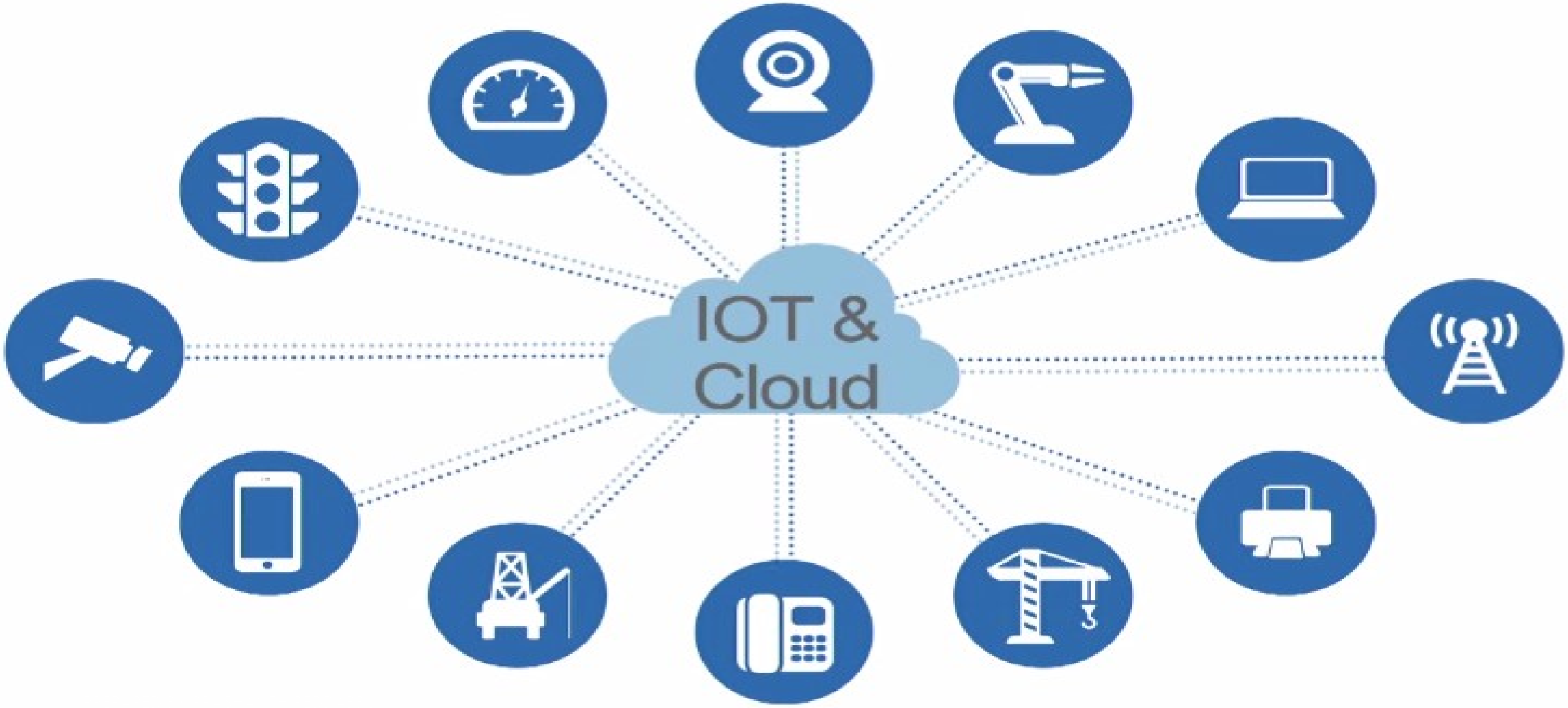
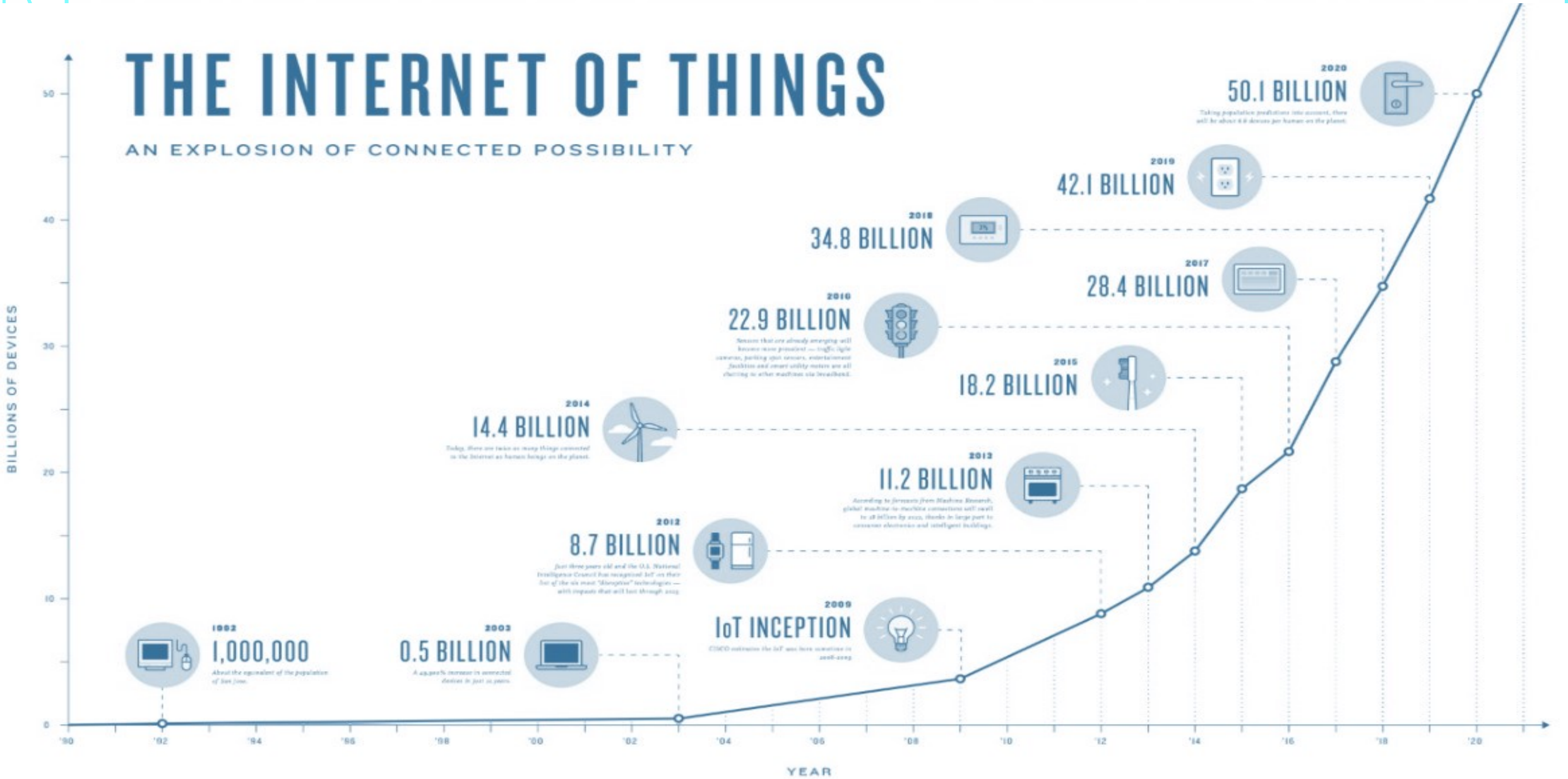
Fog & Edge Computing

IOT & CLOUD COMPUTING?




THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
YEAR
1992
1,000,000
About the equivalent of the population of San Jose.
2003
0.5 BILLION
A 49,900% increase in connected devices in just 10 years.
2009
IoT INCEPTION
2010
22.9 BILLION
2012
8.7 BILLION
2012
11.2 BILLION
2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.
2015
18.2 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION
Taking population predictions into account, there will be about 6.6 devices per human on the planet.

WHY NOT CLOUD?

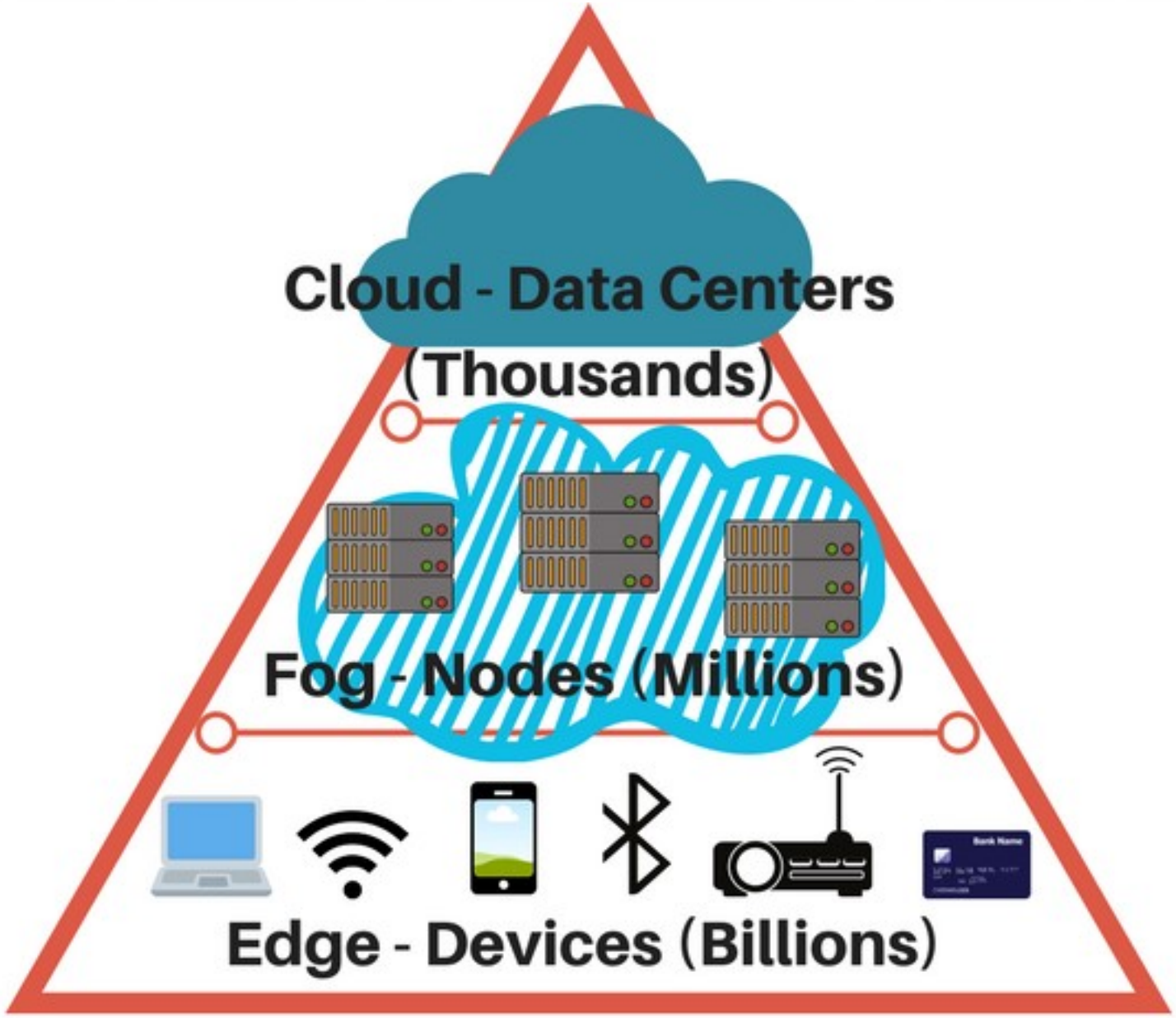
- As the volume of data created by connected devices continues to grow, it has become cumbersome and unrealistic for each device to send its raw data to a central location for processing.
- This model of sending everything to the cloud has caused bandwidth challenges, latency issues, and delays in processing.
- Edge Computing and Fog Computing are trends that represent the scale coming back into balance after the mass migration of data and processes to the cloud or centralized enterprise data centers.

WHY NOT CLOUD?

- In response to these growing challenges, organizations are deploying smaller processing data centers closer to where the data is created.
- This intermediate processing is often referred to as **Fog Computing**.
- Think of these small localized data centers as gatekeepers to the cloud or a clearinghouse for sorting millions of bits of data to include only the meaningful analysis.

FOG COMPUTING AND EDGE COMPUTING DEFINED

- Some use the terms Fog Computing and Edge Computing interchangeably when in fact, they are not the same thing. As devices get “smarter” more computing is taking place at the device level rather than in the Fog.
- Technically speaking, Edge computing is the functionality at the device level while Fog Computing is the intermediate processing that happens in servers outside the cloud.
- As a basic example, consider a device with 100 different sensors programmed to take readings every 10 minutes. Edge computing is where the device combines the readings from the 100 sensors to a single data point that gets sent into the Fog every 10 minutes. Fog Computing allows those data points to be collected closer to the source and compiled into a single daily report that is sent to the central data center once.


Cloud - Data Centers
(Thousands)
Fog - Nodes (Millions)
Edge - Devices (Billions)

FOG COMPUTING

Fog refers to the network connections between edge devices and the cloud.

NEED FOR FOG COMPUTING

- Why can’t do all in cloud?
  - Cloud computing frees the enterprise and the end user from many details.
  - This bliss becomes a problem for latency-sensitive applications.

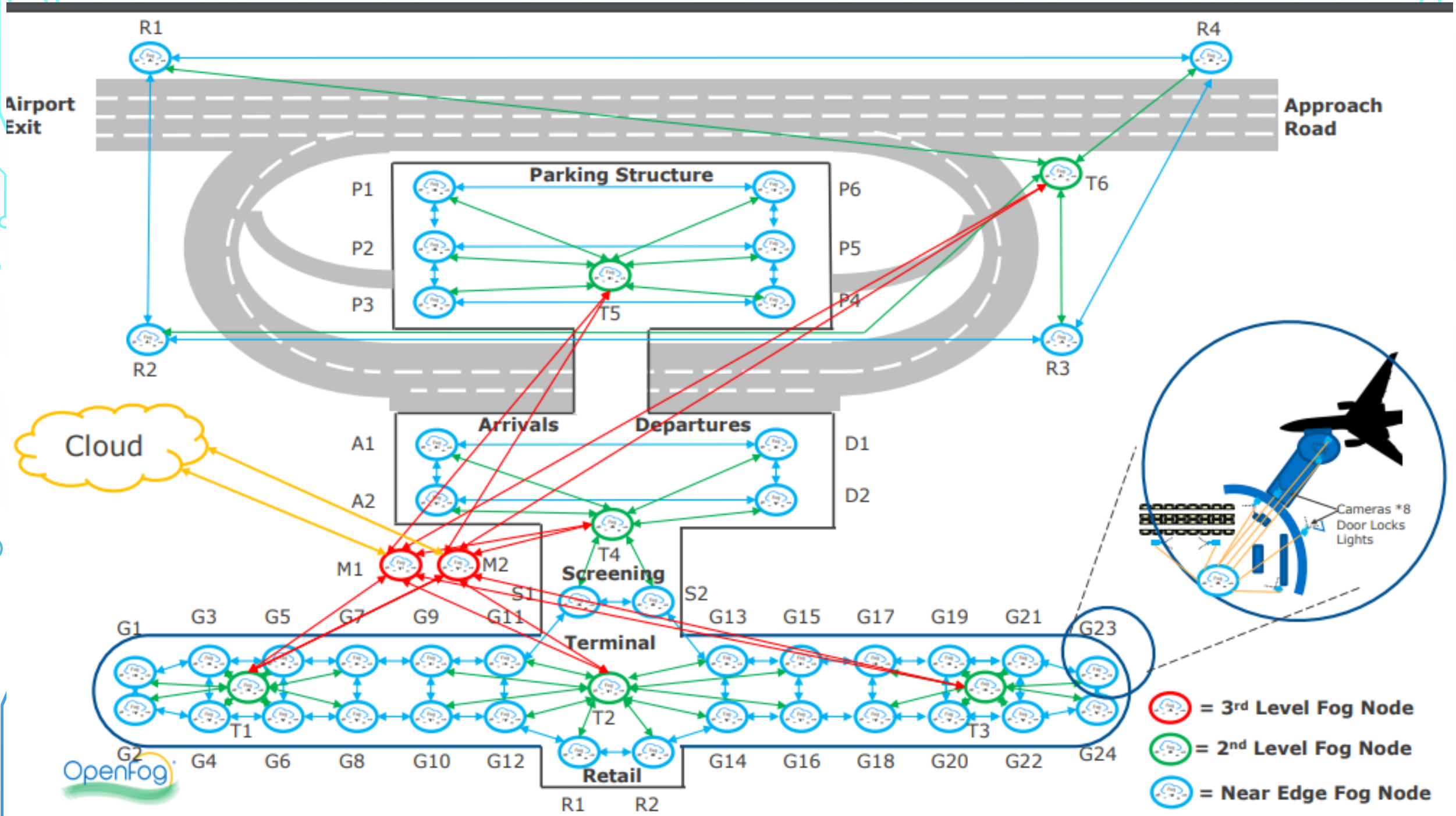
- Why can’t do all in end systems?
  - Physical constraints: Energy, space, etc.,

FOG DEPLOYMENT

- Fog includes edge computing, but fog would also incorporate the network needed to get processed data to its final destination.
- Backers of the OpenFog Consortium, an organization headed by Cisco, Intel, Microsoft, Dell EMC and academic institutions like Princeton and Purdue universities, are developing reference architectures for fog and edge computing deployments.

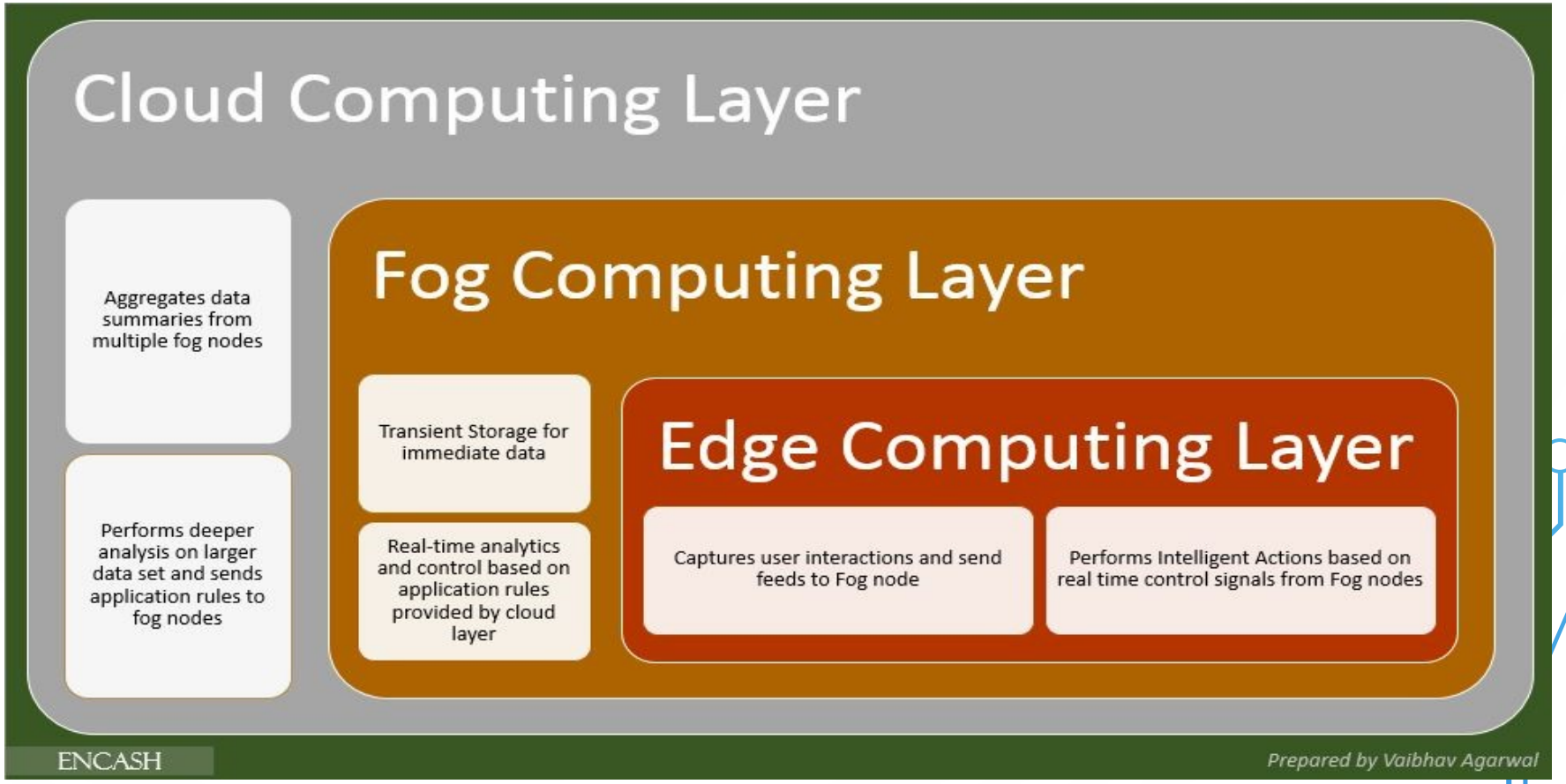
The pillars describe requirements to every part of the fog supply chain: component manufacturers, system vendors, software providers, application developers.

Security	Scalability	Open	Autonomy	RAS	Agility	Hierarchy	Programmability
• Trust • Attestation • Privacy	• Localized command, control & processing • Orchestration & Analytics • Avoidance of network taxes	• Resource visibility & control • White box decision making • Interop & Data normalization	• Flexible • Cognition & agility • Value of data	• Reliability • Availability • Serviceability	• Tactical & strategic decision making • Data to wisdom	• Fully cloud enabled • Computational & System • Autonomy at all levels	• Programmable SW/HW • Virtualization & multi-tenant • App Fluidity


R1
R4
Airport Exit
Approach Road
Parking Structure
P1
P2
P3
P4
P5
P6
T5
T6
R2
R3
Cloud
Arrivals
Departures
A1
A2
D1
D2
T4
M1
M2
Screening
S1
S2
Terminal
G1
G2
G3
G4
G5
G6
G7
G8
G9
G10
G11
G12
G13
G14
G15
G16
G17
G18
G19
G20
G21
G22
G23
G24
T1
T2
T3
Retail
R1
R2
Cameras *8
Door Locks
Lights
= 3rd Level Fog Node
= 2nd Level Fog Node
= Near Edge Fog Node
OpenFog

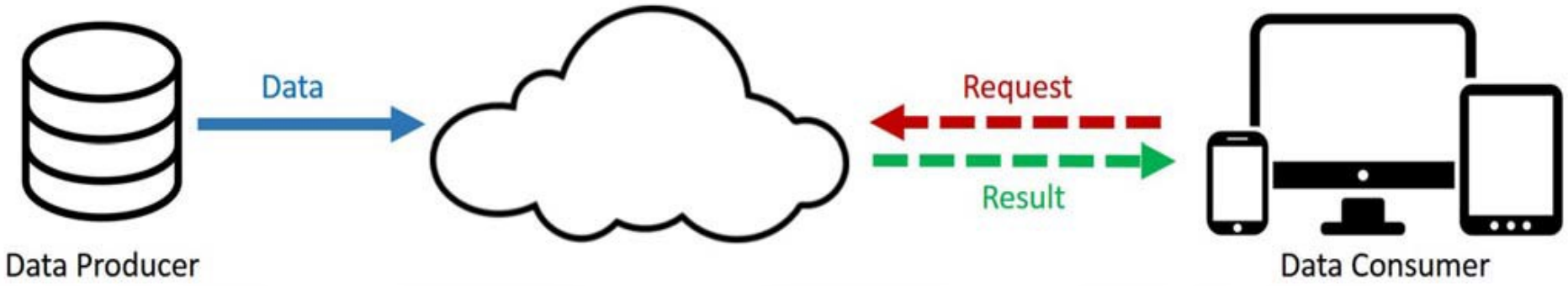
EDGE COMPUTING

- Edge refers more specifically to the computational processes being done close to the edge devices.



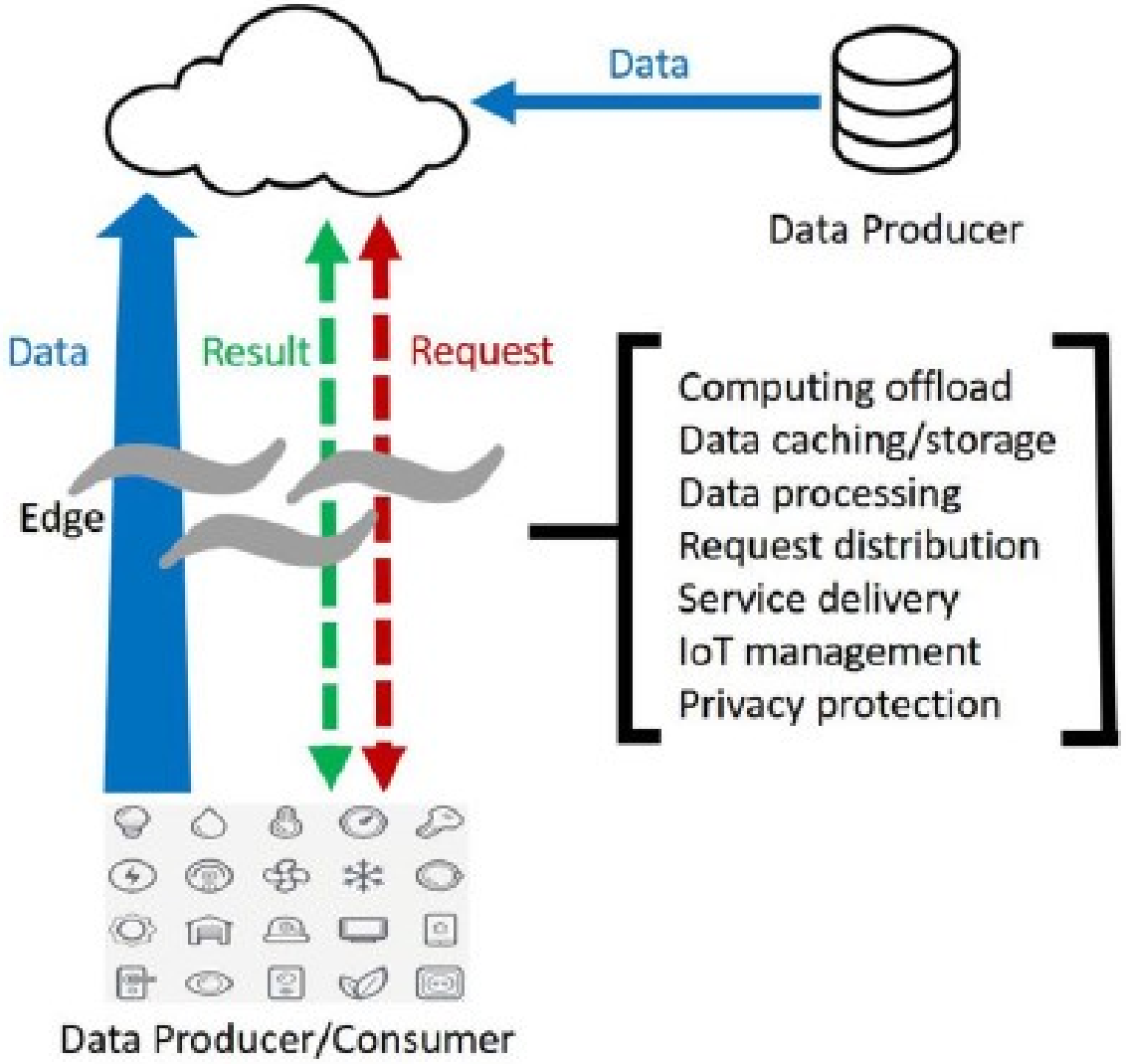
Why do we need edge computing

- Push from cloud services
- Pull from IoT
- Change From Data Consumer to Producer



What is edge computing

- We define “edge” as any computing and network resources along the path between data sources and cloud data centers.
- Is Edge computing interchangeable with fog computing?



EDGE COMPUTING TERMS AND DEFINITIONS

- **Edge devices**: These can be any device that produces data. These could be sensors, industrial machines or other devices that produce or collect data.
- **Edge**: What the edge is depends on the use case. In a telecommunications field, perhaps the edge is a cell phone or maybe it's a cell tower. In an automotive scenario, the edge of the network could be a car. In manufacturing, it could be a machine on a shop floor; in enterprise IT, the edge could be a laptop.
- **Edge gateway**: A gateway is the buffer between where edge computing processing is done and the broader fog network. The gateway is the window into the larger environment beyond the edge of the network.

EDGE COMPUTING TERMS AND DEFINITIONS

- **Fat client**: Software that can do some data processing in edge devices. This is opposed to a thin client, which would merely transfer data.
- **Edge computing equipment**: Edge computing uses a range of existing and new equipment. Many devices, sensors and machines can be outfitted to work in an edge computing environment by simply making them Internet-accessible. Cisco and other hardware vendors have a line of ruggedized network equipment that has hardened exteriors meant to be used in field environments. A range of compute servers, converged systems and even storage-based hardware systems like Amazon Web Service's Snowball can be used in edge computing deployments.
- **Mobile edge computing**: This refers to the buildout of edge computing systems in telecommunications systems, particularly 5G scenarios.

Case study

1. Cloud offloading
2. Video analytics
3. Smart home
4. Smart city
5. Collaborative edge

CLOUD OFFLOADING

- In the cloud computing paradigm, most of the computations happen in the cloud, which means data and requests are processed in the centralized cloud.
- However, such a computing paradigm may suffer longer latency (e.g., long tail latency), which weakens the user experience.
- In edge computing, the edge has certain computation resources, and this provides a chance to offload part of the workload from cloud.
- In the traditional content delivery network, only the data is cached at the edge servers. This is based on the fact that the content provider provides the data on the Internet, which is true for the past decades.
- In the IoT, the data is produced and consumed at the edge. Thus, in the edge computing paradigm, not only data but also operations applied on the data should be cached at the edge.

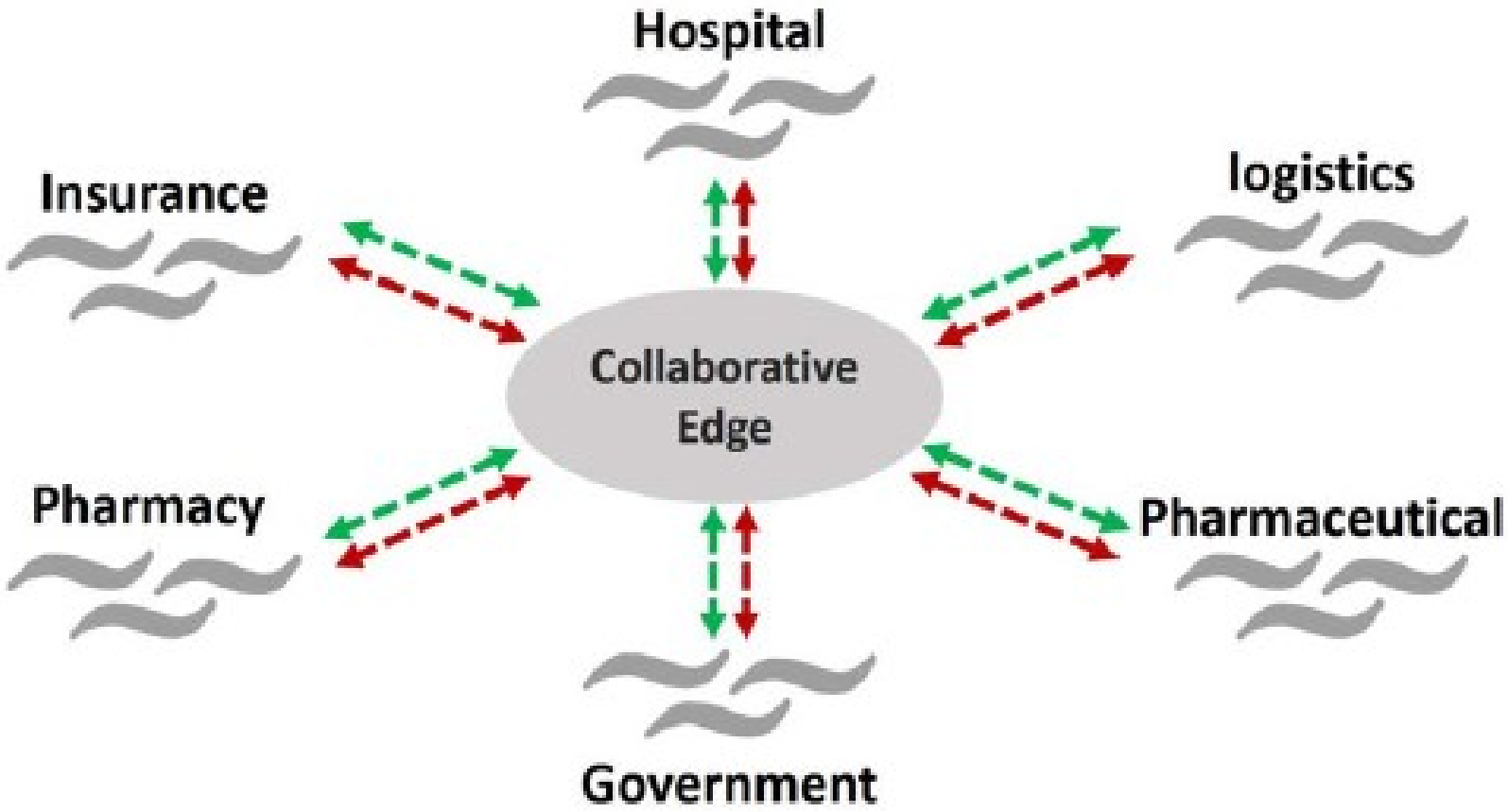
VIDEO ANALYTICS (FINDING A LOST CHILD)

- The widespread of mobilephones and network cameras make video analytics an emerging technology.
- Cloud computing is no longer suitable for applications that requires video analytics due to the long data transmission latency and privacy concerns.
- Nowadays, different kinds of cameras are widely deployed in the urban area and in each vehicle. When a child is missing, it is very possible that this child can be captured by a camera.
- However, the data from the camera will usually not be uploaded to the cloud because of privacy issues or traffic cost, which makes it extremely difficult to leverage the wide area camera data. Even if the data is accessible on the cloud, uploading and searching a huge quantity of data could take a long time, which is not tolerable for searching a missing child.
- With the edge computing paradigm, the request of searching a child can be generated from the cloud and pushed to all the things in a target area. Each thing, for example, a smart phone, can perform the request and search its local camera data and only report the result back to the cloud.

SMART HOME

- IoT would benefit the home environment a lot. Some products have been developed and are available on the market such as smart light, smart TV, and robot vacuum.
- However, just adding a Wi-Fi module to the current electrical device and connecting it to the cloud is not enough for a smart home.
- In a smart home environment, besides the connected device, cheap wireless sensors and controllers should be deployed to room, pipe, and even floor and wall. These things would report an impressive amount of data and for the consideration of data transportation pressure and privacy protection, this data should be mostly consumed in the home.
- This feature makes the cloud computing paradigm unsuitable for a smart home.
- Nevertheless, edge computing is considered perfect for building a smart home: with an edge gateway running a specialized edge operating system (edgeOS) in the home, the things can be connected and managed easily in the home, the data can be processed locally to release the burdens for Internet bandwidth, and the service can also be deployed on the edgeOS for better management and delivery.

COLLABORATIVE EDGE



EDGE COMPUTING SECURITY

- There are two sides of the edge computing security coin. Some argue that security is theoretically better in an edge computing environment because data is not traveling over a network, and it's staying closer to where it was created. The less data in a corporate data center or cloud environment, the less data there is to be vulnerable if one of those environments is comprised.
- The flip side of that is some believe edge computing is inherently less secure because the edge devices themselves can be more vulnerable. In designing any edge or fog computing deployment, therefore, security must be a paramount. Data encryption, access control and use of virtual private network tunneling are important elements in protecting edge computing systems.

SUMMARY