 points)	168 of 797 resources	
Enable advanced threat protection	+ **0%** (0 points)	8 of 11 resources	
Custom recommendations	+ **0%** (0 points)	1033 of 2183 resources	
Enable MFA *Completed*	+ **0%** (0 points)	None	

Security Center | Security alerts

Showing 40 subscriptions

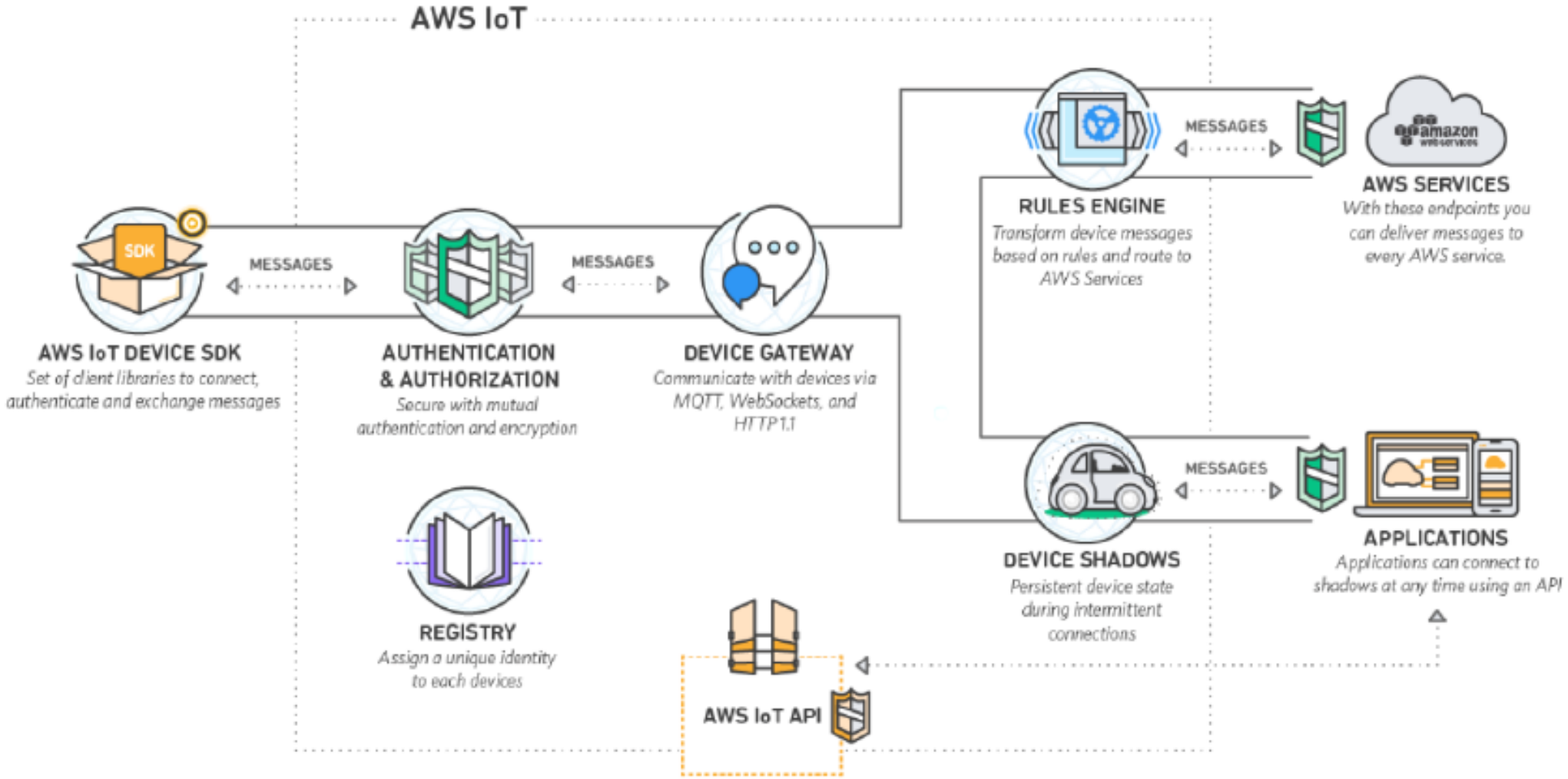
Filter Download CSV report Suppression rules (preview)



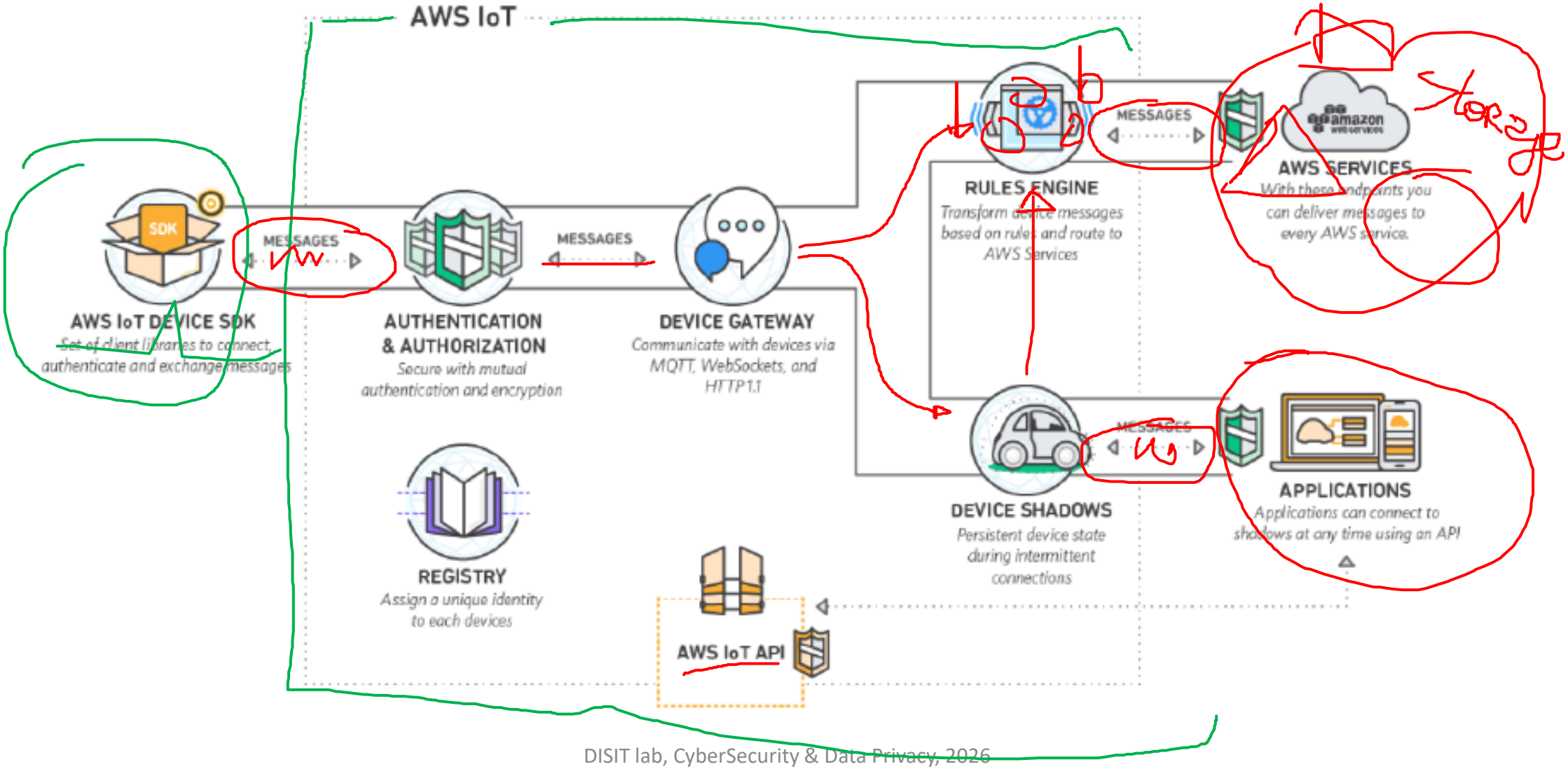
High severity 31
Medium severity 31
Low severity 20

	Description	Count	Date	State	Severity
	Security incident detected from same source	1	08/26/20	Active	High
	Security incident detected	1	08/23/20	Active	High
NEW	Suspicious process executed [seen multiple times]	1	08/29/20	Active	High
	Potential SQL Injection	2	08/26/20	Active	High
	Potential SQL Brute Force attempt	1	08/26/20	Active	High
	Attempted logon by a potentially harmful application	1	08/26/20	Active	High
	Access from a Tor exit node to a storage file share	2	08/24/20	Active	High
	Access from a Tor exit node to a storage blob container	1	08/24/20	Active	High

AWS – Amazon IoT (1)



AWS – Amazon IoT (1)



AWS – Amazon IoT (2)

- Data collected by Rules Engine and Device Shadows. AWS Lambda event-driven, serverless computing platform
- AWS Lambda programming language:
  - Java, Node.js, Python, Go, .NET, Ruby
- MQTT, MQTT over WebSocket, HTTPS
- AWS Cloud Security: TLS, x.509, IAM, Amazon Cognito, Federated Identities, Application Security, regulatory frameworks…

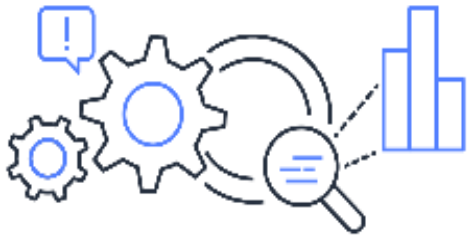
AWS – Amazon IoT (3)

Previeni

Definisci le autorizzazioni e le identità dell'utente, nonché le misure di protezione dell'infrastruttura e dei dati per una strategia di adozione di AWS uniforme e pianificata.

Rileva

Ottieni visibilità sul profilo di sicurezza della tua organizzazione con servizi di registrazione e monitoraggio. Inserisci queste informazioni in una piattaforma scalabile per la gestione, il test e l'audit degli eventi.



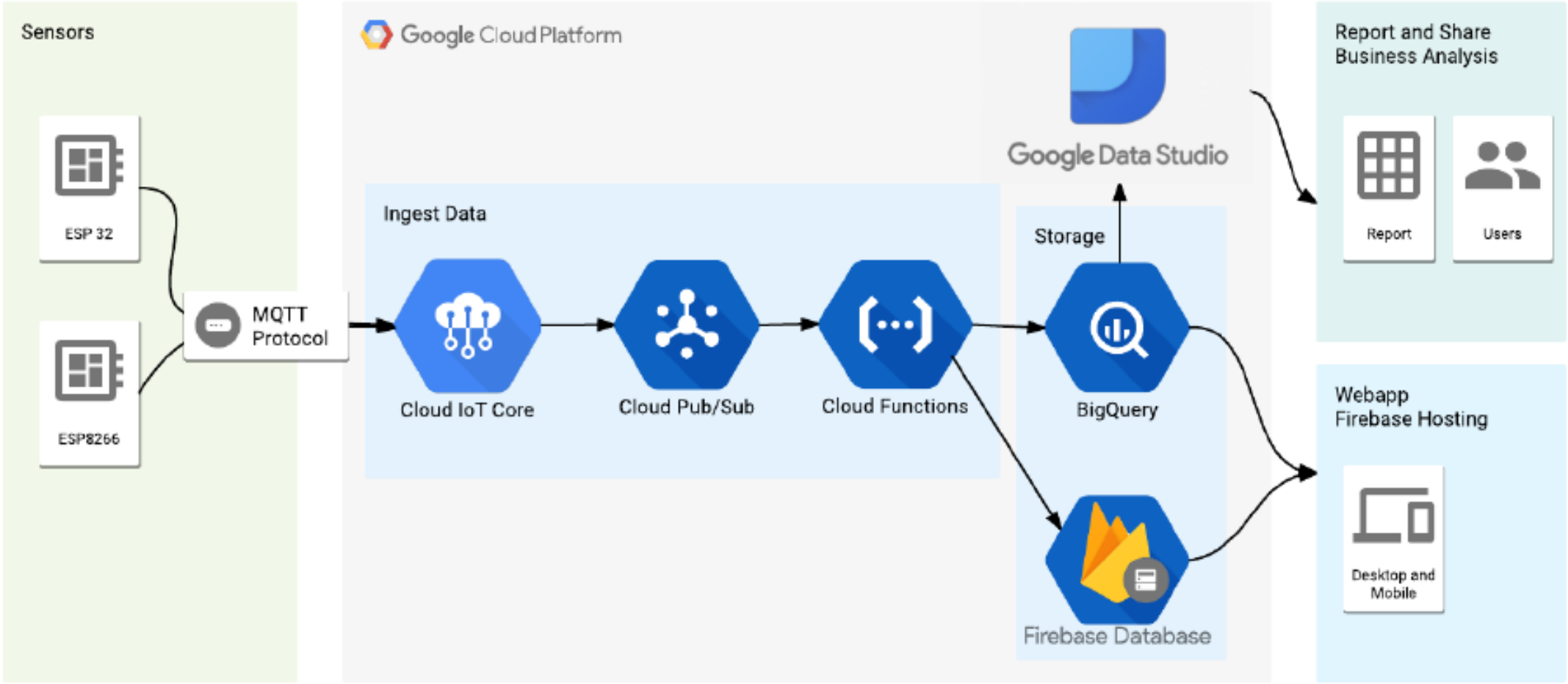
Rispondi

Risposta agli incidenti e ripristino automatizzati per aiutare a spostare l'attenzione principale dei team di sicurezza dalla risposta all'analisi della causa principale.

Risolvi

Sfrutta l'automazione guidata dagli eventi per risolvere rapidamente e proteggere il tuo ambiente AWS quasi in tempo reale.

Google IoT (1)


Sensors
ESP 32
ESP8266
MQTT Protocol
Google Cloud Platform
Ingest Data
Cloud IoT Core
Cloud Pub/Sub
Cloud Functions
Storage
Google Data Studio
BigQuery
Firebase Database
Report and Share Business Analysis
Report
Users
Webapp Firebase Hosting
Desktop and Mobile

Google IoT (2)

- Clout IoT Core that communicate with internal functionalities, in a Pub/Sub and Dataflow manner
- Cloud Functions can be written using:
  - JavaScript, Python 3, Go, or Java runtimes
- MQTT, HTTP
- Google Device security: TLS, JSON Token, IAM, x.509, PKI, Key rotation, …

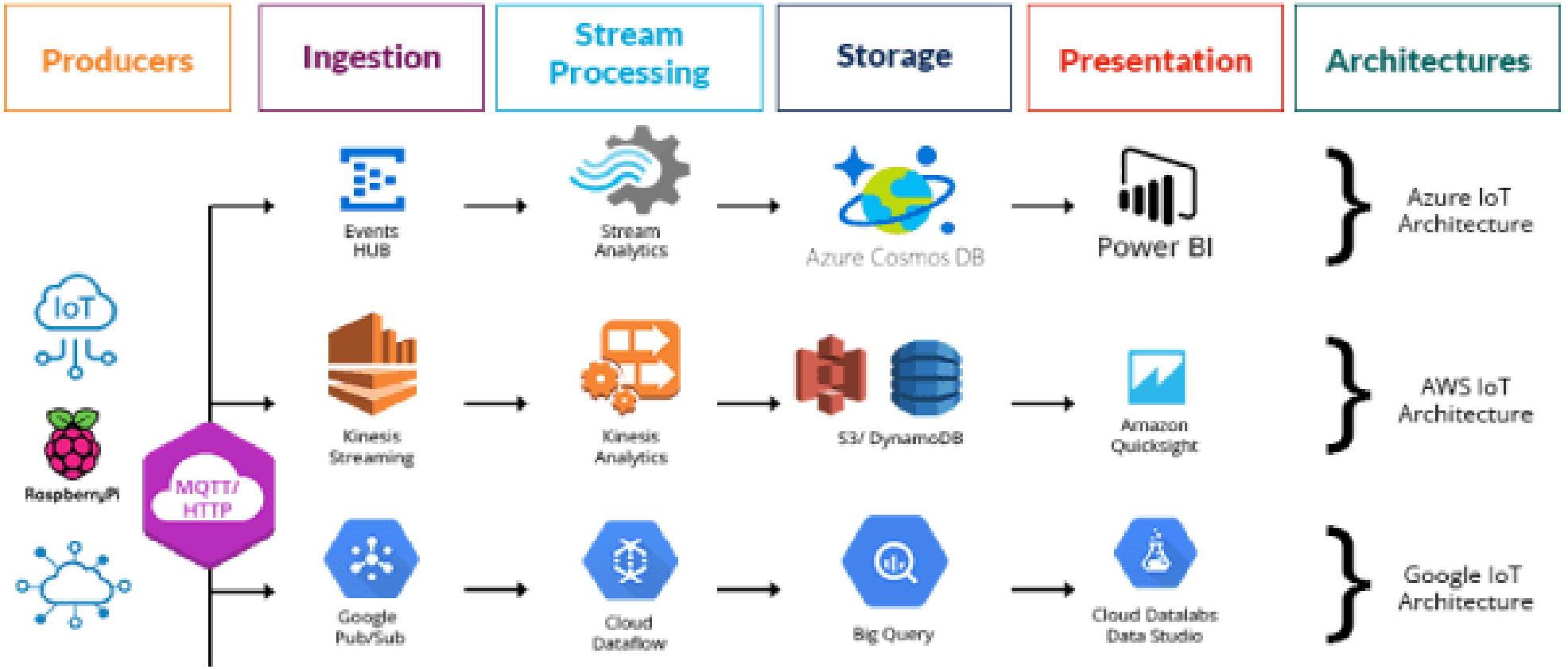
Google IoT (3)

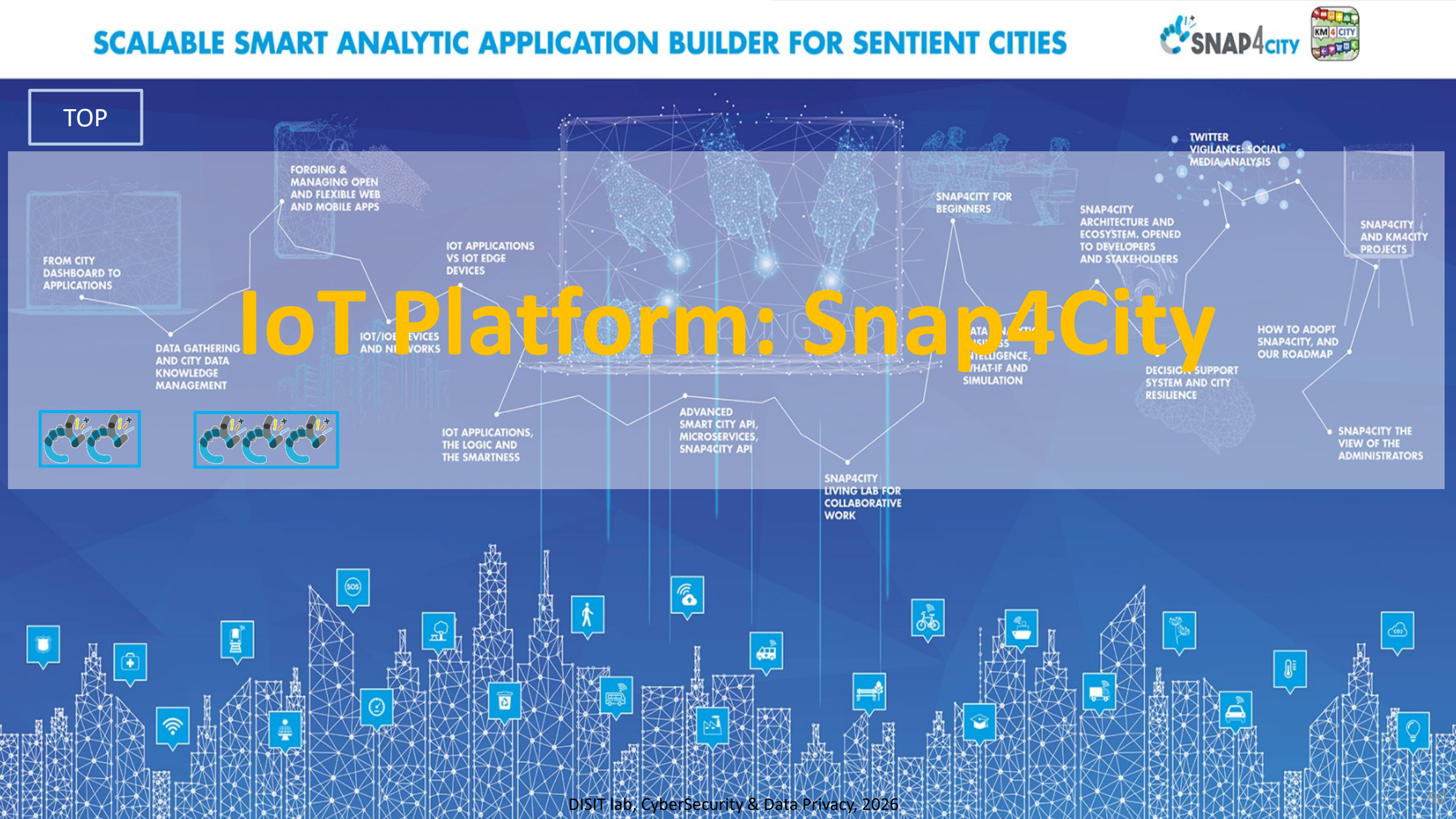
- Application Security Requirements for IoT Devices

- Security Requirements
  1. Best Secure Coding Practices Should be Followed
  2. Use of TLS for all Network Communications
  3. Verified Firmware Updates
  4. Scalable Process for Firmware Updates
  5. Strong Authentication Mechanisms
  6. Unique MAC Addresses
  7. No Communication With third-party Servers
  8. No Hardcoded Credentials
  9. Unique & Replaceable Certificates
  10. Commitment to Security Updates
  11. Minimum Service Exposure
  12. WiFi Must Use WPA2
  13. Bluetooth Security
  14. Sync Clocks with NTP
  15. No External Network Connectivity
  16. Use of Non-WiFi Wireless Interfaces
  17. Identification and Delivery of Open Source Components
  18. Graceful Degradation
  19. Test Resilience

- Recommendations
  1. Provide Facilities for Remote Logging
  2. IEEE 802.1x Support with Certificates
  3. Certificate-Based Mutual Authentication
  4. Perfect Forward Secrecy Support
  5. IPv6 Support
  6. Honor DHCP/IPv6 RA Options
  7. Transparent Patch Management
- Guidelines
  1. IEEE 802.1AR Secure Device Identity
  2. Secure/Verified Boot
  3. Manufacturer Usage Descriptions

IoT Architectures comparison





IoT Platform: Snap4City

100% OPEN SOURCE

THE POWER OF ARTIFICIAL INTELLIGENCE AT THE SERVICE OF YOUR OPERATION AND PLAN

SNAP4CITY · KM4CITY

www.snap4city.org

UNIVERSITÀ DEGLI STUDI FIRENZE · DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE · DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

Powered by FIWARE

FREE TRIAL

PEN Test Passed

EU GDPR COMPLIANT

SNAP4 Appliances and Dockers Installations

EUROPEAN OPEN SCIENCE CLOUD

Node-RED

JS Foundation

EØ15 digital ecosystem

NVIDIA

OPERATION AND PLAN - CONTROL ROOMS - DECISION SUPPORT SYSTEMS - WHAT-IF ANALYSIS - OPTIMIZATION - APPLICATIONS

HORIZONTAL AI PLATFORM

MOBILITY AND TRANSPORT

SMART ENERGY AND SMART BUILDING

ENVIRONMENT AND WASTE MANAGEMENT

CITY USER'S SERVICES AND TOURISM MANAGEMENT

SNAPADVISOR

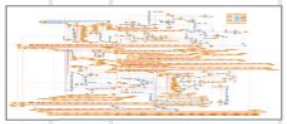
BUSINESS INTELLIGENCE - SIMULATIONS - VISUAL ANALYTICS - SYNOPTICS - GRAPHICAL WIDGETS - ANALYTICS

DASHBOARDS, WIDGETS
TEMPLATES

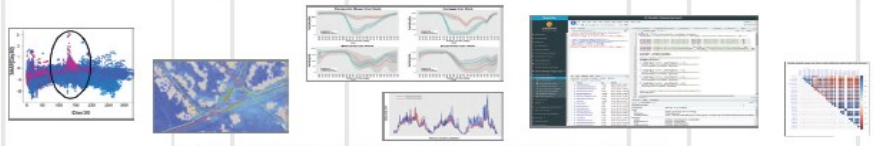
PREDICTION - ANOMALY DETECTION - CLUSTERING - ROUTING - SENTIMENT NLP - TRAFFIC FLOW - PEOPLE FLOWS - SDG
15 MIN CITY INDEX - KPI - HEATMAPS - ORIGIN DESTINATION - MAPS - VECTOR FIELD - ETC...

API - MICROSERVICES - GIS - BPM
VIDEO - REPORTS - MAPS - 3D ...

- DEVELOMENT ENVIRONMENT AND METHODOLOGY
- VISUAL PROGRAMMING, ML, AI, HPC
- TRAINING COURSES



EXPERT SYSTEM, KNOWLEDGE BASE
SEMANTIC REASONING
SMART DATA MODEL
IOT DEVICE MODELS, DATA SPACES



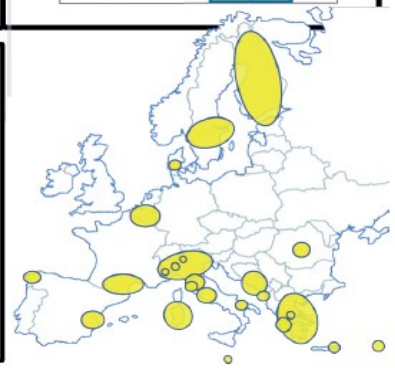
BIG DATA ANALYTICS, ARTIFICIAL INTELLIGENCE
EXPLAINABLE AI, MACHINE LEARNING, GENERATIVE AI
OPERATIVE RESEARCH, STATISTICS

VISUAL PROGRAMMING, ADAPTERS
DATA FLOWS, WORKFLOWS
PARALLEL DISTRIBUTED PROCESSING
DATA DRIVEN

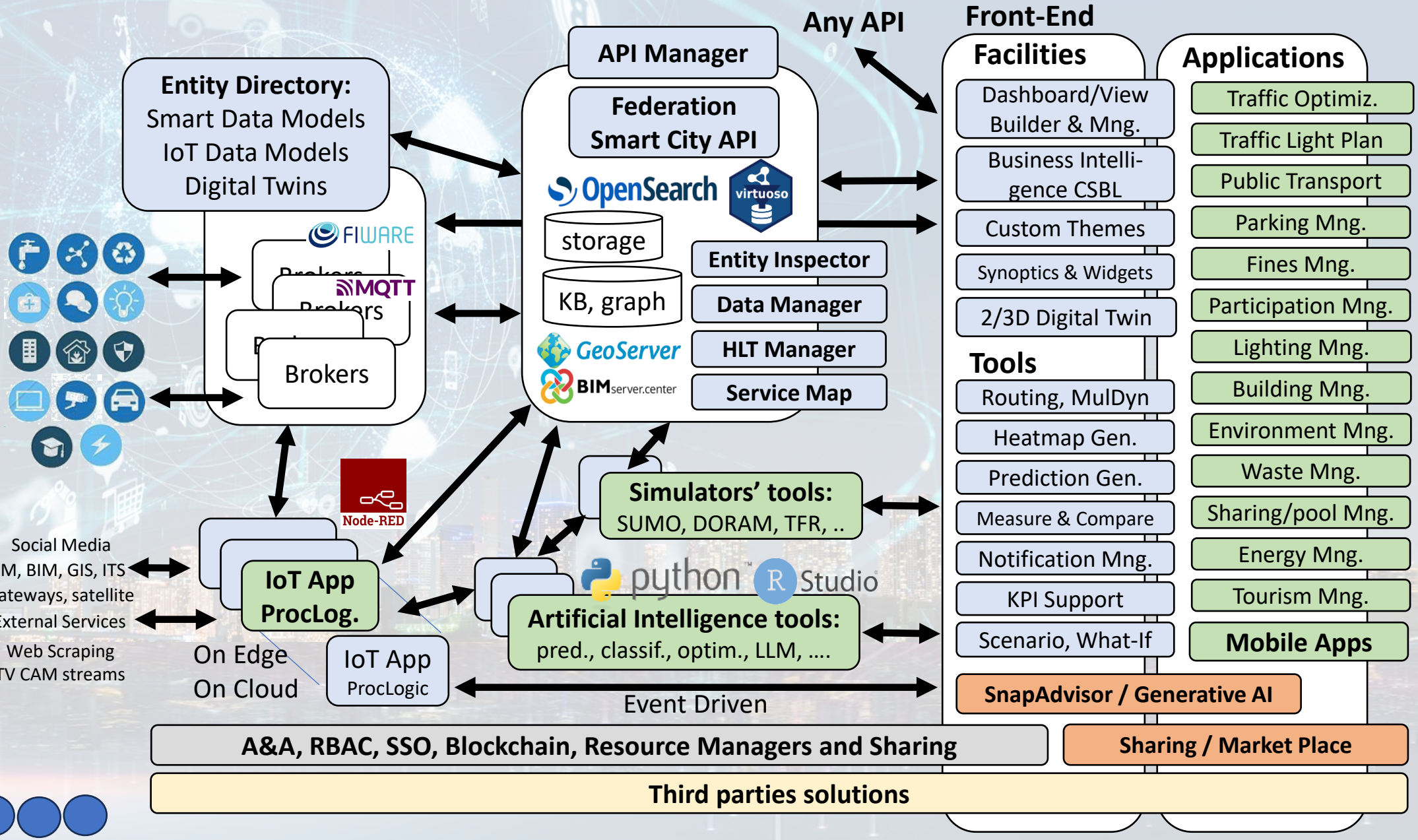
FULL INTEROPERABILITY, ANY: DATA, BROKERS, NETWORKS AND VERTICALS

NATIVE AND EXTERNAL APPLICATIONS

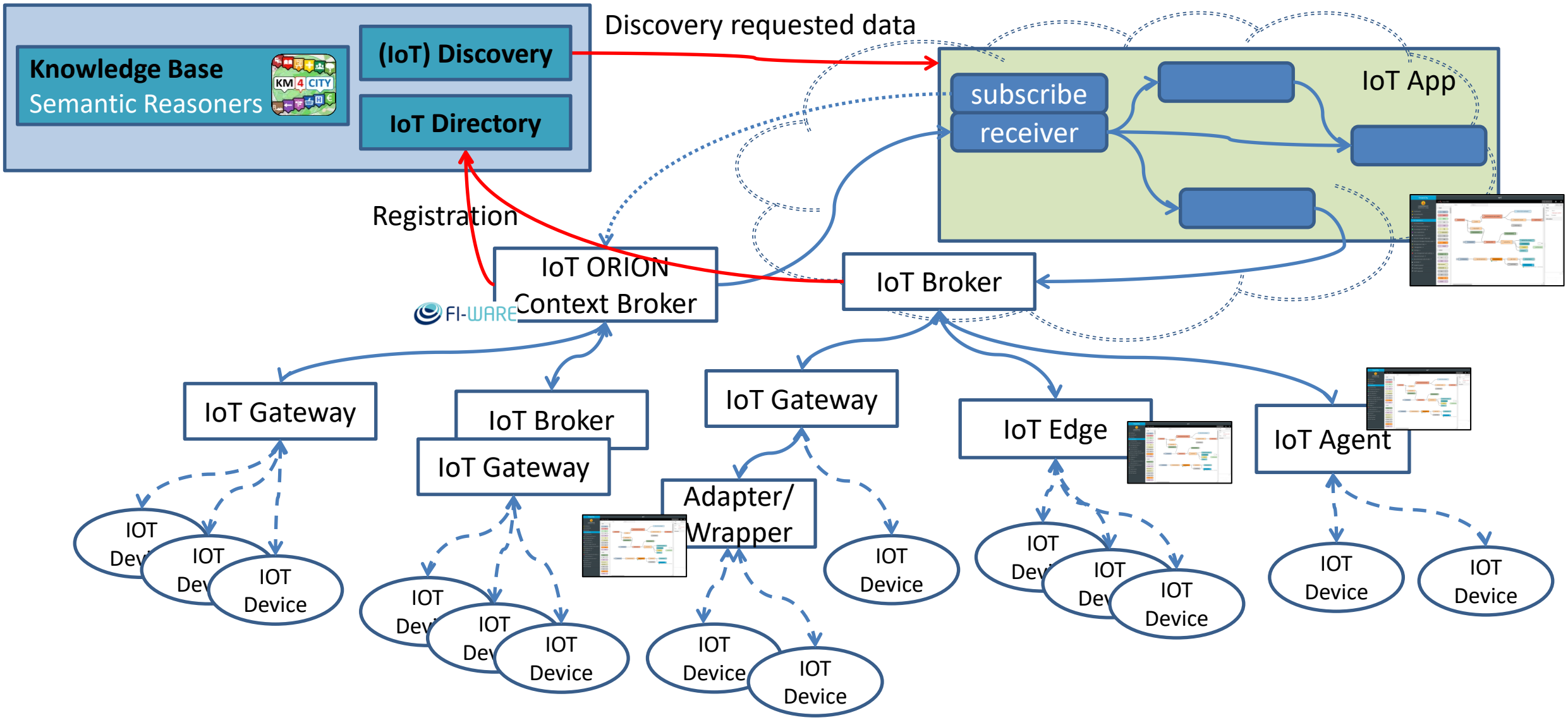
- Smart Parking
- Smart Light
- Smart Waste
- Smart Energy
- Smart Building
- Smart Tourism
- ...



Technical Architecture



IoT Network


Knowledge Base
Semantic Reasoners
(IoT) Discovery
IoT Directory
Discovery requested data
subscribe
receiver
IoT App
Registration
IoT ORION
Context Broker
FI-WARE
IoT Broker
IoT Gateway
IoT Broker
IoT Gateway
IoT Gateway
Adapter/
Wrapper
IoT Edge
IoT Agent
IOT
Device

IoT main components

- IoT Device
- IoT Router (with/without computation capabilities)
- IoT Broker (+ Shadowing)
- IoT Device Directory
- IoT User Management
- IoT Service Bus (Pub/Sub, Rule-engine, Data-driven)
- IoT Analytics
- IoT Data repository
- IoT Applications (off-grid/on-cloud)
- IoT Dashboards

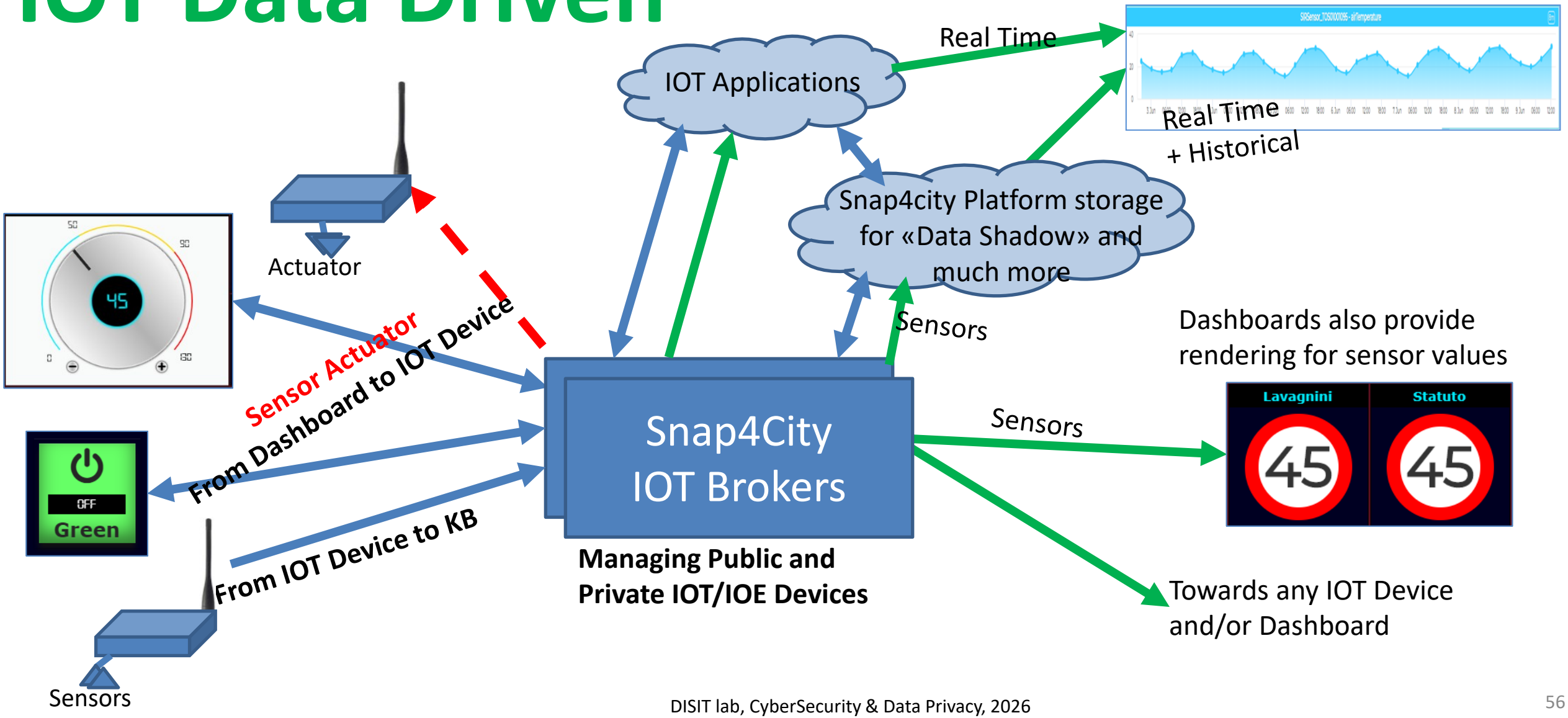
Standards and Interoperability (5/2022)

Compliant with:

- **IOT:** NGSI V2/LD, LoRa, LoRaWan, MQTT, AMQP, COAP, OneM2M, TheThingsNetwork, SigFOX, Libelium, IBIMET/IBE, Enocean, Zigbee, DALI, ISEMC, Alexa, Sonoff, HUE Philips, Tplink, BACnet, TALQ, Protocol Buffer, KNX, ..
- **General**: HTTP, HTTPS, TLS, Rest Call, SMTP, TCP, UDP, SOAP, WSDL, FTP, FTPS, WebSocket, WebSocket Secure, GML, WFS, WMS, RTSP, ONVIF, AXIS TVCam, CISCO Meraki, OSM, Copernicus, The Weather Channel, Open Weather, OLAP, ….
- **Formats**: JSON, GeoJSON, XML, CSV, GeoTIFF, OWL, WKT, KML, SHP, db, XLS, XLSX, TXT, HTML, CSS, SVG, IFC, XPDL, OSM, Enfuser FMI, …
- **Database**: Open Search, MySQL, Mongo, HBASE, SOLR, SPARQL, ODBC, JDBC, Elastic Search, Phoenix, OBD2, PostGres, MS Azure, ..
- **Industry**: OPC/OPC-UA, OLAP, ModBUS, RS485, RS232,..
- **Mobility**: DATEX, GTFS, Transmodel, ETSI, ..
- **Social**:Twitter, FaceBook, Telegram, ..
- **Events**: SMS, EMAIL, CAP, RSS Feed, ..
- **OS**: Linux, Windows, Android, Raspberry Pi, Local File System, ESP32, etc.

https://www.snap4city.org/65

IOT Data Driven



IoT Devices

IoT Device Models

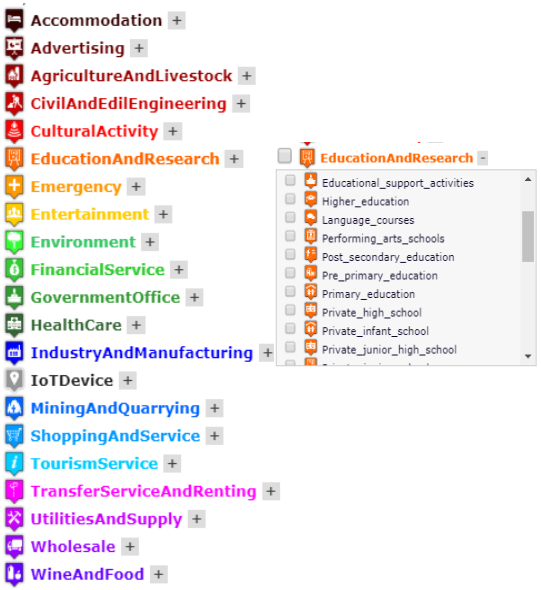
IoT Device

- Name:…..
- Model:…..
- Position: …….

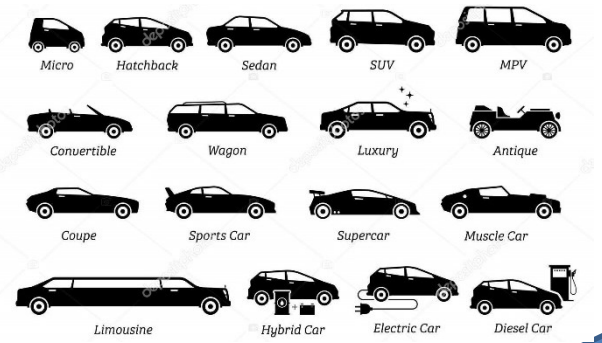
IoT Device Variables

- **dateObserved: …….**
- ID:
- Status: ready
- Temperature: 70%
- WaterLevel: 35%
- UsedCapsBox: 30%
- Power: OK
- …..

- Conceptually are IoT Devices with sensors/actuators, IN/IN-OUT
- They are classified in terms of nature/subnature
- For Searching and showing on maps and dashboards **HLT of IoT Devices** can be:
  - **IoT Device Models**, for example: «personal coffee machine»
  - **IoT Device** name, for example: «mycoffemachine1», «CM23»
  - **IoT Device Variable**, for example: «Temperature»



Mobile Devices

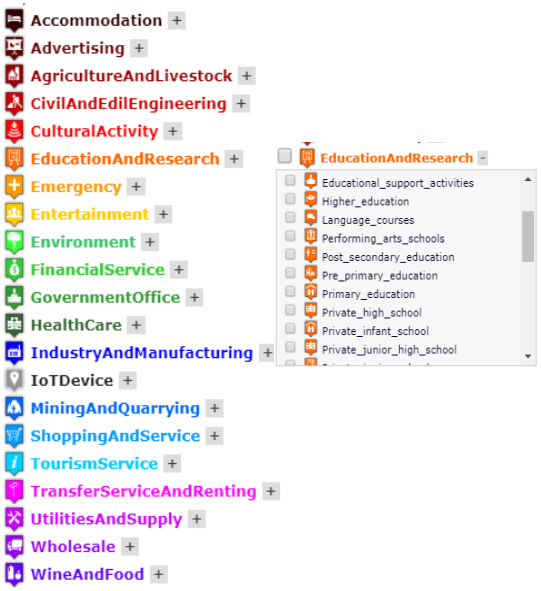


Mobile Device Models

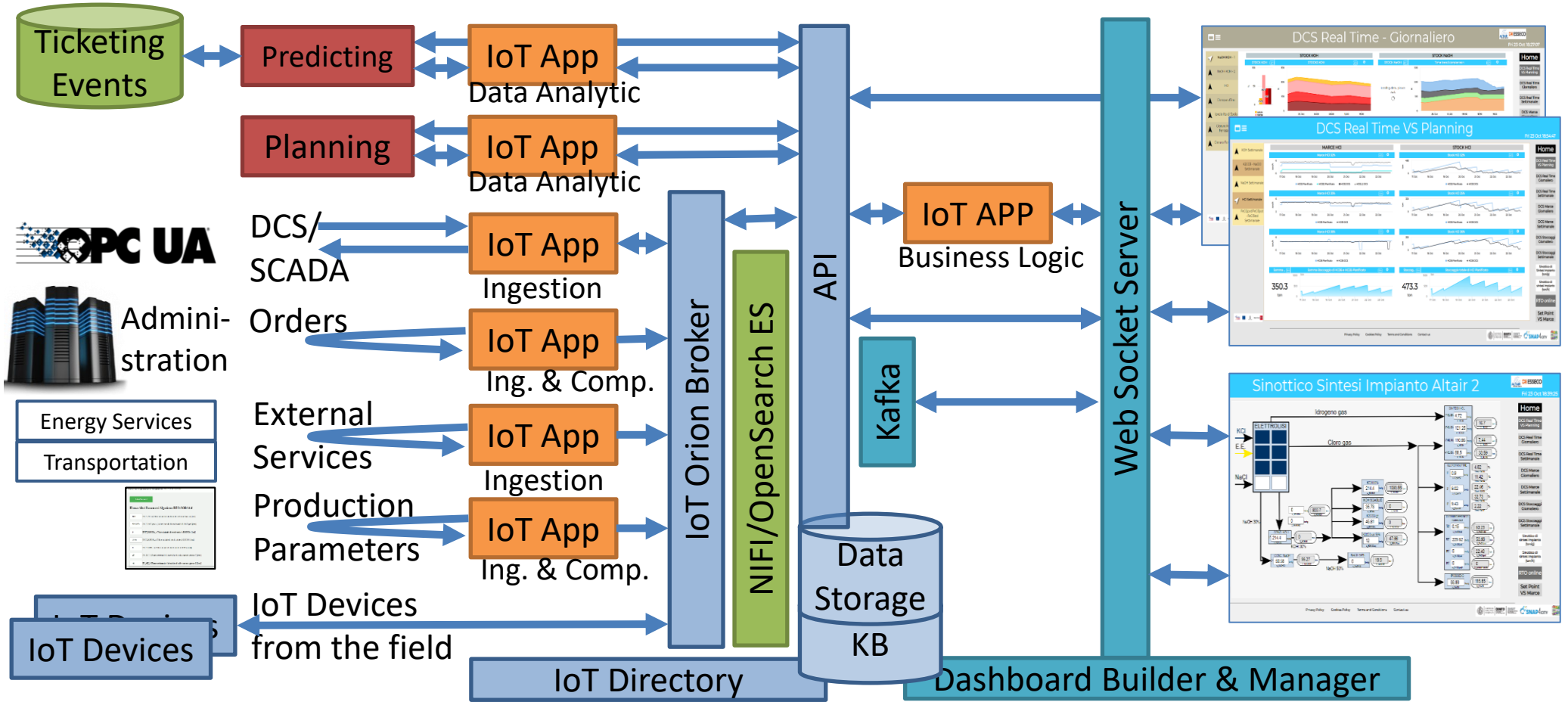
Mobile Device
- Name:…..
- Model:…..
- Spec:…

Mobile Device Variables
- ID:
- **dateObserved: ……..**
- Status: ready
- Temperature: 70%
- Gasoline: 35%
- Velocity: 231,3 Km/h
- **Position: 44.3223, 11.3432**
- …..

- They are a special case of IoT Devices
  - they are managed as IoT Devices in the system
- They are classified in terms of nature/subnature
- For Searching and showing on maps and dashboards, they are different
  HLT of Mobile Devices can be:
  - **Mobile Device Model**, for example: «sedan»
  - **Mobile Device** name, for example: «BMW JD7356HD», «Ford KO786KK»
  - **Mobile Device Variable**, for example: «velocity»

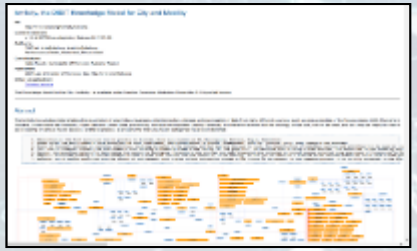


Snap4Industry IOT Architecture



Data Analytics on Snap4City platform

Swagger



Ontology Schema

LOG.disit.org

Big Data Store Facility

Smart City API from Knowledge Base and other tools

TensorFlow

NVIDIA CUDA

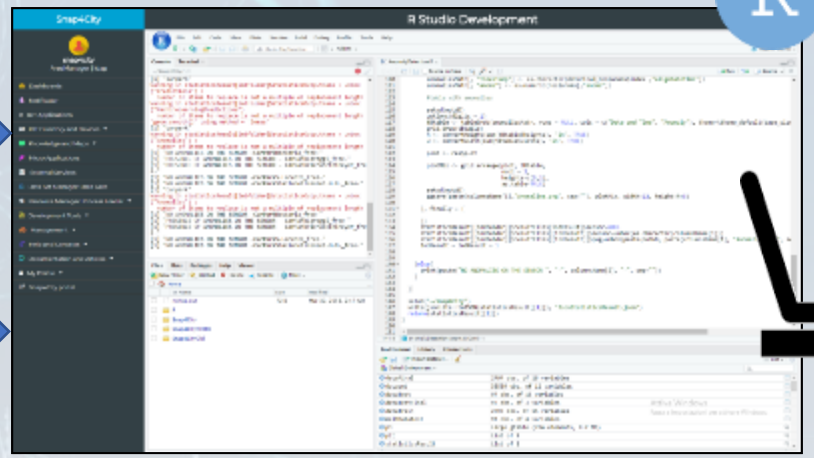
python

jupyter

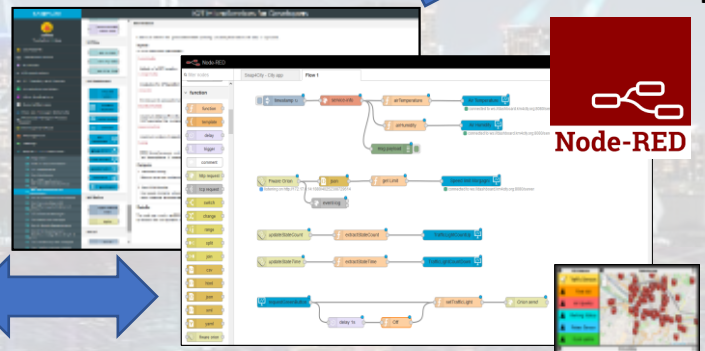
R Studio

SNAP4CITY

KM4CITY



Creating MicroServices



Using them into IOT Applications

Saving / Sharing reusing

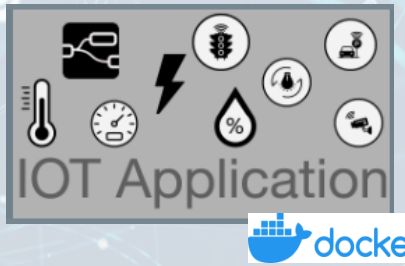
Resource Manager

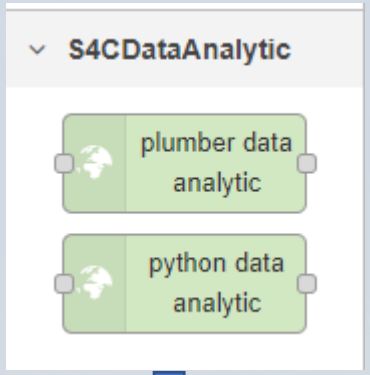
Data Analytic Container

1

Develop .py **or** .r program on (i) Snap4City platform online, or (ii) your Development Machine.
The code has to respect the guidelines provided. For examples see:
https://www.snap4city.org/641
https://www.snap4city.org/645

2 Open an advanced IoT App / Node-RED

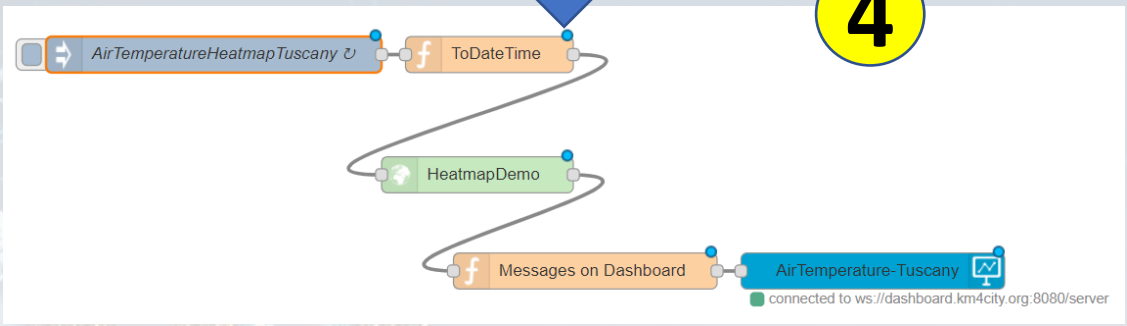




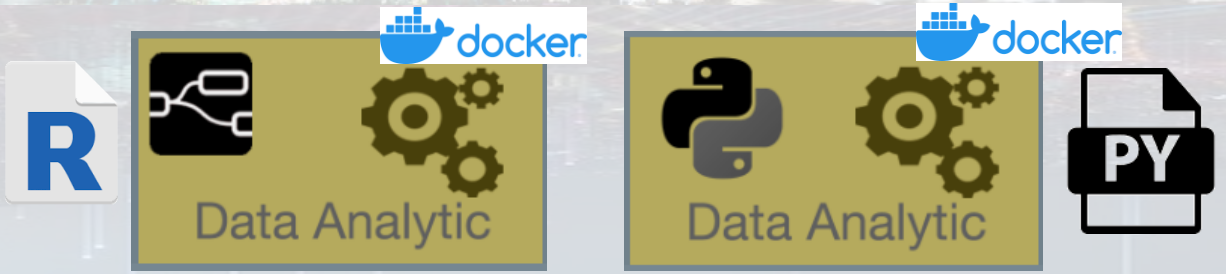
3

Use Snap4City Data Analytic Node, and load in the code you developed

4



5 Deploy the IoT App → Snap4City Container Manager based on Marathon/Mesos is creating a Container for your Data Analytic code



Platform Management: docker, SNAP4CITY

Presentation: Control Room, Dashboards, Synoptics, Wizards, Widgets, Visual Analytics Applications, Mobile Apps
Telegram, Bot, …
SNAP4CITY, OpenSearch

External Interoperability: Smart City API, general API and accounting
SNAP4CITY, ASCAPI, WebSocket

Node-RED
IoT Applications
Data Flow Logic

Operation:
Reporting | Simulation | Heatmapping | Traffic Flows | Tip. Time Trend | .....
R Studio, python, docker, ...
Analysis | WorkFlow Tickets BPM | Sentiment Analysis | ..... | Open to any module and system
Data Analytics | Predictions | Anomaly detection | Statistics | Artificial Intelligence | Routing | Internal GIS GeoServer | ckan | openMAINT | BIMserver.center | …

Internal Interoperability: API, MicroServices
SNAP4CITY, ASCAPI, WebSocket, FIWARE

Data Management: data modeling, data storage, noSQL,
semantic modeling, city entities, aggregation, normalization, knowledge base
nifi, OpenSearch, virtuoso
NGSI V1, V2 FIWARE
Linked Data triples

Data Collection: data mining, harvesting, integration,
transformation, data models,
FIWARE, Node-RED
Any protocol and format
Any protocol and format

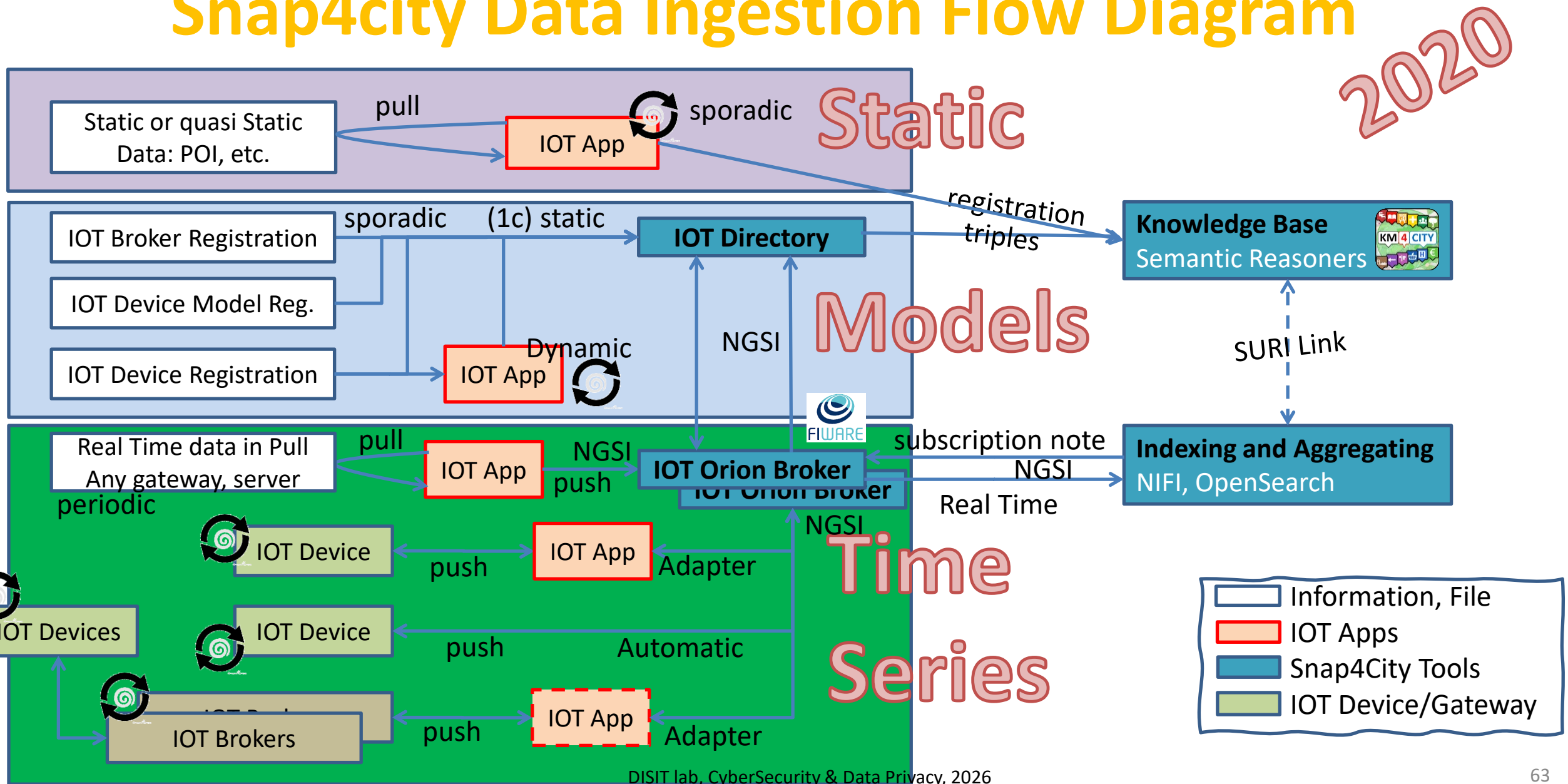
Connectivity: wired, wireless (Lora, 5G, 4G, 3G, Wi-Fi, etc…), IoT Edge, etc.
Node-RED
Any protocol and format
Any protocol and format

Authentication and Authorization: KEYCLOAK, OpenLDAP, SNAP4CITY
GDPR compliant


Device Layer

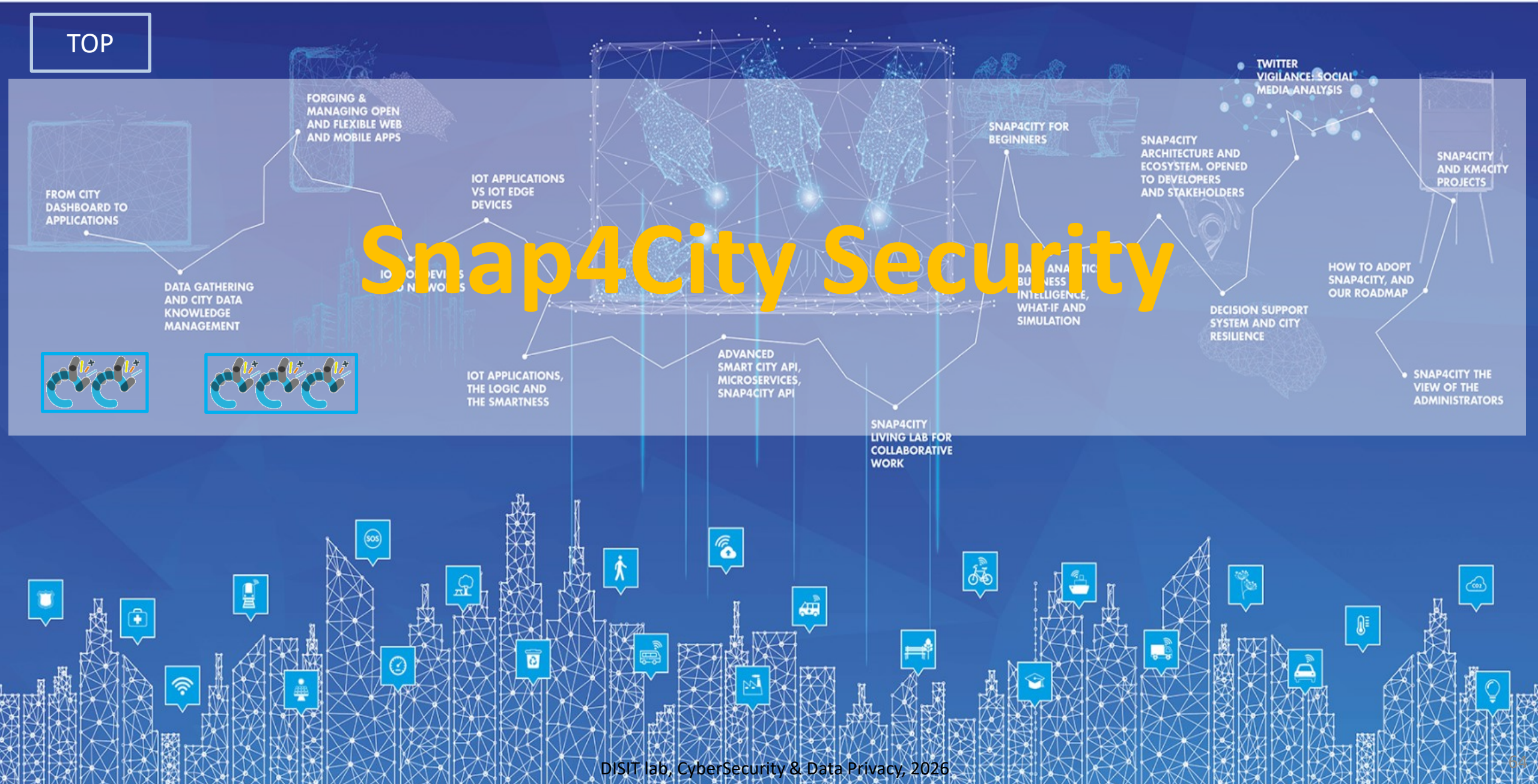
GIS | BIM | Gateways | External Services | Web Scraping | Social Media
External Third Party Services

Snap4city Data Ingestion Flow Diagram



SCALABLE SMART ANALYTIC APPLICATION BUILDER FOR SENTIENT CITIES

TOP



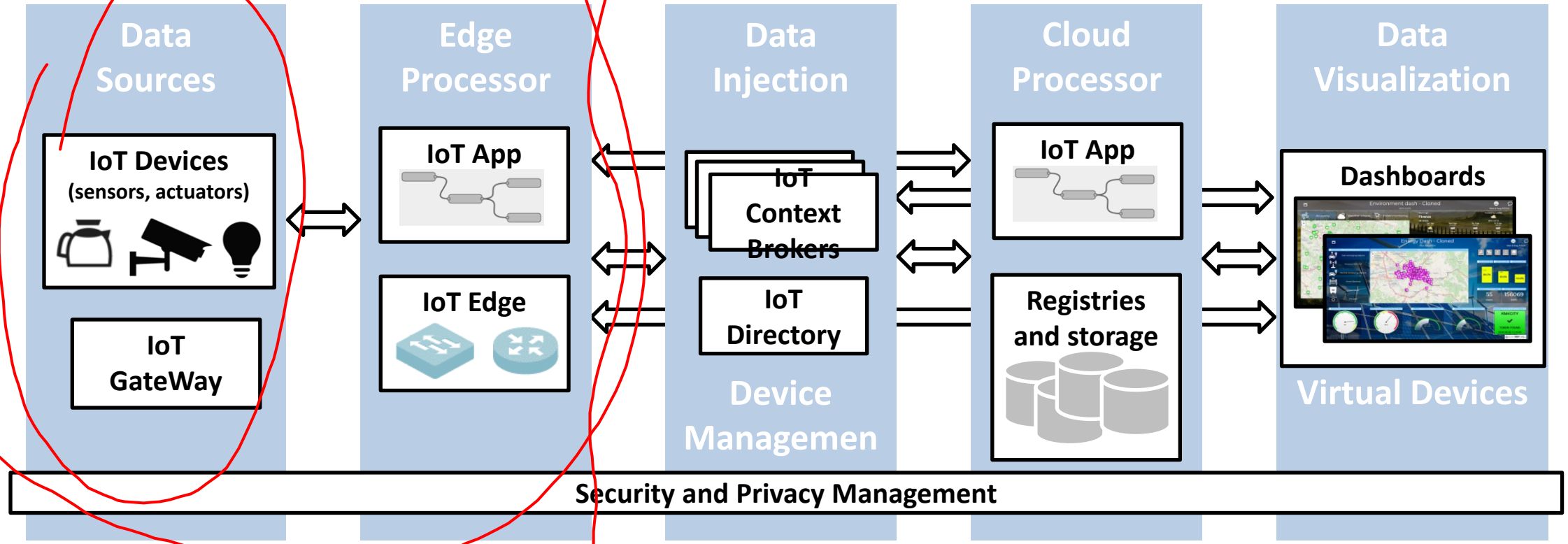
Snap4City Security

Complexity in Smart City IOT Platforms

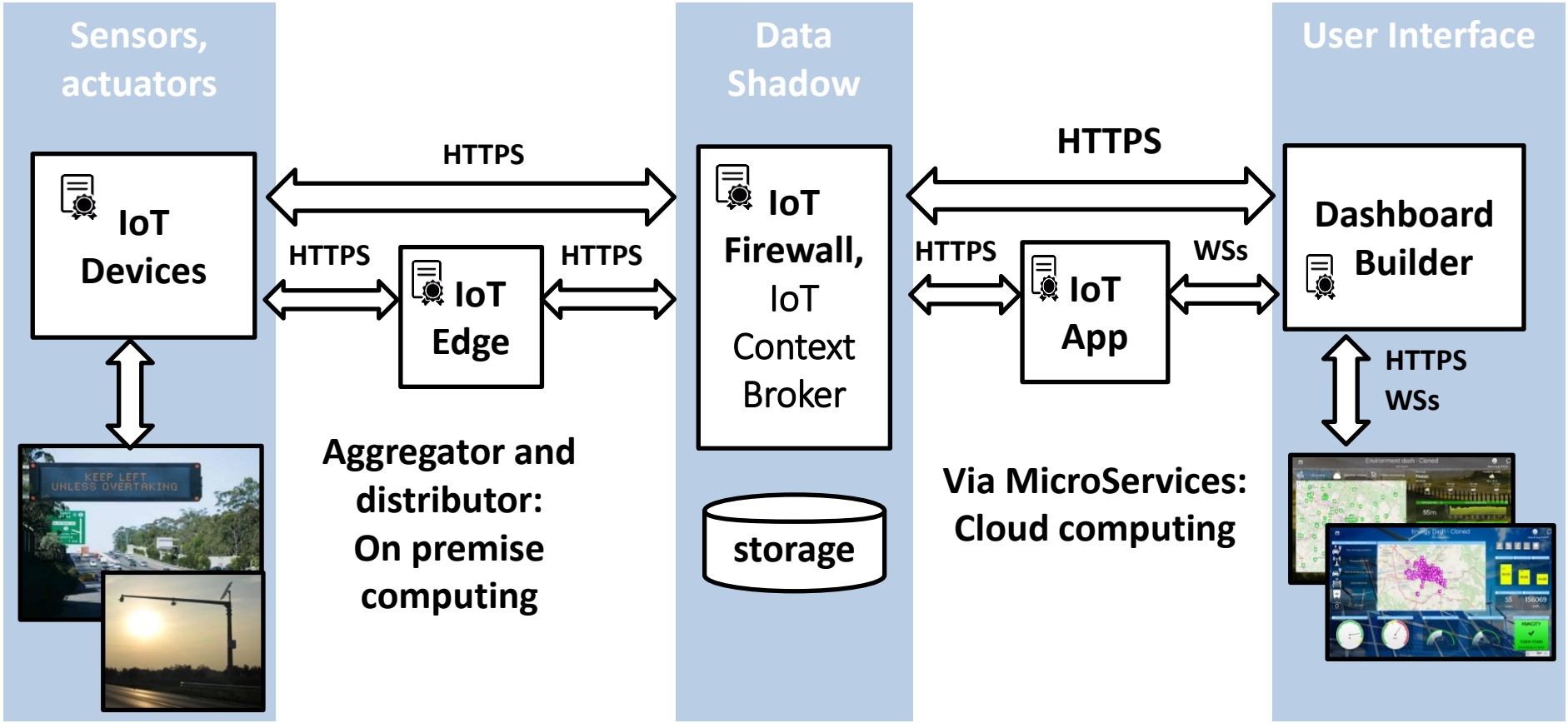
End to End security

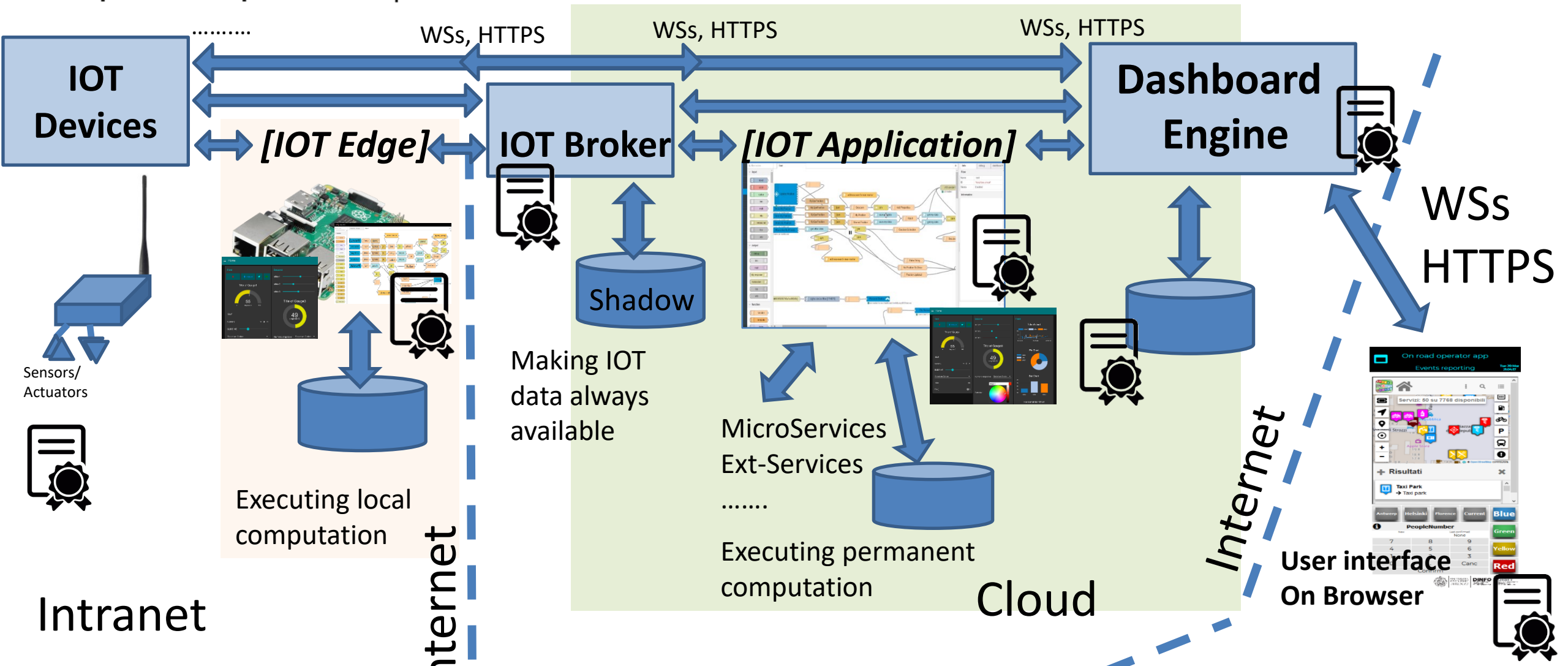
– From IOT Devices to Dashboard (user interface)

- H2M
- M2M



The secure stack





End 2 end security

IOT Devices

.....

WSs, HTTPS

WSs, HTTPS

WSs, HTTPS

Dashboard Engine

[IOT Edge]

IOT Broker

[IOT Application]

WSs HTTPS

Sensors/ Actuators

Executing local computation

Shadow

Making IOT data more available

MicroServices
Ext-Services
.....

Executing permanent computation

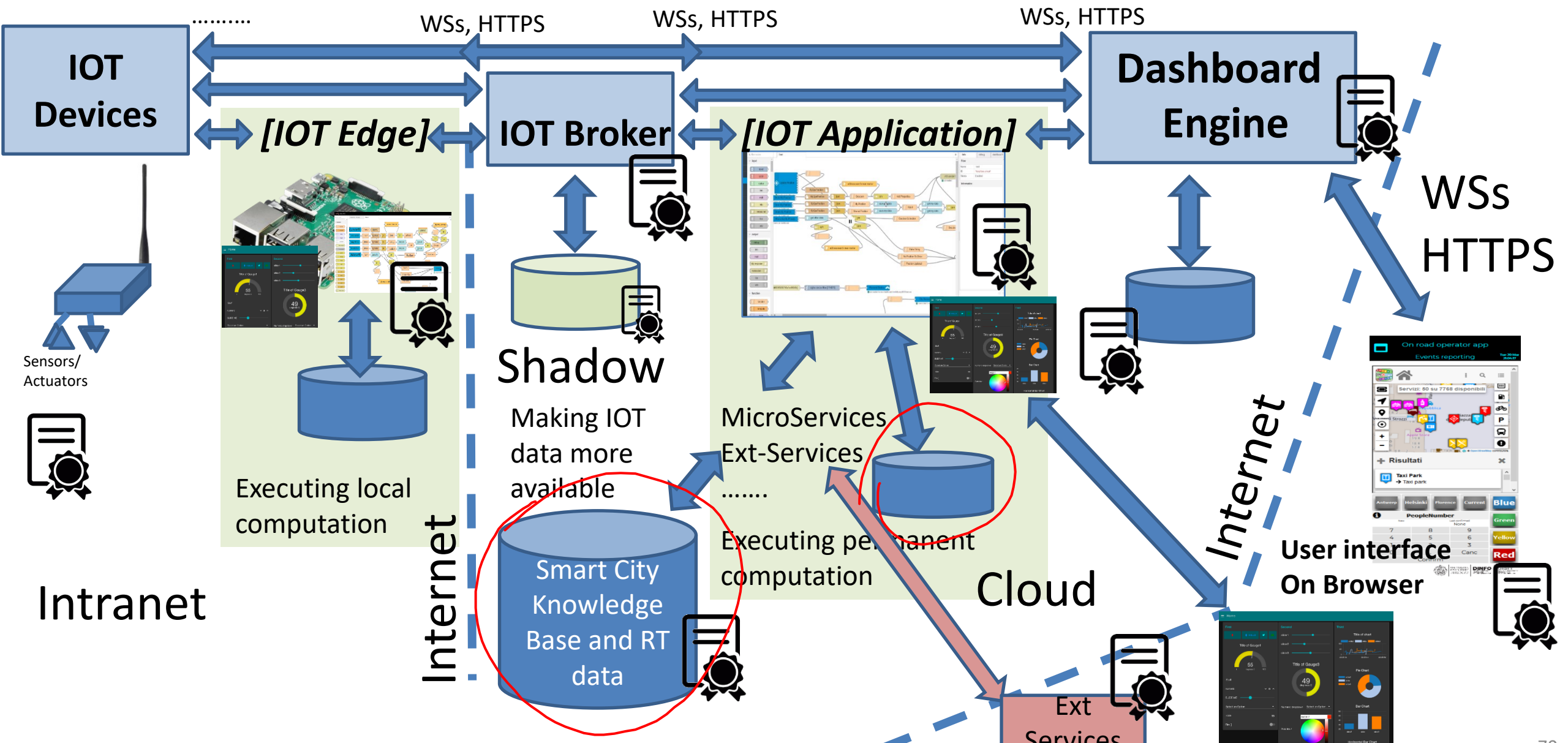
Internet

Internet

Intranet

Cloud

User interface On Browser


.....
WSs, HTTPS
WSs, HTTPS
WSs, HTTPS
IOT Devices
[IOT Edge]
IOT Broker
[IOT Application]
Dashboard Engine
WSs
HTTPS
Sensors/
Actuators
Executing local computation
Shadow
Making IOT data more available
MicroServices
Ext-Services
.....
Executing permanent computation
Internet
Smart City Knowledge Base and RT data
Cloud
Internet
Ext Services
User interface On Browser
Intranet

Grouping on Data Lake

IOT Devices

.....

WSs, HTTPS

WSs, HTTPS

WSs, HTTPS

Dashboard Engine

[IOT Edge]

IOT Broker

[IOT Application]

WSs HTTPS

Sensors/ Actuators

Shadow

Making IOT data more available

Executing local computation

MicroServices
Ext-Services
.....

Executing permanent computation

Smart City Knowledge Base and RT data

Internet

Internet

Cloud

Ext Services

User interface On Browser

Intranet

Grouping on Data Lake

IOT Devices

.....

WSs, HTTPS

WSs, HTTPS

WSs, HTTPS

[IOT Edge]

IOT Broker

[IOT Application]

Dashboard Engine

WSs HTTPS

Sensors/ Actuators

Executing local computation

Shadow

Making IOT data more available

Data Analytics

MicroServices
Ext-Services
.....

Executing permanent computation

Smart City Knowledge Base and RT data

Parallel Computing

Ext Services

Cloud

Internet

Internet

Intranet

User interface On Browser

.....

WSs, HTTPS

WSs, HTTPS

WSs, HTTPS

IOT Devices

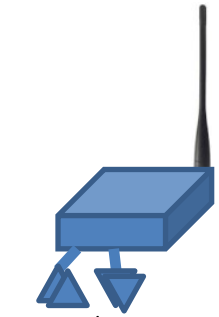
[IOT Edge]

IOT Broker

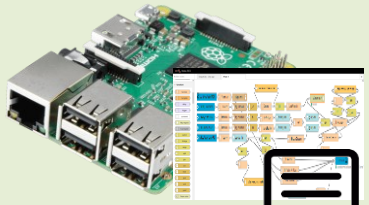
[IOT Application]

Dashboard Engine

WSs HTTPS



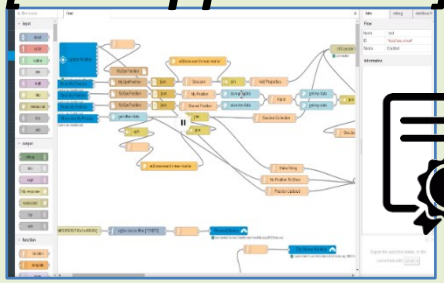
Sensors/ Actuators



Executing local computation

Shadow

Making IOT data more available



MicroServices
Ext-Services
.....

Executing permanent computation

Internet

User Profile Manager

Living Lab Dev Tools

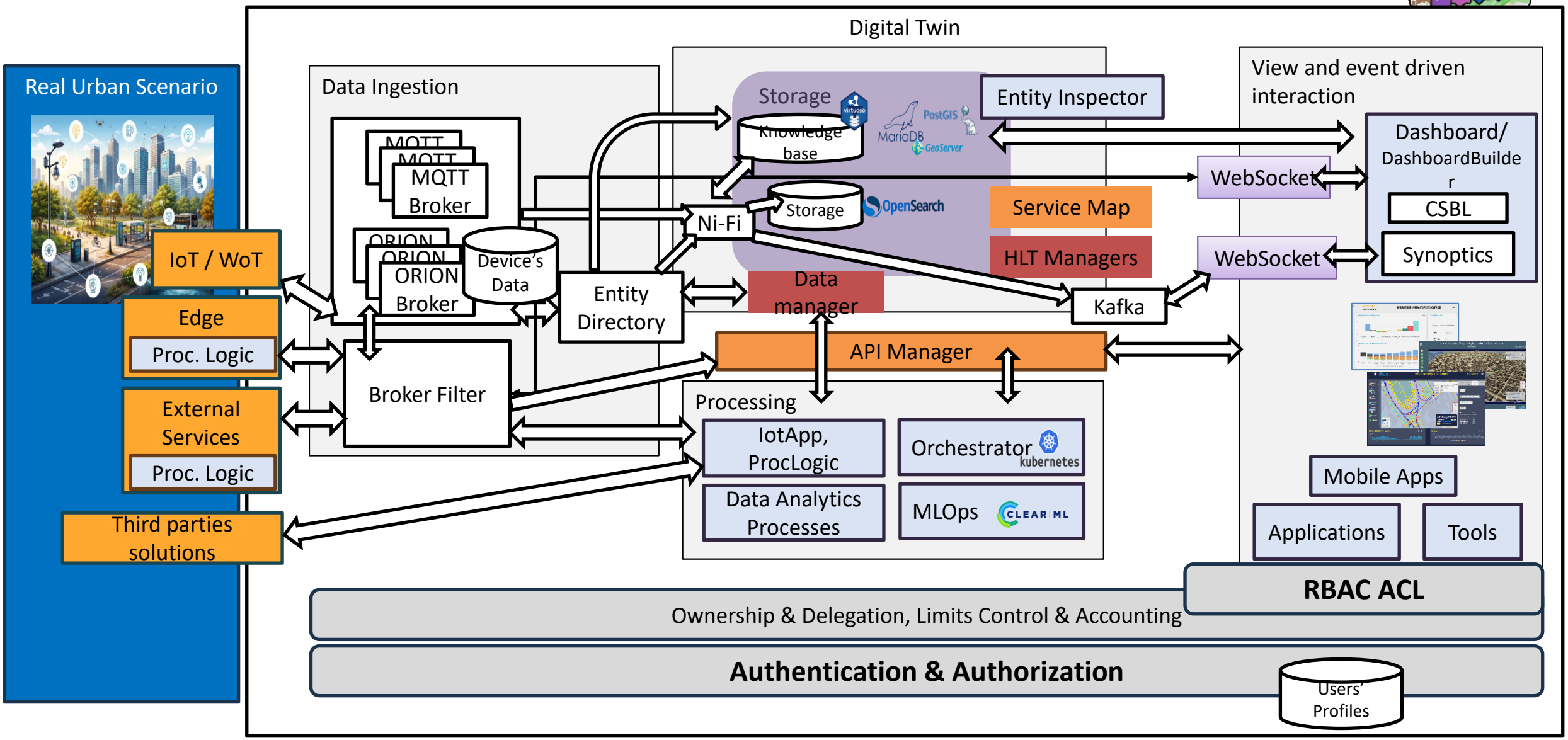
Cloud

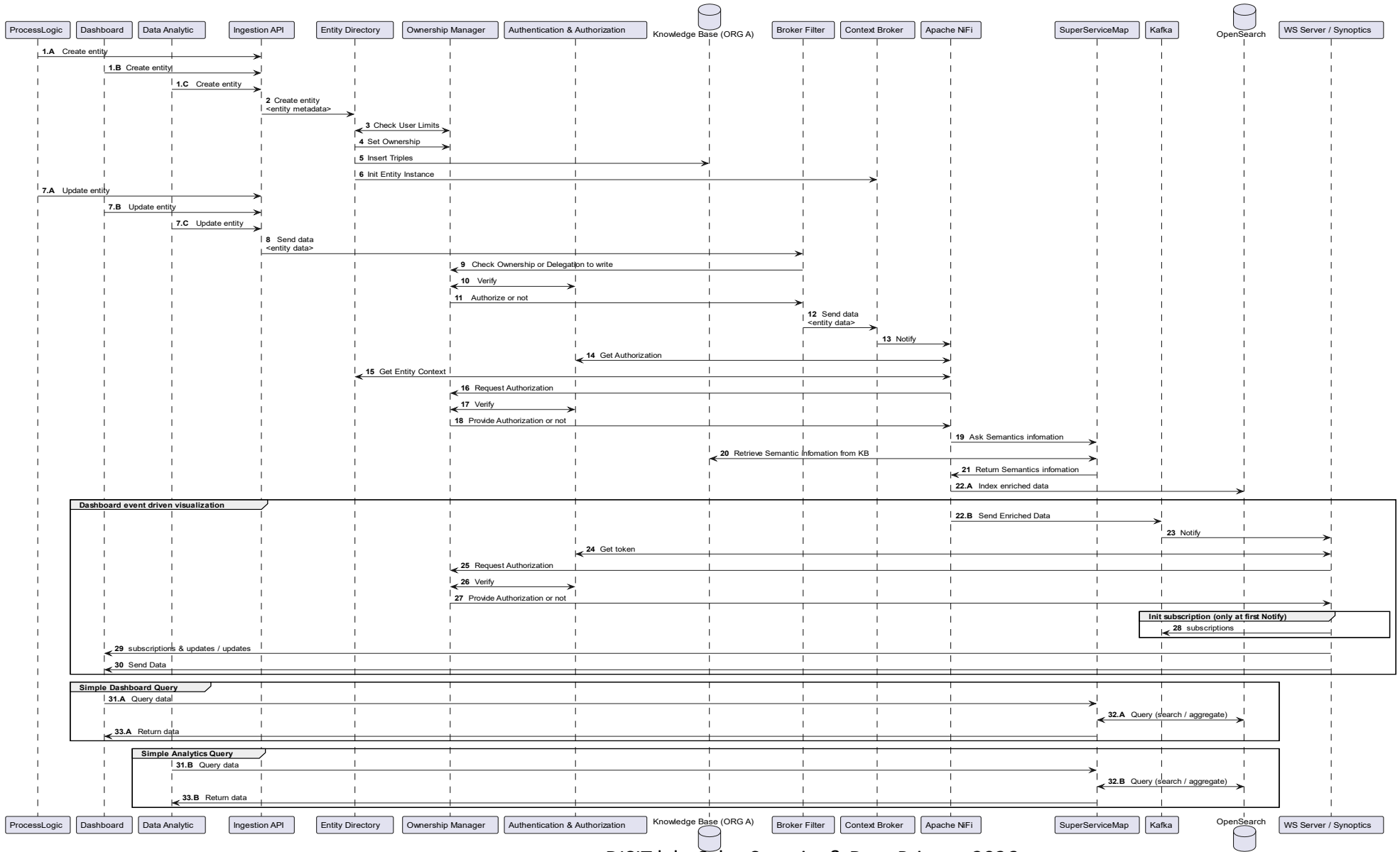
Internet

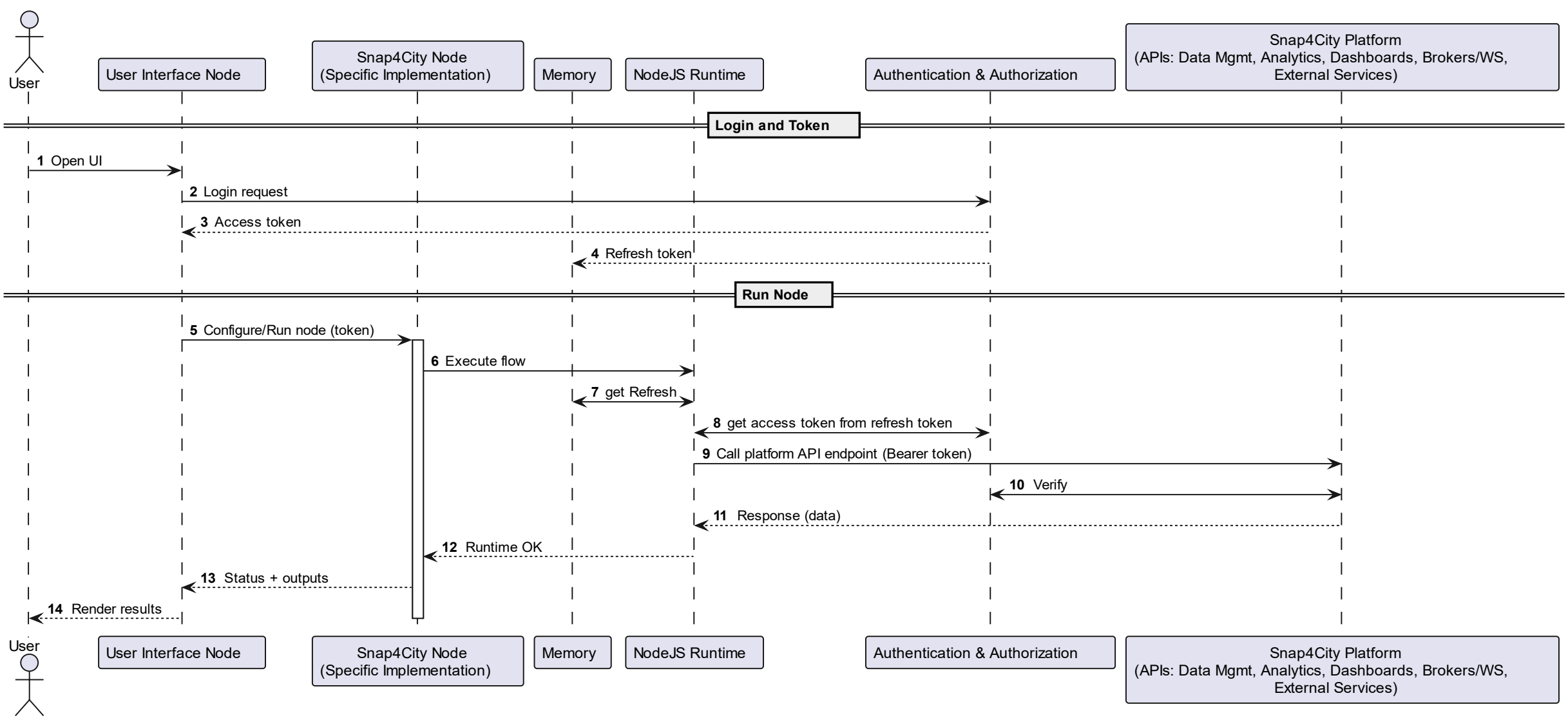
User interface On Browser

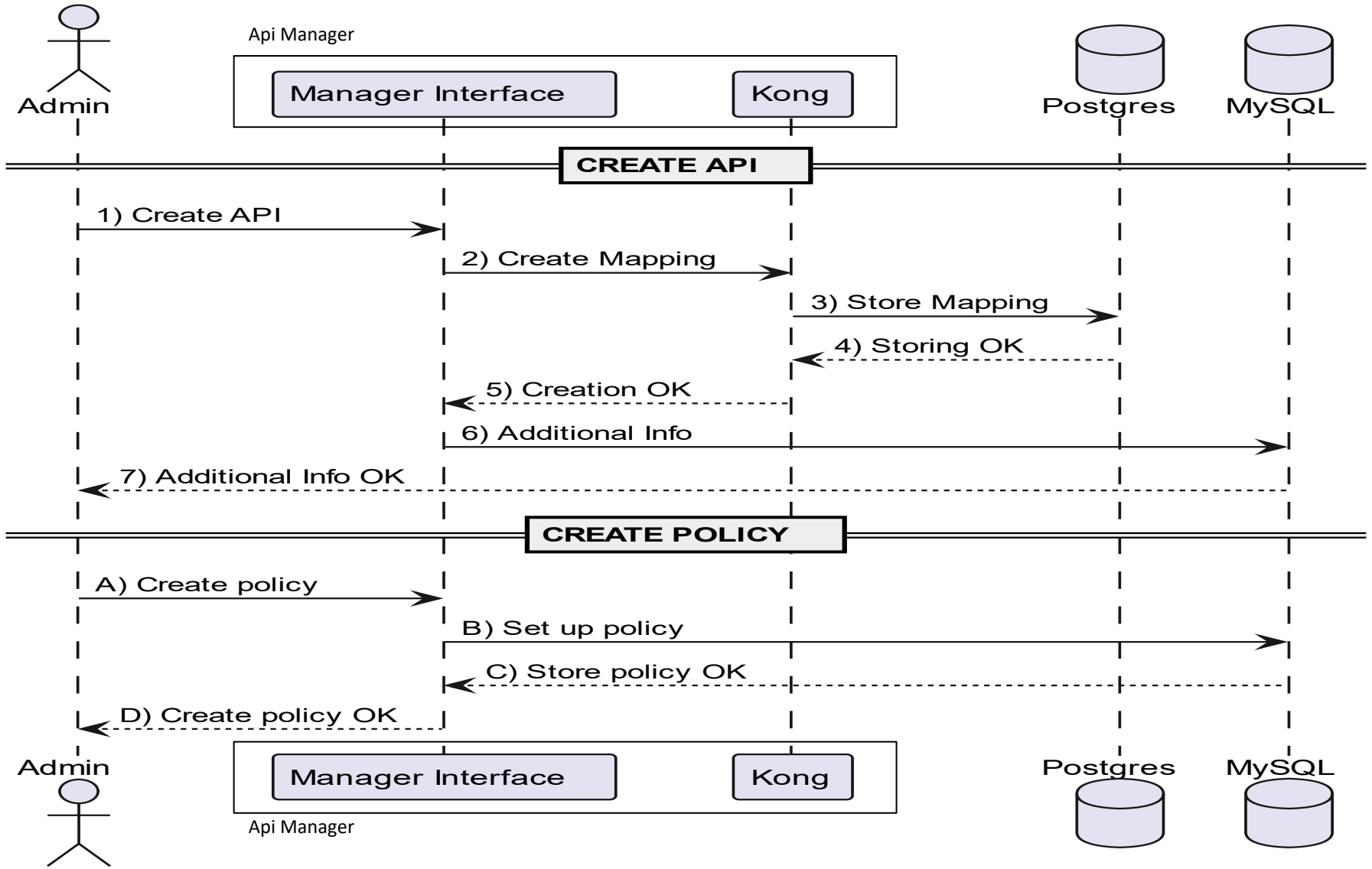
Intranet

Authentication and Authorization


Digital Twin
Real Urban Scenario
Data Ingestion
Storage
Knowledge base
Entity Inspector
View and event driven interaction
Dashboard/ DashboardBuilder
CSBL
Synoptics
WebSocket
WebSocket
MQTT Broker
ORION Broker
Device's Data
Ni-Fi
Storage
Service Map
HLT Managers
Data manager
Kafka
Entity Directory
API Manager
IoT / WoT
Edge
Proc. Logic
External Services
Proc. Logic
Third parties solutions
Broker Filter
Processing
IotApp, ProcLogic
Orchestrator
Data Analytics Processes
MLOps
Mobile Apps
Applications
Tools
RBAC ACL
Ownership & Delegation, Limits Control & Accounting
Authentication & Authorization
Users' Profiles


ProcessLogic
Dashboard
Data Analytic
Ingestion API
Entity Directory
Ownership Manager
Authentication & Authorization
Knowledge Base (ORG A)
Broker Filter
Context Broker
Apache NiFi
SuperServiceMap
Kafka
OpenSearch
WS Server / Synoptics
1.A Create entity
1.B Create entity
1.C Create entity
2 Create entity <entity metadata>
3 Check User Limits
4 Set Ownership
5 Insert Triples
6 Init Entity Instance
7.A Update entity
7.B Update entity
7.C Update entity
8 Send data <entity data>
9 Check Ownership or Delegation to write
10 Verify
11 Authorize or not
12 Send data <entity data>
13 Notify
14 Get Authorization
15 Get Entity Context
16 Request Authorization
17 Verify
18 Provide Authorization or not
19 Ask Semantics infomation
20 Retrieve Semantic infomation from KB
21 Return Semantics infomation
22.A Index enriched data
Dashboard event driven visualization
22.B Send Enriched Data
23 Notify
24 Get token
25 Request Authorization
26 Verify
27 Provide Authorization or not
Init subscription (only at first Notify)
28 subscriptions
29 subscriptions & updates / updates
30 Send Data
Simple Dashboard Query
31.A Query datal
32.A Query (search / aggregate)
33.A Return data
Simple Analytics Query
31.B Query data
32.B Query (search / aggregate)
33.B Return data

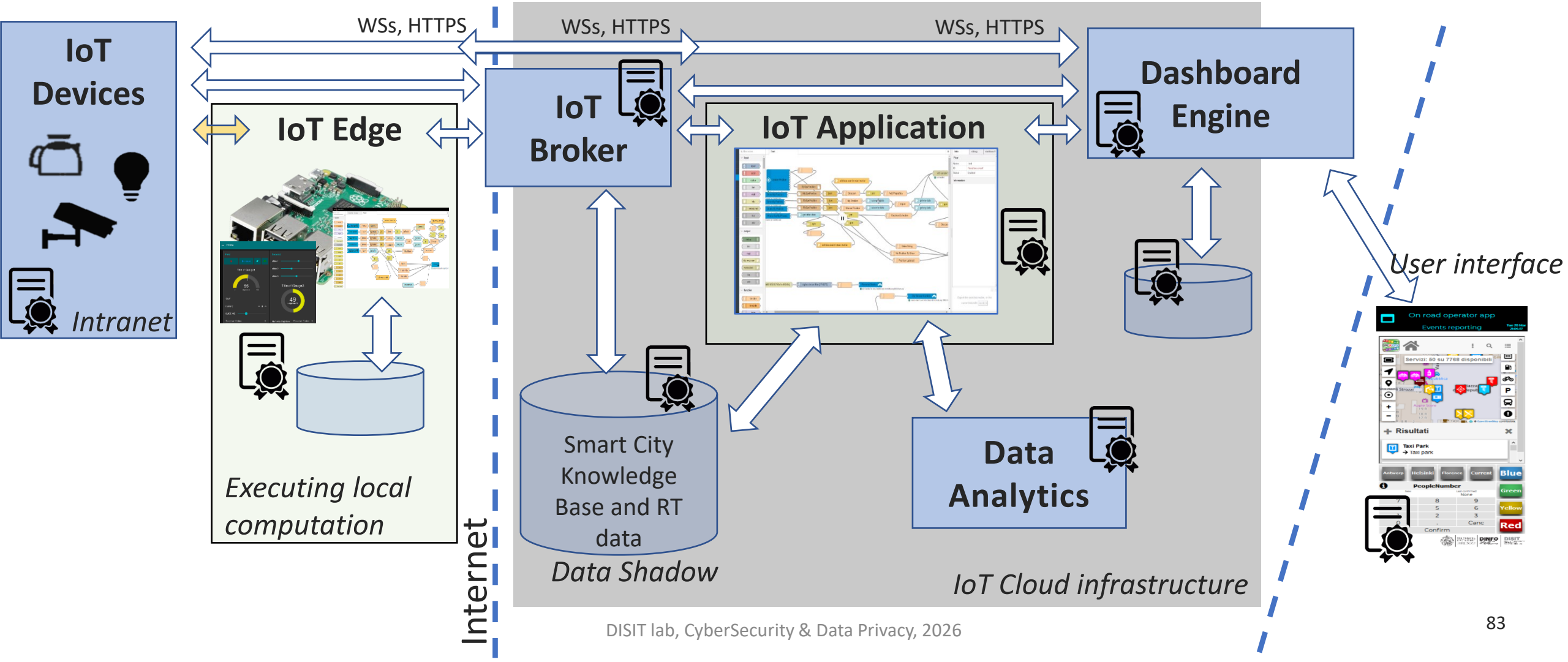

Snap4City Node - Sequence
User
User Interface Node
Snap4City Node (Specific Implementation)
Memory
NodeJS Runtime
Authentication & Authorization
Snap4City Platform (APIs: Data Mgmt, Analytics, Dashboards, Brokers/WS, External Services)
Login and Token
1 Open UI
2 Login request
3 Access token
4 Refresh token
Run Node
5 Configure/Run node (token)
6 Execute flow
7 get Refresh
8 get access token from refresh token
9 Call platform API endpoint (Bearer token)
10 Verify
11 Response (data)
12 Runtime OK
13 Status + outputs
14 Render results


Api Manager
Admin
Manager Interface
Kong
Postgres
MySQL
CREATE API
1) Create API
2) Create Mapping
3) Store Mapping
4) Storing OK
5) Creation OK
6) Additional Info
7) Additional Info OK
CREATE POLICY
A) Create policy
B) Set up policy
C) Store policy OK
D) Create policy OK
Admin
Manager Interface
Kong
Postgres
MySQL
Api Manager

Security IoT Requirements

- **Supporting security among**
  - IoT Brokers, IoT Discovery, IoT Applications, Dashboards, Storage, etc…
  - Authenticated Connections: H2M, M2M
  - Secure Communications: H2M, M2M
  - Authorization according to the role, group, organization of the user
- **Deliver Open Software on well known platforms, end-2-end secure IoT stack**
  - Arduino, ESP32, Raspberry Pi, Linux, Windows, Android, etc.
- **GDPR recommendation:**
  - Individuals must provide explicit consent to data collections
  - Right to be forgotten
  - Provide easy access to individuals data
  - Explanation about how automated decision are computed against personal data
  - Disclosure within 72 hours of data breach
  - Data protection by design

End-to-end security



Security and Privacy Management

- **From proprietary server:**
  - The device are registered and data collected by the proprietary servers: SigFOX, TheThingsNetwork, etc.
  - SigFOX: the server provides K1, K2 to read the data or subscribe
  - TTN: other kind of keys are used for the same purpose
- **From Open Solutions**
  - K1, K2 can be produced for IoT Device registration, subscription, etc.
  - K1, K2, plus SHA1/3 of Certificate to establish TLS connection
  - Certificate and credentials for the mutual authentications (for TLS connection)

- **Ownership and delegation**
  - Identification of user data type
- **User's group, organization. User's roles**
  - User's grants and rights to access data
- **Auditing, right to be forgotten**
  - Values, Devices, Brokers, IoT App, Dashboards, User Profiles, time series, etc.
  - Data breach intrusion detection
- **Assessment**
  - User and device limit constrains

On regards GDPR (1)

- Assessment and auditing
- CMS for personal data information, encryption
- Explicit Consent, Ownership and delegation

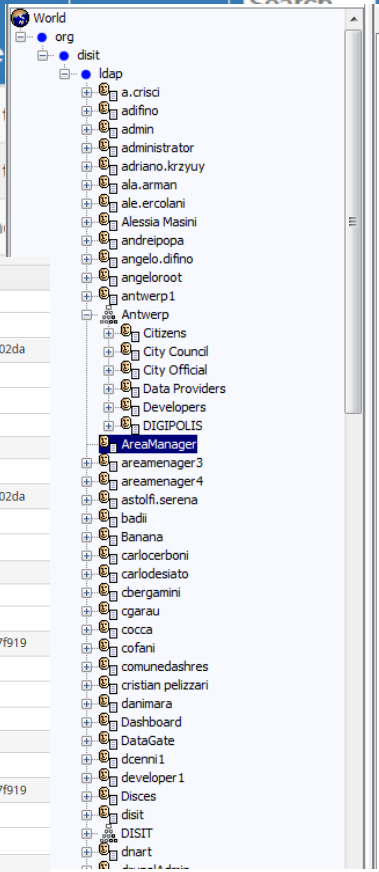
- Roles and organization (groups) to permits fine access control

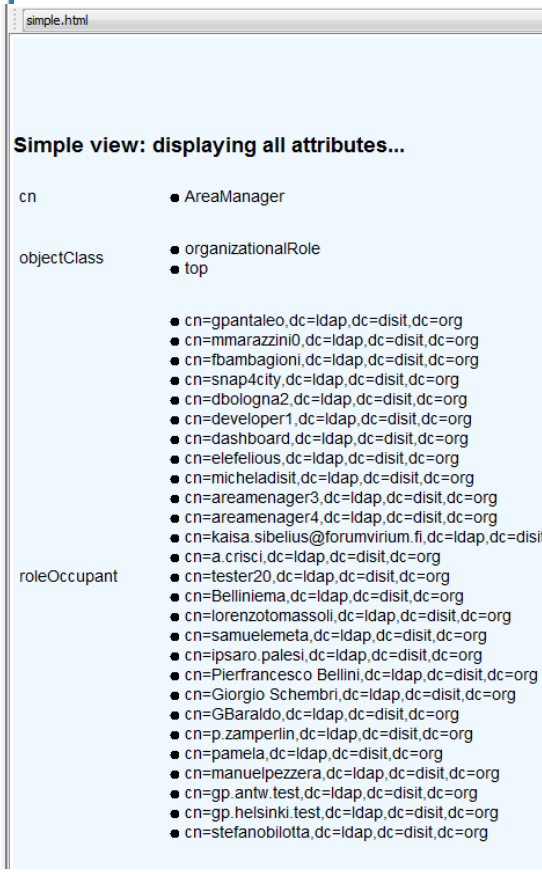
- Any collected data labelled with
  - Data of collection
  - Data of injection
  - Data of elapsing
  - Data of deleting
- +process to purge elapsed data

On regards GDPR (2)

Id	Date and Time (From... / To... / Search)	Username (Search...)	Variable name (Search...)	Motivation (Search...)	Access Type (Search)	Query	Error Message	ip_address
1789	2018-05-21 13:00:34				WRITE		The passed DATA has	
1788	2018-05-21 13:00:33	prova			READ		The passed DATA has	
1787	2018-05-21 13:00:33	adifino			READ	last=10&first=4	The passed request in	
1786	2018-05-21 13:00:33							
1785	2018-05-21 13:00:32	adifino						
1784	2018-05-21 12:59:04							
1783	2018-05-21 12:59:03							
1782	2018-05-21 12:59:03							
1781	2018-05-21 12:59:02	prova						

Time	Event Type	Details	
7/19/18 5:22:05 PM	LOGIN	Client	orionbrokerfilter
		User	f0ec0db7-60c8-4fb5-8820-bea6fd6602da
		IP Address	192.168.1.82
		Details	+
7/19/18 5:21:36 PM	LOGIN	Client	orionbrokerfilter
		User	f0ec0db7-60c8-4fb5-8820-bea6fd6602da
		IP Address	192.168.1.82
		Details	+
7/19/18 5:20:54 PM	CODE_TO_TOKEN	Client	drupal
		User	becfdf0a-dee4-4d9b-9510-638712d7f919
		IP Address	192.168.1.82
		Details	+
7/19/18 5:20:53 PM	LOGIN	Client	drupal
		User	becfdf0a-dee4-4d9b-9510-638712d7f919
		IP Address	192.168.1.82
		Details	+
7/19/18 5:20:53 PM	CODE_TO_TOKEN	Client	php-dashboard-builder
		User	becfdf0a-dee4-4d9b-9510-638712d7f919
		IP Address	192.168.1.82
		Details	+



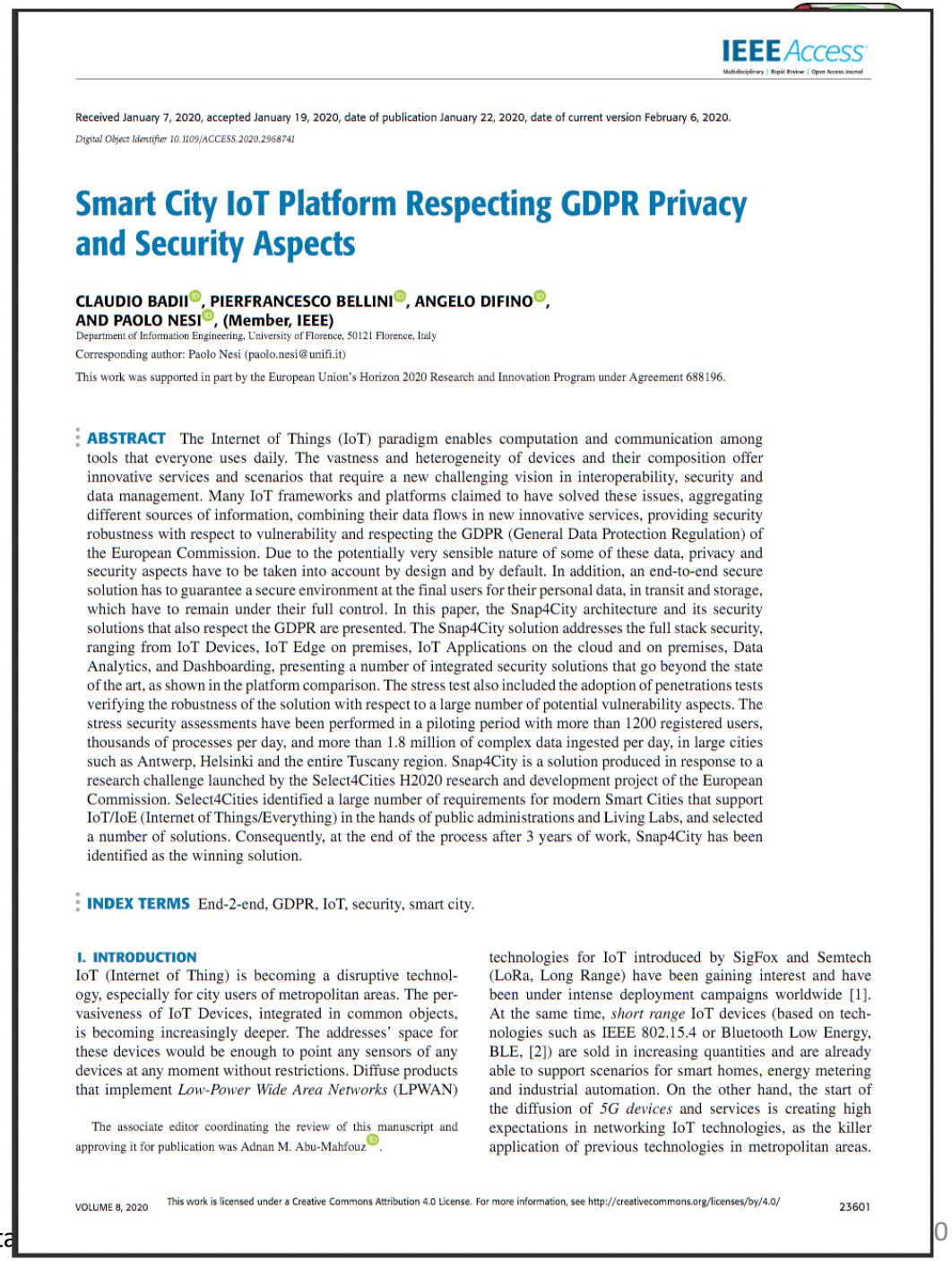


- Unified Login → via Keyclock + LDAP
- My Personal Data
- Data auditing
- Federated modules
- IoT Directory and certificates
- IoT Button
- IoT Dashboard

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE | DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

IEEE Access

- C. Badii, P. Bellini, A. Difino, P. Nesi, "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects", accepted for publication on IEEE Access, 2020. 10.1109/ACCESS.2020.2968741 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8966344



IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 7, 2020, accepted January 19, 2020, date of publication January 22, 2020, date of current version February 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968741

Smart City IoT Platform Respecting GDPR Privacy and Security Aspects

CLAUDIO BADII, PIERFRANCESCO BELLINI, ANGELO DIFINO, AND PAOLO NESI, (Member, IEEE)
Department of Information Engineering, University of Florence, 50121 Florence, Italy
Corresponding author: Paolo Nesi (paolo.nesi@unifi.it)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Program under Agreement 688196.

ABSTRACT The Internet of Things (IoT) paradigm enables computation and communication among tools that everyone uses daily. The vastness and heterogeneity of devices and their composition offer innovative services and scenarios that require a new challenging vision in interoperability, security and data management. Many IoT frameworks and platforms claimed to have solved these issues, aggregating different sources of information, combining their data flows in new innovative services, providing security robustness with respect to vulnerability and respecting the GDPR (General Data Protection Regulation) of the European Commission. Due to the potentially very sensible nature of some of these data, privacy and security aspects have to be taken into account by design and by default. In addition, an end-to-end secure solution has to guarantee a secure environment at the final users for their personal data, in transit and storage, which have to remain under their full control. In this paper, the Snap4City architecture and its security solutions that also respect the GDPR are presented. The Snap4City solution addresses the full stack security, ranging from IoT Devices, IoT Edge on premises, IoT Applications on the cloud and on premises, Data Analytics, and Dashboarding, presenting a number of integrated security solutions that go beyond the state of the art, as shown in the platform comparison. The stress test also included the adoption of penetrations tests verifying the robustness of the solution with respect to a large number of potential vulnerability aspects. The stress security assessments have been performed in a piloting period with more than 1200 registered users, thousands of processes per day, and more than 1.8 million of complex data ingested per day, in large cities such as Antwerp, Helsinki and the entire Tuscany region. Snap4City is a solution produced in response to a research challenge launched by the Select4Cities H2020 research and development project of the European Commission. Select4Cities identified a large number of requirements for modern Smart Cities that support IoT/IoE (Internet of Things/Everything) in the hands of public administrations and Living Labs, and selected a number of solutions. Consequently, at the end of the process after 3 years of work, Snap4City has been identified as the winning solution.

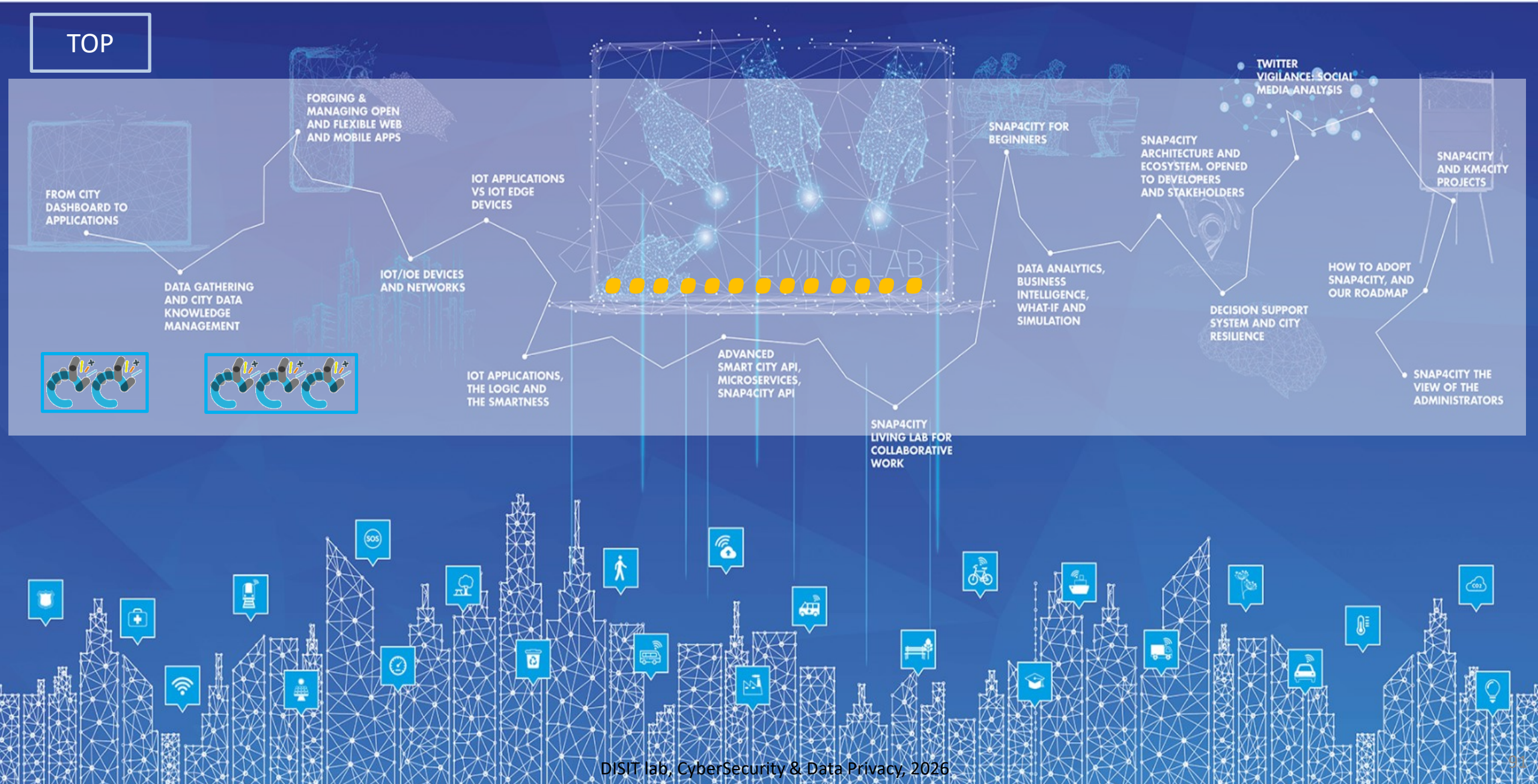
INDEX TERMS End-2-end, GDPR, IoT, security, smart city.

I. INTRODUCTION

IoT (Internet of Thing) is becoming a disruptive technology, especially for city users of metropolitan areas. The pervasiveness of IoT Devices, integrated in common objects, is becoming increasingly deeper. The addresses' space for these devices would be enough to point any sensors of any devices at any moment without restrictions. Diffuse products that implement *Low-Power Wide Area Networks* (LPWAN) technologies for IoT introduced by SigFox and Semtech (LoRa, Long Range) have been gaining interest and have been under intense deployment campaigns worldwide [1]. At the same time, *short range* IoT devices (based on technologies such as IEEE 802.15.4 or Bluetooth Low Energy, BLE, [2]) are sold in increasing quantities and are already able to support scenarios for smart homes, energy metering and industrial automation. On the other hand, the start of the diffusion of *5G devices* and services is creating high expectations in networking IoT technologies, as the killer application of previous technologies in metropolitan areas.

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

SCALABLE SMART ANALYTIC APPLICATION BUILDER FOR SENTIENT CITIES



Any Devices in the IoT ecosystem

- Microcontroller ESP8266, Arduino
- Raspberry boards
- AirQino, Libelium
- Android devices
- PC
- On cloud virtualization

Security Strength	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
≤ 80	2TDEA[21]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

- As much as user friendly VS as much as secure channel
- On embedded devices, cypher suite not always available. Use: TLS_RSA_WITH_AES_256_CBC_SHA
- Impact of certificate size on available heap: NIST Special Publication suggestions: Use 2048, but WARNING close future!

Any Devices in the IoT ecosystem (2)

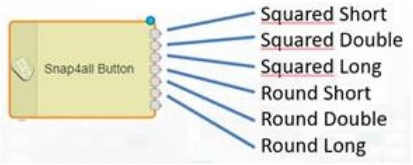
https://www.snap4city.org/drupal/node/276

Home / Snap4All IOT Button: based on ESP32, NGSI compliant secure connection

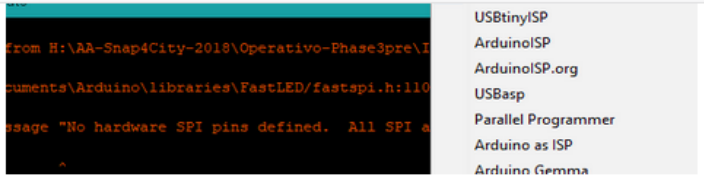
Snap4All IOT Button: based on ESP32, NGSI compl

Snap4All IOT Button Version 3 is based on ESP32: it is an NGSI devices, which can be customize as well. It is a secure device with Mutual authentication and secure encrypted connection.

Once you have registered and configured can connect them by using MicroService Node/block in IOT Application by using:

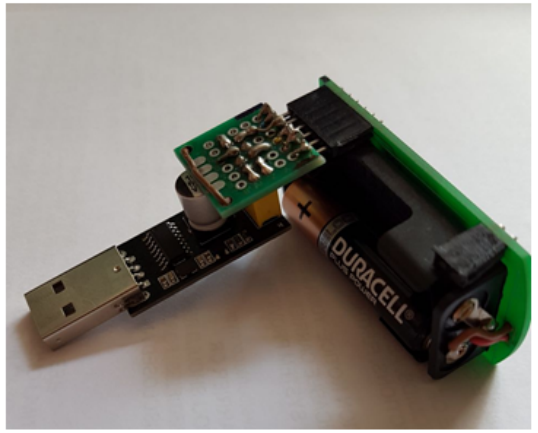


https://www.snap4city.org/drupal/node/277

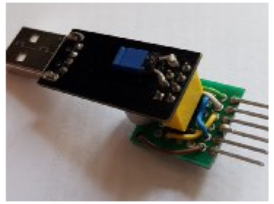


To connect the device to a USB you will need a serial adapter for ESP01 or a USB to Serial adapter.

Pins are connected from left to right: GND, CTS, 3.3V, TX, RX, DTR.



In case you are using an ESP01 programming adapter make sure to connect pin as in photo.



The source code of version 2.0 is: https://www.snap4city.org/download/video/IOTbuttonSmdV2-005a.rar

Any Devices in the IoT ecosystem (3)

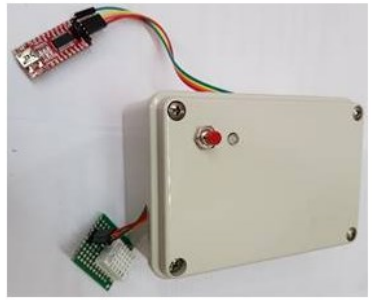
https://www.snap4city.org/drupal/node/329

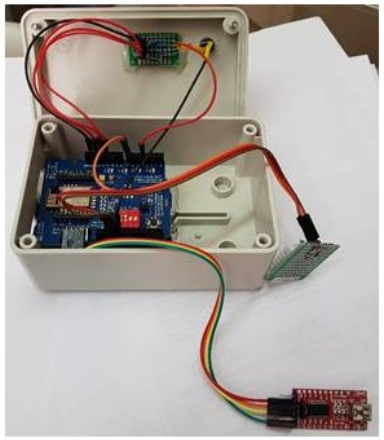
Home / Snap4City: Arduino & ESP8266 IOT Device NGSI

Snap4City: Arduino & ESP8266 IOT Device NGSI

Arduino & ESP8266 – user Guide and developers guide:

It is a secure device with Mutual authentication and secure encrypted connection.





https://www.snap4city.org/drupal/node/518

Home / Solution: using PAX Counters, monitoring museum and events

Solution: using PAX Counters, monit

In this example, the interaction with IOT Devices counting people by using Wi-Fi and Bluetooth sniffing in its vicinity accordi
In Figure 12, a mobile PAXCounter based on ESP32 sending messages to Snap4City via LoraWAN. see https://www.snap4city
Other simpler versions can be located on fixed places, and may also use WiFi to send the obtained measures including additio
22 devices have been installed. The measured values are sent to LoraWan operator The Things Network, which does not provi

Figure 12: A mobile PAX counter based on ESP32.

Museum Case

Considering the example of the museum, one could be interested in monitoring the flow of entering and exiting visitors, hav
store, for example into MyKPI, MyPOI storage via MicroServices. This approach of Snap4City allows at the IOT Developers
an IOT App has been created for PaxCounter to receive in Event Driven mode the new coming from The Things Networ
Dashboard Wizard automatically sees the data entity on the MyKPI and allowed us to automatically create Widgets showing t
and derived data. All the derived values of the initial real time data can be computed in real time, saved on personal storage a
the difference between the people entering the museum and those leaving to obtain the number of people inside the museum in

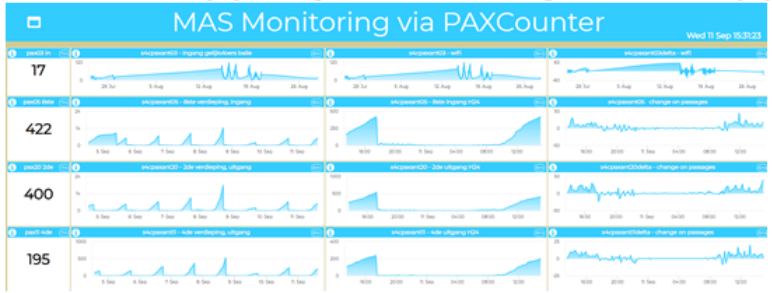
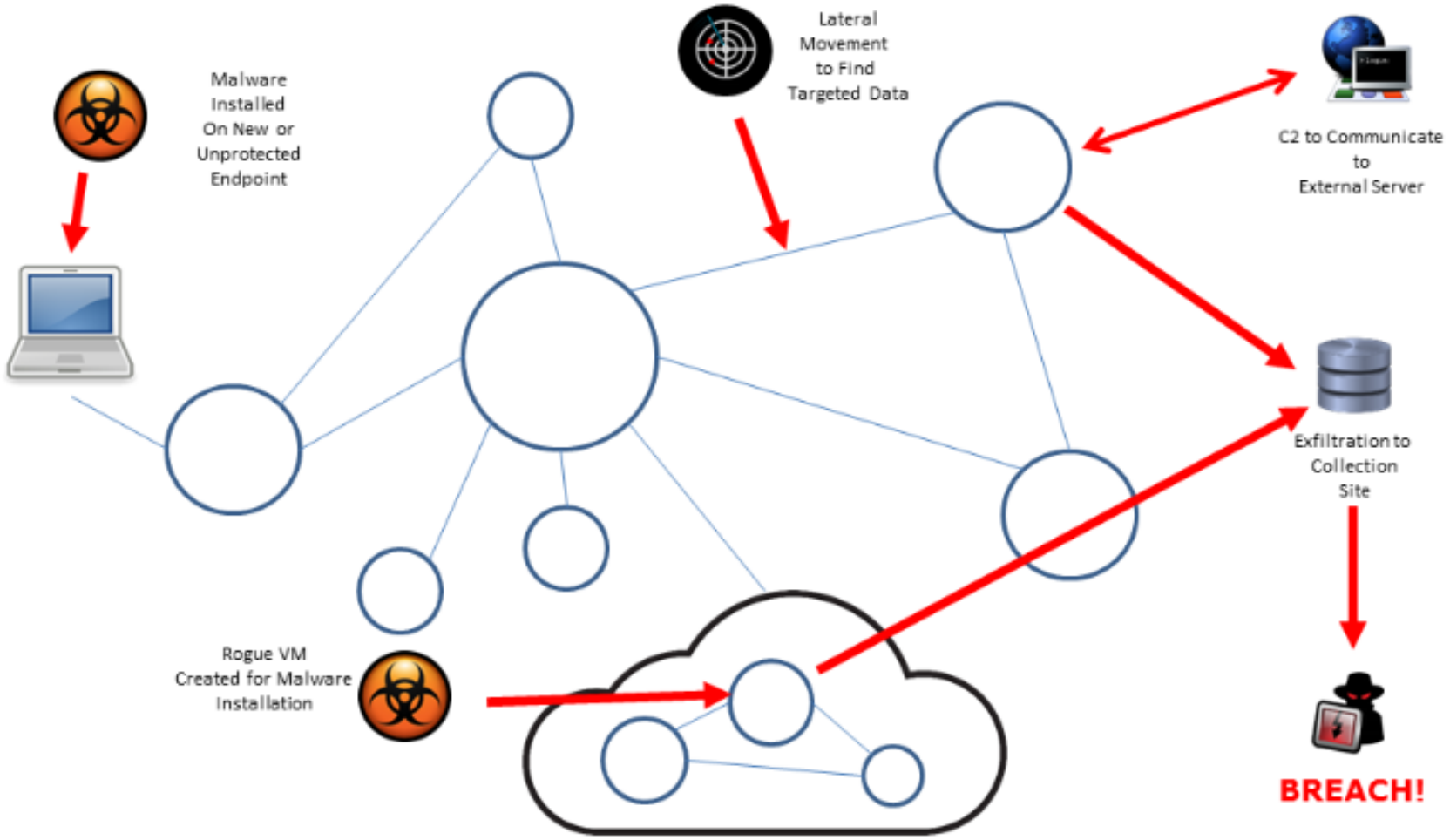


Figure 13: Monitoring MAS Museum people flows.

More on breach (1)

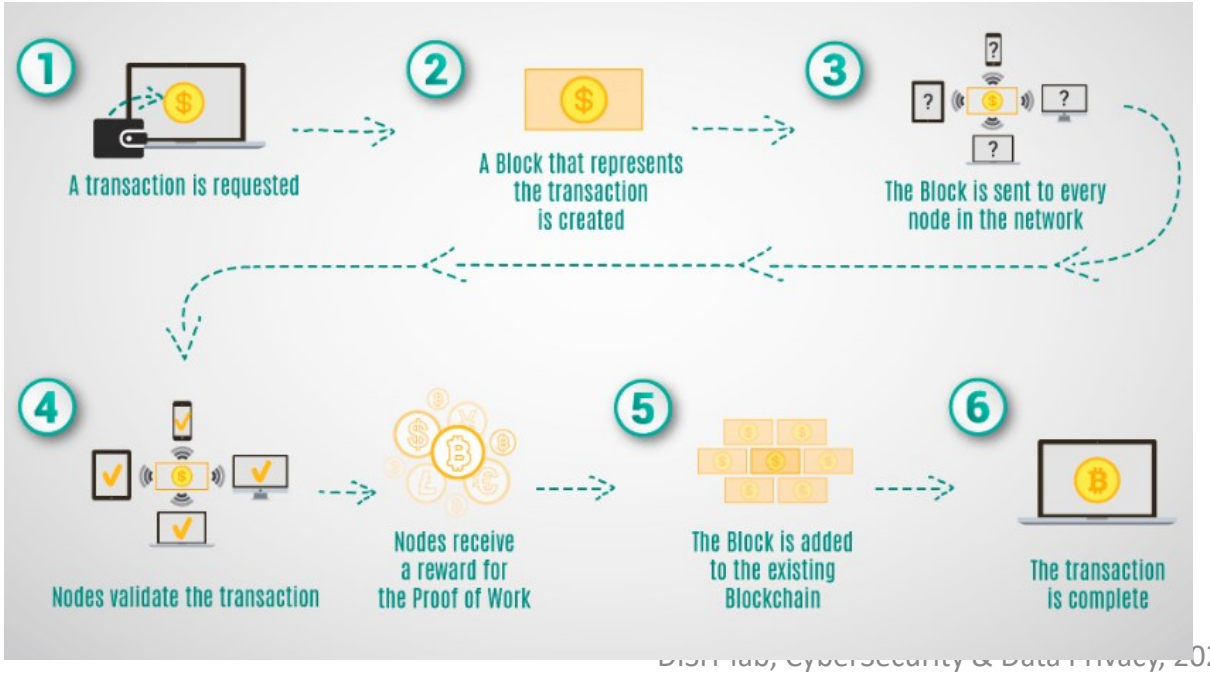
- Dangerous examples of network vulnerabilities include
  - Improperly configured routing causing leak paths in between protected network enclaves or to the Internet itself
  - Temporary or test configurations of firewalls that don't operate as designed or don't get reversed-out properly
  - Password password password
  - Password password password
  - Network analysis in real-time → dashboards, acceptable level of traffic, trigger of alarm → Notification (SMS, Mail, Calls leveraged depending on the sensitivity)
- Two authenticate factors → FIDO2 with hardware support

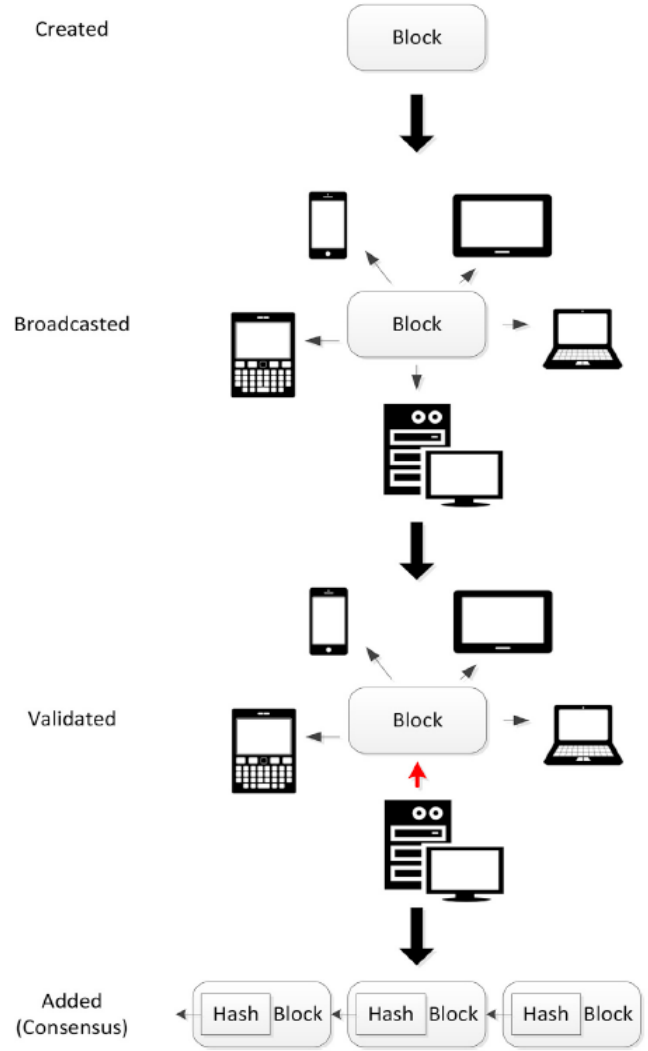
More on breach (2)



Blockchain solution (1)

- One node validates the block (called mining in bitcoin) and broadcasts it back to the network.
- The nodes add the block to their chain of blocks if the blocks is verified and the block correctly references the previous block





Blockchain solution (2)

- Central hub that maintains references of member repository where the datasets are actually stored and distributed
- Delete from Block chain?
- Rule enforcement (everything distributed)?
- … work in progress