IoT System Architectures and Standards

COCSC20

Syllabus

This module will cover the following aspects

- Key considerations for IoT architectures
- Cloud, fog, and edge paradigms
- The role of gateways in IoT
- IoT internetworking approaches
- Standards that enable practical IoT deployment and interoperability

The IoT architectural landscape

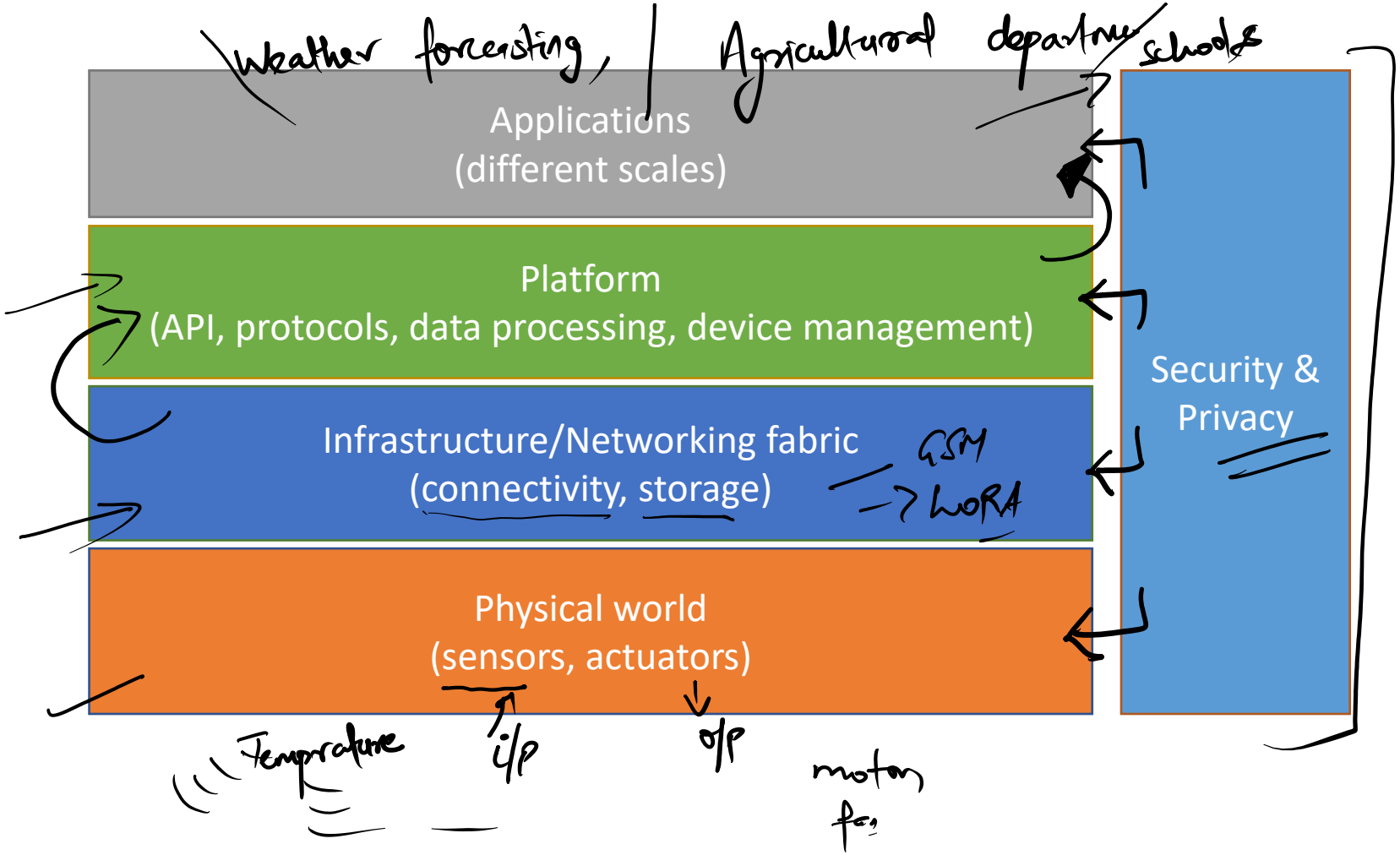
- Thousands of new applications exist, spanning countless domains (verticals).
- Each application has its unique requirements → combining these leads to systems that are complex, difficult to manage, and often proprietary.
- Defining a unified architecture is challenging and interoperability problematic, if there are too many standards to choose from.
- Efforts by multiple entities to define common frameworks, including international standardization bodies, multi-national collaborative research projects, industry consortiums, and large commercial actors.
- Device/protocol documentation is scattered and often difficult to navigate.
- We will focus on the key principles different architectural patterns share and examine some examples.

Key considerations for IoT architectures

- What application domains should be covered?
- Where to place the “intelligence”?
- What networking structure should be employed?
- How to modularize systems, so as to manage complexity and enable programmability?
- What are the cost and scalability implications?

A layered view to IoT architecture

At a high level, stakeholders may converge to a shared vision



This approach enables to break up complexity, share resources more easily, and promote interoperability

Advantages of the layer approach

- Allows IoT device manufacturers to focus strictly on improving their performance, power consumption, etc. – expose only well-defined interfaces to software platforms.
- Easier to share and partition strictly the network and computing resources (slicing); reducing the burden on service providers to build and manage networks – Infrastructure/Network as a Service (IaaS/NaaS) (cloud)
- Enables software/app developers to build applications without having to understand the specifics of a device – Platform as a Service (PaaS)

Security challenges

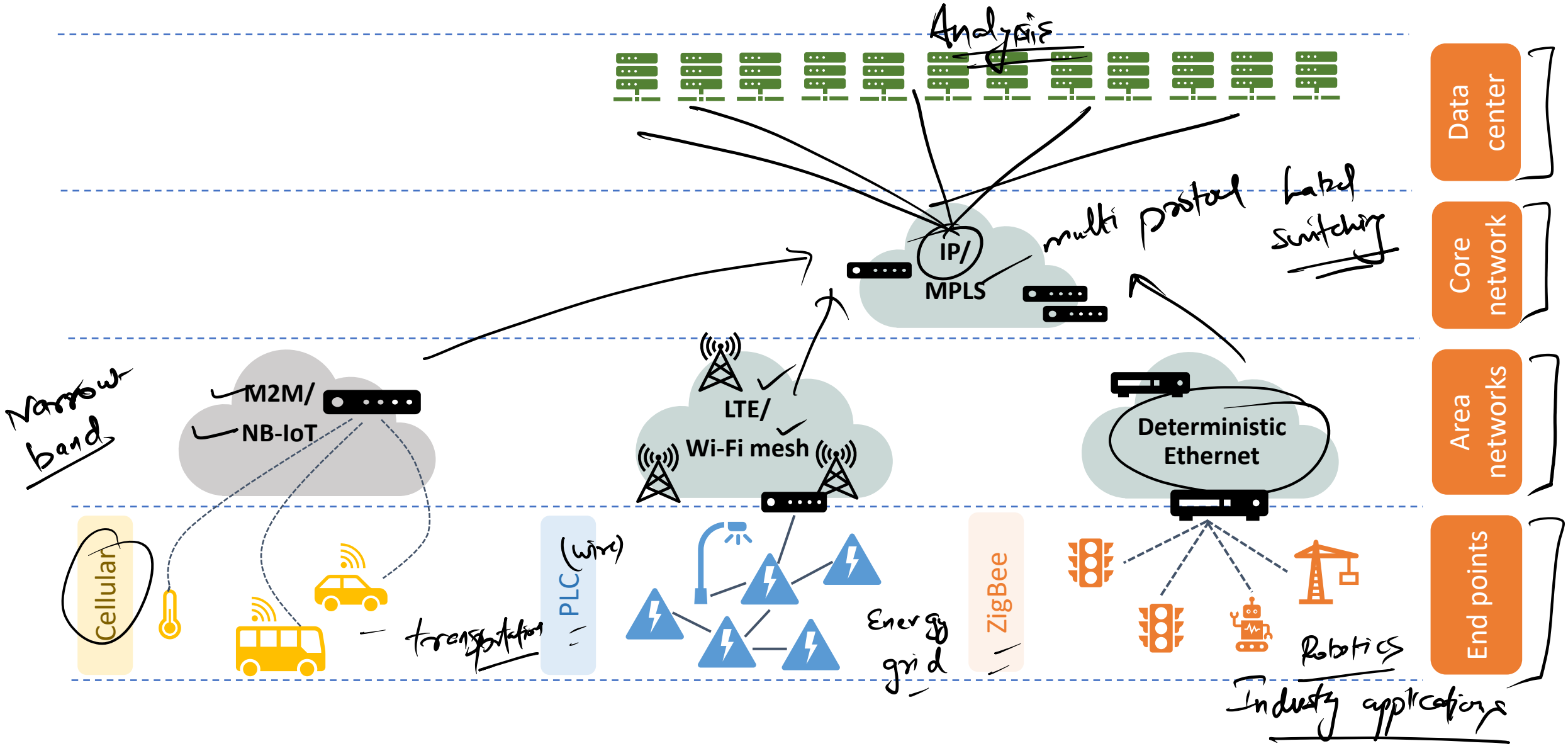
lower to upper layers

How to secure the entire ecosystems, from hardware to application?

- Hardware isolation (Arm TrustZone)
- Middleware (Speculative Store Bypass Barrier – SSBB)
- Network isolation (Software-defined Networking – SDN)
- Data confidentiality in transit (Transport Layer Security – TLS)
- Software isolation (containers)

End-to-end security not straightforward

A practical network-centric view



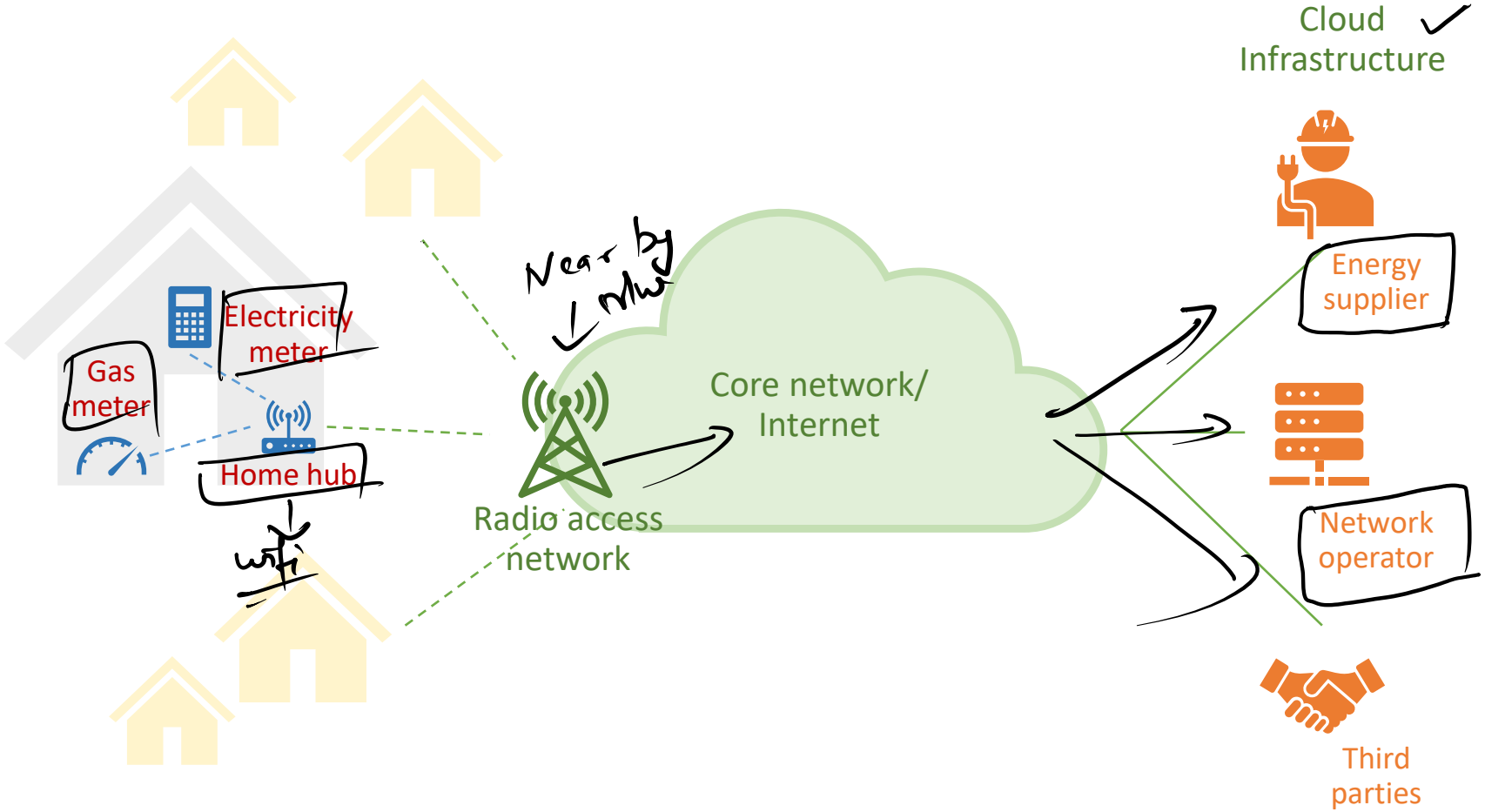
Cloud vs. Fog vs. Edge Computing?

The information processing view

Cloud computing

- Cloud dominated the networked systems landscape until recently.
- All intelligence on powerful servers, including relational databases, control functions, data analytics engines, web interfaces, etc.
- End devices merely information gatherers
  - sensors
- Might not scale as the number of IoT devices grows, and applications continue to diversify and generate more data.

Example: Smart metering



- Sensing performed by simple sensors
- Information relayed by home hub over cellular network
- Data processed in the cloud by different stakeholders

Cloud vs. Fog vs. Edge

The information processing view

- Pushing some of the intelligence closer to the device, for e.g., to access networks or gateways
- This includes data aggregation, compression, (partial) processing, making localized decisions
- IoT devices kept simple, no direct communication with end servers, still battery powered
- Resource management implemented across different network layers – management could be regarded as an application

Fog computing

The role of gateways in fog architectures

Data filtering and processing (for e.g., aggregation of summaries, compression, etc.)

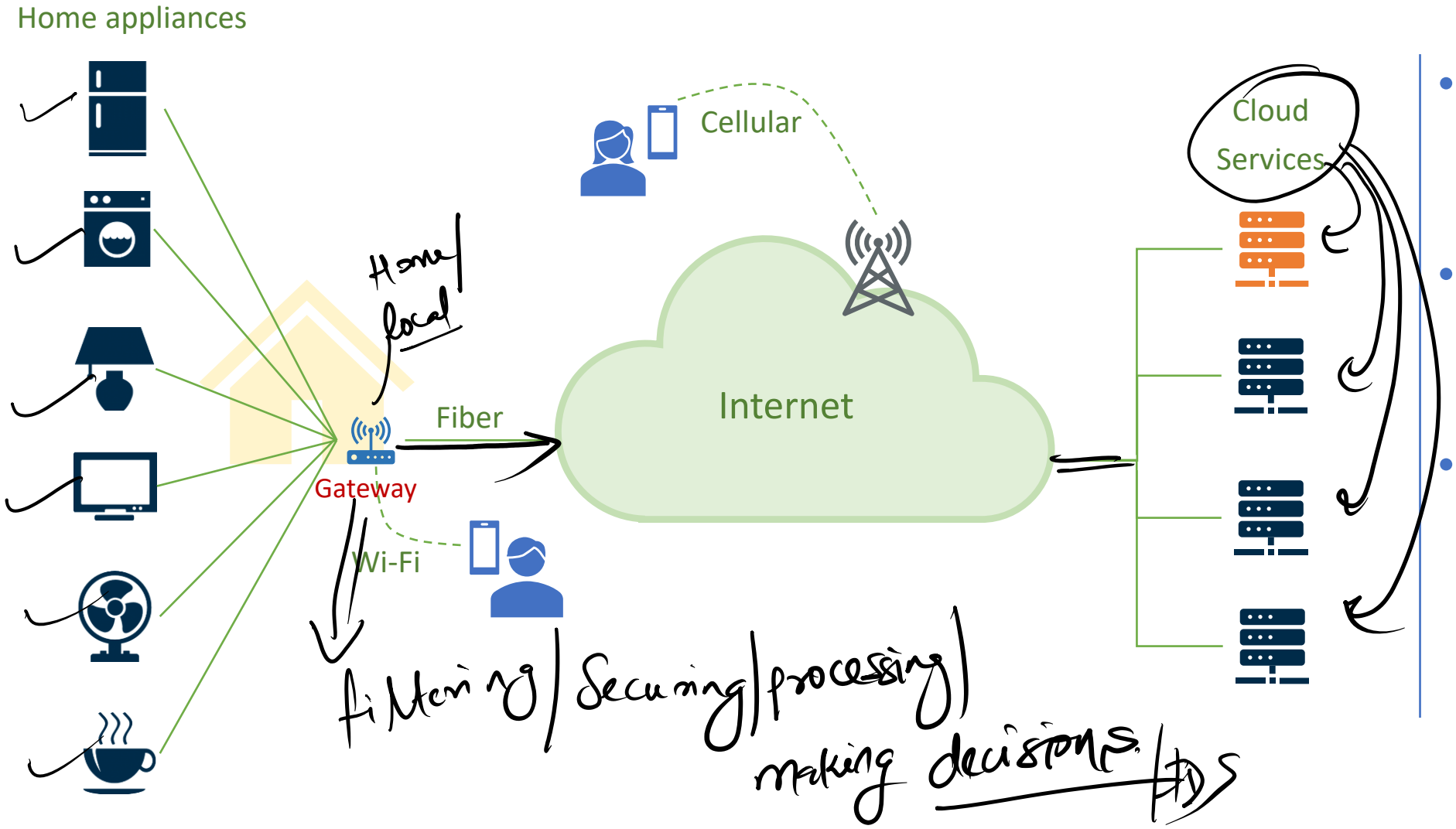
Protocol translation and interfacing between different connectivity technologies

Data flow multiplexing, packet routing

Security (for e.g., data encryption, firewalling)

Scalability problem: as the number of devices grows, so will the number of gateways that are required

Example: Home automation



- Gateway performs protocol translation
- Incorporates basic network intrusion detection system
- Cloud services continue to perform analytics

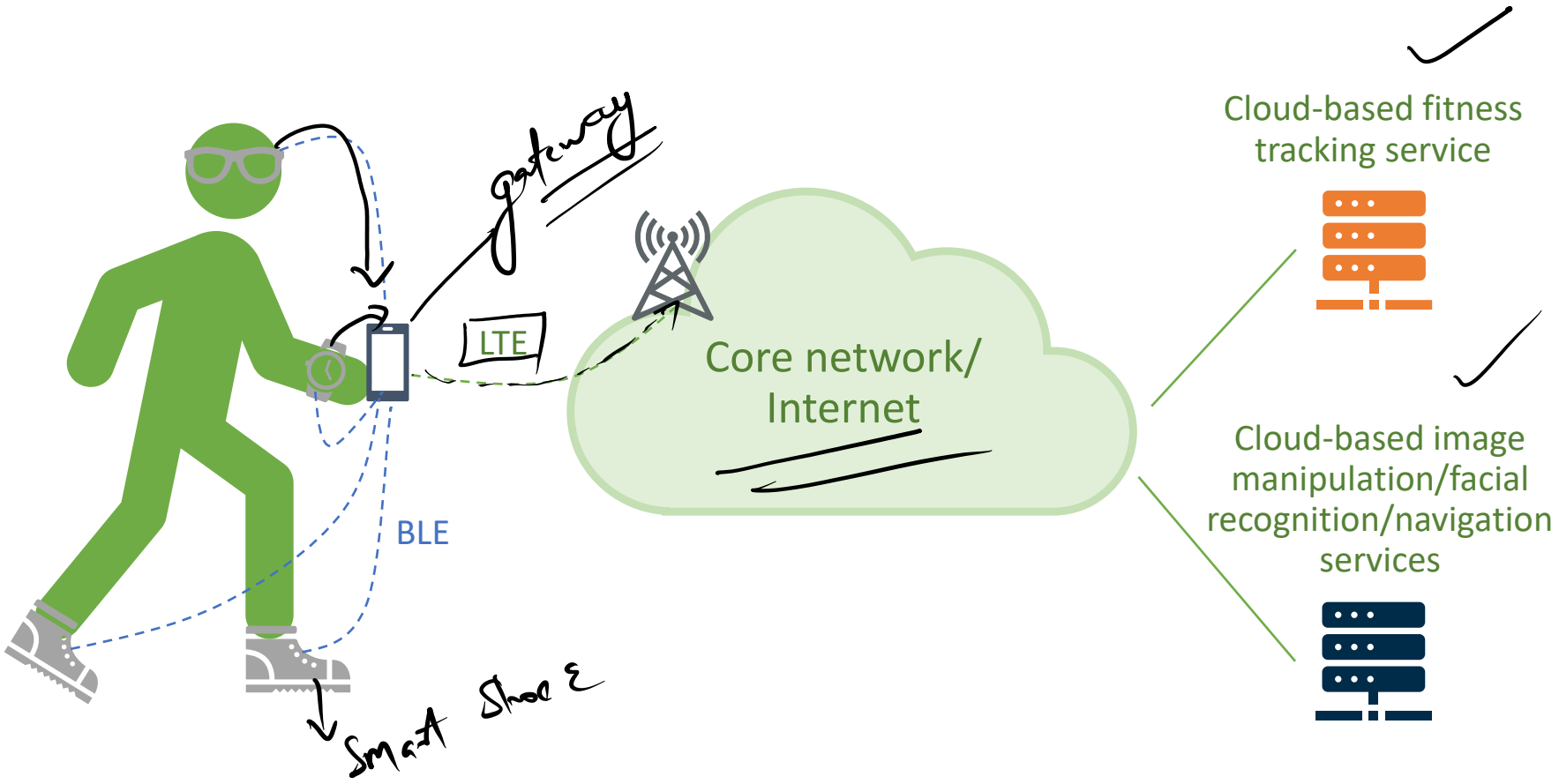
Smartphones as gateways

The fitness and healthcare domain

(Wearable devices)

- Embed multiple networking technologies (Wi-Fi, 3G/4G, Bluetooth/BLE, NFC, etc.)
- Run full TCP/IP stacks, thus maintain end-to-end connectivity with cloud
- Can connect to multiple devices within close proximity simultaneously
- Ability to enforce secure transport (e.g., TLS/HTTPS)
- Sufficient computing power to pre-process/augment collected data

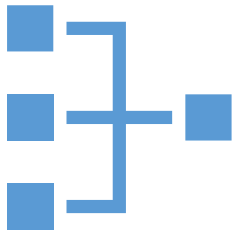
Example: Wearables



- Smartphone communicates over BLE with wearable devices
- Performs minimal information pre-processing
- Relays data to cloud-based services

Cloud vs. Fog vs. Edge

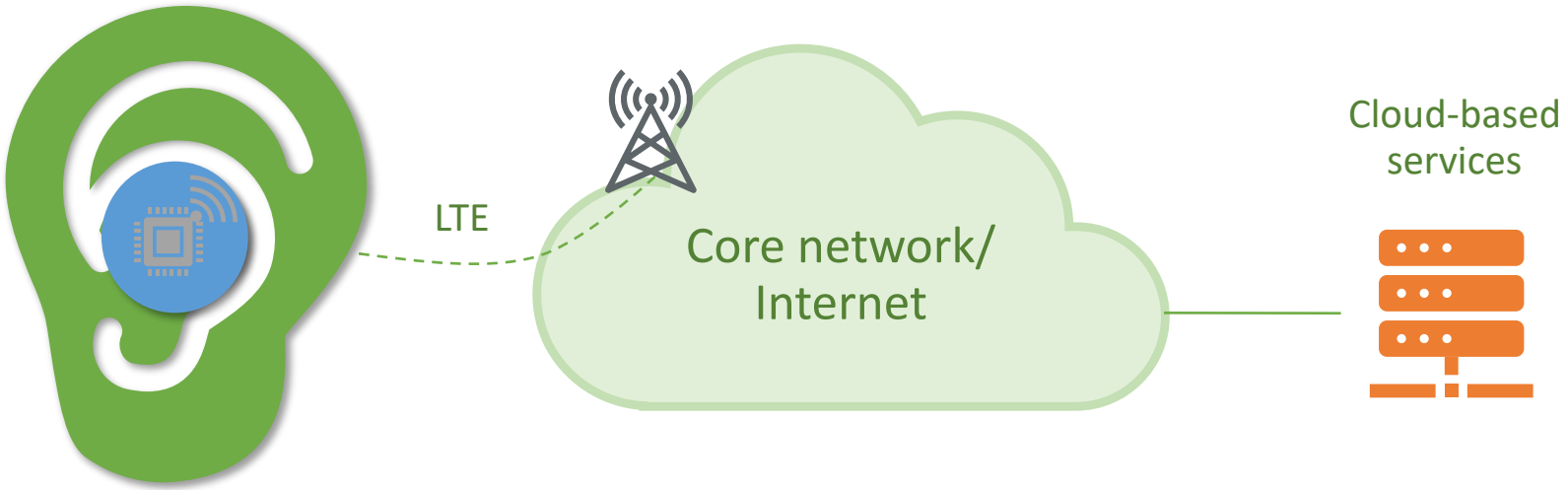
The information processing view



Edge computing

- Pushing compute power, communication capabilities, intelligence down at device level
- Processing as much as possible where data is collected
- Transmitting only key information or summaries
- Enabling new applications: automotive IoT, virtual/augmented reality, in-ear computing

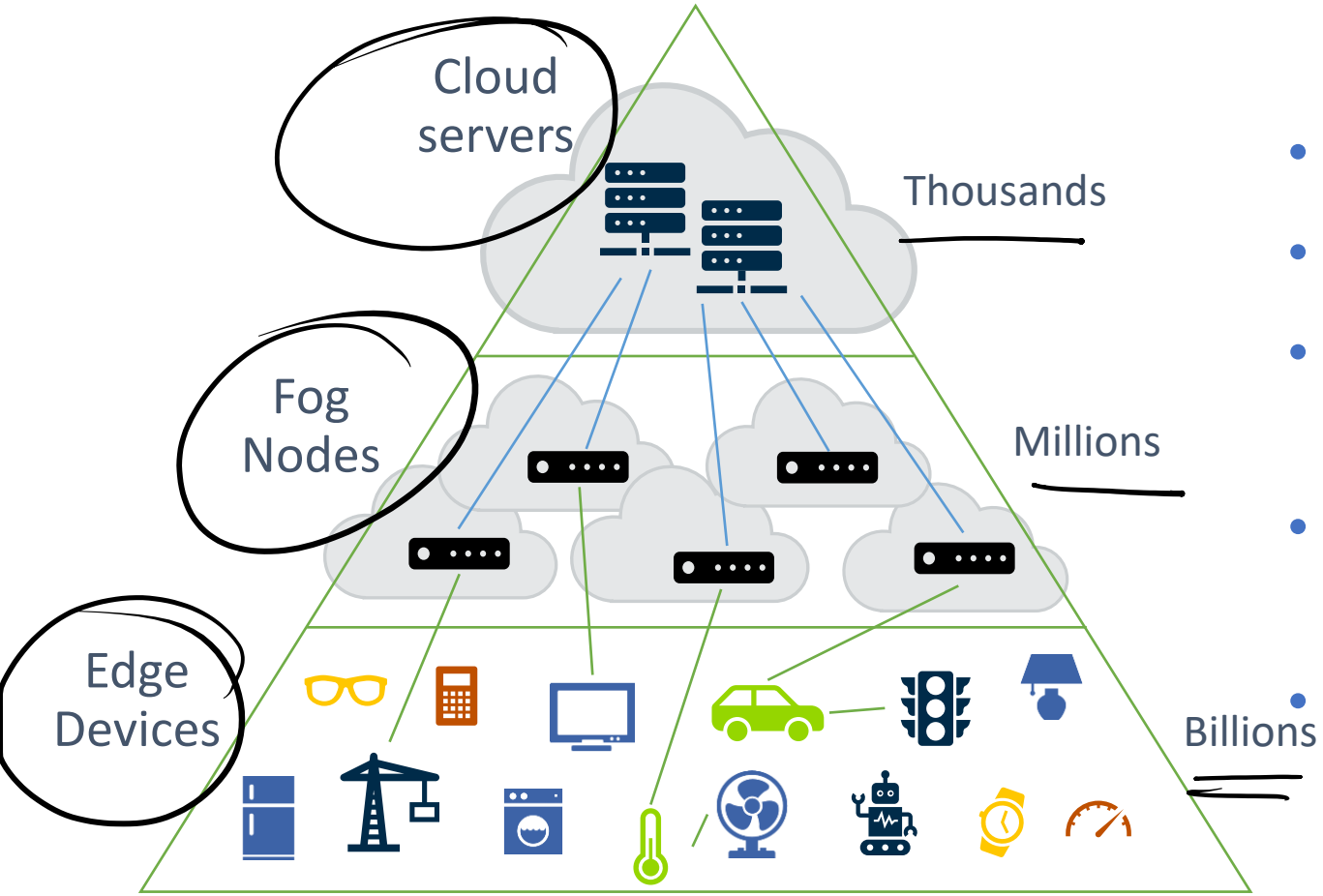
Example: Hearables



- **Hardware:** Low-power chips specialized in computationally intensive tasks (Arm Ethos)
- **Software:** AI libraries optimized for constrained devices (uTensor)
- **Neural networks:** compressed/pruned models

Choosing the right IoT architecture

Performance and cost remain the dominant architectural drivers



- What are the application requirements?
- What data needs to be acted on locally?
- Where is most of the computing power?
- How much networking infrastructure should be deployed/used?
- Where are the trust boundaries?

Standards for IoT

Multiple regulation bodies and industry alliances are standardizing the means by which devices can interact with each another and with gateways or cloud services.

The Institute of Electrical and Electronics Engineers (IEEE)

- Primarily dealing with defining protocols for (wireless) access networks
- Targeting the Industrial, Scientific, and Medical (ISM) bands (e.g., 2.4GHz, 5GHz, 900MHz in some regions, etc.)
- From an IoT perspective, the most relevant technologies include
  - IEEE 802.15.4, on which ZigBee builds, and
  - IEEE 802.11ah (HaLow) that is an amendment to the IEEE 802.11 specification (typically used for Wi-Fi) that enables low-power wide-area networking

Standards for IoT

Multiple regulation bodies and industry alliances are standardizing the means by which devices can interact with each another and with gateways or cloud services.

The 3rd Generation Partnership Project (3GPP)

- Focuses on specifying cellular network architectures and protocols (e.g., GSM, 3G, 4G-LTE, etc.)
- Developing standards for cellular communications tailored to IoT applications
  - LTE-M – compatible with existing LTE networks, easy to roll out, limited to 1Mb/s speeds
  - NB-IoT – deployed in same or different frequency bands, lower capacity (200Kb/s), different modulation and coding schemes, and does not require gateways.

Standards for IoT

The Internet Engineering Task Force (IETF)

- Focuses on specifying protocols that are used across the Internet; these standards are known as Requests for Comments (RFCs)

- IoT relevant standards include
  - Addressing/internetworking for low power devices (IPv6 over Low-Power Wireless Personal Area Networks – 6LoWPAN)
  - Routing (Routing Over Low-power and Lossy networks – ROLL)
  - End-to-end communications (Constrained Application Protocol – CoAP)
  - Security (Datagram Transport Layer Security – DTLS)
  - Software updating (Software Updates for Internet of Things – SUIT)

- Also offers experience-based guidance
  - Example: The JavaScript Object Notation (JSON) Data Interchange Format – RFC 8259

Standards for IoT

Industry alliances

- Bluetooth – wireless personal area networks (WPANs); defines application profiles
- ZigBee – WPANs building on IEEE 802.15.4; inexpensive consumer/industrial applications
- LoRaWAN – LPWAN based on chirp spread spectrum technology

Collaborative associations

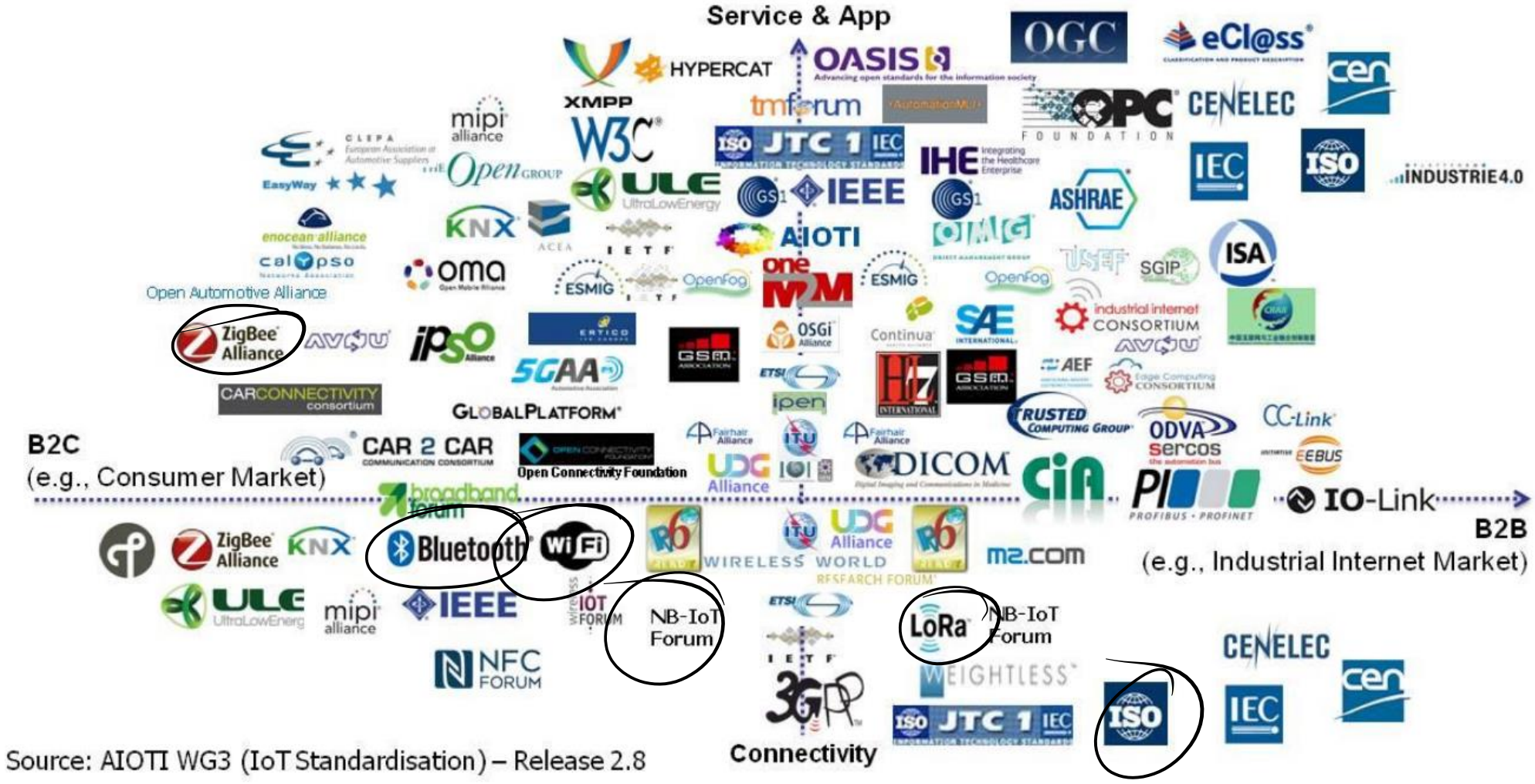
- The Alliance for IoT Innovation (AIoTI) – European Commission framework supporting interaction between IoT players to drive innovation, standardization, and policy.
- Open Connectivity Foundation (OCF) – Industry-led framework aiming to develop IoT standards, interoperability guidelines, and provide a device certification program.

Standards for IoT

Other standardization bodies relevant to IoT

- National Institute of Standards and Technology (NIST) – works on a range of science, technology, and engineering topics
  - Example: Advanced Encryption Standard (AES)
- International Organization for Standardization (ISO) – promotes a broad range of proprietary, industrial, and commercial standards
  - Example: Internet of Things (IoT) – Reference Architecture (ISO/IEC 30141:2018)
- International Telecommunication Union (ITU) – recommendations, reference models
  - Example: ITU-T Y.4000/Y.2060 - Overview of the Internet of things

Choosing among IoT standards is not straightforward



Thank You

Contact me:

gauravsingal789@gmail.com

Gaurav.singal@nsut.ac.in

www.gauravsingal.in

LinkedIn: https://www.linkedin.com/in/gauravsingal789/

Twitter: https://twitter.com/gaurav_singal