Bootcamps for Emerging Technologies and essential Skills

BETES
Discover Technologies, expand opportunities!

Internet of Things

Introduction and Fundamentals of IoT

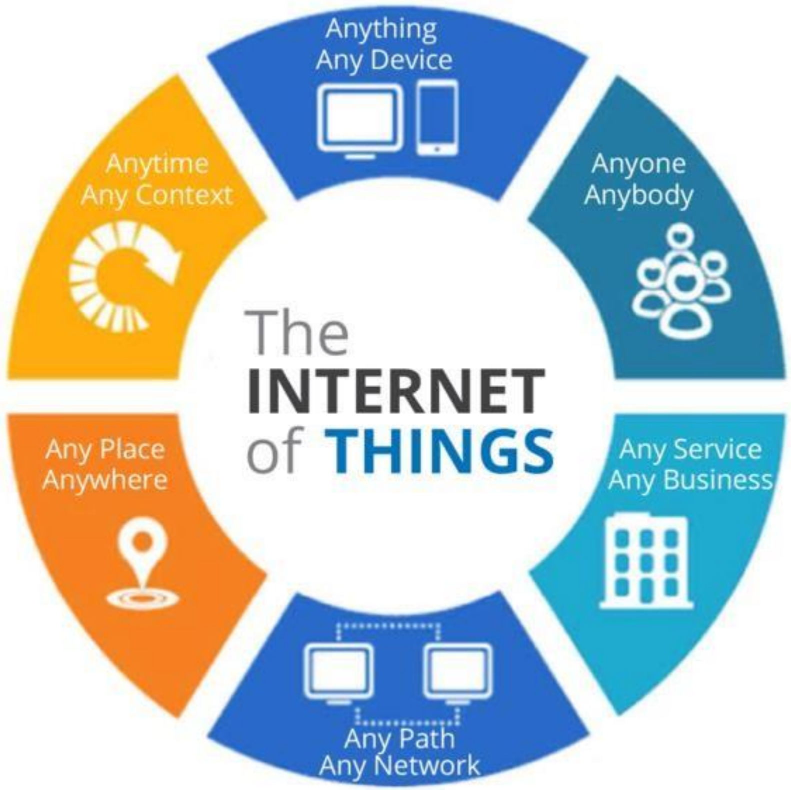
Developed by: ECECT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-CY01-KA210-VET-000082706

Definition

The Internet of Things (IoT) describes the network of physical objects or “things” that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. These devices range from ordinary household objects to sophisticated industrial tools.



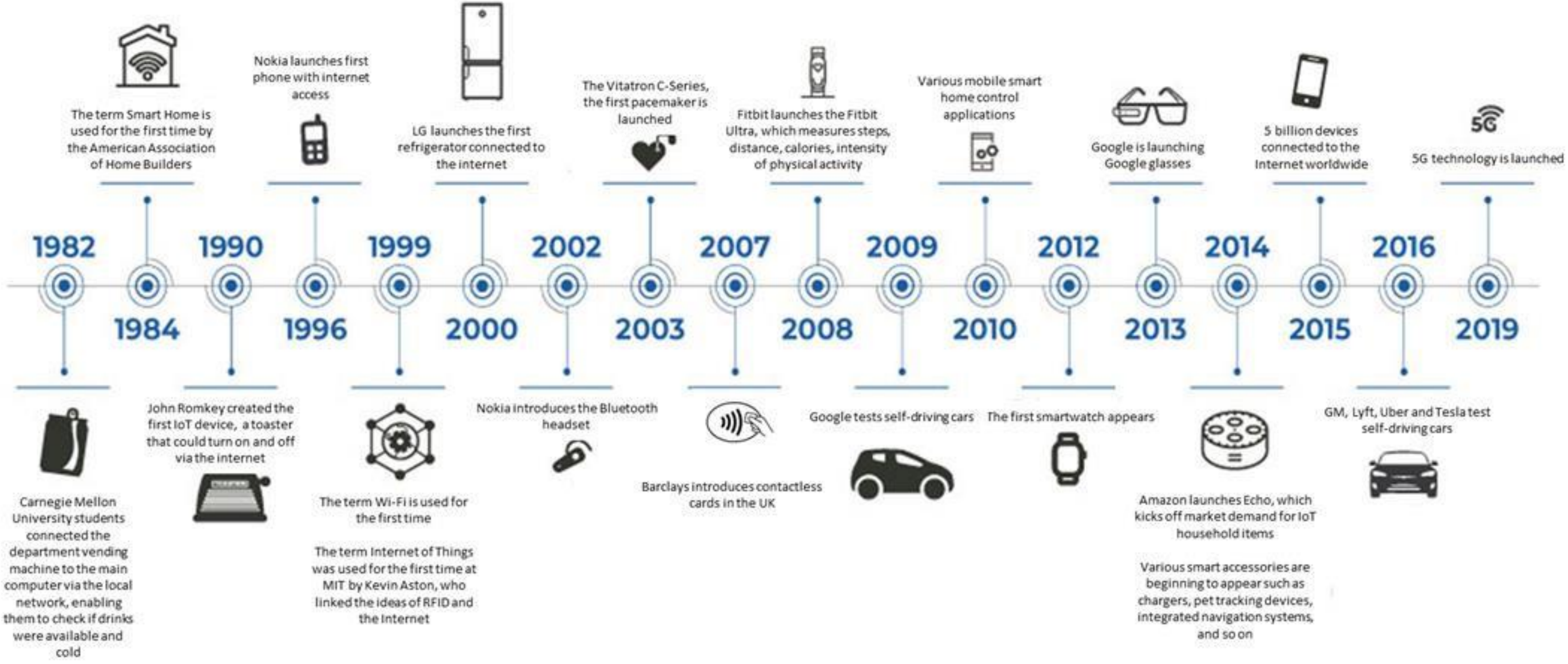
Co-funded by the European Union

What is IoT?

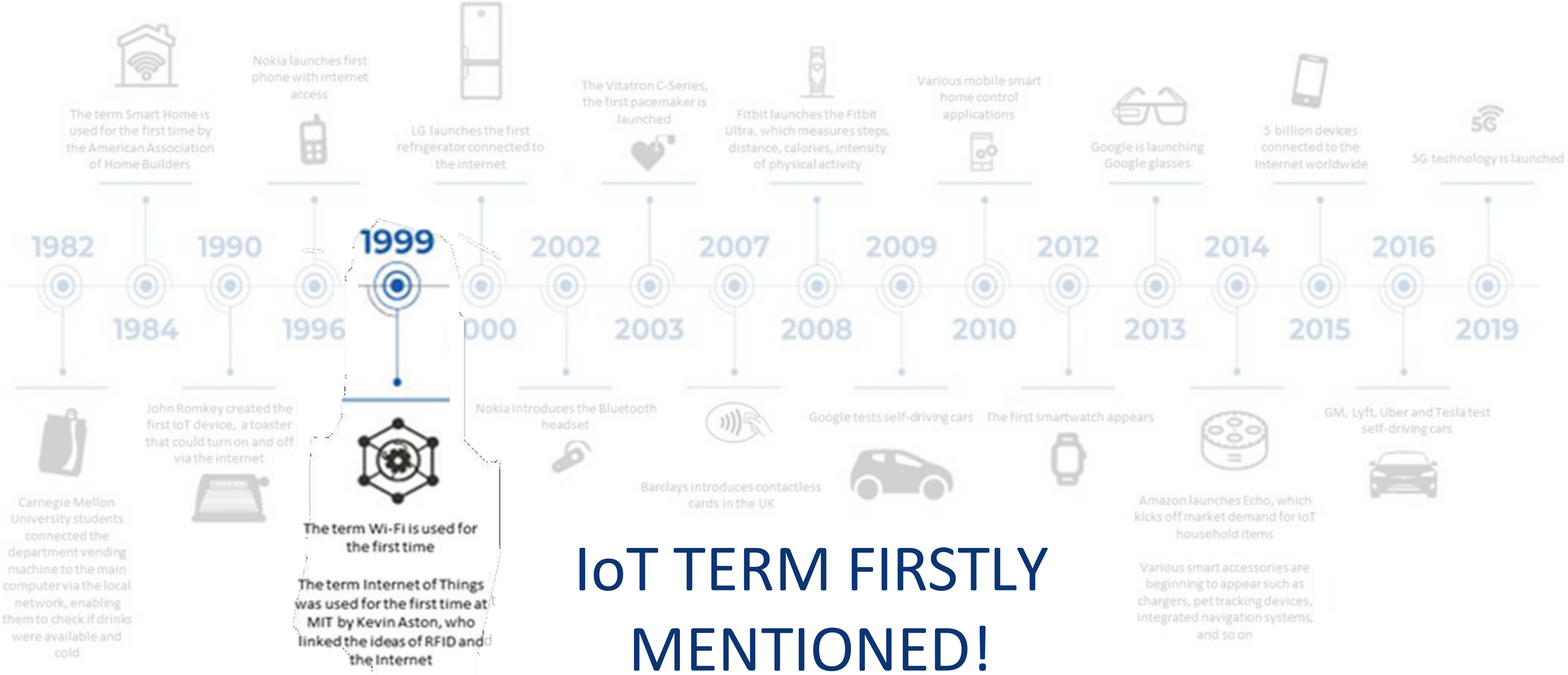
- Definition: Interconnected digital and mechanical devices
- Ubiquity in daily life
- IoT's role in data and connectivity
- Impact on industries and personal life

Co-funded by the European Union

History


1982
Carnegie Mellon University students connected the department vending machine to the main computer via the local network, enabling them to check if drinks were available and cold
1984
The term Smart Home is used for the first time by the American Association of Home Builders
1990
John Romkey created the first IoT device, a toaster that could turn on and off via the internet
1996
Nokia launches first phone with internet access
1999
The term Wi-Fi is used for the first time
The term Internet of Things was used for the first time at MIT by Kevin Aston, who linked the ideas of RFID and the Internet
2000
LG launches the first refrigerator connected to the internet
2002
Nokia introduces the Bluetooth headset
2003
The Vitatron C-Series, the first pacemaker is launched
2007
Barclays introduces contactless cards in the UK
2008
Fitbit launches the Fitbit Ultra, which measures steps, distance, calories, intensity of physical activity
2009
Google tests self-driving cars
2010
Various mobile smart home control applications
2012
The first smartwatch appears
2013
Google is launching Google glasses
2014
Amazon launches Echo, which kicks off market demand for IoT household items
Various smart accessories are beginning to appear such as chargers, pet tracking devices, integrated navigation systems, and so on
2015
5 billion devices connected to the Internet worldwide
2016
GM, Lyft, Uber and Tesla test self-driving cars
2019
5G
5G technology is launched

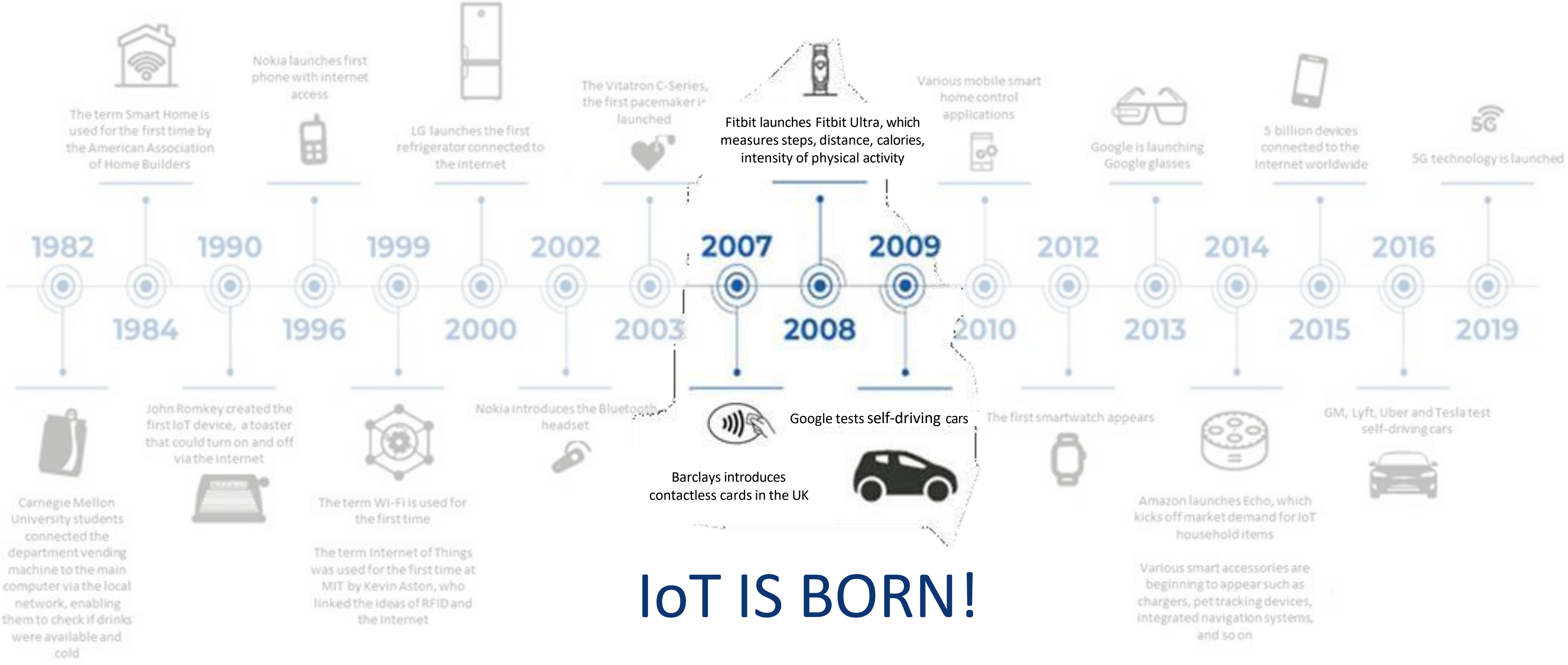
History



IoT TERM FIRSTLY MENTIONED!

Co-funded by the European Union

History



IoT IS BORN!

Co-funded by the European Union

History

2020: IoT steps up in response to COVID-19 crisis

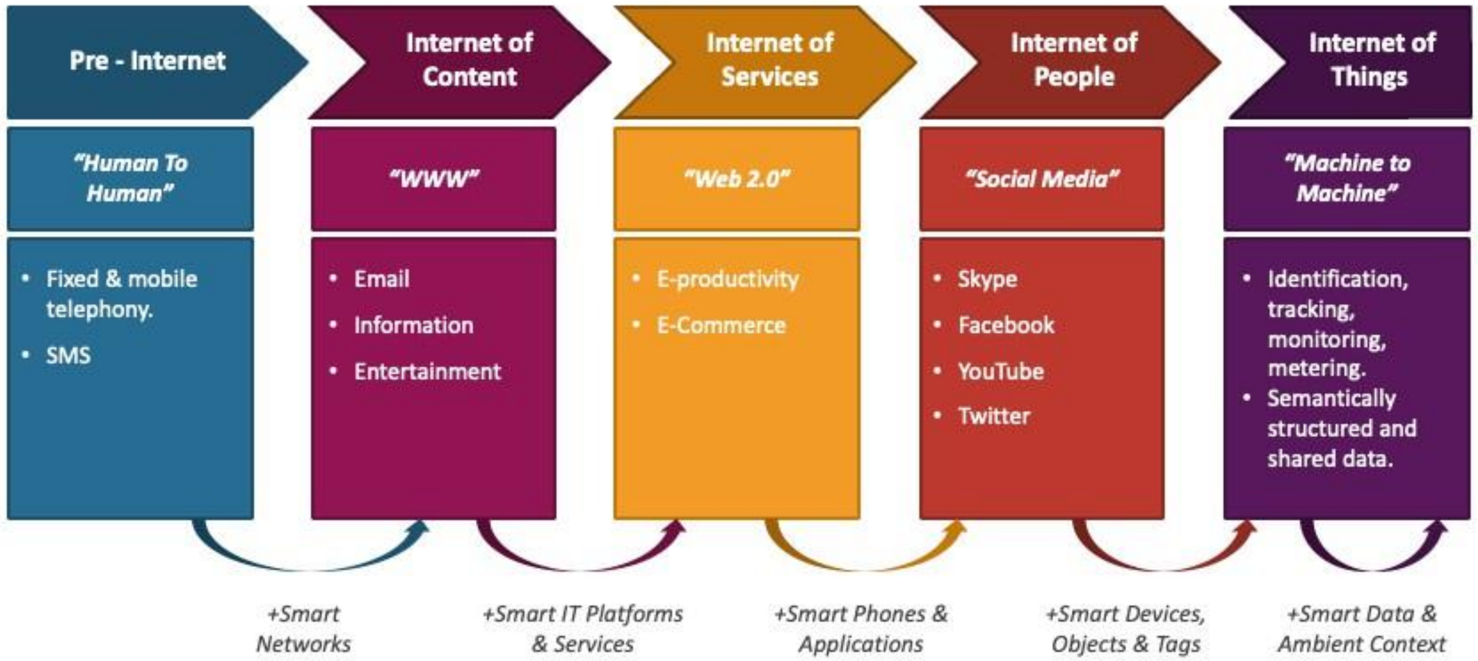
- Remote patient monitoring
- Healthcare facilities management
- Contact Tracing and Social Distancing
- Temperature and Symptom Screening
- Supply chain monitoring
- Quarantine monitoring
- Hygiene monitoring
- Telemedicine and remote consultations
- Research and data collection
- Predictive analysis
- Delivery and logistics
- Smart quarantine management

Enhancing public health responses, minimizing the spread of the virus, and ensuring efficient management of healthcare resources.

Co-funded by the European Union

Evolution of IoT

- Early internet developments
- Advent of wireless technology
- Growth of sensor technology
- Recent advancements and innovations



Co-funded by the European Union

Significance

- **IoT's significance**

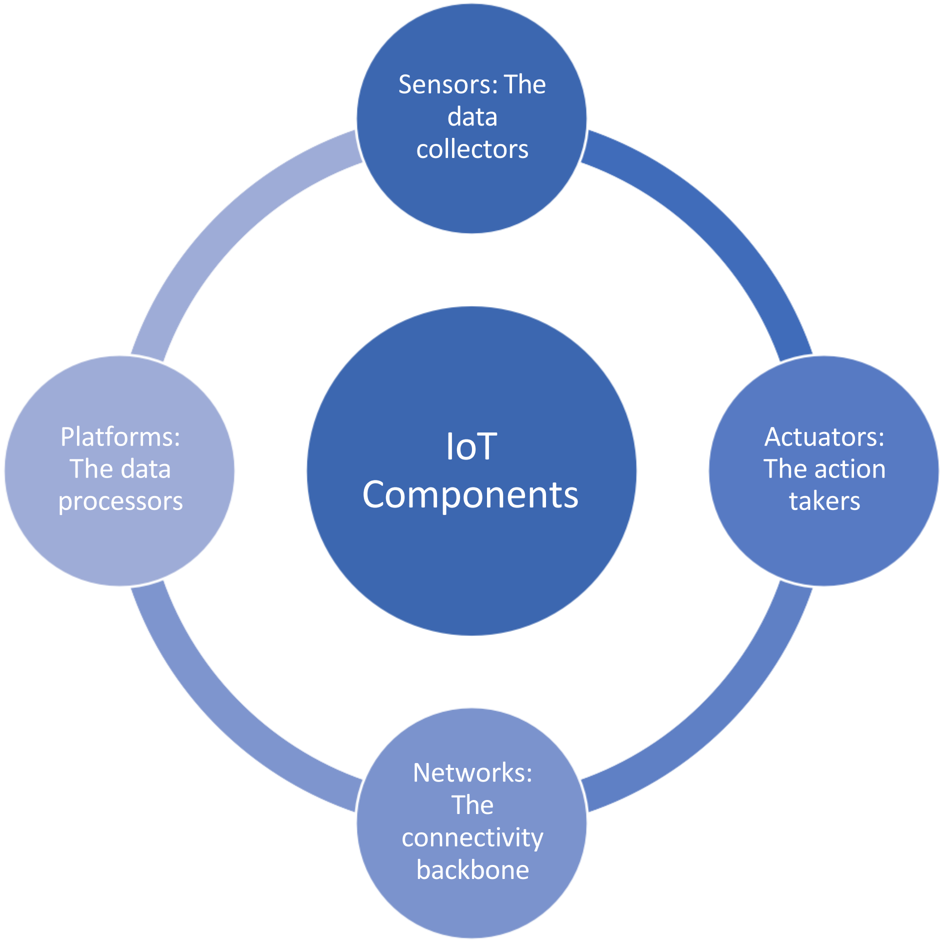
Can connect the physical world with the digital realm, transforming industries, improving quality of life, and paving the way for innovative applications that were once only imaginable.

- **By means of:**
  - Low-cost computing, the cloud, big data, analytics, and mobile technologies
  - With minimal human intervention, physical things can share and collect data
  - Digital systems can record, monitor, and adjust each interaction between connected things

The physical world meets the digital world—and they cooperate!

Co-funded by the European Union

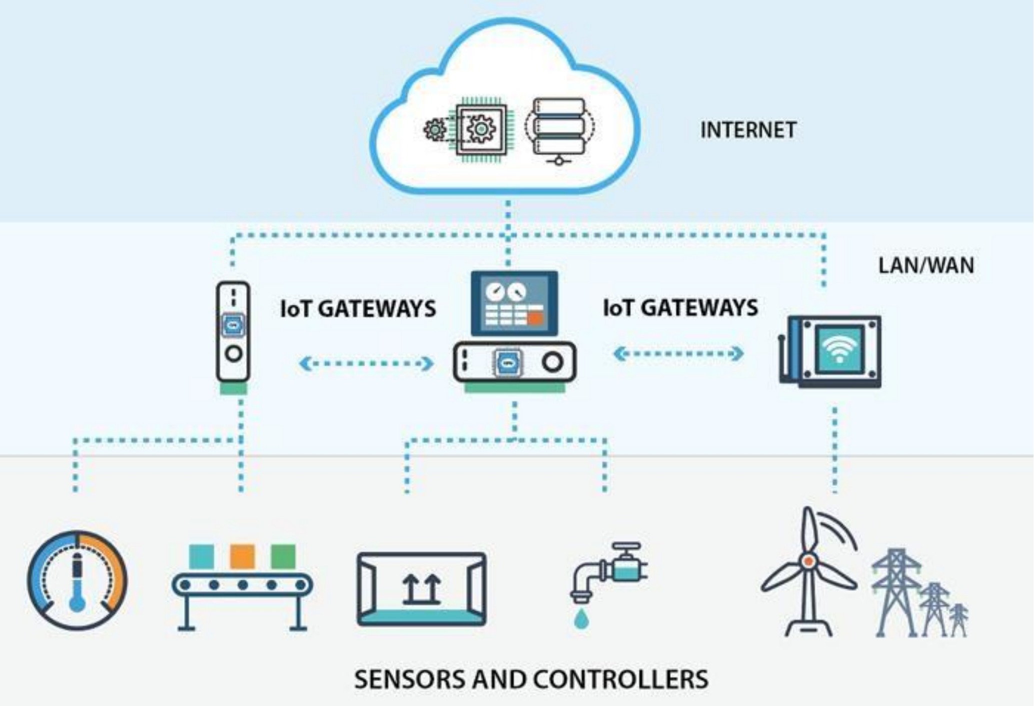
Key Components of IoT



Co-funded by the European Union

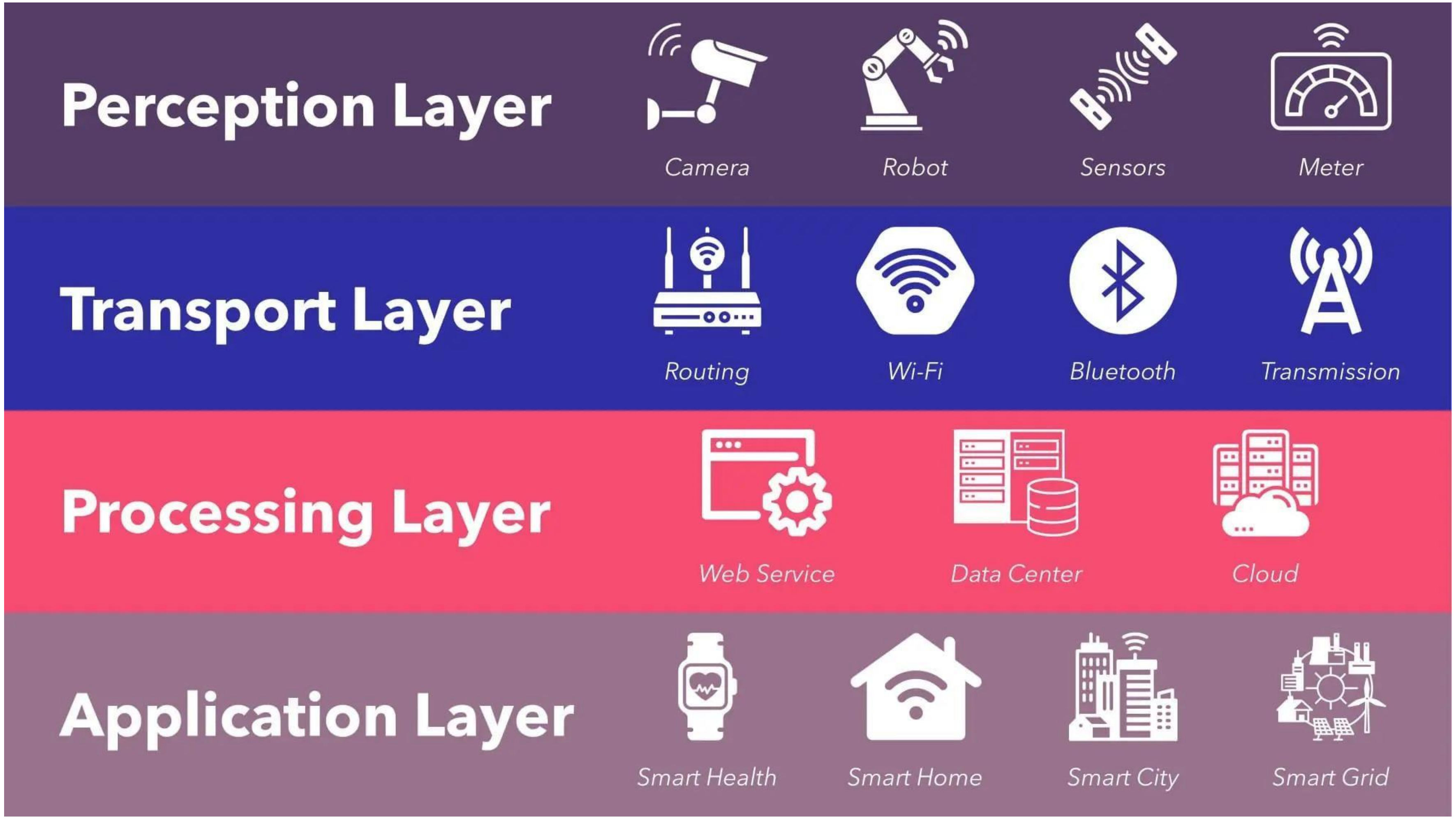
Basic IoT Architecture

- Understanding Layered IoT Architecture
- Components of IoT Architecture: From Sensors to Applications
- Example of a Simple IoT System Architecture



Co-funded by the European Union

TYPICAL IoT Architecture / 4 layers



Co-funded by the European Union

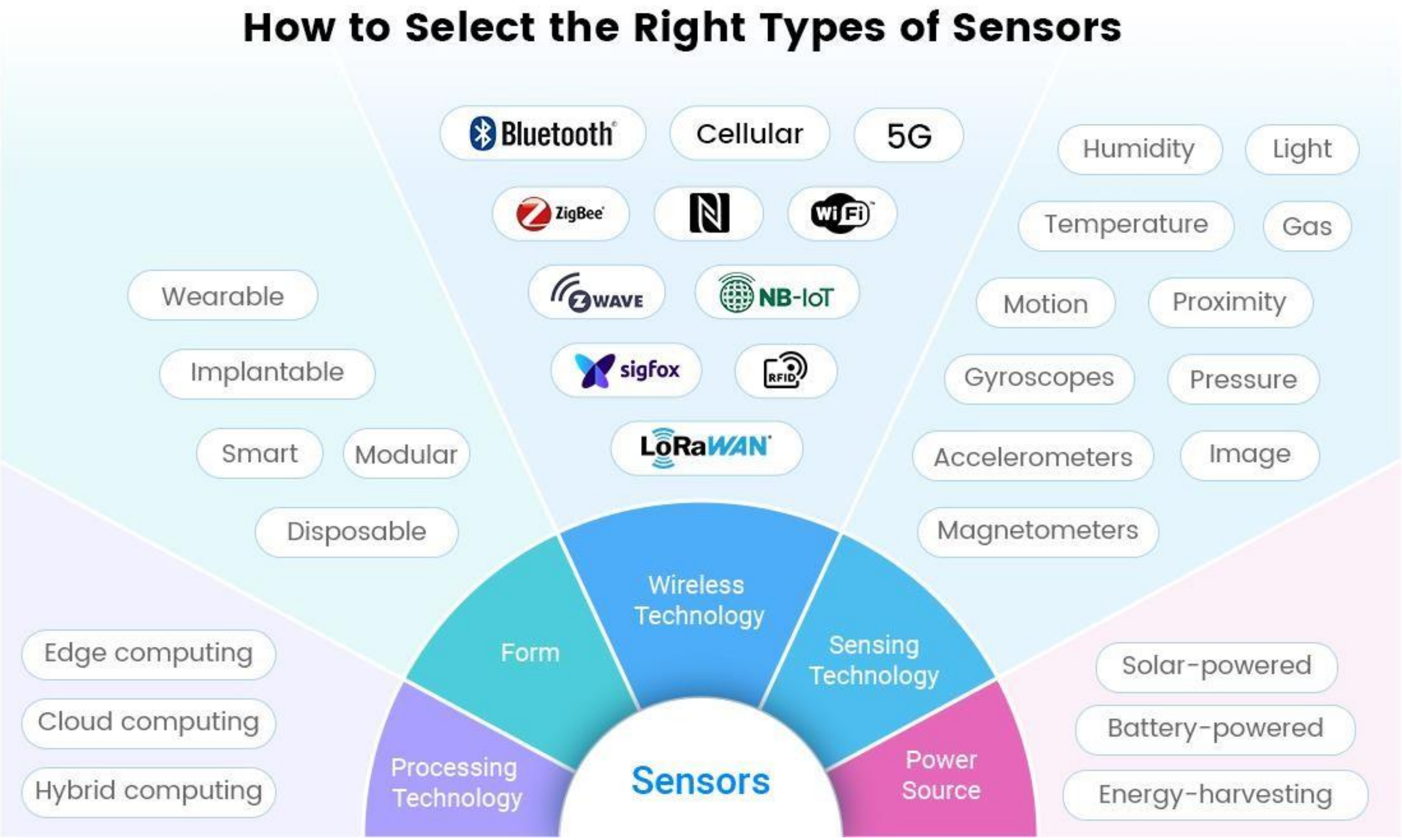
IoT architecture Layers

In the context of IoT, "layers" typically refer to the different levels of an IoT architecture

- **Perception.**
  - This is the hardware layer. Sensors, connected devices, and actuators are all here.
- **Network/Transport layer**
  - Data goes through this layer, so it connects the perception layer with the application layer. Data and gateways are the main players at this layer as they bring the message to the back-end service of an IoT application.
- **Processing Layer**
  - The IoT processing layer is responsible for analyzing and processing data collected from devices before it's delivered to the application layer.
- **Application.**
  - That's what users see and can click or tap. This layer is the starting point of data going through the application from connected devices and back.

Co-funded by the European Union

Understanding IoT Sensors

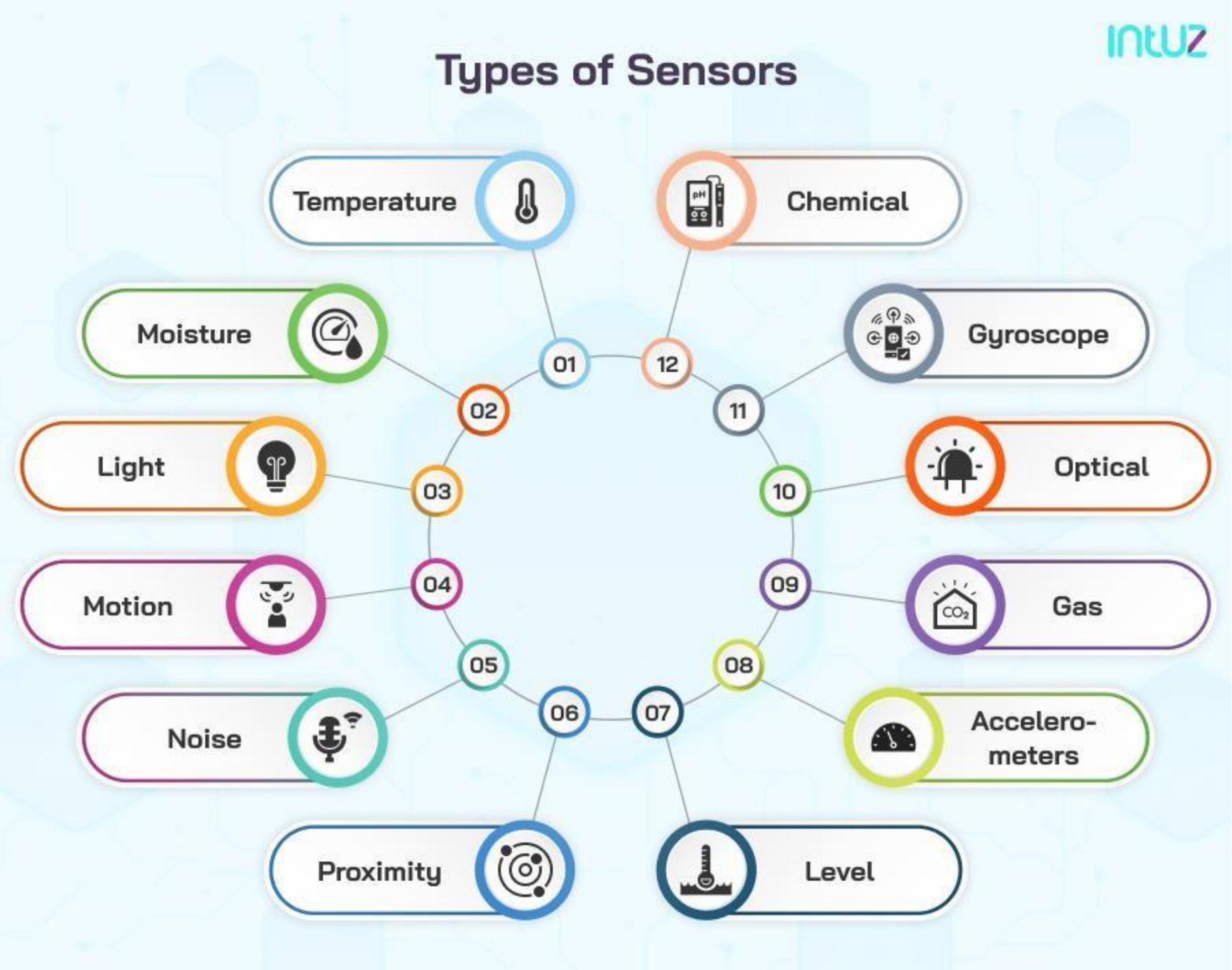


An IoT sensor is a device that detects events or changes in its environment. It's an essential component of the Internet of Things (IoT), as it forms the interface between the real and digital worlds. IoT sensors can measure a wide range of environmental properties such as temperature, pressure, motion, and light intensity, and they're widely used in various applications from smart homes and industrial automation to environmental monitoring and smart cities.

- Key functions: Detecting and measuring environmental data
- Importance in IoT ecosystem for data collection

Co-funded by the European Union

Types of IoT Sensors



- Temperature and Humidity Sensors
- Motion and Proximity Sensors
- Pressure and Level Sensors
- Other common types: Light, Gas, and Acoustic Sensors

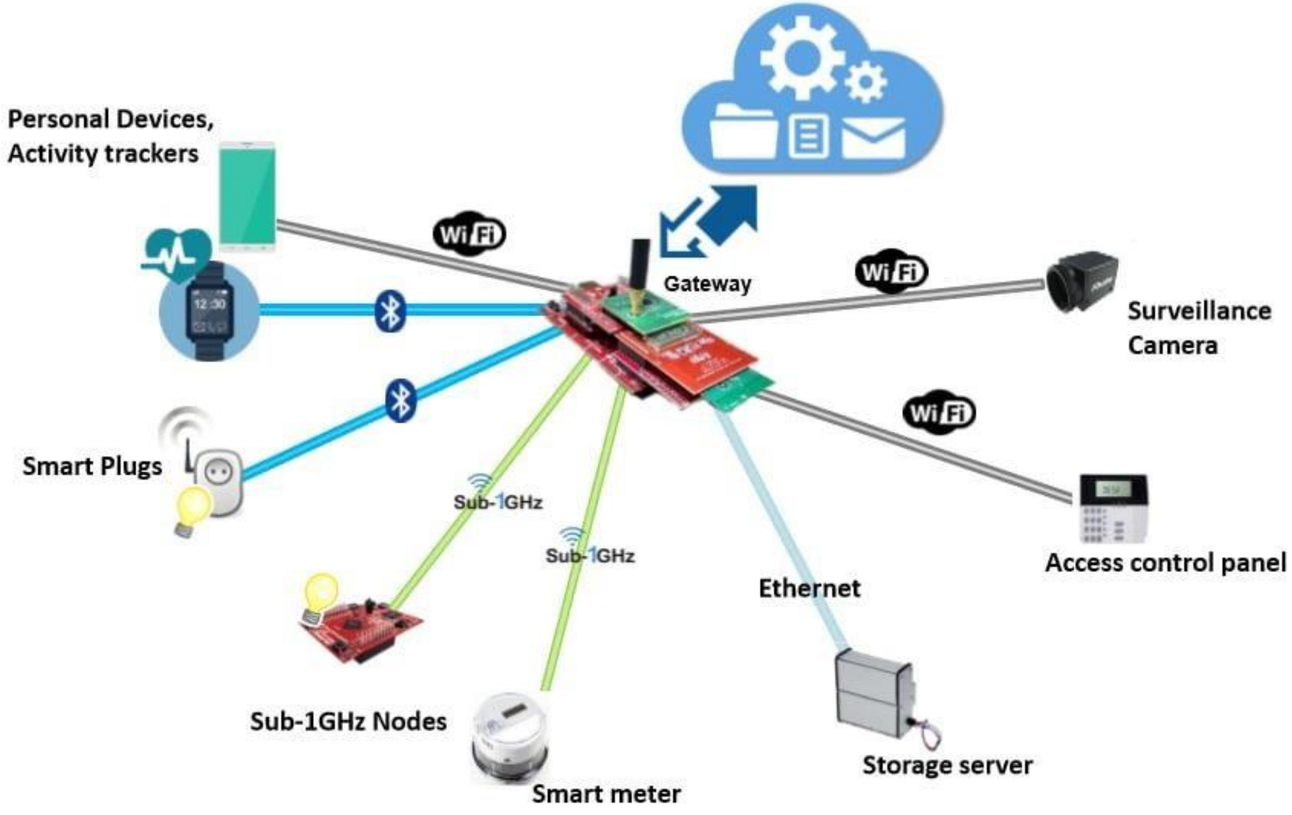
Co-funded by the European Union

Applications of IoT Sensors

- Smart Home Automation (e.g., temperature, lighting)
- Industrial IoT (e.g., pressure, level monitoring)
- Healthcare (e.g., wearable health monitors)
- Environmental Monitoring (e.g., air quality sensors)

Co-funded by the European Union

Understanding IoT Gateways



Definition: A bridge between IoT devices and the network

Smart plugs

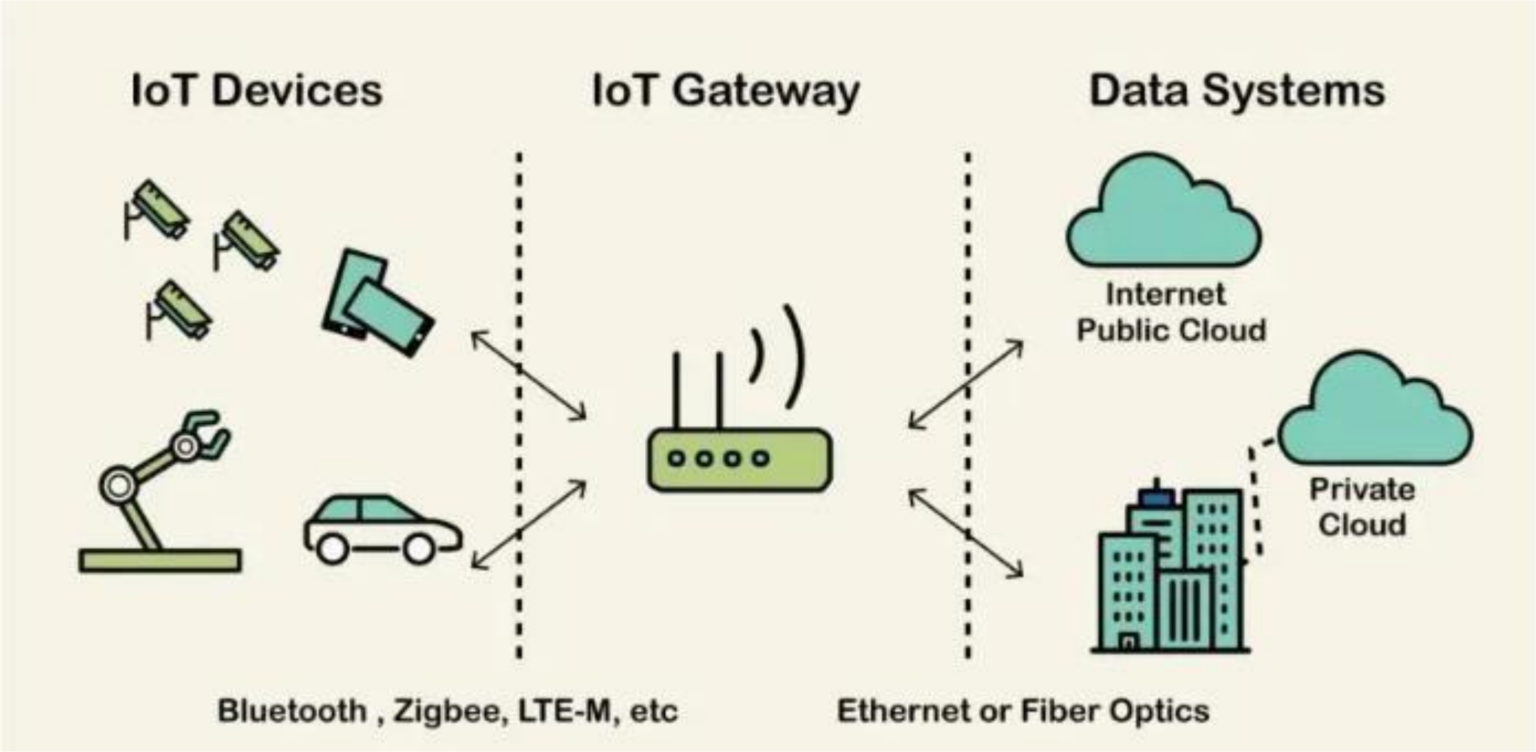
Activity trackers

Smart meters

Wifi / Bluetooth / Sub1Ghz/Ethernet

Co-funded by the European Union

Functions of an IoT Gateway



Data aggregation from multiple sensors

Local data processing and analysis

Secure data transmission to and from the cloud

Co-funded by the European Union

IoT Gateway Frequencies

THE FREQUENCY BANDS OF IOT WIRELESS

data-alliance
Wireless network gear

TECHNOLOGY	FREQUENCY BANDS	CHARACTERISTICS
WI-FI	2.4 GHz & 5 GHz	SHORTER RANGE, HIGHER DATA RATES, LESS PENETRATION.
BLUETOOTH	2.4 GHz	SHORTER RANGE, HIGHER DATA RATES, LESS PENETRATION.
ZIGBEE	2.4 GHz	SHORTER RANGE, HIGHER DATA RATES, LESS PENETRATION.
LORA	443 MHz, 868 MHz & 915 MHz	LONGER RANGE, BETTER PENETRATION, LOWER DATA RATE.
NB-IoT	LTE	VERY HIGH DATA RATES, EXTREMELY LIMITED RANGE AND PENETRATION.
5G IoT	RANGE: SUB-1 GHz TO MMWAVE	VERY HIGH DATA RATES, EXTREMELY LIMITED RANGE AND PENETRATION.

- Common frequency bands: 2.4 GHz, 5 GHz (Wi-Fi), Sub-1 GHz (Zigbee, Z-Wave)
- Frequency selection based on range and bandwidth requirements
- Impact on network performance and device compatibility

Co-funded by the European Union

IoT Gateway Protocols

	MQTT	AMQP	HTTP	CoAP
Abstraction	Pub/Sub	Pub/Sub	Request/Reply	Request/Reply
Architecture	Brokered	P2P or Brokered	P2P	P2P
QoS	3	3	Provided by TCP	Confirmable and no Confirmable
Interoperability	Partial	Yes	Yes	Yes
Real-time	No	No	No	No
Transports	TCP	TCP	TCP	UDP
Subscription Control	hierarchical matching	Exchanges, Queues and bindings	N/A	support for Multicast addressing msgs.
Data Serialization	Undefined	AMQP type system or user defined	No	Configurable
Dynamic Discovery	No	No	No	Yes
Security	SSL	TLS	SSL/TLS	DTLS

- Common protocols: MQTT, CoAP, HTTP/HTTPS, AMQP
- Protocol selection based on use case
- Role in ensuring efficient and secure communication

Co-funded by the European Union

IoT Gateway in Smart Home Applications

- Central hub for smart home devices
- Managing diverse devices and protocols
- Enhancing user experience through seamless integration

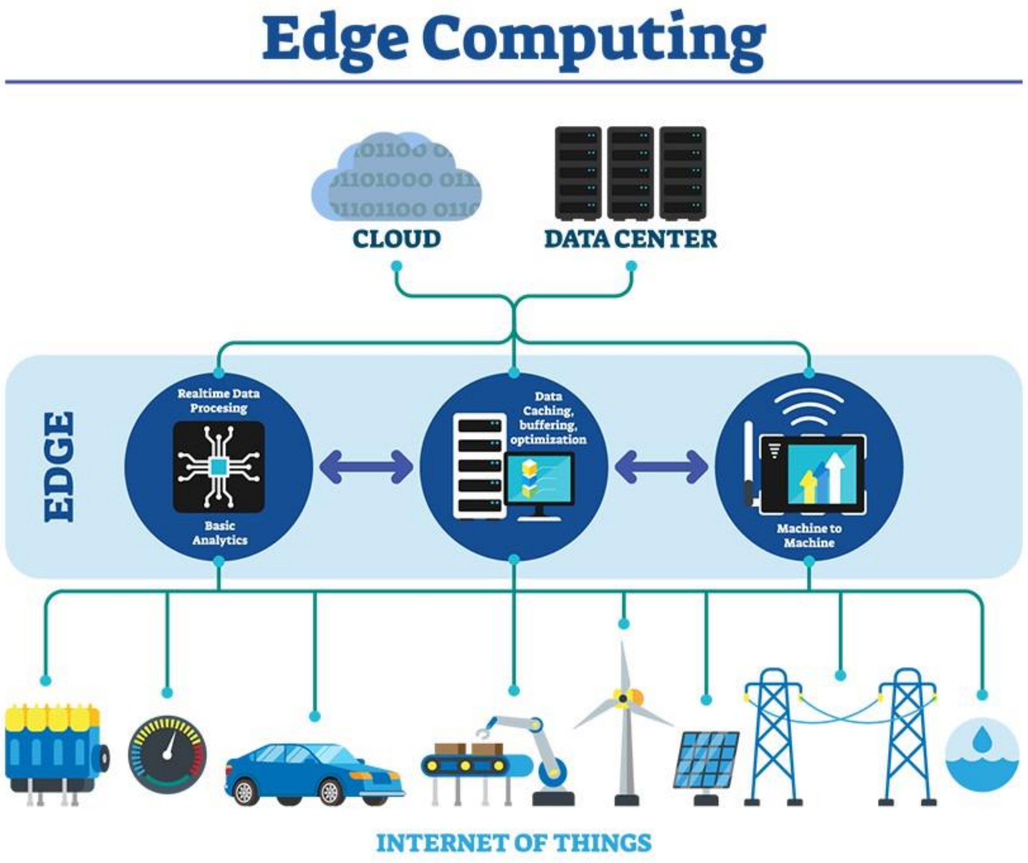
Co-funded by the European Union

What is an Edge Device?

- Definition: A device that processes data at the edge of the network, near the data source
- Key Characteristics: Local data processing, low latency, and reduced bandwidth usage
- Examples: IoT sensors, smart cameras, and routers

Co-funded by the European Union

The Role of Edge Devices in IoT



- Enhancing Real-Time Data Processing: Immediate analysis and response without the need for cloud transmission
- Improving Privacy and Security: Local data processing can reduce the risk of data breaches
- Enabling IoT Scalability: Eases the load on network infrastructure by minimizing data sent to the cloud
- Use Cases: Industrial automation, smart city infrastructure, and healthcare monitoring

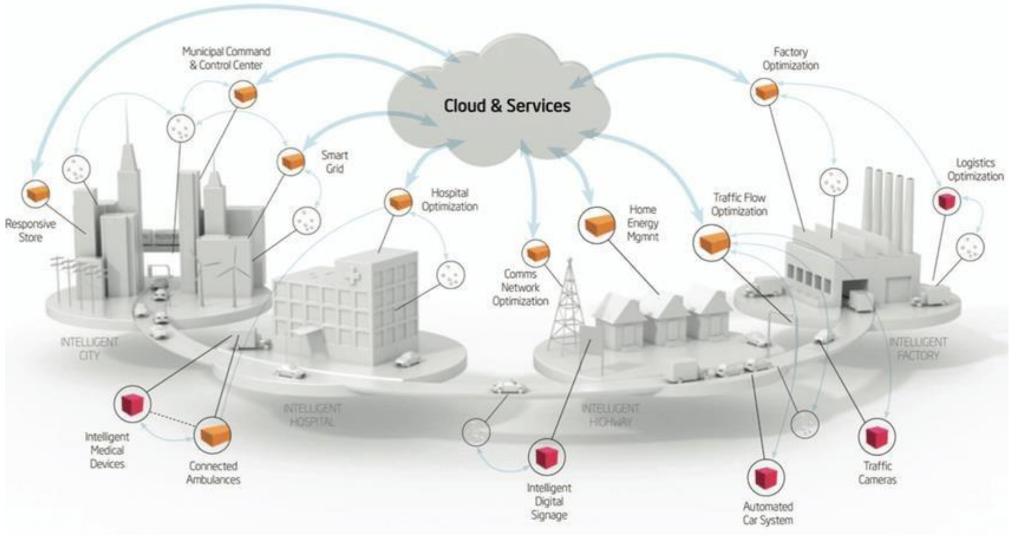
Co-funded by the European Union

Data Centers and Cloud Computing in IoT

- Definition: Centralized platforms for storing and processing IoT data
- Key Functions: Data aggregation, storage, large-scale processing, and analysis
- Benefits: Scalability, flexibility, and enhanced computational power

Co-funded by the European Union

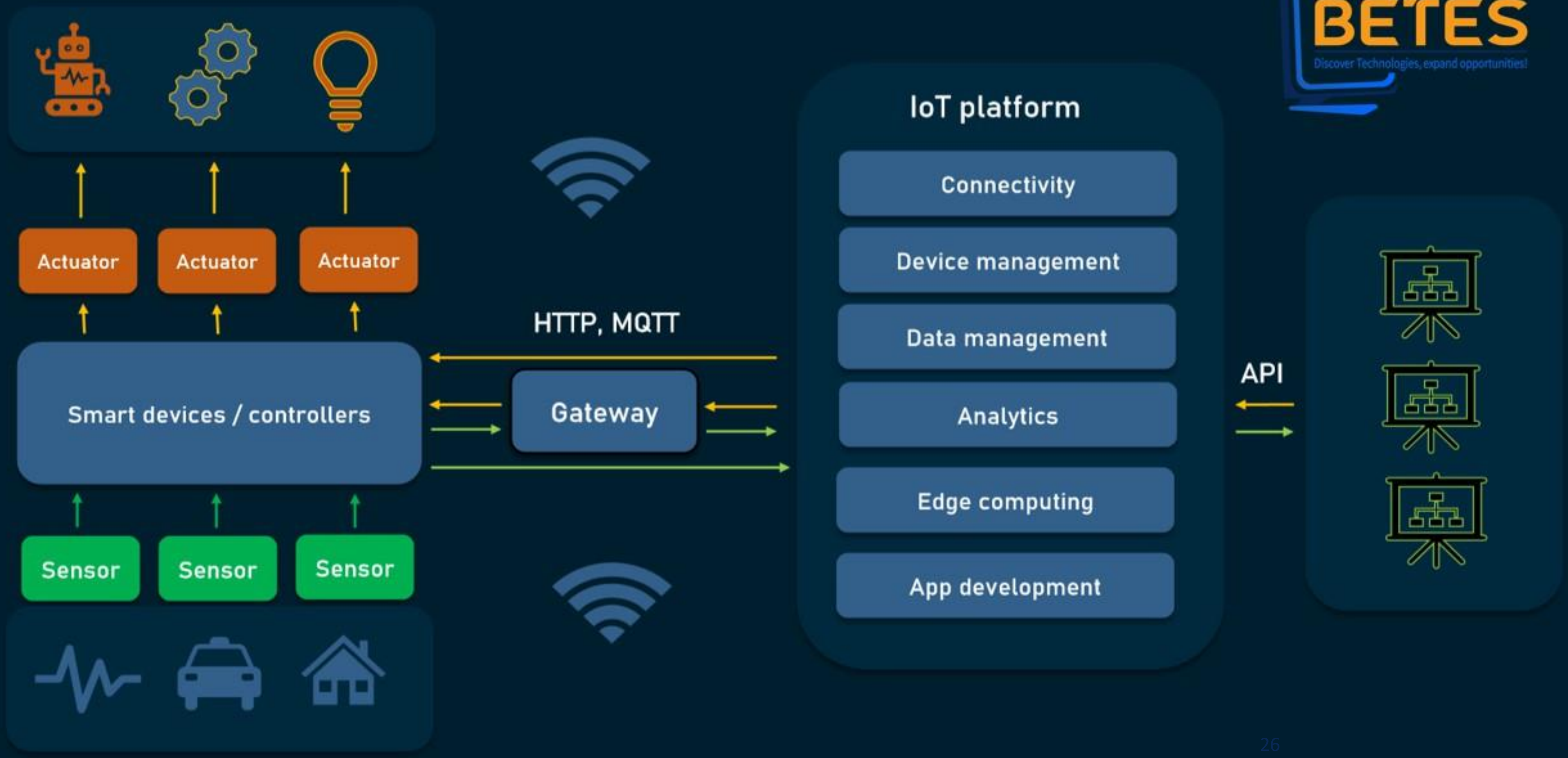
Example of Cloud Computing in IoT



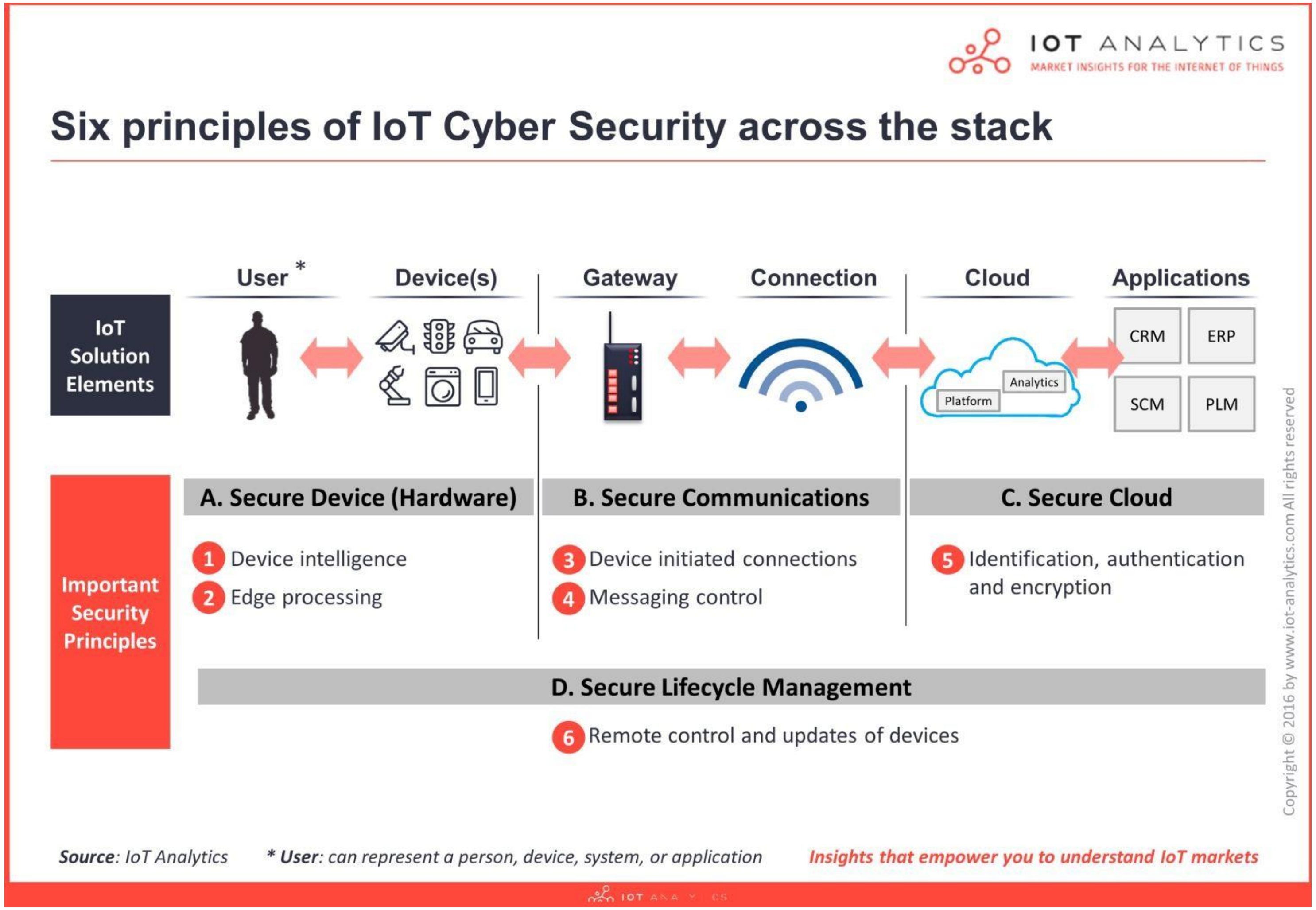
- Smart City Infrastructure
  - Cloud-based platforms managing data from various city sensors (traffic, pollution, energy)
  - Data analysis for urban planning and real-time public service adjustments
- Healthcare Monitoring Systems
  - Cloud platforms aggregating patient data from wearable devices
  - Remote monitoring, predictive analytics for patient care

Co-funded by the European Union

IoT infrastructure



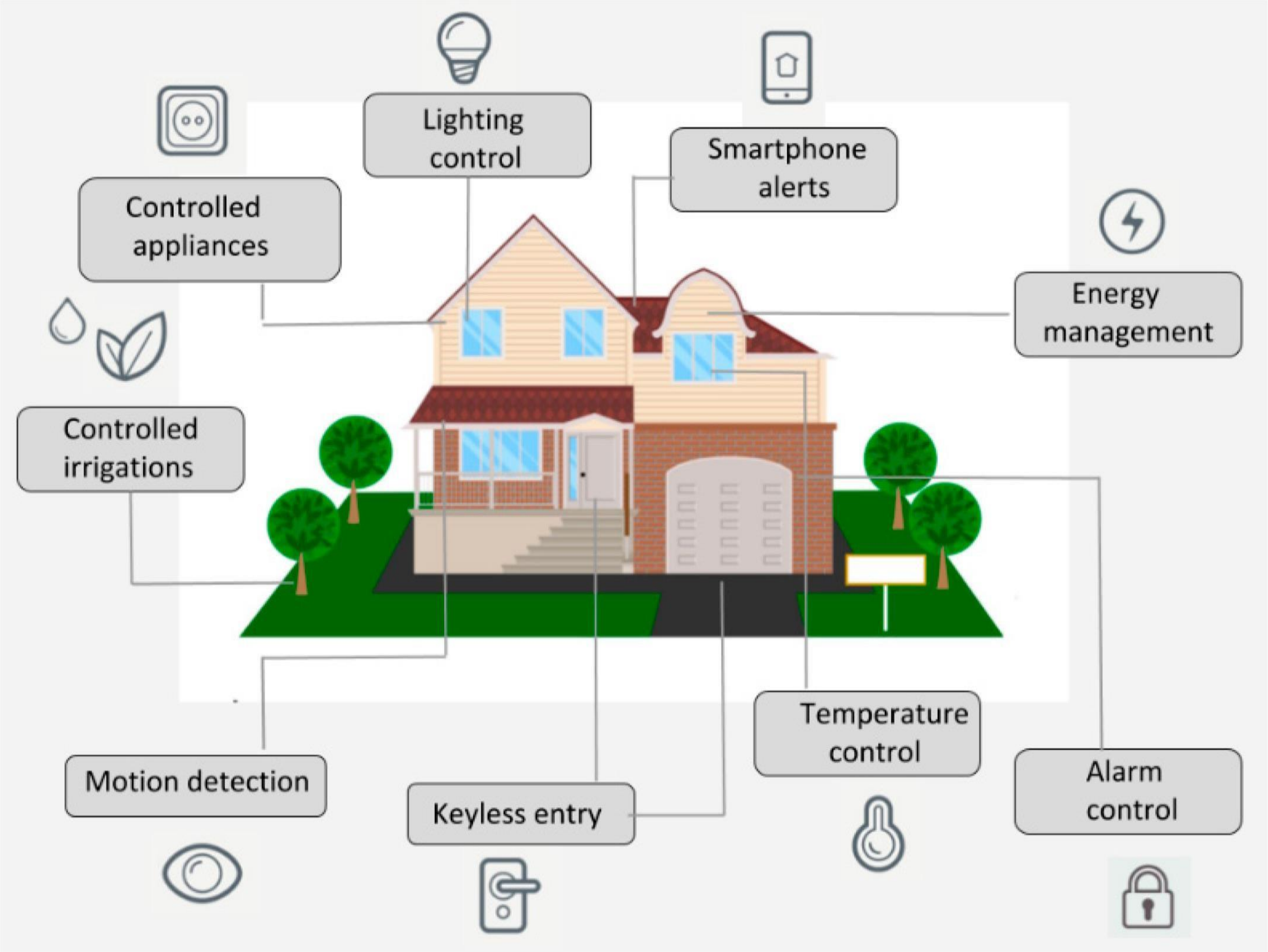
Introduction to IoT Security



- Basic Concepts of IoT Security
- Common Security Challenges in IoT
- Fundamental Security Measures for IoT Devices

Co-funded by the European Union

IoT Case Study: Smart Homes



- Overview of smart home technology
- IoT devices commonly used in smart homes
- Benefits and challenges of smart homes
- Future trends in smart home technology

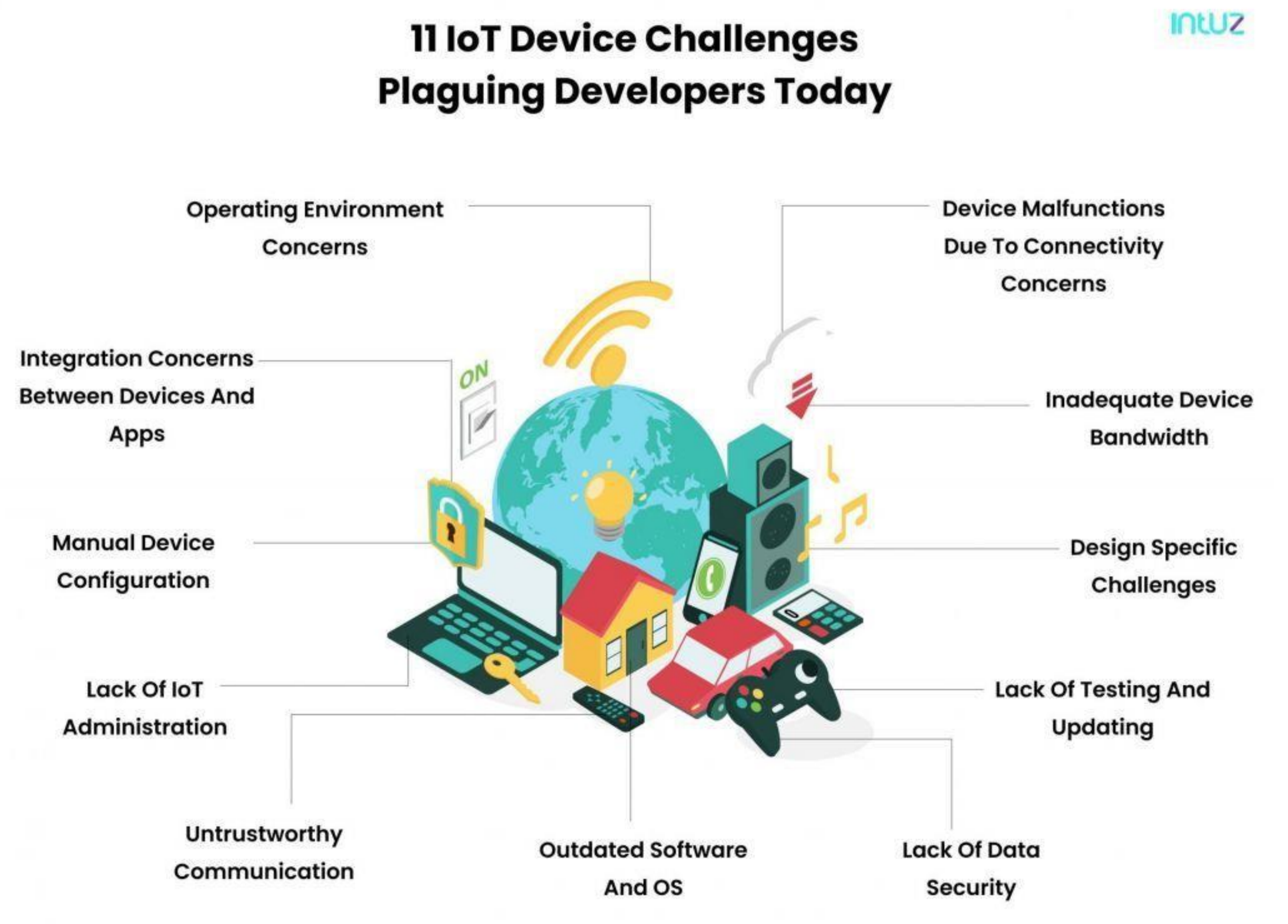
Co-funded by the European Union

IoT Case Study: Wearable Devices

- Types of wearable IoT devices
- Health and fitness tracking
- Wearables in medical monitoring
- Future potential of wearables

Co-funded by the European Union

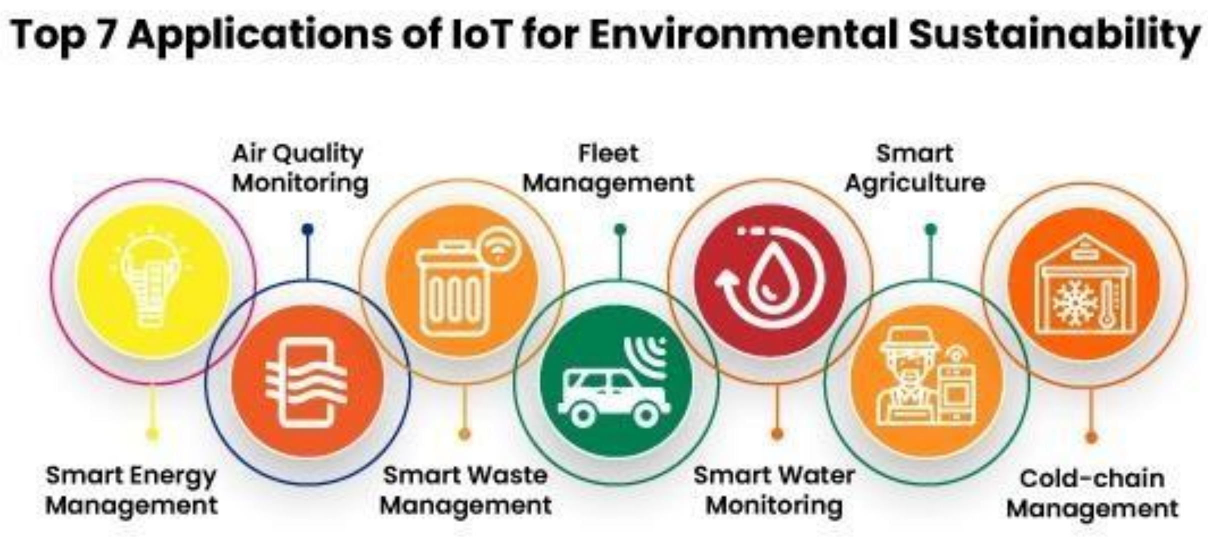
Current Challenges in IoT



- Scalability issues
- Security and privacy concerns
- Interoperability between devices
- Energy management and sustainability

Co-funded by the European Union

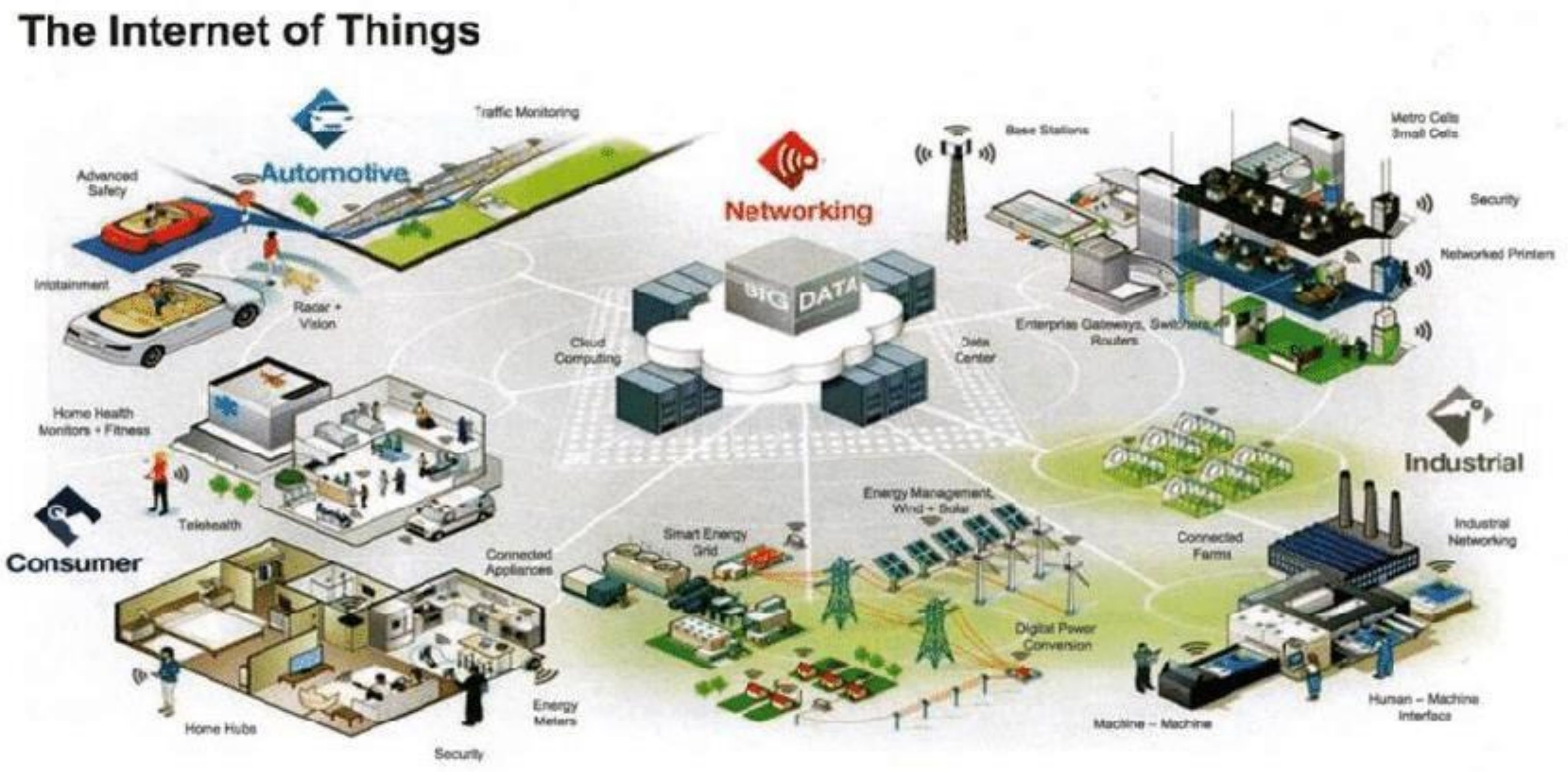
IoT and Environmental Impact



- IoT for environmental monitoring
- Energy efficiency and IoT
- IoT in waste reduction
- Challenges: e-waste and resource consumption

Co-funded by the European Union

IoT and Society

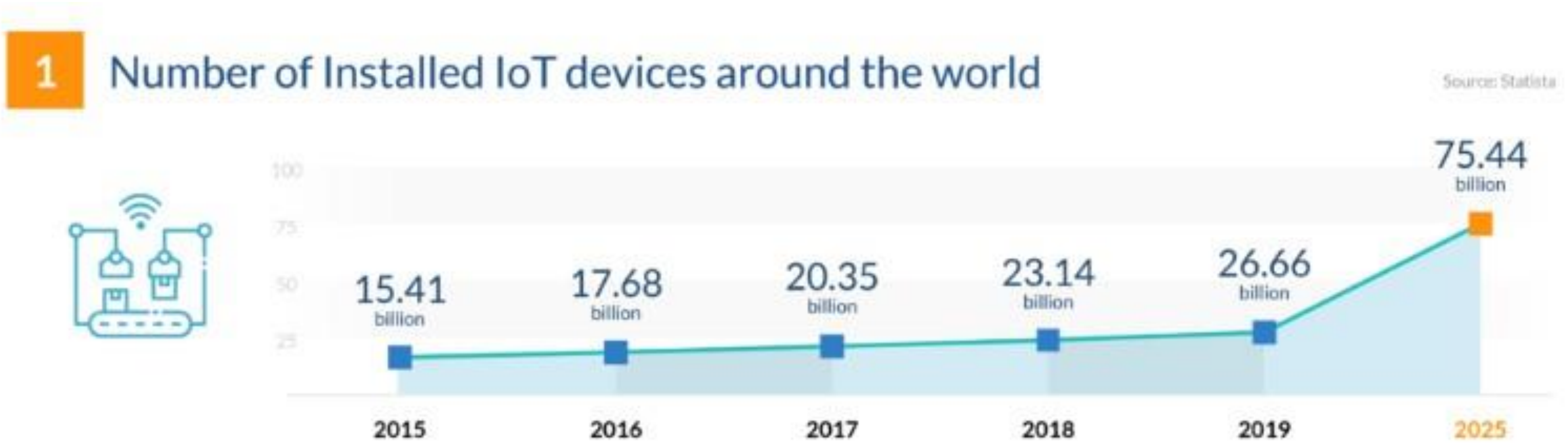


- IoT's role in societal change
- Ethical considerations of IoT
- IoT in education and workforce development
- Bridging the digital divide with IoT

5G use cases


FACTORIES OF THE FUTURE
1 Time-critical process control
2 Non time-critical factory automation
3 Remote control
4 Intra/Inter-enterprise communication
5 Connected goods
ENERGY
1 Grid access
2 Grid backhaul
3 Grid backbone
e-HEALTH
1 Assets and interventions management in Hospital
2 Robotics
3 Remote monitoring
4 Smarter medication
24h
MEDIA & ENTERTAINMENT
1 Ultra High Fidelity Media
2 On-site Live Event Experience
3 User/Machine Generated Content
4 Immersive and Integrated Media
5 Cooperative Media Production
6 Collaborative Gaming
AUTOMOTIVE
1 Automated driving
2 Share My View
3 Bird's Eye View
4 Digitalization of Transport and Logistics
5 Information Society on the road

Future Predictions for IoT

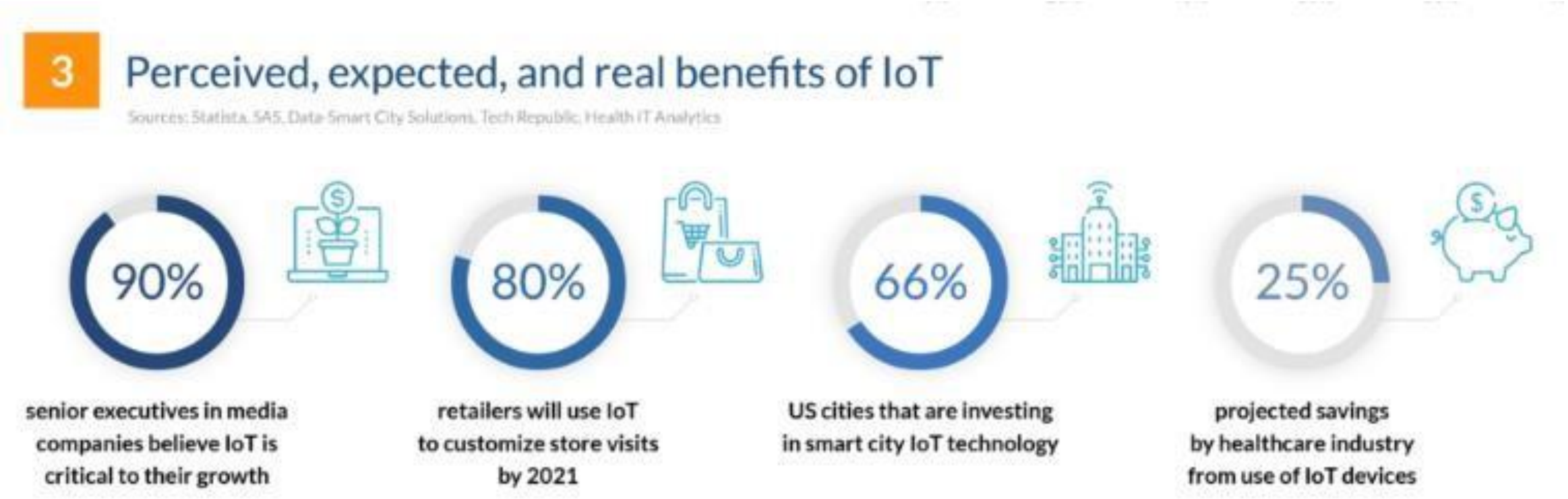


Co-funded by the
European Union

Future Predictions for IoT

Co-funded by the European Union

Future Predictions for IoT



Co-funded by the European Union

Bootcamps for Emerging Technologies and essential Skills

BETES
Discover Technologies, expand opportunities!

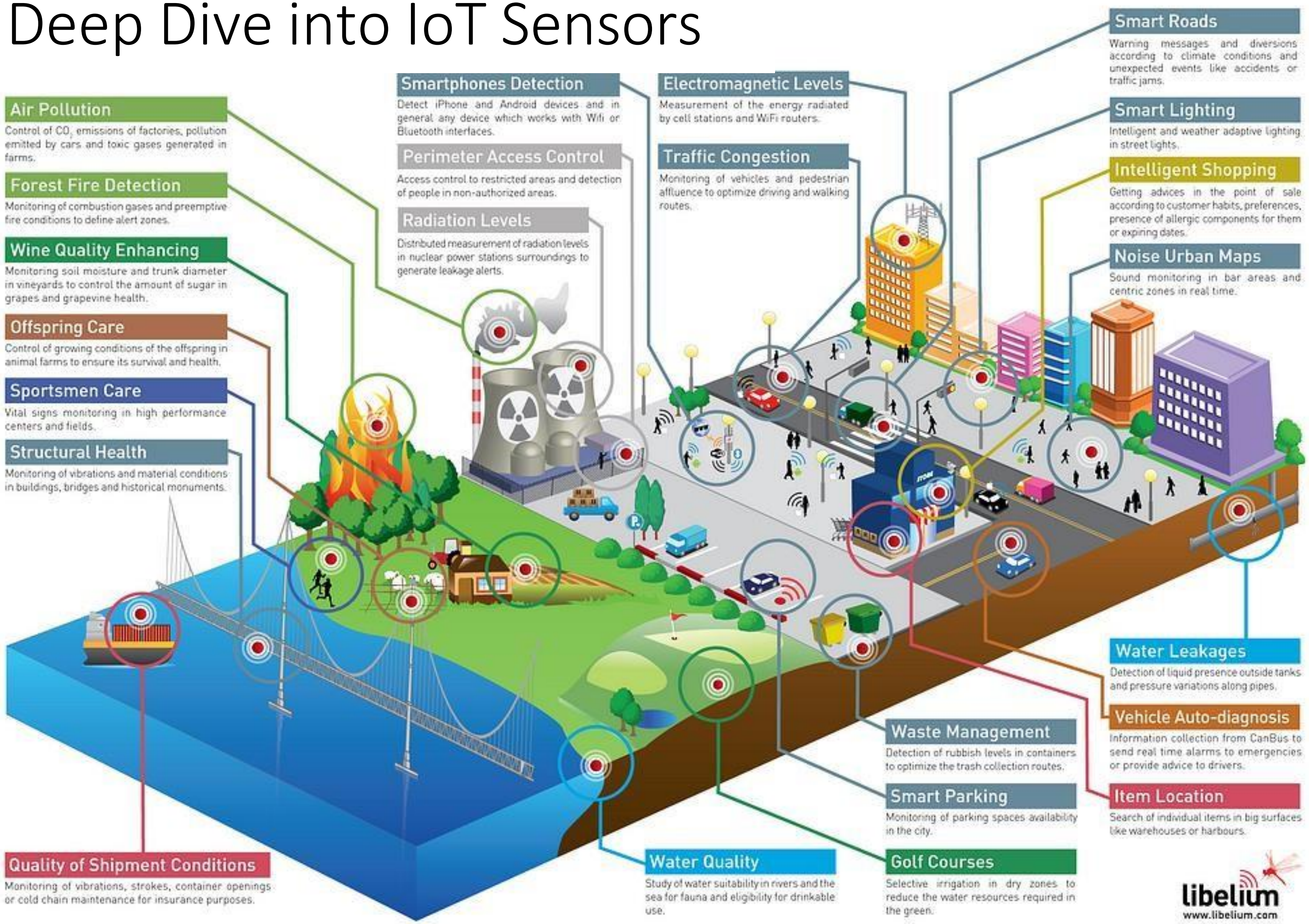
Internet of Things

IoT Technologies and Infrastructure

Developed by: ECECT

Co-funded by the European Union

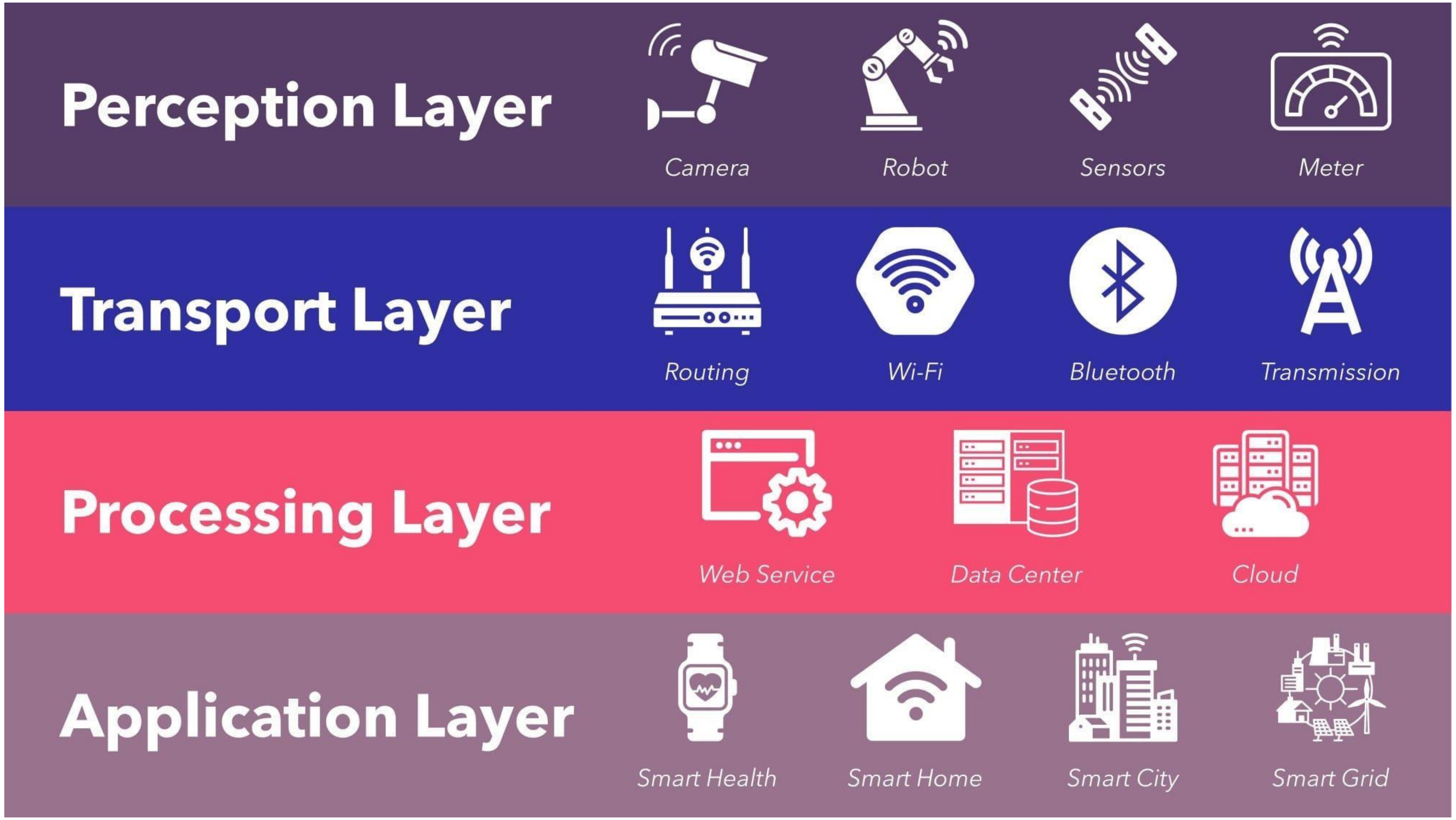
Deep Dive into IoT Sensors



- Types of sensors used in IoT
- Sensor capabilities and data collection
- KPIs – Key Performance indicators
- Distance, frequency, availability, cost, bandwidth, power requirements, network availability

Co-funded by the European Union

Building IoT Architectures



Key components of IoT architecture

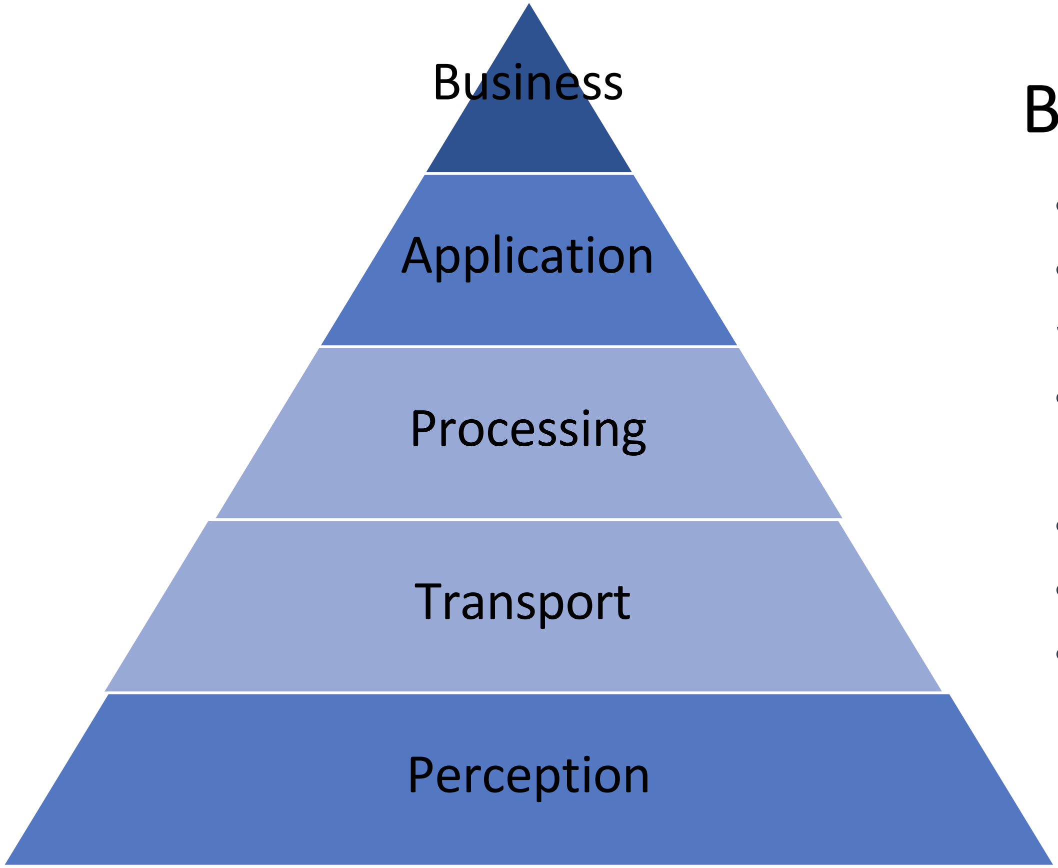
- **Devices/Things/Perception Layer:** These are physical objects embedded with sensors, software, and other technologies to collect and exchange data.
- **Connectivity/Transport Layer:** The means by which data is collected from devices and sent to the cloud. It can be via cellular, satellite, WiFi, Bluetooth, or LPWAN.
- **Data Processing:** Once the data gets to the cloud, software performs processing on the acquired data.
- **Application Layer/ User Interface:** The interface through which users can access information. It might be a web dashboard displaying data analytics results.

Action Management: Devices take automated actions based on the insights derived from analytics on collected data.

Security: Security protocols are essential to protect information sharing and privacy.

Co-funded by the European Union

Five Layers

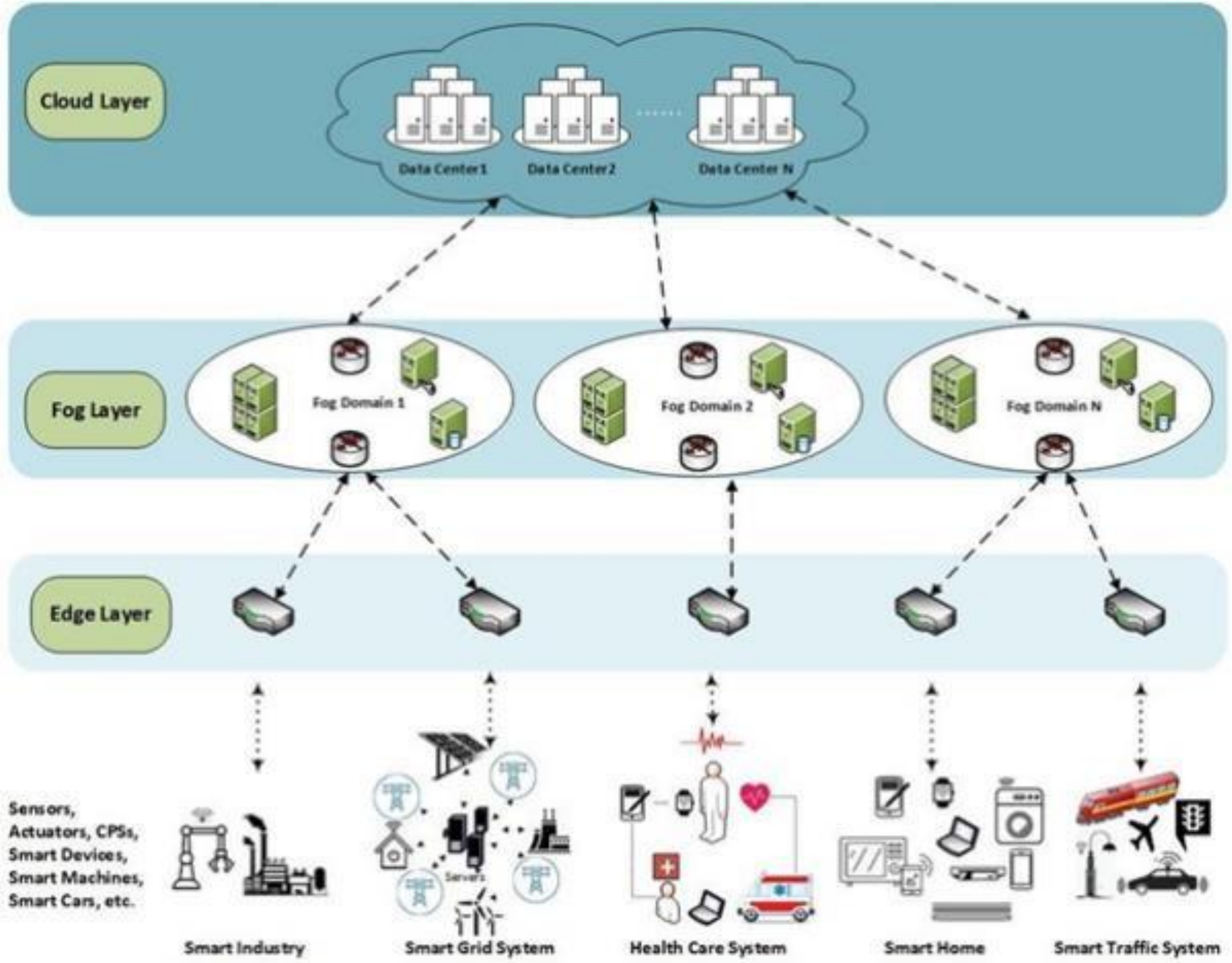


Business layer

- Business logic and rules for IoT system behavior.
- Responsible for setting the system's overall objectives, workflows, and policies.
- Uses data processed by other layers for actionable insights and decision-making.
- Aligns IoT operations with broader business goals.
- Translates IoT data into tangible business value.
- Crucial for enterprises to improve processes, enhance customer experiences, and generate new revenue through IoT solutions.

Co-funded by the European Union

EDGE/FOG/CLOUD layers



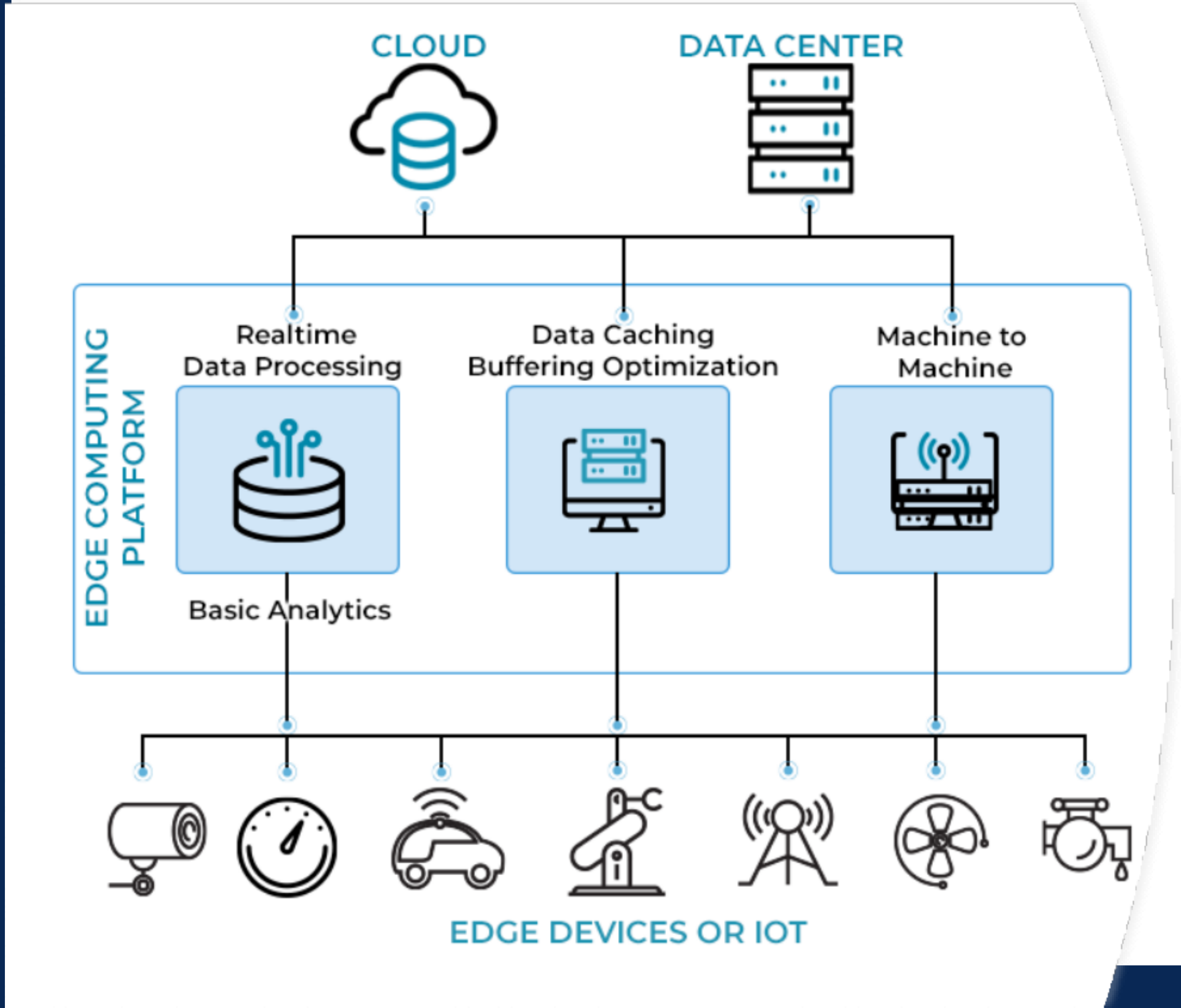
Example of a common IoT architecture

- Edge + Cloud computing
- Importance of scalable architecture

Co-funded by the European Union

Edge Computing in IoT

Edge computing represents a shift in data processing, bringing computation closer to the source of data.



Localized Data Processing: Edge computing involves processing data near the data source or at the network edge, rather than relying solely on a central data-processing warehouse.

Reduces Latency: By processing data closer to where it's generated, edge computing significantly reduces latency and improves response times.

Advantages

Bandwidth Optimization: Minimizes the amount of data that needs to be sent over the network, reducing bandwidth usage.

Improved Performance: Enhances the performance of applications by processing data locally, leading to faster insights and actions.

Reduced Server Load: Decreases the load on central servers, which can improve efficiency and reduce costs.

Applications in IoT

Real-Time Processing: Ideal for IoT applications requiring real-time analysis and decision-making.

Autonomous Operations: Supports autonomous systems like self-driving cars, where immediate data processing is crucial.

Edge computing represents a shift in data processing, bringing computation closer to the source of data. : Useful in remote industrial, agricultural, or infrastructure monitoring where

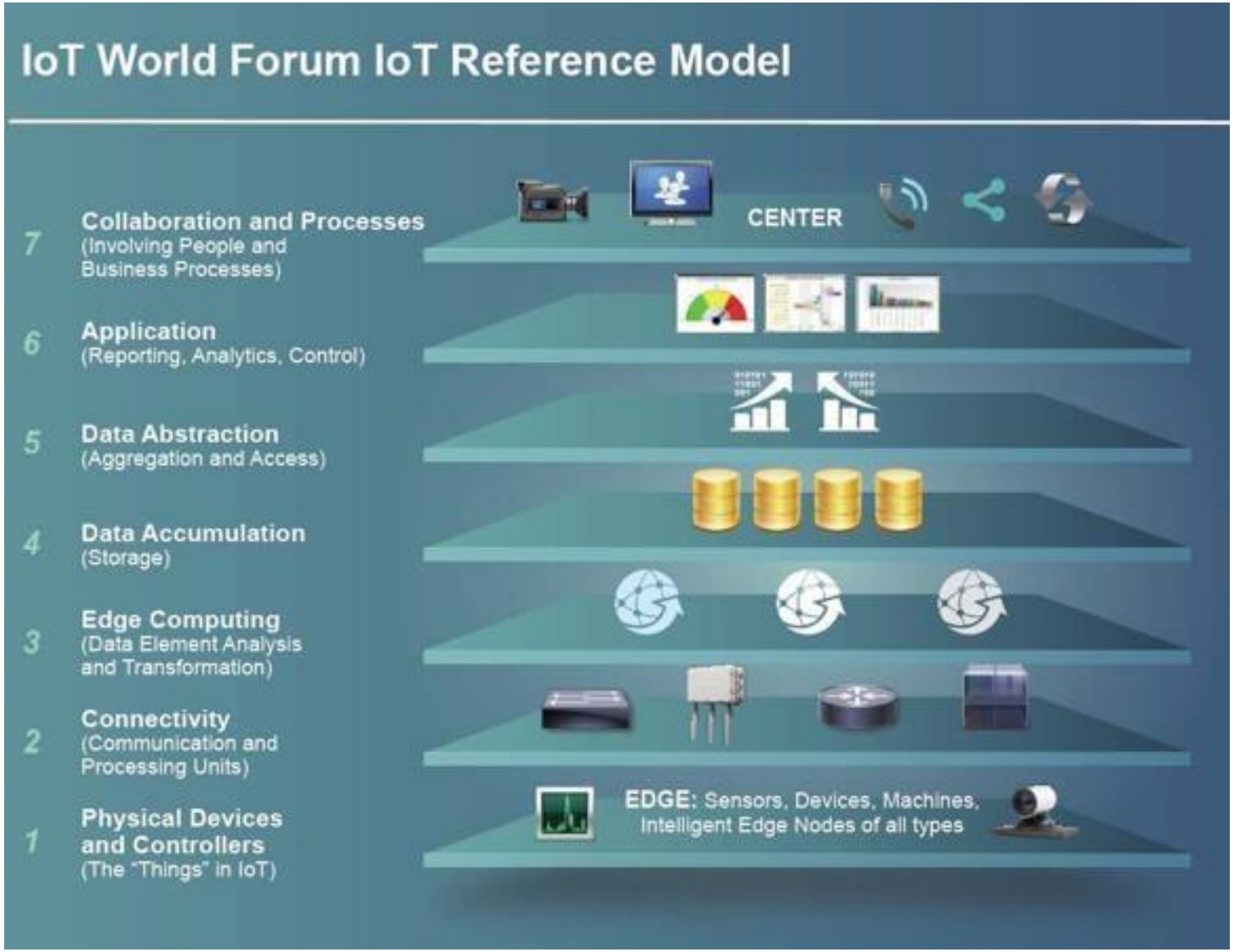
Co-funded by the European Union

SIX LAYERS

1. **IoT devices.** The layer of devices includes not only connected items but also any supplementary hardware like connectors, Internet gateways, power blocks and so on. In other words, this layer is all about hardware and nothing else.
2. **Edge computing. The main principle behind this concept is bringing data sources as close as possible to the connected devices. Imagine your data cloud as a real cloud in the sky. Do you see the edges of this cloud? That is where data nodes are located to make sure that data goes to IoT devices faster and safer. Beyond a doubt, those nodes have to be a separate layer in the IoT architecture.**
3. **Connectivity and data transport.** It is somewhat similar to network layer but it specifically aims at moving data back and forth between layers while the network layer's scale is connection of the IoT system to backend services.
4. **IoT platforms.** Modern IoT platforms usually exist in clouds, where the whole IoT stack assembles together. That's why the main purpose of IoT platforms is to connect data, IoT devices, and applications in one efficient system
5. **Data management.** Your IoT system needs to do a lot of things with data. Gathering, storage, modeling according to business logic, sorting, and other processes require a special attention and a separate layer for them.
6. **Application.** Application means application, and we've already discussed it.

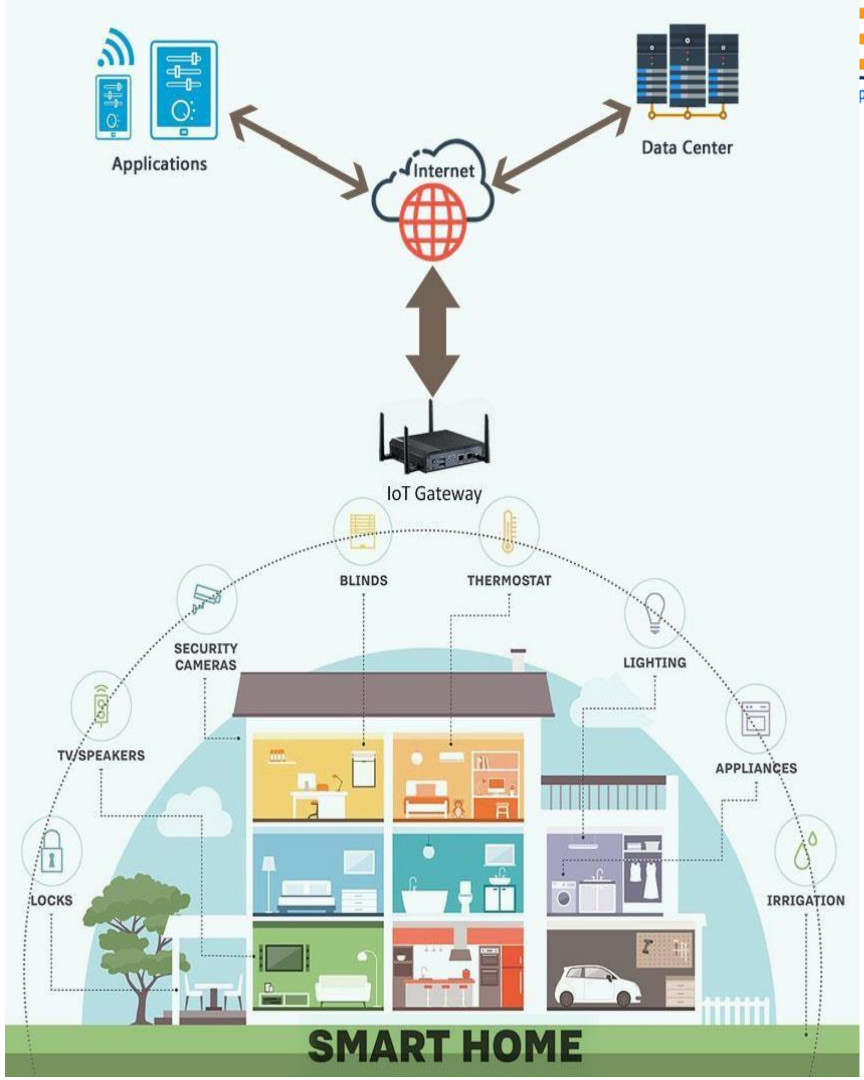
Co-funded by the European Union

SEVEN LAYERS



Co-funded by the European Union

Typical Smart home IoT Architecture example



Funded by the Erasmus+ Programme of the European Union

Co-funded by the European Union

Typical IoT/networking Topologies

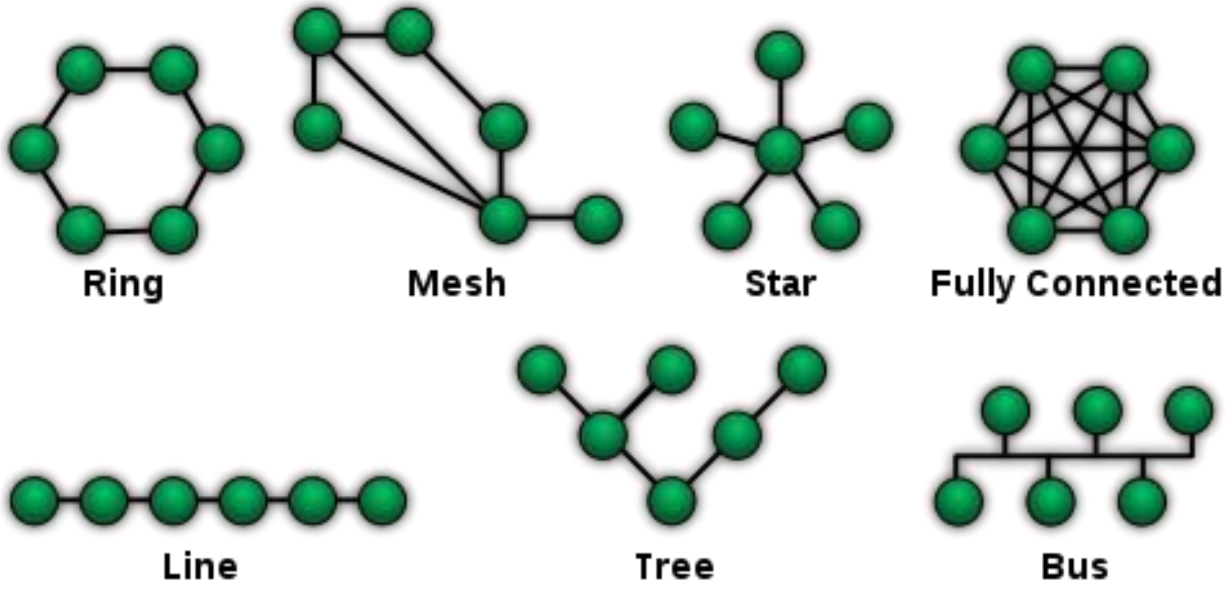
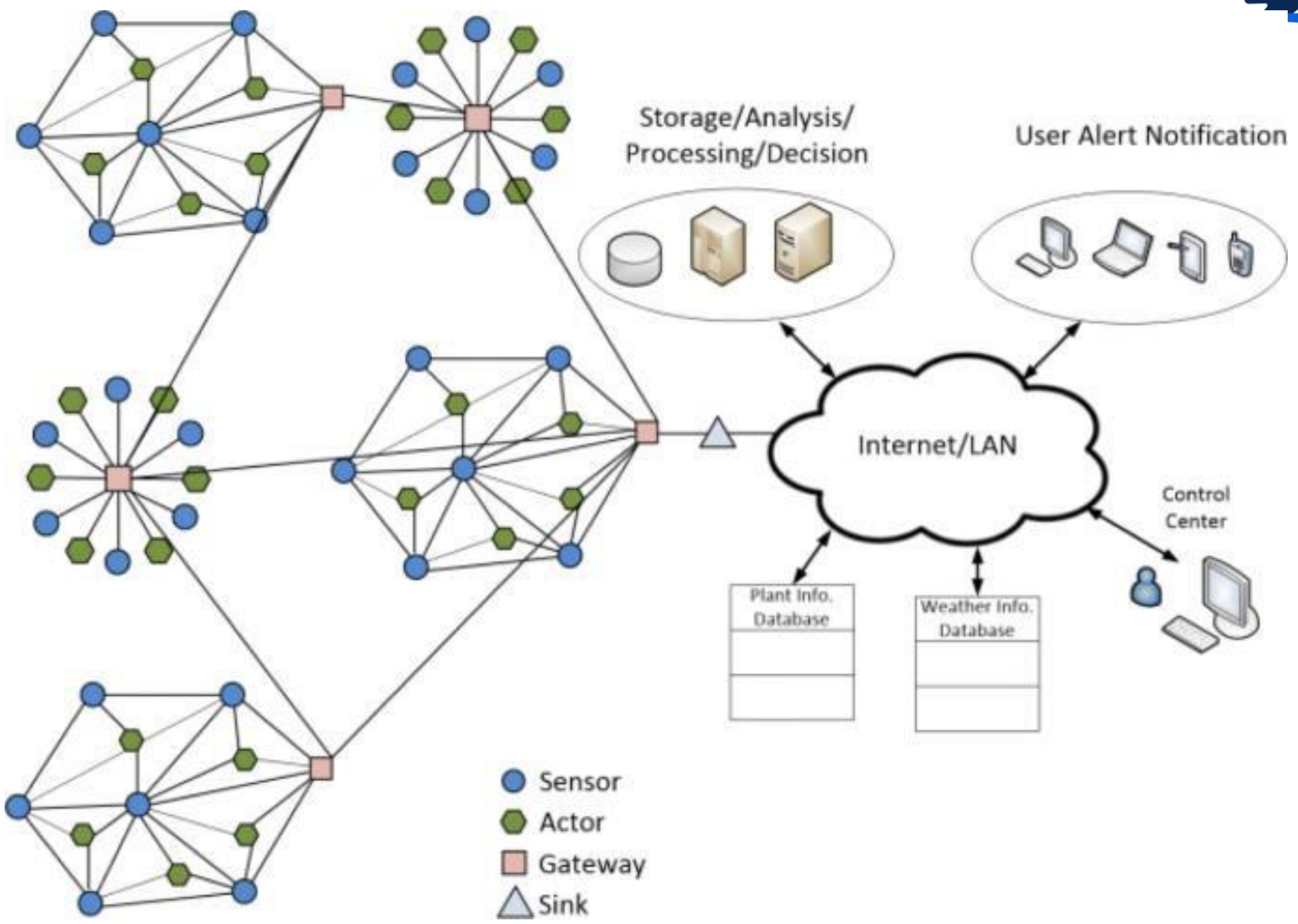


Image used courtesy of [ITPRC]

Co-funded by the European Union

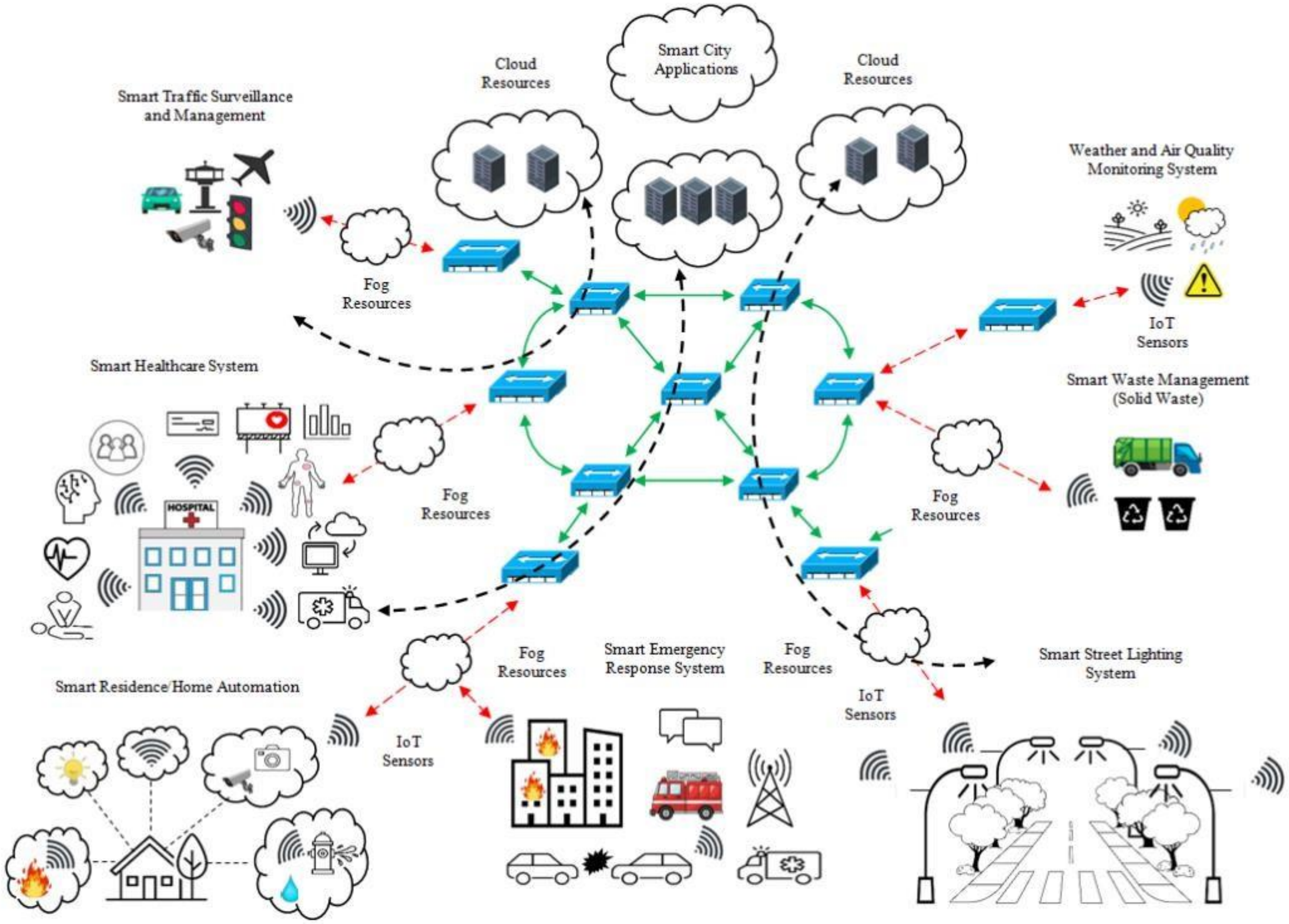
Typical for smart city



Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
European Union

SMART CITY / example



- Traffic
- Healthcare
- Home automation
- Waste management
- Weather
- Smart street lighting
- Emergency response

Building IoT Architectures (1)

- **Scalability and Flexibility**
  - Accommodate growth in devices and data.
  - Adapt to evolving technologies and needs.
- **Security and Privacy**
  - Robust measures for device, data, and network security.
  - Address privacy concerns, especially for consumer data.
- **Interoperability and Standards**
  - Smooth integration with diverse devices and systems.
  - Adherence to established IoT standards and protocols.
- **Data Management and Analytics**
  - Effective handling and analysis of large data volumes.
  - Extract actionable insights from IoT data.
- **Reliability and Availability**
  - Ensure continuous operation and fault tolerance.
  - Support critical functions dependably.

Co-funded by the European Union

Building IoT Architectures (2)

- **User Experience and Usability**
    - Focus on intuitive interfaces and meaningful information.
    - Ensure ease of use for end-users.
- **Energy Efficiency**
    - Design for low-power operation.
    - Consider energy harvesting technologies.
- **Cost-Effectiveness**
    - Balance initial deployment and ongoing operational costs.
    - Consider total cost of ownership.
- **Regulatory Compliance**
    - Adhere to data protection and industry-specific regulations.
    - Avoid legal and ethical issues.
- **Network Connectivity and Protocols**
    - Choose suitable connectivity options (Wi-Fi, Bluetooth, etc.).
    - Opt for appropriate communication protocols.

Co-funded by the European Union

Building IoT Architectures (3)

- **Integration with Existing Systems**
  - Seamless integration with current infrastructure.
  - Leverage existing investments.
- **Future-Proofing**
  - Design with emerging technologies in mind.
  - Allow for future upgrades and expansions.
- **Environmental Considerations**
  - Account for physical and environmental challenges.
  - Ensure durability and resilience in harsh conditions.

Co-funded by the European Union

Sensors – Key performance indicators (1)

1. Accuracy and Precision

Description: Measures how close the sensor readings are to the actual values and how consistently they can reproduce these readings.

Importance: Critical for ensuring the reliability of data collected by IoT sensors.

2. Response Time

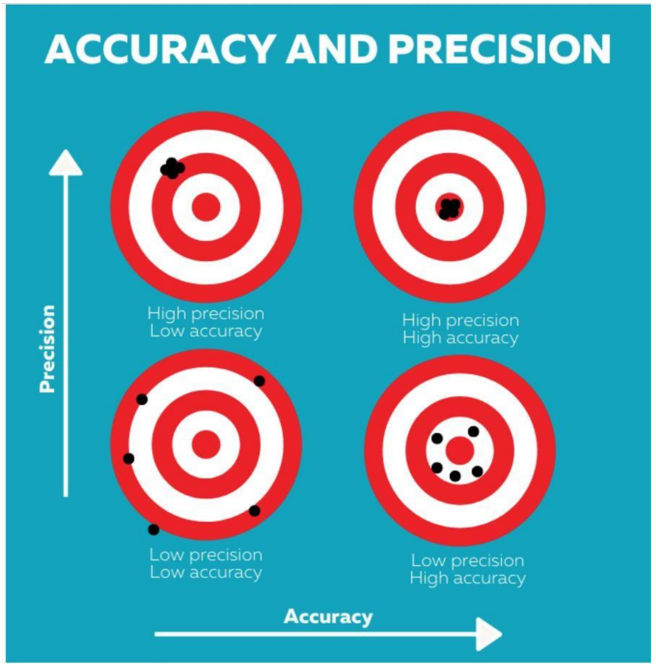
Description: The time it takes for a sensor to respond to a stimulus and provide a reading.

Importance: Essential in applications requiring real-time data, such as safety monitoring systems.

3. Energy Efficiency

Description: The amount of power a sensor consumes to perform its functions.

Importance: Particularly important for battery-powered or energy-harvesting sensors in remote or inaccessible locations.



Co-funded by the European Union

Sensors – Key Performance Indicators (2)

4. Data Transmission Rate

Description: The speed at which the sensor can transmit data to the network or gateway.

Importance: Affects the overall performance of real-time monitoring and control systems.

5. Range and Sensitivity

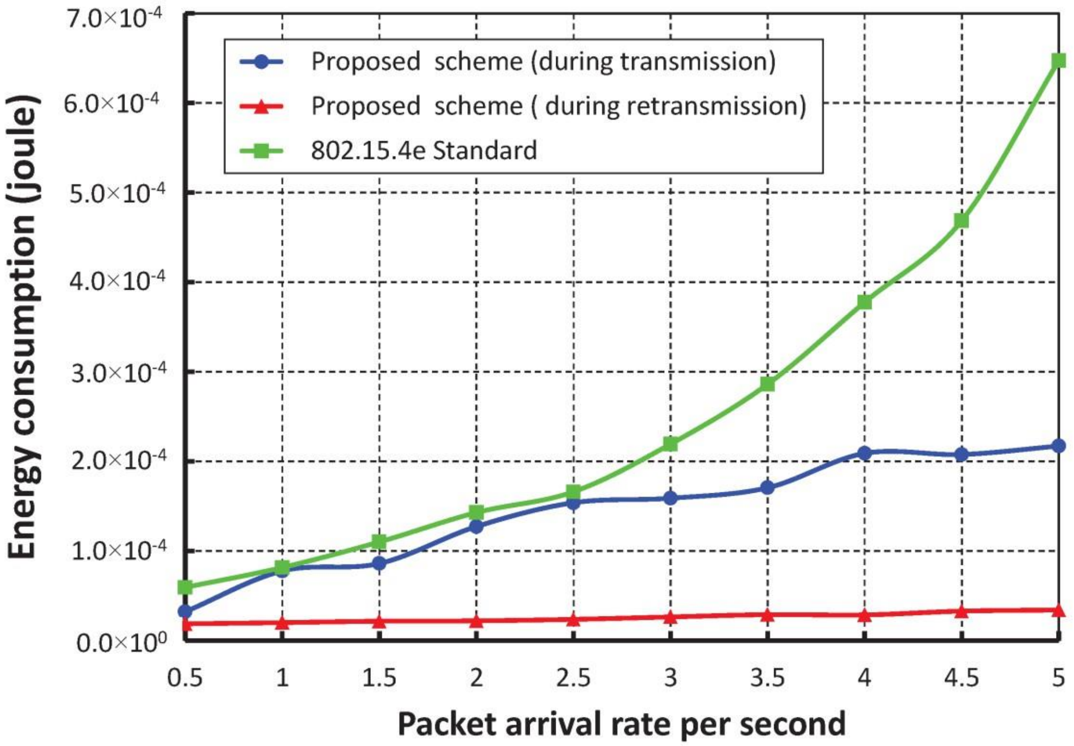
Description: The operational range of the sensor and its ability to detect small or subtle changes.

Importance: Determines the suitability of sensors for specific applications, especially in harsh or challenging environments.

6. Connectivity and Network Reliability

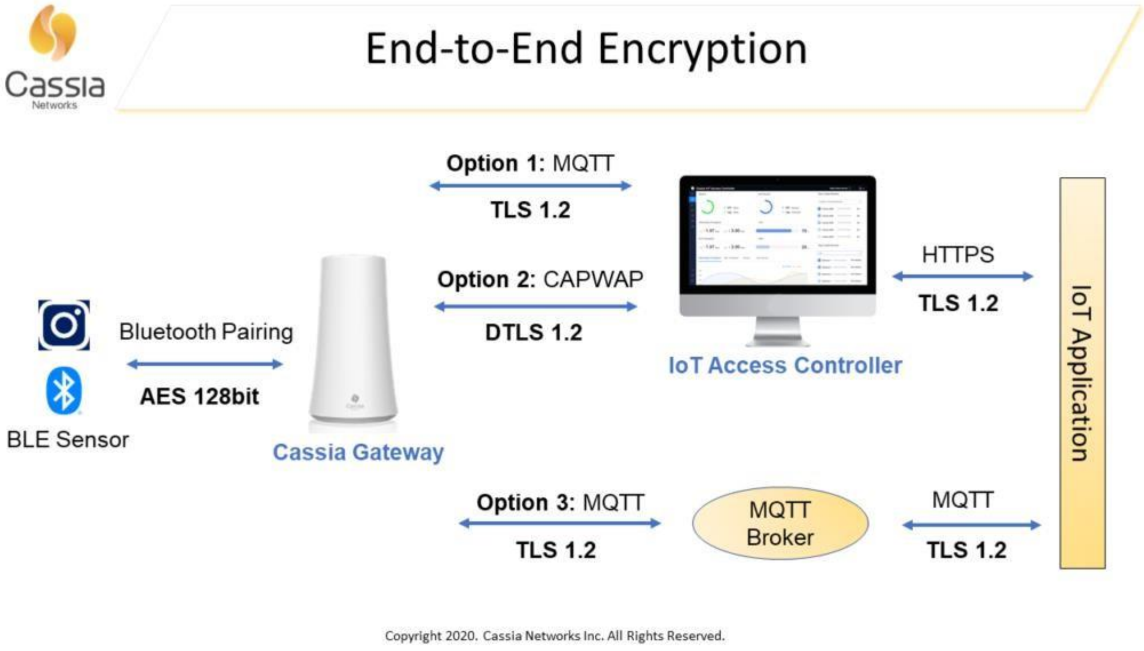
Description: The ability of the sensor to maintain a consistent and reliable connection with the network.

Importance: Ensures uninterrupted data flow and communication within the IoT system.



Co-funded by the European Union

Sensors – Key Performance Indicators (3)



7. Scalability

Description: The ability to integrate additional sensors into the existing network without significant performance degradation.

Importance: Crucial for expanding IoT systems and adding new functionalities.

8. Durability and Maintenance Requirements

Description: The sensor's resistance to wear and tear and the frequency of required maintenance.

Importance: Affects the long-term operational costs and reliability of IoT deployments.

9. Security

Description: The sensor's ability to protect data and resist unauthorized access or tampering.

Importance: Vital for maintaining the integrity and confidentiality of IoT data, especially in sensitive applications.

Co-funded by the European Union

Sensors – Key Performance Indicators (4)

10. Cost-Effectiveness

Description: The overall cost of acquiring, deploying, and maintaining the sensor relative to its benefits.

Importance: Impacts the return on investment (ROI) and economic viability of IoT projects.

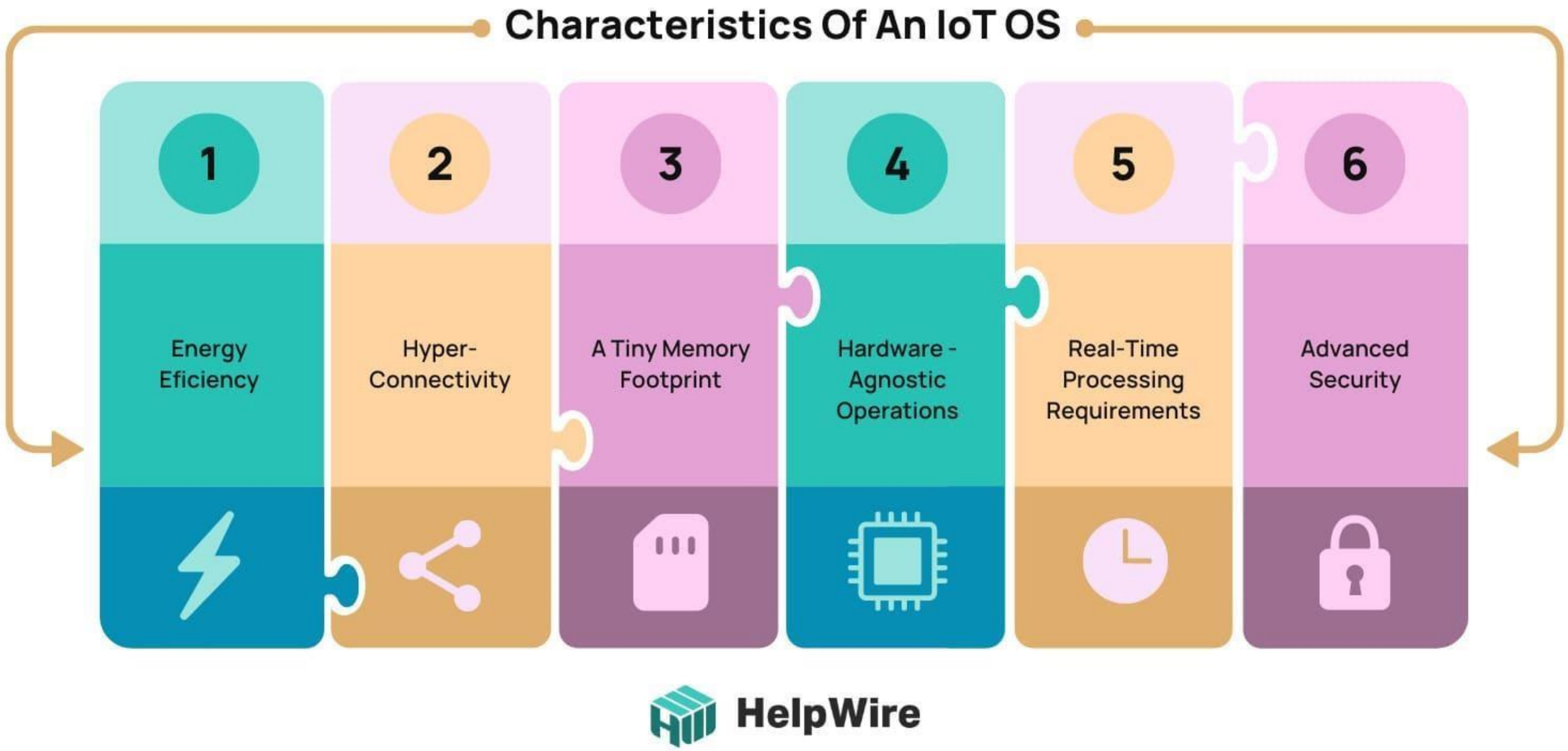
Co-funded by the European Union

IoT Operating Systems

- Overview of operating systems in IoT
- Characteristics of IoT-specific OS

Co-funded by the European Union

IoT Operating Systems



Co-funded by the European Union

IoT Communication protocols / KPIs (1)

- **Speed or Data Rate:** the amount of information to be transmitted within a time duration. It is usually expressed in bps (bits per second), kbps, Mbps, or Gbps.
- **Range:** the maximum distance between two intercommunicating nodes. It mainly depends upon the transmitting power, the frequency band used, and the type of modulation. It can be also affected by the meteorological conditions or the physical placement of the nodes.
- **Power Consumption:** the amount of energy that a node needs to work within its lifetime. This parameter defines the need for permanent power or the use of a battery. Since there are many applications using batteries, thus power consumption is a critical parameter.

Co-funded by the European Union

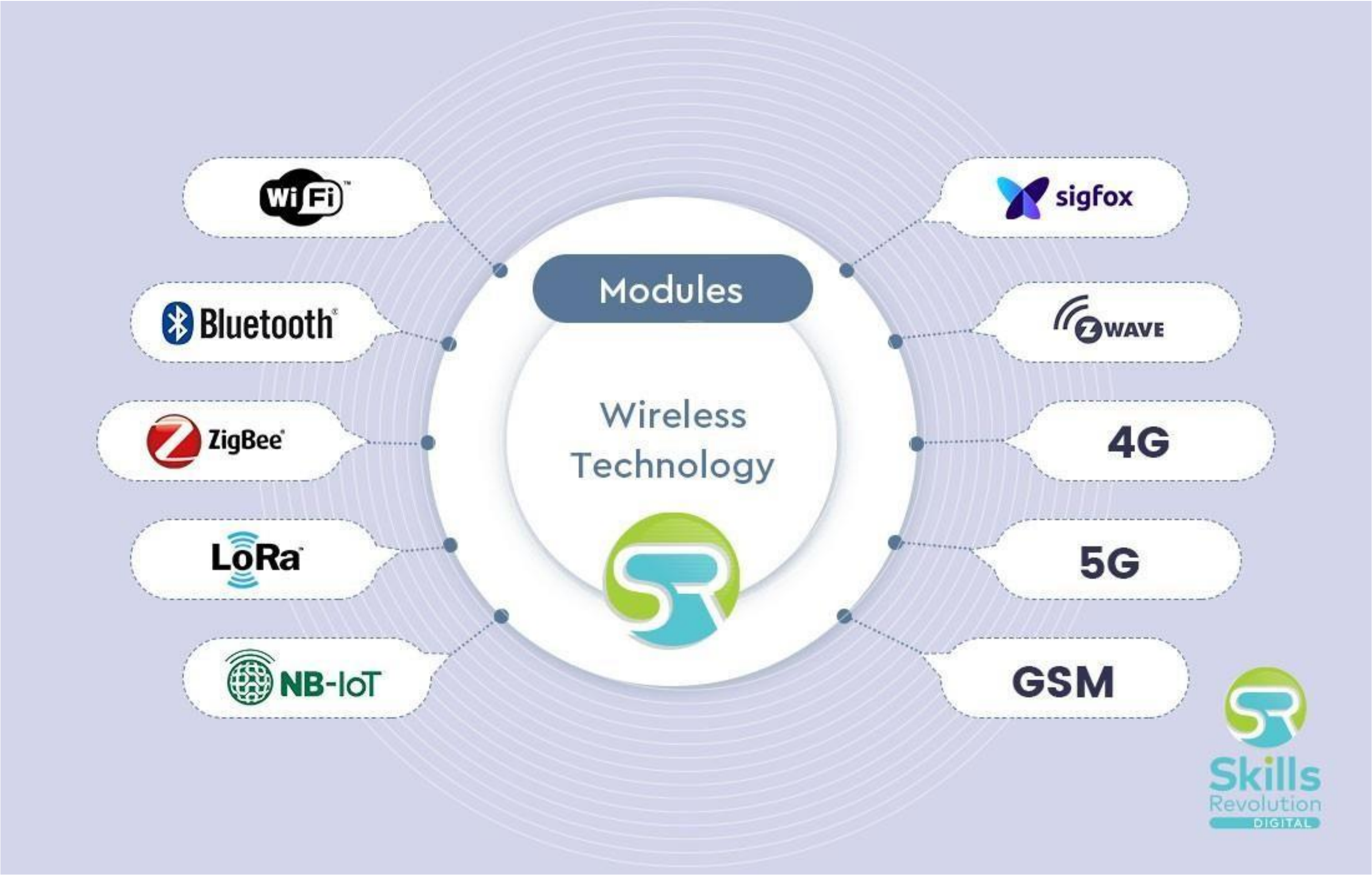
IoT Communication protocols / KPIs (2)

- **Interoperability:** the capability to exchange information between nodes, even if they are of different types.
- **Scalability:** the challenge of deploying a higher number of nodes, increasing the number of end-users, as well as the amount of data to store and process without the need of migrating the technology.
- **Cost:** the price of installing and maintaining a specific technology. Power consumption, maintenance, and scalability have a big impact on the network cost.
- **Network Topology:** the way nodes communicate with each other. Topologies can be the same as those used in traditional networks. Star, mesh, point-to-point, and point-to-multipoint are some examples

Co-funded by the European Union

IoT Connectivity: Beyond Wi-Fi and Bluetooth

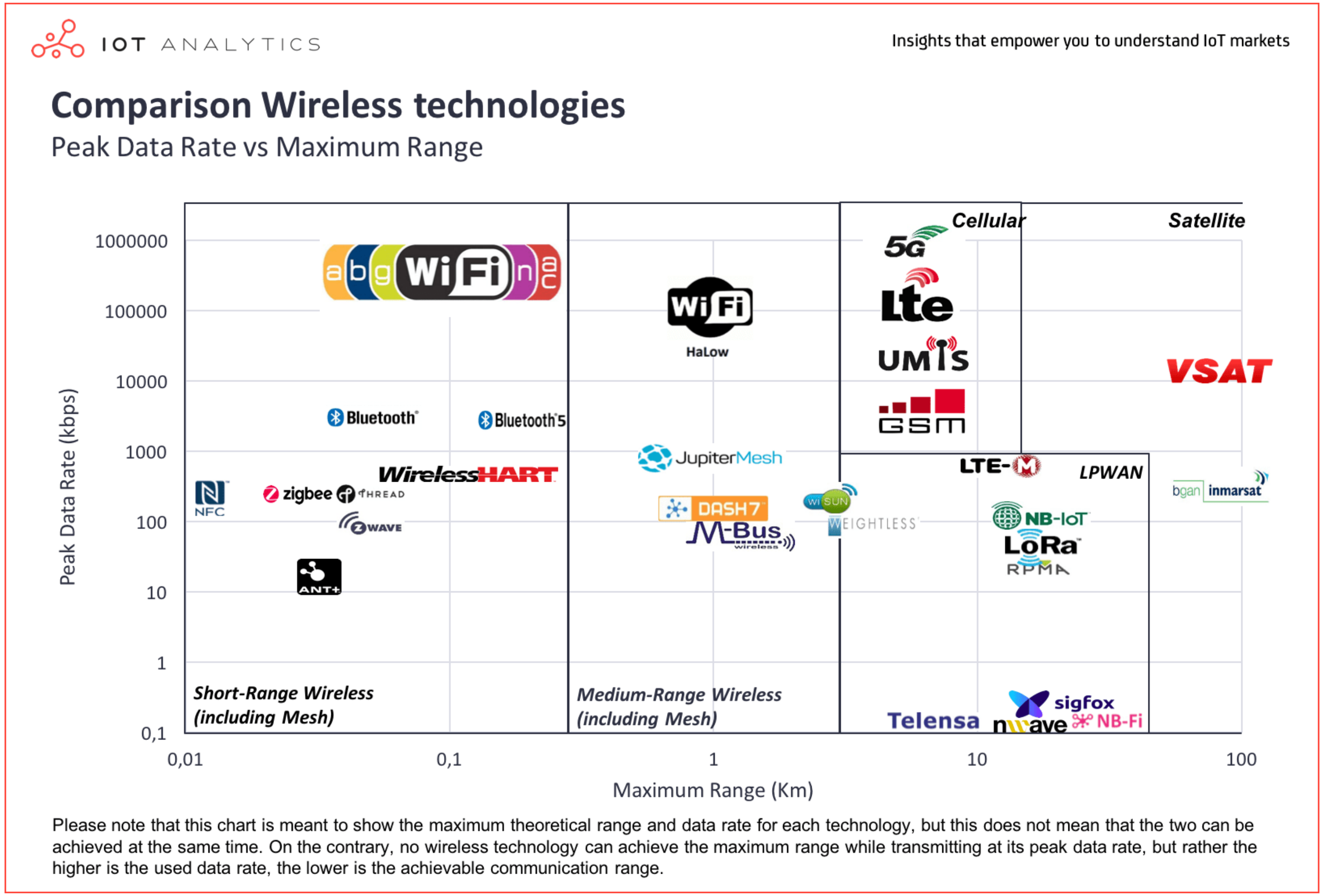
- **WiFi**: A common wireless networking technology that allows devices to communicate over short distances.
- **Bluetooth**: A wireless technology standard for exchanging data over short distances from fixed and mobile devices.
- **ZigBee**: A specification for a suite of high-level communication protocols using small, low-power digital radios.
- **LoRa**: Stands for Long Range, a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology.
- **NB-IoT**: Narrowband IoT, a low power wide area network radio technology standard that enables a wide range of cellular devices and services.
- **Sigfox**: A global network designed to connect low-energy objects to the internet wirelessly.
- **Z-Wave**: A wireless communications protocol used primarily for home automation.
- **4G**: Fourth generation of broadband cellular network technology, succeeding 3G.
- **5G**: The fifth generation of cellular network technology, offering higher speeds and more reliable connections on smartphones and other devices than ever before.
- **GSM**: Stands for Global System for Mobile communications, one of the leading digital cellular systems.



Co-funded by the European Union

IoT Connectivity: Beyond Wi-Fi and Bluetooth

Trade-off Between Range and Data Rate: Wireless technologies demonstrate a balance between communication range and data throughput.
Increased Range Lowers Data Rate: As the distance over which data is transmitted increases, the maximum achievable data rate typically decreases.
Signal Limitations: Wireless signal strengths diminish over distance, affecting the speed and reliability of data transfer.
Power Consumption Concerns: Longer range communications usually require more power, influencing technology selection based on available power sources.
Designing for IoT Applications: The choice of wireless technology for IoT must consider the necessary data rate against the required operational range.
Balancing Throughput and Coverage: Effective IoT deployment involves striking a balance between high-speed data needs and the geographical area covered by the network.



Co-funded by the European Union

Wireless Communication protocols

Zigbee: A low-power, mesh network protocol suitable for home automation and industrial applications.

LoRaWAN: A long-range, low-power protocol for wide-area IoT networks, often used for applications like smart cities and agriculture.

NB-IoT (Narrowband IoT): A cellular technology designed for low-power, wide-area IoT connectivity with better coverage compared to traditional cellular networks.

Sigfox: A proprietary, low-power, wide-area network (LPWAN) technology known for its simplicity and efficiency in transmitting small amounts of data over long distances.

Bluetooth Low Energy (BLE): A low-power wireless communication protocol commonly used in IoT applications, especially for short-range connections between devices and smartphones.

Wi-Fi: Commonly used for high-speed internet access; operates on 2.4 GHz and 5 GHz frequencies.

Co-funded by the European Union

Wireless IoT Communication

Protocol	Optimized for Extended Battery Life	Nominal Range Limit	Typical Data Rate	Spectrum
NFC	✓	Personal (<10m)	2Mbps	ISM 2.4GHz unlicensed
Bluetooth®	✓	Contact (<4cm)	100kbps	ISM 13.56MHz unlicensed
WiFi™	✗	Local (<100m)	>100Mbps	ISM 2.4GHz/5GHz unlicensed
LoRaWAN™	✓	Metro (>10km)	<50kpbs	ISM 900Mhz, 868MHz, 433MHz unlicensed
NB-IoT	✓	Metro (>10km)	200kbps	Licensed cellular
2G | 3G	✗	Metro (>30km)	<2Mbps	Licensed cellular
4G LTE 2600mhz	✗	Metro (>30km)	>100Mbps	Licensed cellular
5G	✗	Metro (>30km)	>10Gbps	Licensed cellular

Co-funded by the European Union

IoT Protocols

IOT ANALYTICS

Your Global IoT Market Research Partner

5 things to know about IoT protocols

1. There is no one-size-fits-all IoT protocol
2. Protocols purpose-made for IoT are seeing increased adoption (CoAP, MQTT, AMQP)
3. Software is becoming more important to managing IoT connectivity
4. "Ease of use" and "reliability" are most important when choosing a new protocol
5. Decision making for IoT protocols has become a multi-stakeholder exercise

Source: IoT Analytics Research 2022, We welcome republishing of images but require source citation with link to original post and company website.

Co-funded by the European Union

MQTT (Message Queuing Telemetry Transport): A lightweight, publish-subscribe protocol designed for low-bandwidth, high-latency, or unreliable networks. It's widely used in IoT for its efficiency.

CoAP (Constrained Application Protocol): Designed for resource-constrained devices and low-power networks, CoAP is an application layer protocol with RESTful principles.

HTTP/HTTPS: The standard web protocols are used in IoT applications, especially for devices that can connect to the internet via Wi-Fi or Ethernet.

AMQP (Advanced Message Queuing Protocol): A messaging protocol that enables efficient and secure communication between IoT devices and cloud-based applications.

Co-funded by the European Union

IoT Protocols

- Overview of networking in IoT
- Different networking technologies and protocols
- Choosing the right technology for your IoT solution

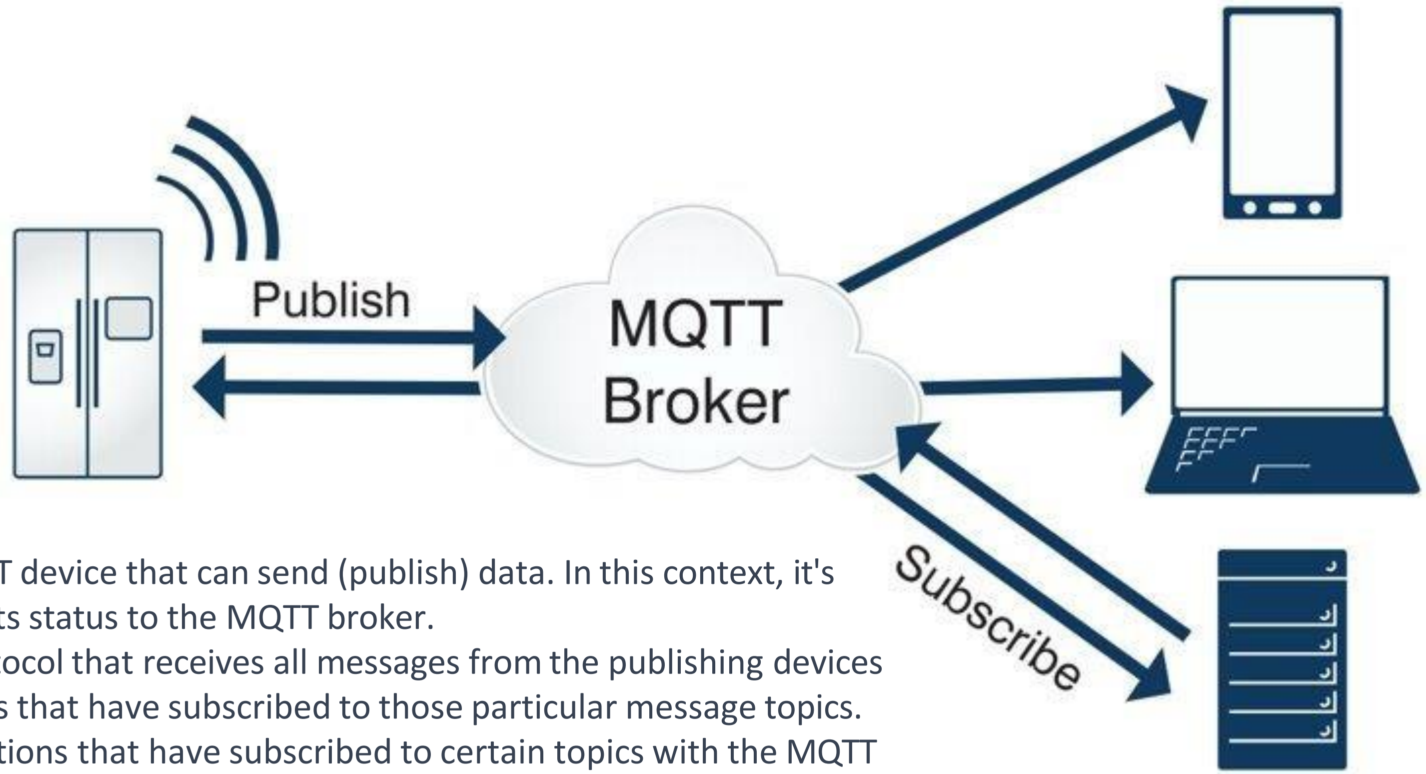
	MQTT	CoAP	AMQP	HTTP
Base protocol	TCP	UDP	TCP	TCP
Paradigm	Publish/Subscribe	Request/Response or Publish/Subscribe	Publish/Subscribe or Request/Response	Request/Response
Header Size	2 Bytes	4 Bytes	8 Bytes	Undefined
Message Size	Small and Undefined (up to 256 MB)	Small and Undefined	Negotiable and Undefined	Large and Undefined
Reliability	QoS 0 - At most once QoS 1 - At least once QoS 2 - Exactly once	CON Message NON Message	Settle Format Unsettle Format	Limited (via TCP)
Standards	OASIS, Eclipse Foundations	IETF, Eclipse Foundation	OASIS, ISO/IEC	IETF and W3C
Licensing	Open Source	Open Source	Open Source	Free

Co-funded by the European Union

IoT Protocols - MQTT

MQTT stands for Message Queuing Telemetry Transport.

It is an extremely simple and lightweight messaging protocol (subscribe and publish) designed for limited devices and networks with high latency, low bandwidth or unreliable networks.



Device with Publish Ability: This represents an IoT device that can send (publish) data. In this context, it's shown as a Fridge with a sensors that publishes its status to the MQTT broker.
MQTT Broker: The central node in the MQTT protocol that receives all messages from the publishing devices and then distributes these messages to any clients that have subscribed to those particular message topics.
Subscribing Devices: These are devices or applications that have subscribed to certain topics with the MQTT broker and will receive updates when new messages are published on those topics. The image shows a smartphone and a laptop as subscribers, which could represent a user receiving a notification when the door opens or a server that logs the door's status.
Database Storage: This is often included in MQTT architectures as a means to store data published to the broker for historical analysis or auditing purposes.

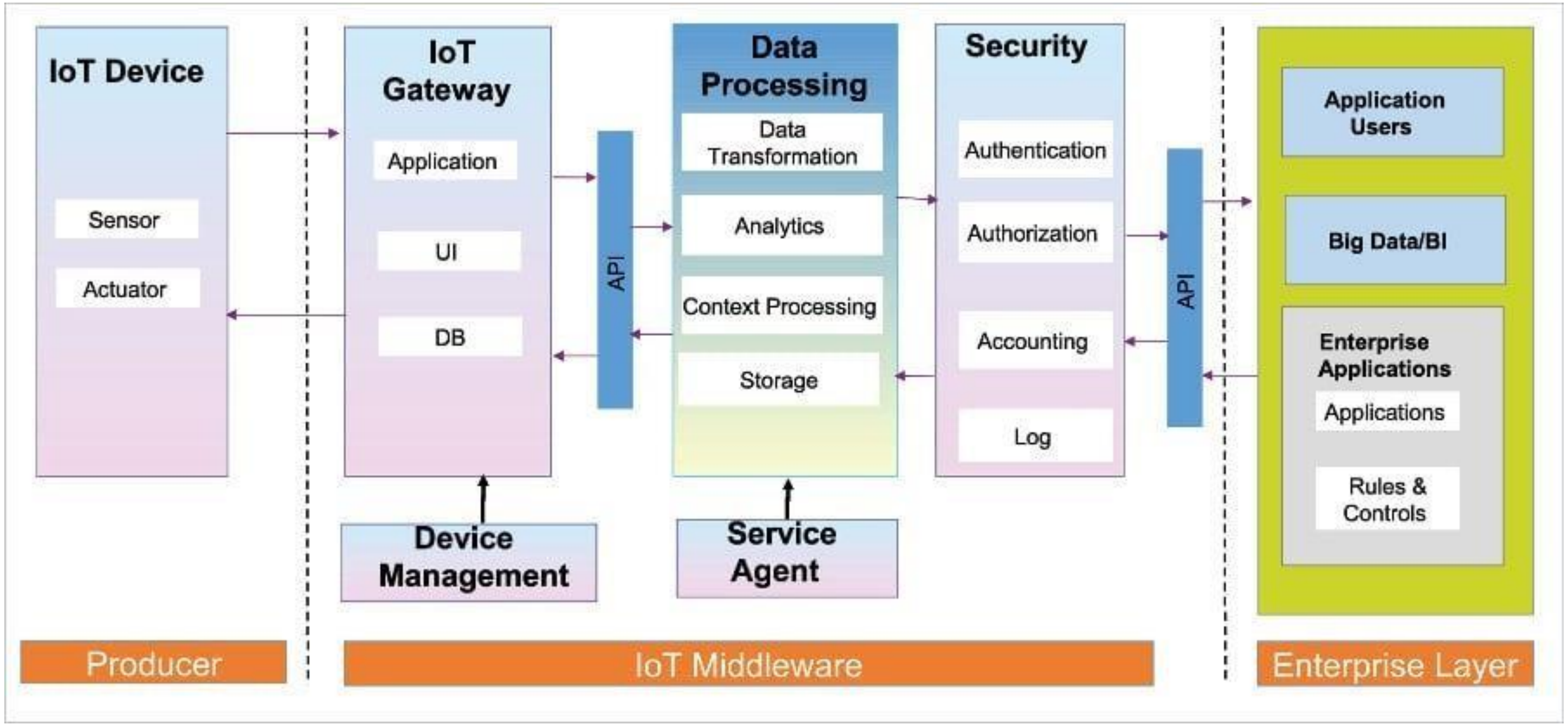
Co-funded by the European Union

MQTT

1. **Lightweight Protocol**: MQTT is designed to be a lightweight protocol with a small code footprint, making it ideal for use in situations where network bandwidth is limited or devices have limited processing power.
2. **Publish-Subscribe Model**: It operates on a publish-subscribe model, where devices publish messages to a central server, called a broker, under topic names. Other devices can subscribe to these topics to receive messages.
3. **Efficient Message Delivery**: MQTT ensures efficient delivery of messages, supporting different levels of Quality of Service (QoS) to guarantee message delivery.
4. **Low Bandwidth Usage**: Due to its lightweight nature, MQTT is suitable for networks with limited bandwidth, such as cellular networks or remote locations.
5. **Reliability in Unstable Networks**: It's designed to work well in unstable network environments, making it a good choice for IoT applications where network connectivity may be intermittent.
6. **Security**: While MQTT itself does not define any security mechanisms, it can be run over secure channels such as TLS/SSL to ensure secure message transmission.
7. **Use Cases**: Commonly used in remote sensing and control applications, home automation, and in scenarios where a small code footprint is required or network bandwidth is at a premium.

Co-funded by the European Union

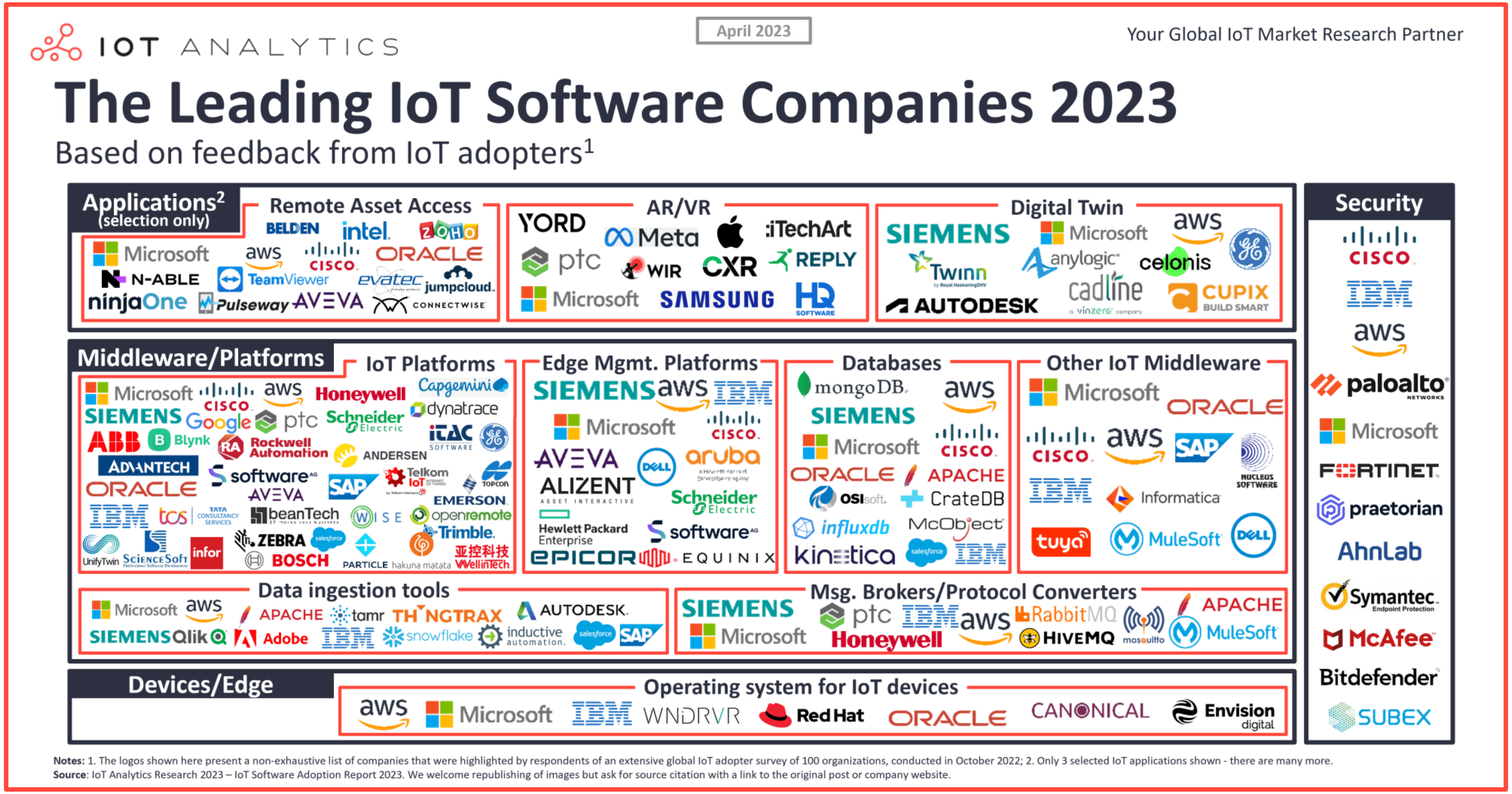
IoT Middleware Solutions



- **Interface**: Provides an interface for the interaction between hardware and software components.
- **Data Processing**: Handles data processing, filtering, and management to convert raw data into actionable insights.
- **Communication Protocols**: Supports various communication protocols to ensure seamless data transfer.
- **Security**: Implements security measures to protect data integrity and privacy.
- **Scalability**: Enables the integration of a growing number of IoT devices without performance degradation.

Co-funded by the European Union

IoT Middleware Solutions

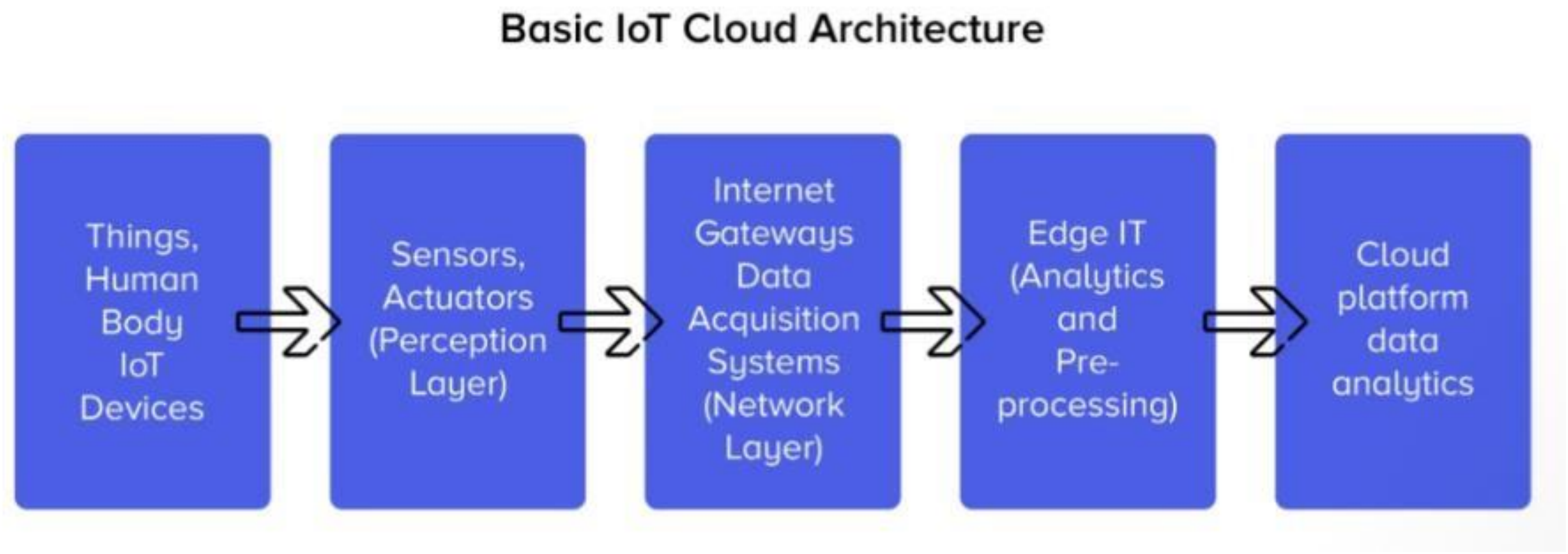


Examples of IoT middleware platforms

- Google IoT
- Microsoft Azure IoT
- IBM Watson
- Amazon services IoT
- Cisco IoT cloud connect

Co-funded by the European Union

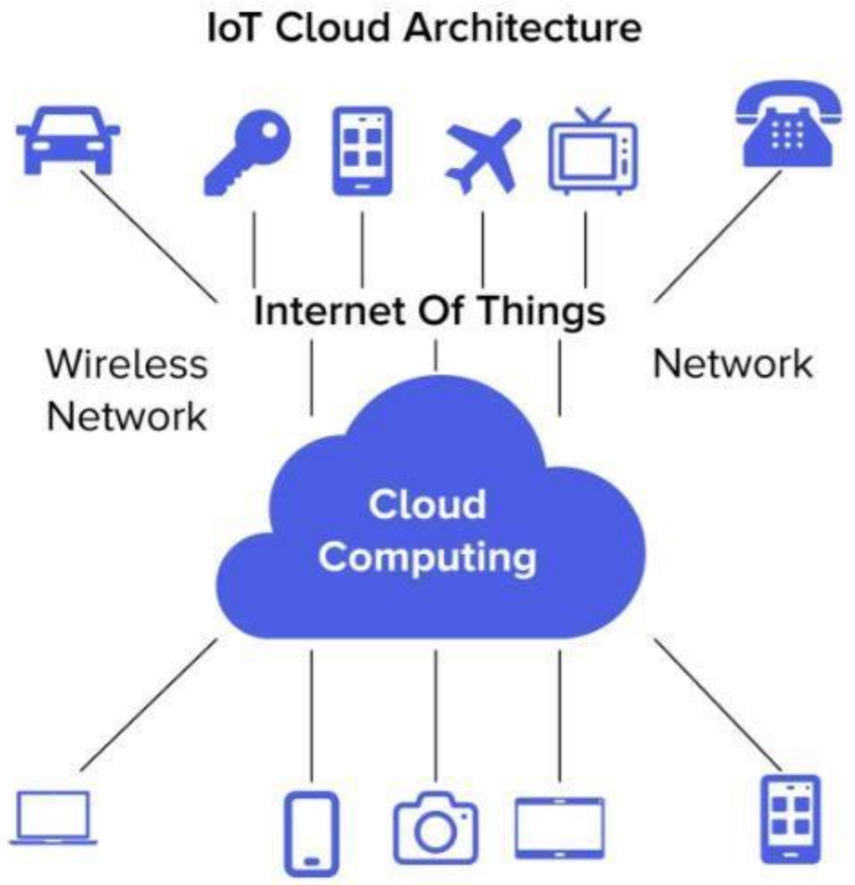
Cloud Computing in IoT



Co-funded by the European Union

Cloud Computing in IoT

- **Centralized Data Storage**: Provides a centralized platform for storing vast amounts of data generated by IoT devices.
- **Advanced Data Processing**: Offers powerful computing resources for complex data processing and analytics.
- **Scalability**: Easily scales to accommodate the growing number of IoT devices and the corresponding increase in data.
- **Device Management**: Facilitates the management and monitoring of a large number of distributed IoT devices.



Co-funded by the
European Union

Cloud Integration in IoT

Enhanced Data Analysis: Cloud platforms can analyze large datasets, providing deeper insights and enabling data-driven decision-making.

Cost-Effectiveness: Reduces the need for on-premises infrastructure, lowering capital and operational expenses.

Global Accessibility: Offers remote access to data and management tools, enabling control from anywhere in the world.

Real-Time Processing and Action: Allows for real-time data processing, leading to timely responses and actions.

Reliability and Redundancy: Ensures data integrity and availability through reliable storage solutions and backup mechanisms.

Security: Provides robust security measures, including data encryption and secure access controls, to protect sensitive IoT data.

Integration with Other Services: Enables seamless integration with other cloud services like AI, machine learning, and third-party applications.

Support for Innovation: Facilitates rapid development and deployment of new IoT applications and services.

Co-funded by the European Union

IOT ANALYTICS

Feb 2022

Your Global IoT Market Research Partner

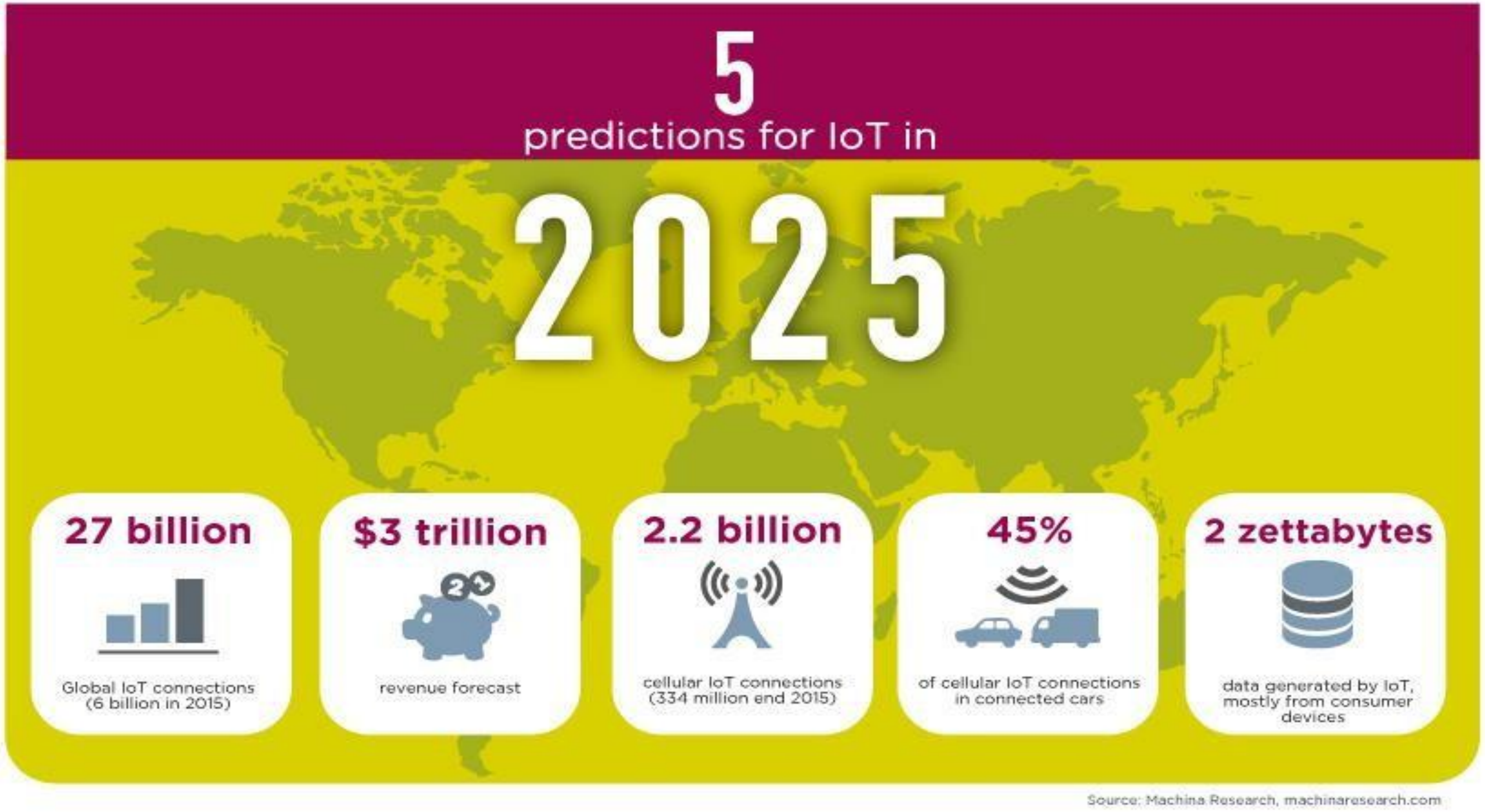
IoT cloud: Microsoft Azure vs. AWS vs. Google Cloud

	Number of listed IoT cloud services	1 Application management/ enablement	2 Device management	3 Data management/ enablement	4 Other IoT cloud services
Azure	9	Azure IoT Central Azure Digital Twins	Azure IoT Hub	Azure IoT Edge Azure Time Series Insights Azure Percept	Azure Sphere Azure RTOS Azure Defender for IoT
aws	13	AWS IoT TwinMaker AWS IoT Events AWS IoT Roborunner AWS IoT FleetWise	AWS IoT Device Management AWS IoT 1-Click	AWS IoT Core AWS IoT Analytics AWS IoT SiteWise AWS IoT Greengrass	AWS IoT Device Defender Free RTOS AWS IoT ExpressLink
Google Cloud	1		IoT Core		

Note: Google Cloud lists 4 other services for IoT but all of them are of general nature and also apply for non-IoT scenarios (e.g., BigQuery). They are therefore not classified as an IoT service.
Source: IoT Analytics Research, Company websites. We welcome republishing of images but ask for source citation with a link to the original post and company website.

Co-funded by the European Union

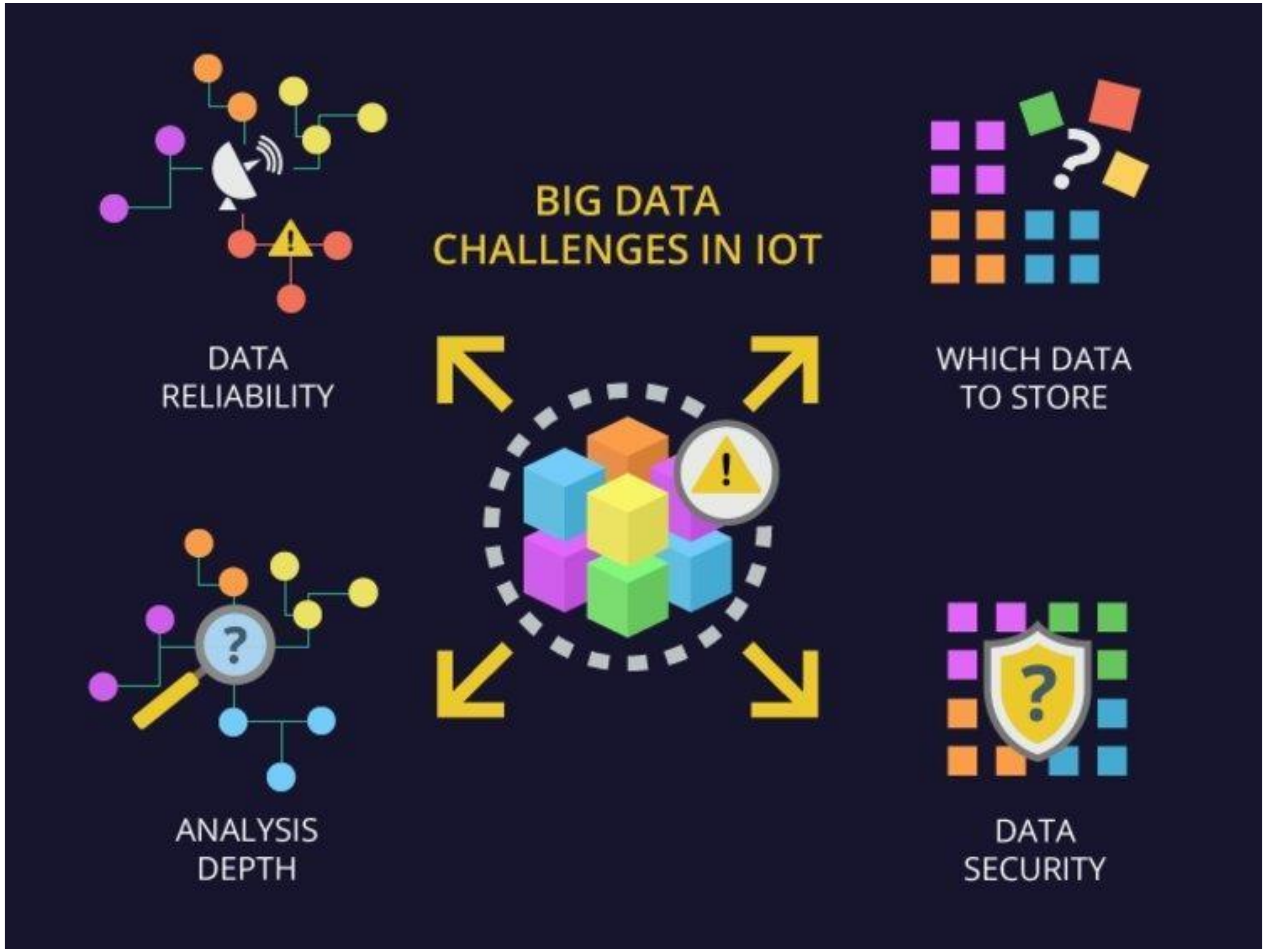
IoT and Big Data



- Role of IoT in generating big data

Co-funded by the European Union

IoT and Big Data

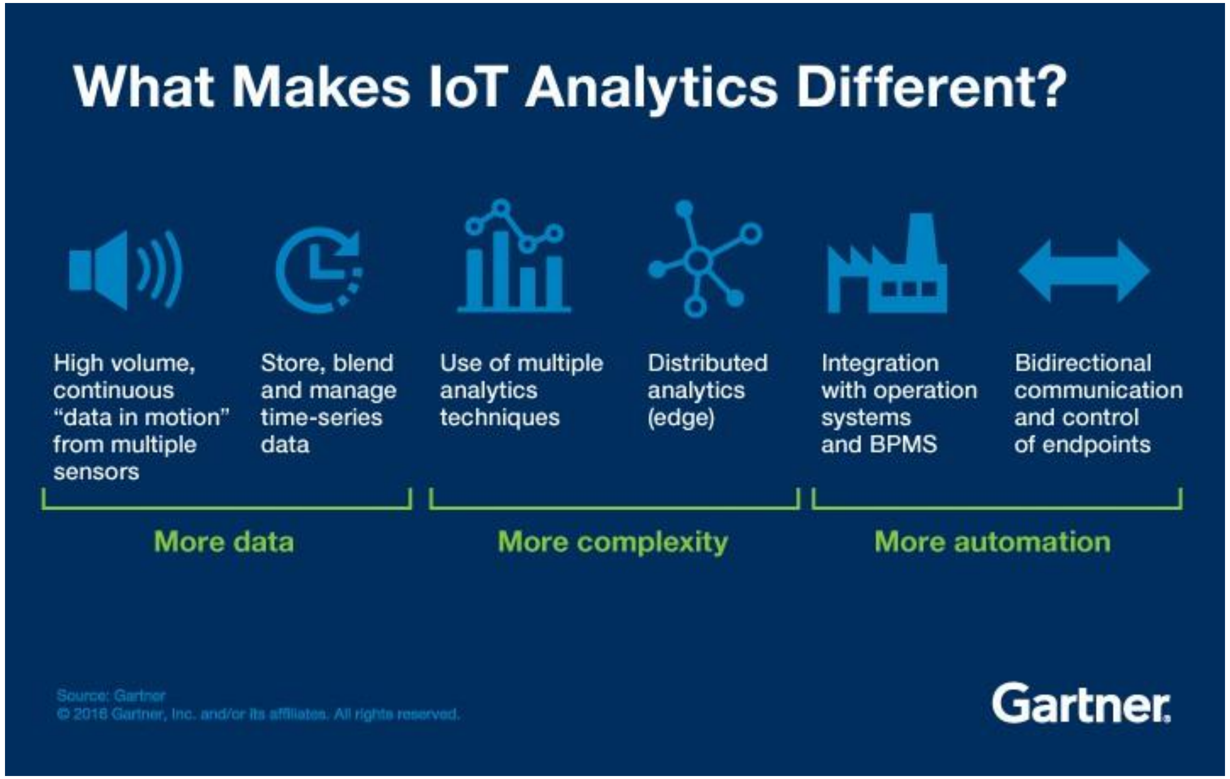


- Analyzing and leveraging IoT data

Co-funded by the
European Union

IoT Data Analytics

- **High Volume, Continuous "Data in Motion"**: IoT devices generate large amounts of data continuously, which is often referred to as "data in motion" due to its real-time nature.
- **Store, Blend, and Manage Time-Series Data**: IoT analytics involves storing and managing time-stamped data that can be analyzed to track changes over time.
- **Use of Multiple Analytics Techniques**: It employs a variety of analytical methods to make sense of the data collected from IoT devices.
- **Distributed Analytics (Edge)**: Analysis is often conducted at or near the source of data collection (the "edge" of the network) to reduce latency.
- **Integration with Operation Systems and BPMS (Business Process Management Systems)**: IoT analytics is often integrated with operational systems and BPMS to enhance business processes.
- **Bidirectional Communication and Control of Endpoints**: Allows for two-way interaction between the analytics system and the IoT devices, enabling not just data collection but also the ability to control the devices based on analytical insights.



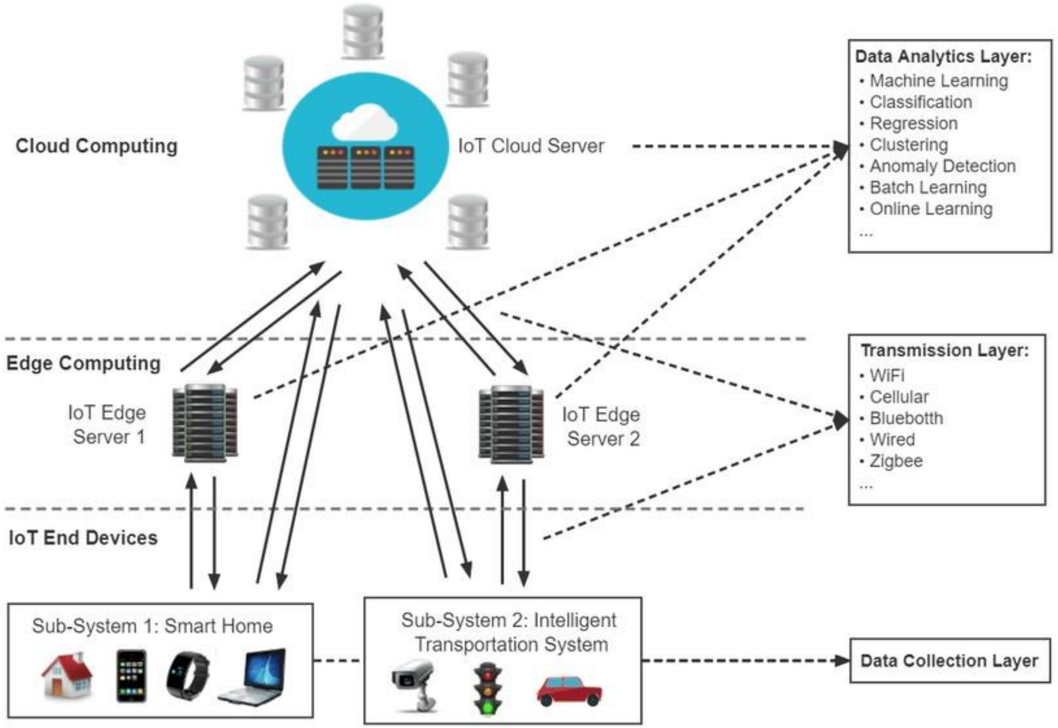
IoT analytics deals with increasing data volumes, the complexity of managing and analyzing this data grows, which in turn drives a need for more sophisticated automation solutions.

Co-funded by the European Union

IoT Data Analytics / Example

- **Cloud Computing**: Represents centralized servers in the cloud that are capable of handling intensive data analytics tasks, such as machine learning, classification, regression, clustering, anomaly detection, batch learning, and online learning. These servers are typically robust and can manage large-scale data processing and complex analytics.
- **Edge Computing**: Consists of IoT Edge Servers 1 and 2 that are closer to the data sources. These servers can perform preprocessing, filtering, and local data analysis to reduce latency and bandwidth use by not sending all data to the cloud.
- **IoT End Devices**: These are devices in different subsystems, such as a smart home system with various home automation devices, and an intelligent transportation system with connected vehicles and traffic management tools. They are the sources of data.
- **Data Collection Layer**: This is the foundation where data is initially collected from IoT devices, which can include a wide array of sensors and actuators.
- **Transmission Layer**: Includes various communication protocols and connectivity options such as WiFi, Cellular, Bluetooth, Wired, and Zigbee, which are used to transmit data between the end devices, edge servers, and the cloud.

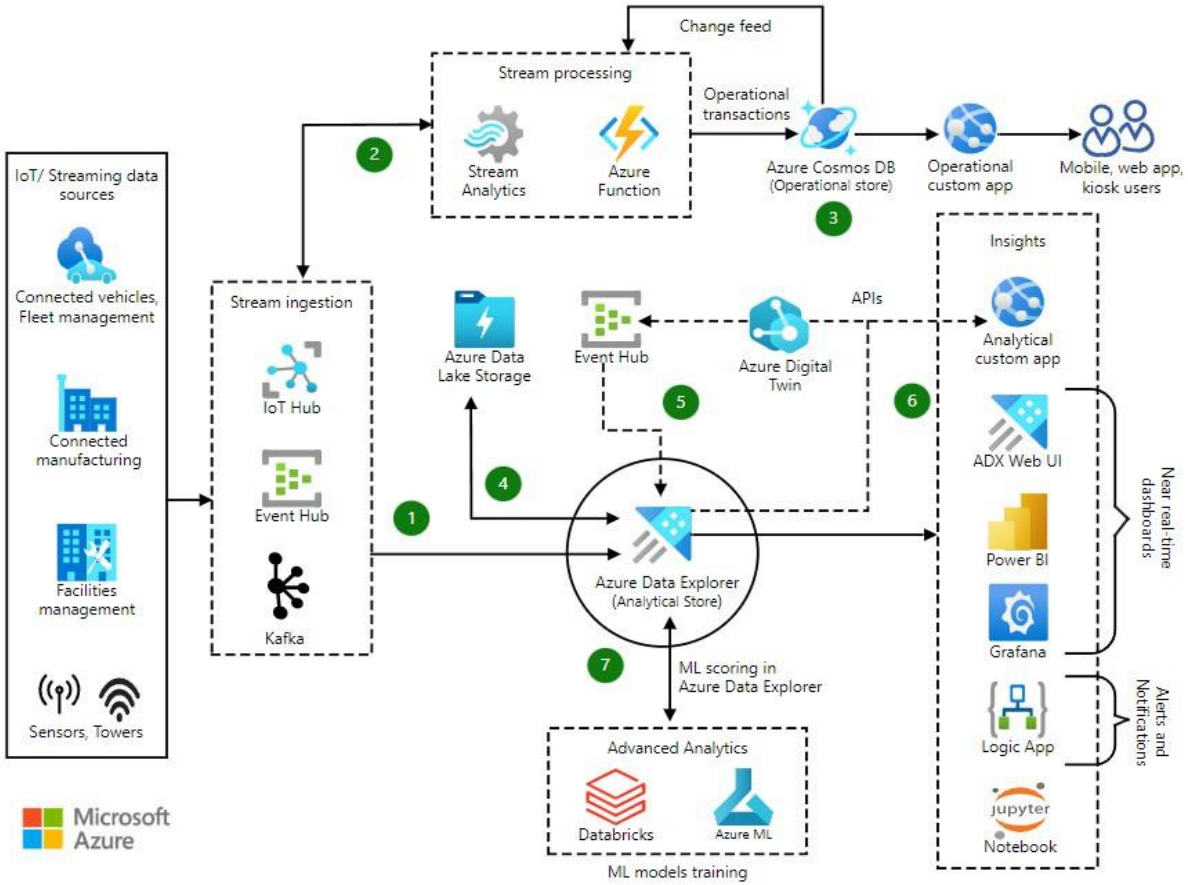
The structure shown emphasizes the layered approach in IoT systems, where different layers have distinct roles but work cohesively to manage data flow, processing, and analysis. This kind of architecture allows for flexibility, scalability, and efficient data handling, crucial for the dynamic nature of IoT applications.



Co-funded by the European Union

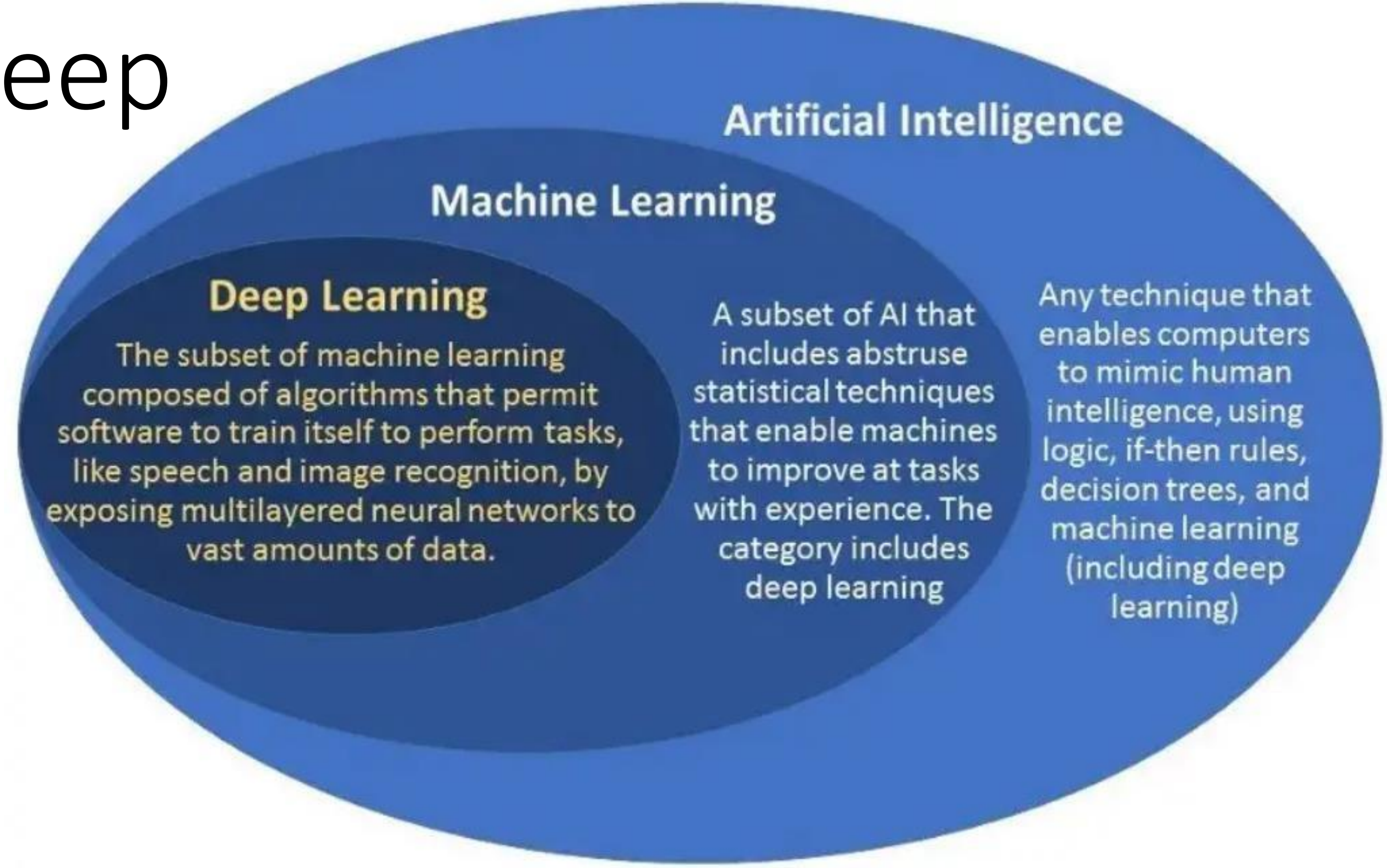
IoT Data Analytics / Microsoft Azure

1. **Stream Ingestion**: IoT data streams are ingested through services like Azure IoT Hub, Event Hubs, or Kafka. This includes data from various sources such as connected vehicles, manufacturing equipment, and facility management systems.
2. **Stream Processing**: The ingested data is then processed in real-time using Azure Stream Analytics and Azure Functions. This allows for immediate analysis and response to the data as it flows into the system.
3. **Operational Transactions**: The processed data can be used to update operational systems, like Azure Cosmos DB, which is designed to handle transactional data at scale.
4. **Data Storage**: Simultaneously, data is stored for further analysis in Azure Data Lake Storage, ensuring that the raw data can be accessed and analyzed later.
5. **Digital Twin Integration**: Azure Digital Twins are integrated to create a virtual representation of physical environments, enabling advanced simulations and state management.
6. **APIs for Insights**: APIs are used to access the processed data, which can be utilized to build custom applications for deeper insights or to trigger actions based on the data.
7. **Analytics and Machine Learning**: Azure Data Explorer is used as an analytical store where advanced analytics are performed, and machine learning models can be applied using Azure ML for scoring.



Co-funded by the European Union

AI /ML/Deep Learning



Co-funded by the European Union

A.I and Machine Learning and IoT

Agriculture

- IoT and AI/ML advancements can significantly enhance agricultural productivity.
- Agriculture is a crucial human activity, where improved technologies can lead to higher yields.
- Increased yields contribute to a happier and healthier human population.
- Projections indicate that to meet the global food demand, worldwide food production must increase by 70% by 2050.

Healthcare

- AI/ML and IoT technologies are pivotal for enhancing healthcare quality.
- Intelligent assisted living environments are crucial for home-based healthcare, especially for chronic patients.
- These environments integrate a patient’s clinical history with an individual care process model.
- IoT technologies enable continuous monitoring of patients' living conditions, facilitating timely and personalized care.

Co-funded by the European Union

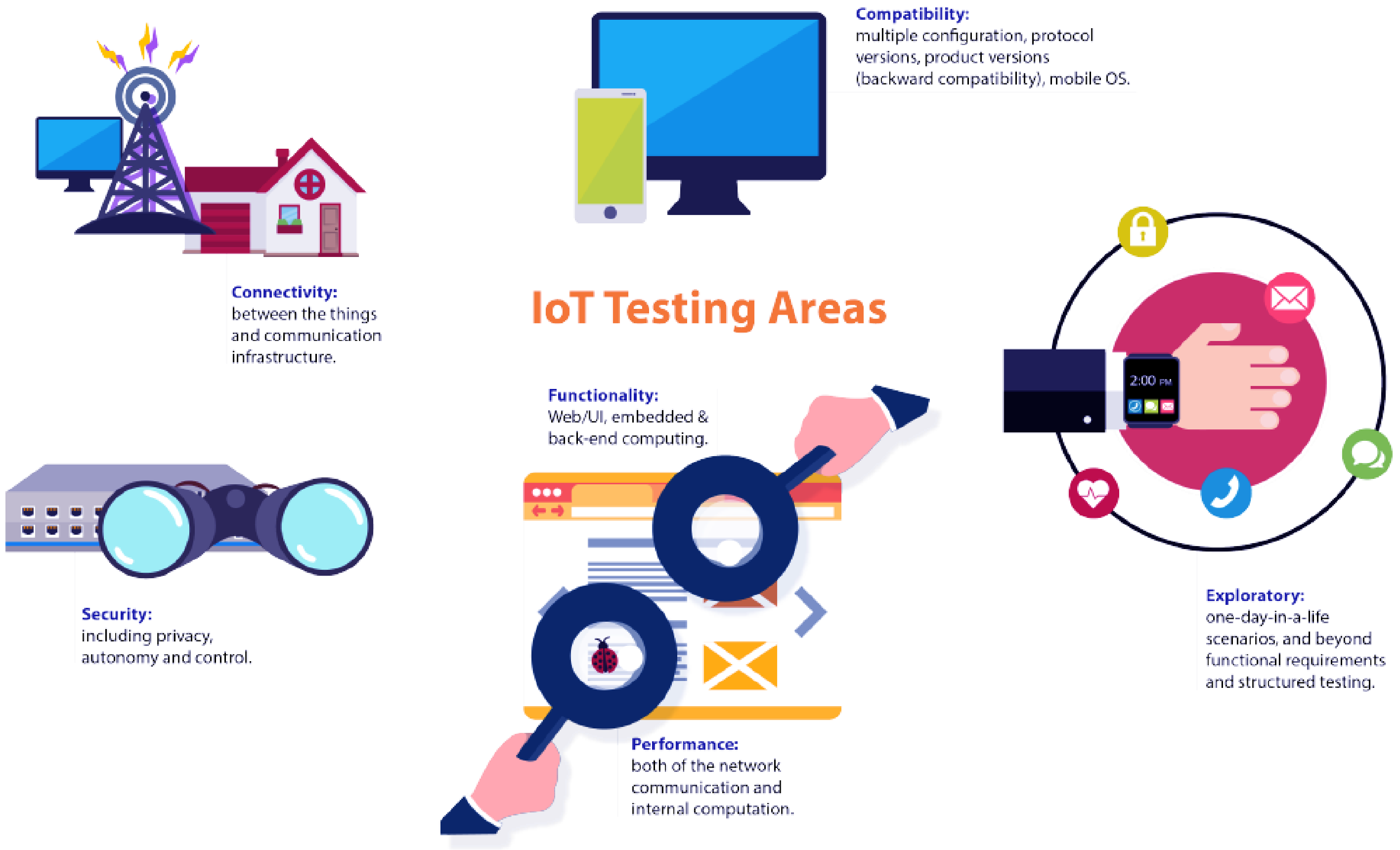
Digital Twins- CITY

- https://youtu.be/Oz3U2Ice_DI?si=4hx_scutY0Wxznk2

Co-funded by the European Union

IoT Testing and Quality Assurance

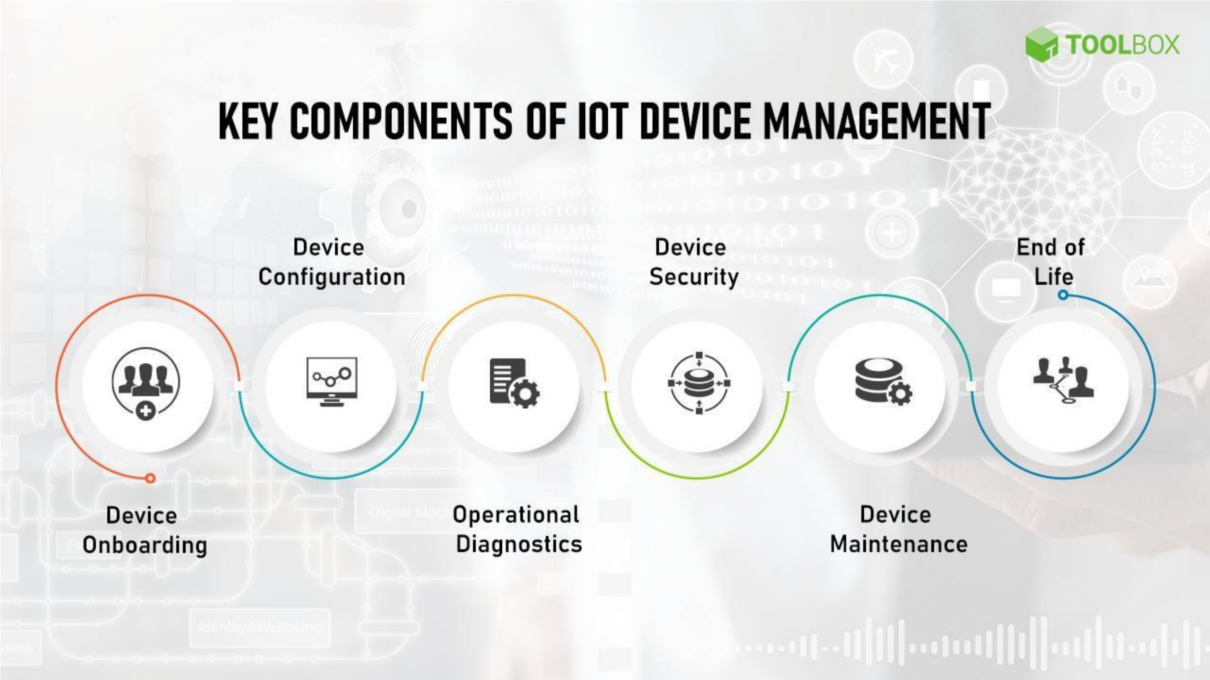
- **Functionality**: Testing the user interface, embedded systems, and backend computing to ensure they operate as expected.
- **Performance**: Assessing both the network communication efficiency and the processing capabilities of the IoT device or system.
- **Security**: Ensuring that data privacy is maintained and that devices have the necessary autonomy and control mechanisms in place.
- **Connectivity**: Verifying the ability of the IoT devices to connect and communicate with each other and with the infrastructure.
- **Compatibility**: Checking that devices work across various configurations, protocols, product versions, are backward compatible, and operate correctly on different mobile operating systems.
- **Exploratory**: Engaging with real-world scenarios to uncover issues beyond the scope of standard functional requirements and structured testing.



Co-funded by the European Union

IoT device life cycle

Device Onboarding: The initial setup and registration of IoT devices onto a network, including authentication and provisioning.
Device Configuration: Setting up devices with the correct configurations to communicate with the network and other devices, and to perform their intended functions.
Operational Diagnostics: Monitoring devices to ensure they are functioning correctly, and diagnosing any operational issues that arise.
Device Security: Implementing measures to protect devices from unauthorized access and cyber threats.
Device Maintenance: Regular updates and repairs to maintain the device's functionality over its operational lifetime.
End of Life: Properly decommissioning devices that are no longer functional or supported, including safely removing them from the network and disposing of them in a secure manner.



Co-funded by the European Union

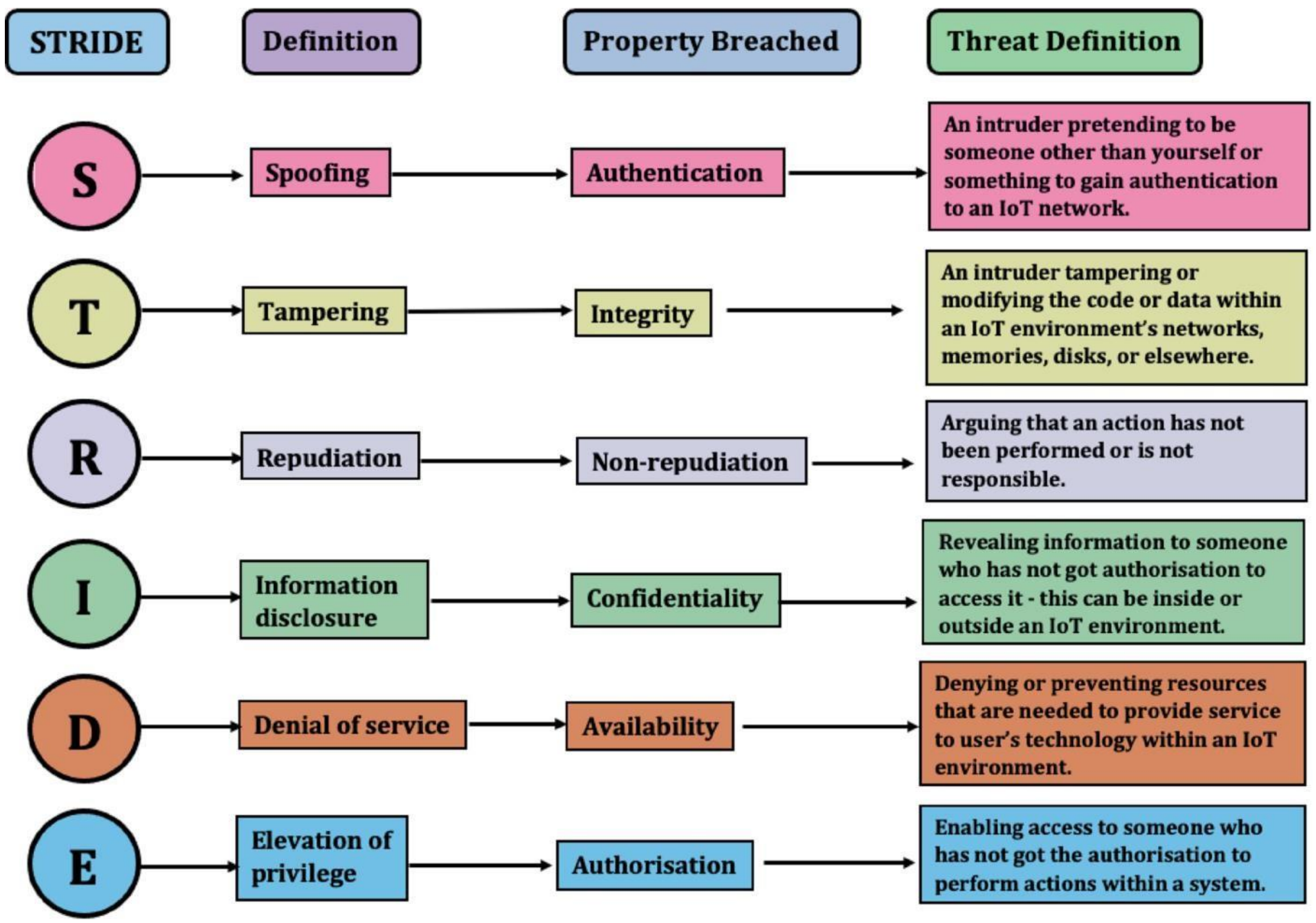
IoT Deployment challenges

- **Security Challenges**: This includes dealing with unsecured devices and the capacity of networks to block unwanted traffic or detect suspicious behavior.
- **Network Challenges**: Challenges here involve ensuring scalability and diversity of the network, providing open network interfaces, and enabling low-power communication for devices.
- **New and Complex Dependencies**: This refers to the difficulties in modeling human behaviors within IoT systems, often called "human-in-the-loop."
- **Software Development Challenges**: These challenges encompass handling big data (considering volume, variety, and velocity), as well as enabling self-configuration for software (SW), hardware (HW), and networking configurations.

Co-funded by the European Union

IoT attacks

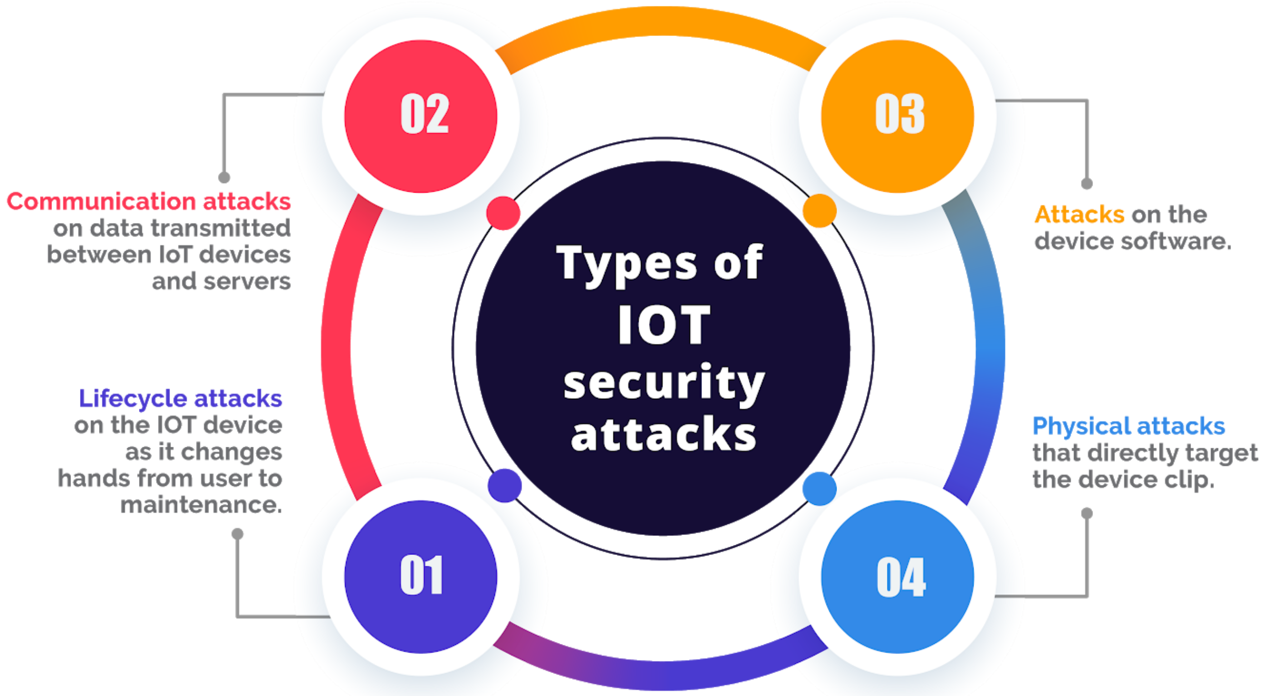
- **Spoofing**: This threat involves an attacker impersonating another user or device to gain unauthorized access to a system, breaching authentication mechanisms.
- **Tampering**: This refers to the unauthorized alteration of data or code within a system, which breaches the integrity of the system.
- **Repudiation**: This involves performing an action within a system and then denying having performed that action, breaching non-repudiation assurances.
- **Information Disclosure**: This is the unauthorized access and exposure of confidential information, breaching confidentiality.
- **Denial of Service (DoS)**: This attack prevents legitimate users from accessing services by overwhelming the system, breaching availability.
- **Elevation of Privilege**: This occurs when an attacker gains higher access rights than they are authorized for, breaching authorization controls.



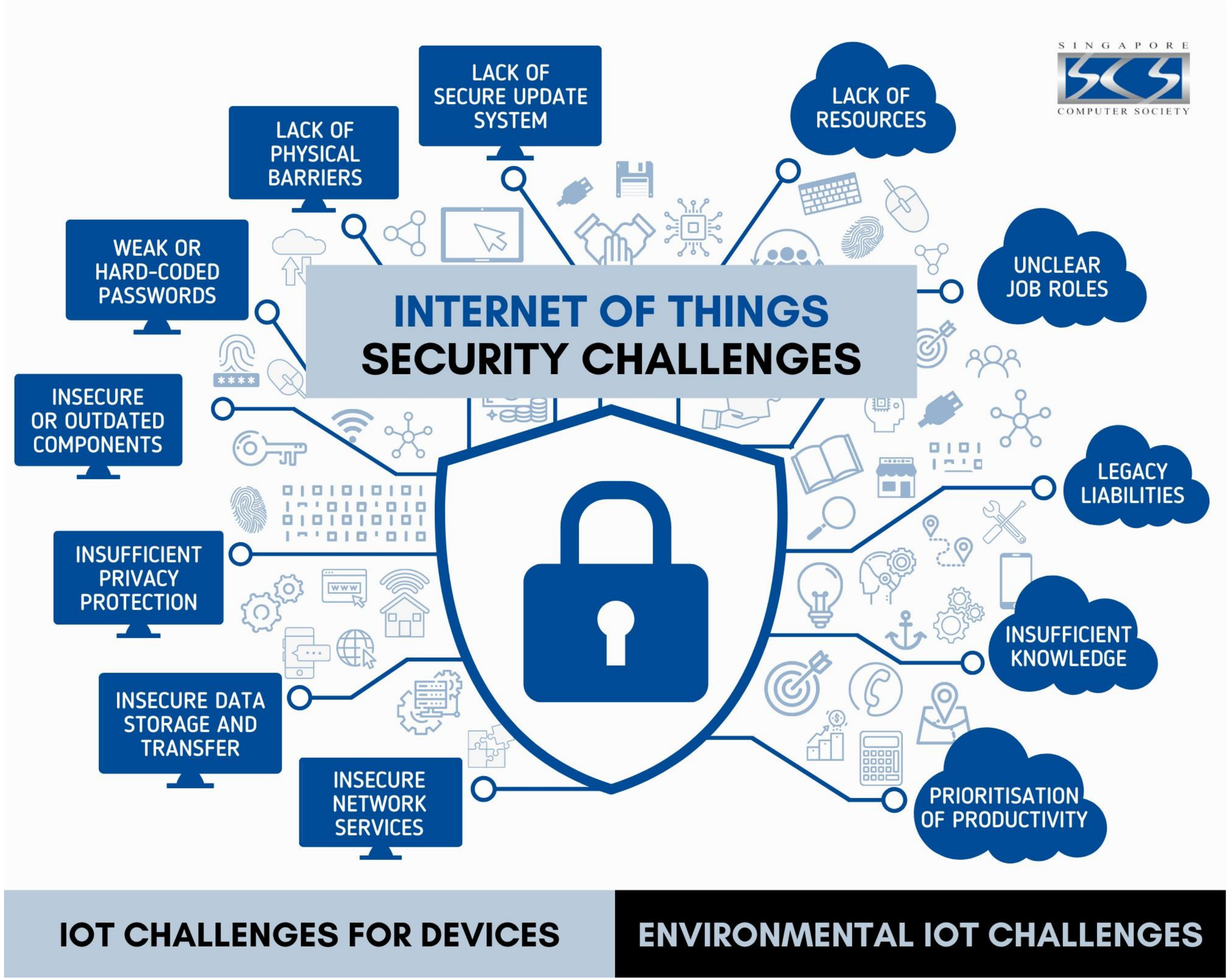
Co-funded by the European Union

IoT Security Measures

1. **Lifecycle Attacks**: These attacks occur as the IoT device transitions through different stages from initial use to maintenance, targeting vulnerabilities that may emerge during the device's lifecycle.
2. **Communication Attacks**: These target the data transmitted between IoT devices and servers, aiming to intercept, alter, or disrupt the flow of information.
3. **Attacks on Device Software**: These are directed at the software running on IoT devices, including firmware and applications, aiming to exploit software vulnerabilities.
4. **Physical Attacks**: These involve direct tampering with the hardware of the IoT devices, such as microchips and sensors, to manipulate or damage the device.



Co-funded by the European Union



Co-funded by the European Union

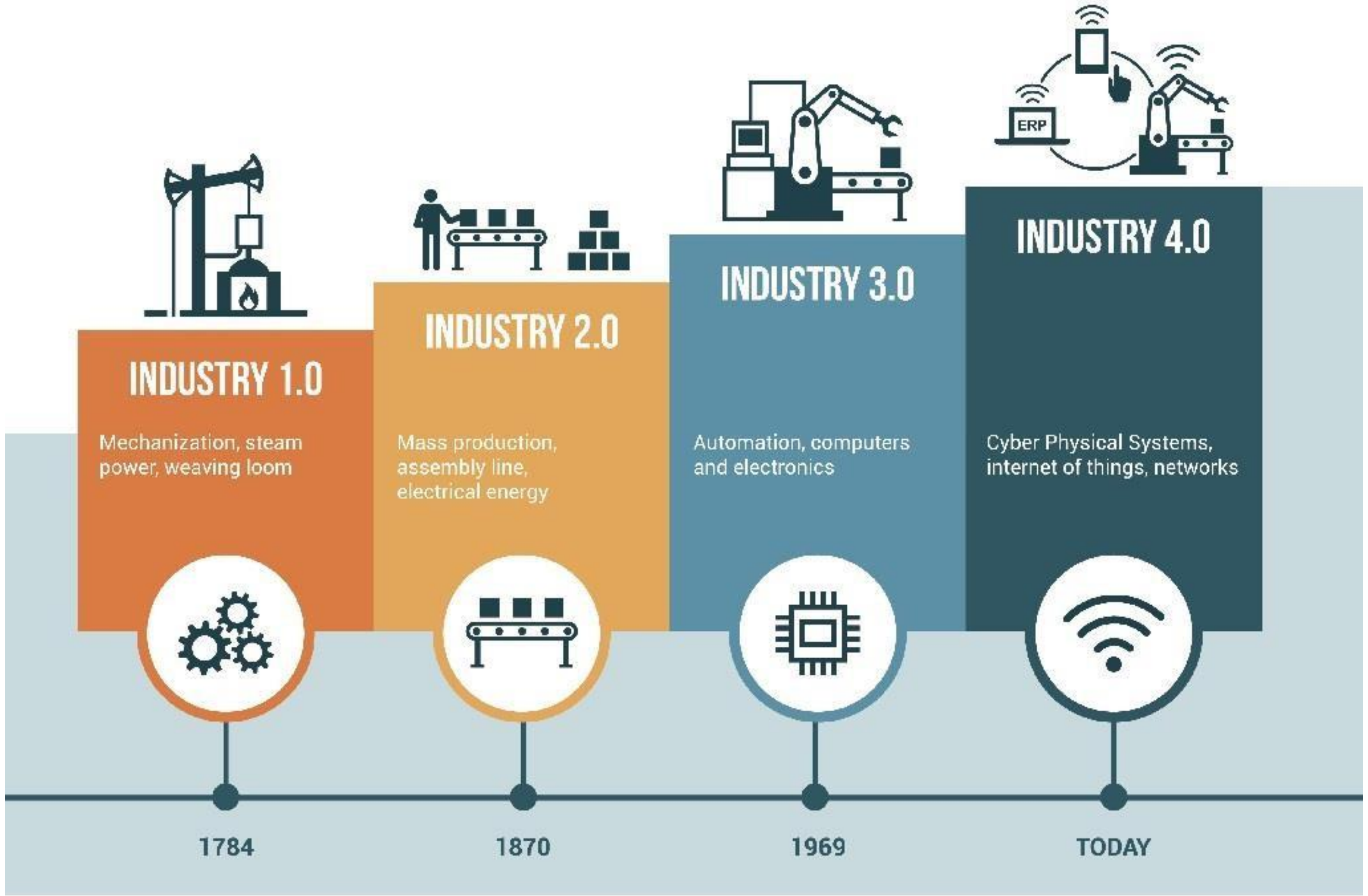
Bootcamps for Emerging Technologies and essential Skills

Internet of Things

IoT in Business and Industry Applications

Developed by: ECECT

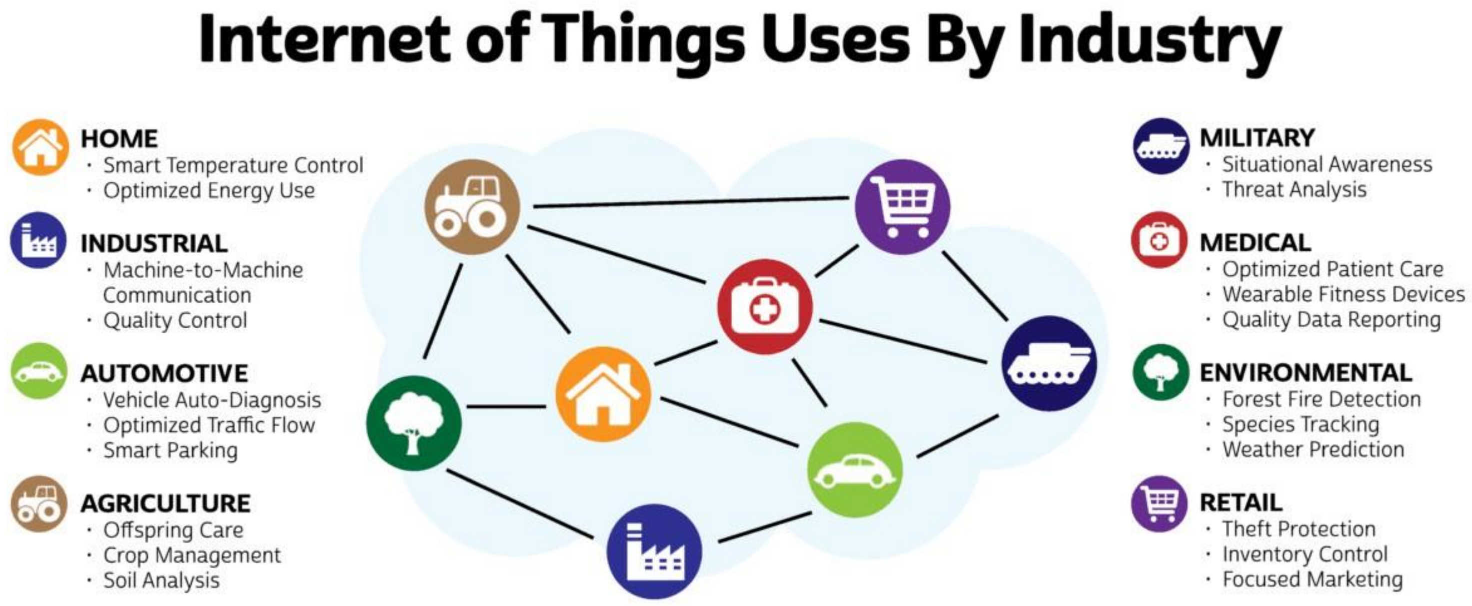
IoT in Business and Industry Applications



- **Industry 1.0**: Dated around 1784, marking the transition to mechanized production methods. This era was characterized by the introduction of mechanical systems powered by water and steam, such as the weaving loom.
- **Industry 2.0**: Starting around 1870, this period saw the emergence of mass production, assembly lines, and the use of electrical energy.
- **Industry 3.0**: Taking off around 1969, this phase was defined by the use of electronics and information technology to further automate production. Automation, computers, and electronics were the main innovations driving this era.
- **Industry 4.0**: Represents the current trend in the industrial sector, focusing on interconnectivity, automation, machine learning, and real-time data. This phase is characterized by cyber-physical systems, the Internet of Things (IoT), and networked communications.

Co-funded by the European Union

Overview of IoT in Business



Home: Incorporates smart temperature control and energy optimization.

Industrial: Focuses on machine-to-machine communication and quality control.

Automotive: Includes vehicle diagnostics, traffic optimization, and smart parking.

Agriculture: Encompasses offspring care, crop management, and soil analysis.

Military: Involves situational awareness and threat analysis.

Medical: Covers optimized patient care, wearable fitness devices, and data reporting.

Environmental: Addresses forest fire detection, species tracking, and weather prediction.

Retail: Deals with theft protection, inventory control, and targeted marketing.

Co-funded by the European Union

IoT in Smart Cities: In-Depth

Smart Parking: Utilizing IoT for real-time information on parking space availability to reduce traffic and pollution.

Weather Sensors: Deployed across the city for accurate, hyper-local weather data collection.

Digital Signage: Interactive signs for public information, advertising, and emergency alerts.

Acoustic Sensors: Monitoring sound levels, potentially for law enforcement or urban planning.

Water & Gas Metering: Smart meters for efficient utility tracking and billing.

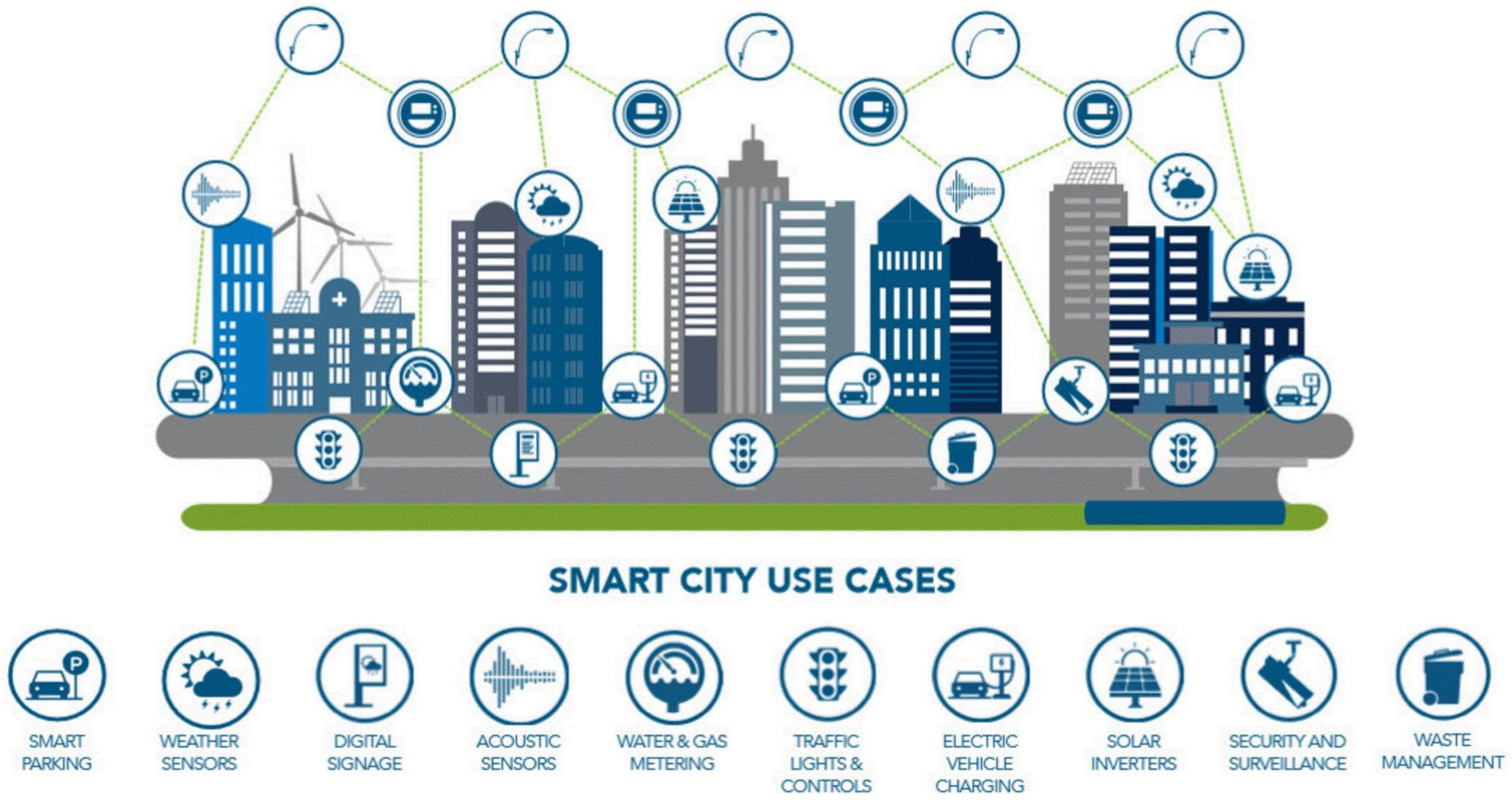
Traffic Lights & Controls: Intelligent traffic management systems to optimize flow and reduce congestion.

Electric Vehicle Charging: Networked charging stations for supporting sustainable transportation.

Solar Inverters: Integration of solar energy into the power grid.

Security and Surveillance: Advanced monitoring systems for public safety.

Waste Management: IoT-enabled waste collection for enhanced efficiency and sustainability.



Co-funded by the European Union

Internet of Things (IoT)

underpin the infrastructure for
the connected Smart City.

1. **TRANSPORTATION CONGESTION SENSORS**
Smart transportation systems use sensors to detect congestion and bottlenecks in traffic patterns. They also rely on cameras to enforce speed and traffic infractions. In doing so, these tools gather real time information that can be used by city DOTs to make mobility networks safer and more efficient.

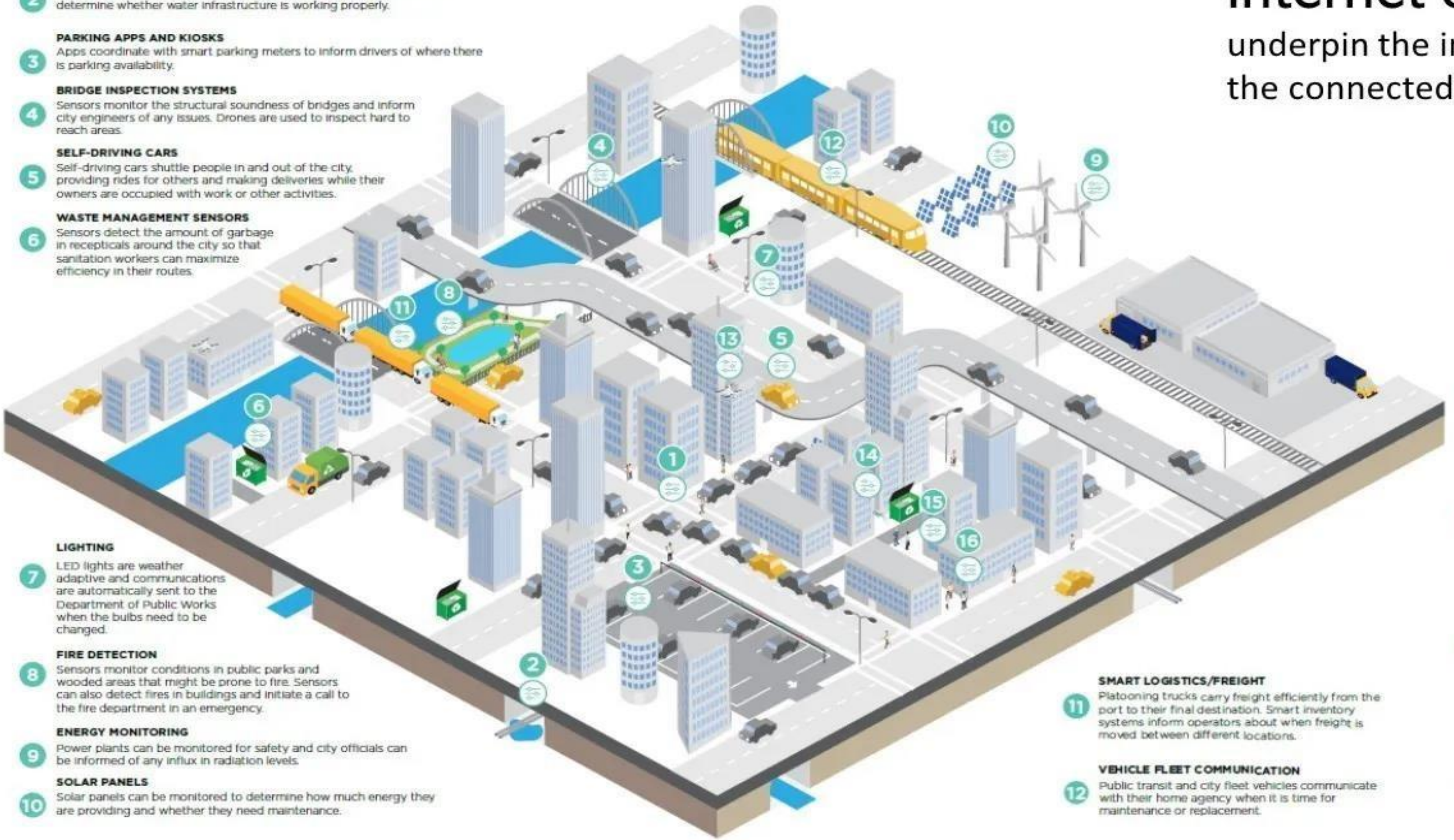
2. **WATER AND WASTEWATER MONITORING**
Monitoring devices can detect leaks as well as changes in water pressure to determine whether water infrastructure is working properly.

3. **PARKING APPS AND KIOSKS**
Apps coordinate with smart parking meters to inform drivers of where there is parking availability.

4. **BRIDGE INSPECTION SYSTEMS**
Sensors monitor the structural soundness of bridges and inform city engineers of any issues. Drones are used to inspect hard to reach areas.

5. **SELF-DRIVING CARS**
Self-driving cars shuttle people in and out of the city, providing rides for others and making deliveries while their owners are occupied with work or other activities.

6. **WASTE MANAGEMENT SENSORS**
Sensors detect the amount of garbage in recepticals around the city so that sanitation workers can maximize efficiency in their routes.



7. **LIGHTING**
LED lights are weather adaptive and communications are automatically sent to the Department of Public Works when the bulbs need to be changed.

8. **FIRE DETECTION**
Sensors monitor conditions in public parks and wooded areas that might be prone to fire. Sensors can also detect fires in buildings and initiate a call to the fire department in an emergency.

9. **ENERGY MONITORING**
Power plants can be monitored for safety and city officials can be informed of any influx in radiation levels.

10. **SOLAR PANELS**
Solar panels can be monitored to determine how much energy they are providing and whether they need maintenance.

11. **SMART LOGISTICS/FREIGHT**
Platooning trucks carry freight efficiently from the port to their final destination. Smart inventory systems inform operators about when freight is moved between different locations.

12. **VEHICLE FLEET COMMUNICATION**
Public transit and city fleet vehicles communicate with their home agency when it is time for maintenance or replacement.

13. **DRONES**
Drones can be used for law enforcement and firefighting, as rural ambulances, for infrastructure inspections, and for environmental monitoring. Commercial uses include precision farming, aerial photography, and in the near future, package delivery.

14. **SURVEILLANCE CAMERAS**
Cameras ensure security by monitoring activity in areas that are not frequented by public safety officers. Areas that are not open to public access can be monitored to keep unauthorized personnel out.

15. **BODY CAMERAS**
Public safety officers can wear body cameras that capture footage of interactions between themselves and city residents to ensure safety for both parties.

16. **WEARABLE DETECTION**
Cities can build in smartphone and wearable detection sensors so that people can be an active part of the internet ecosystem, communicating with the city, and with each other.

17. **BROADBAND INFRASTRUCTURE**
A reliable internet ecosystem is the glue that holds the internet of things together.

IoT in Retail

IoT Implementation in Retail: It's emphasized that starting with IoT in retail can be simple and high-value, enhancing insights into customer behavior, competition, and product performance.

Customer Interaction: Shoppers can interact with beacons and other IoT devices to provide retailers with additional data and enhance the shopping experience.

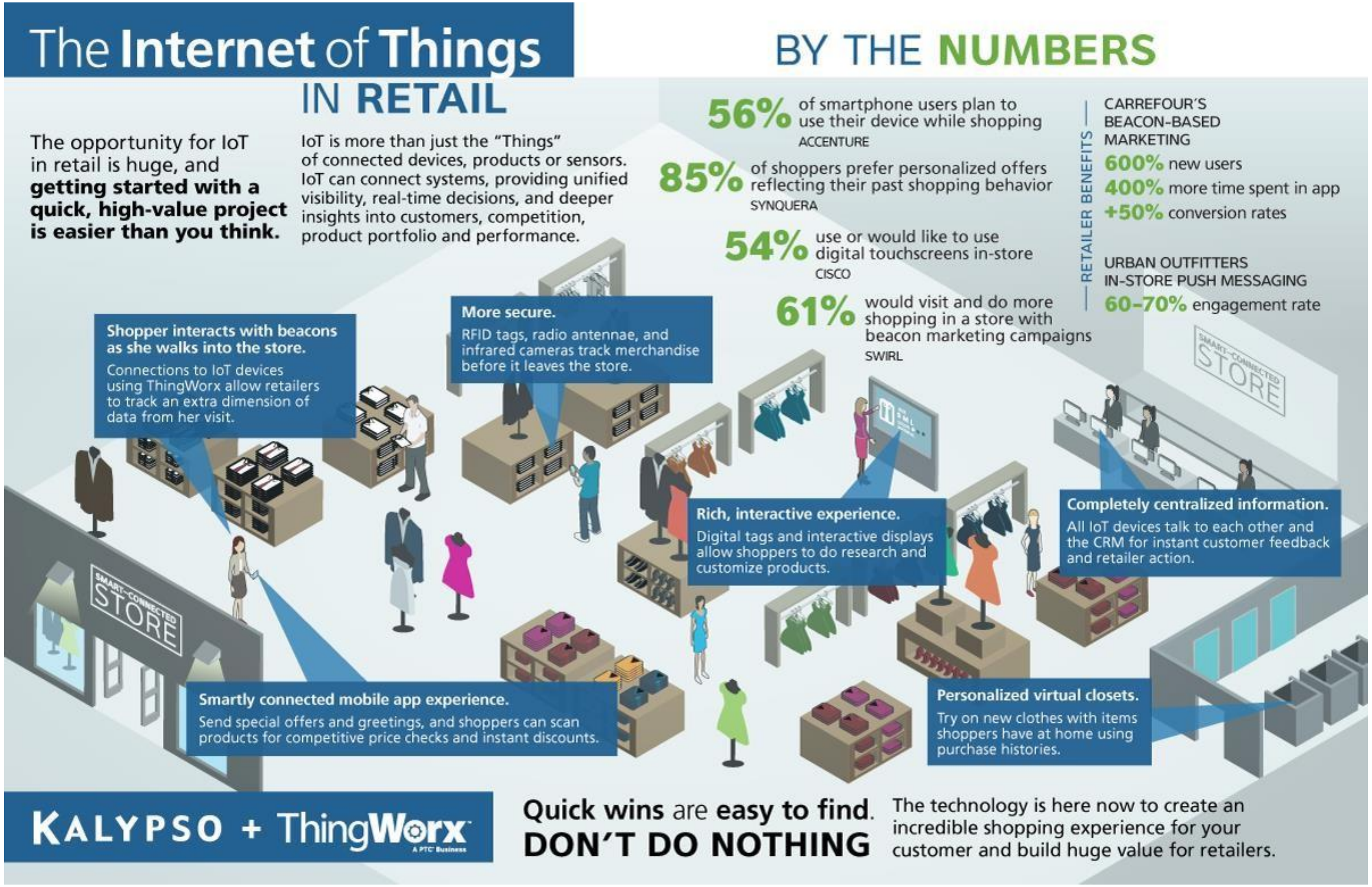
Security Measures: The use of RFID tags, radio antennae, and infrared cameras for tracking merchandise and enhancing store security is mentioned.

Experience Enhancement: The image suggests that IoT enables a richer shopping experience through interactive displays and digital tags, and helps personalize the experience through mobile apps and virtual closets.

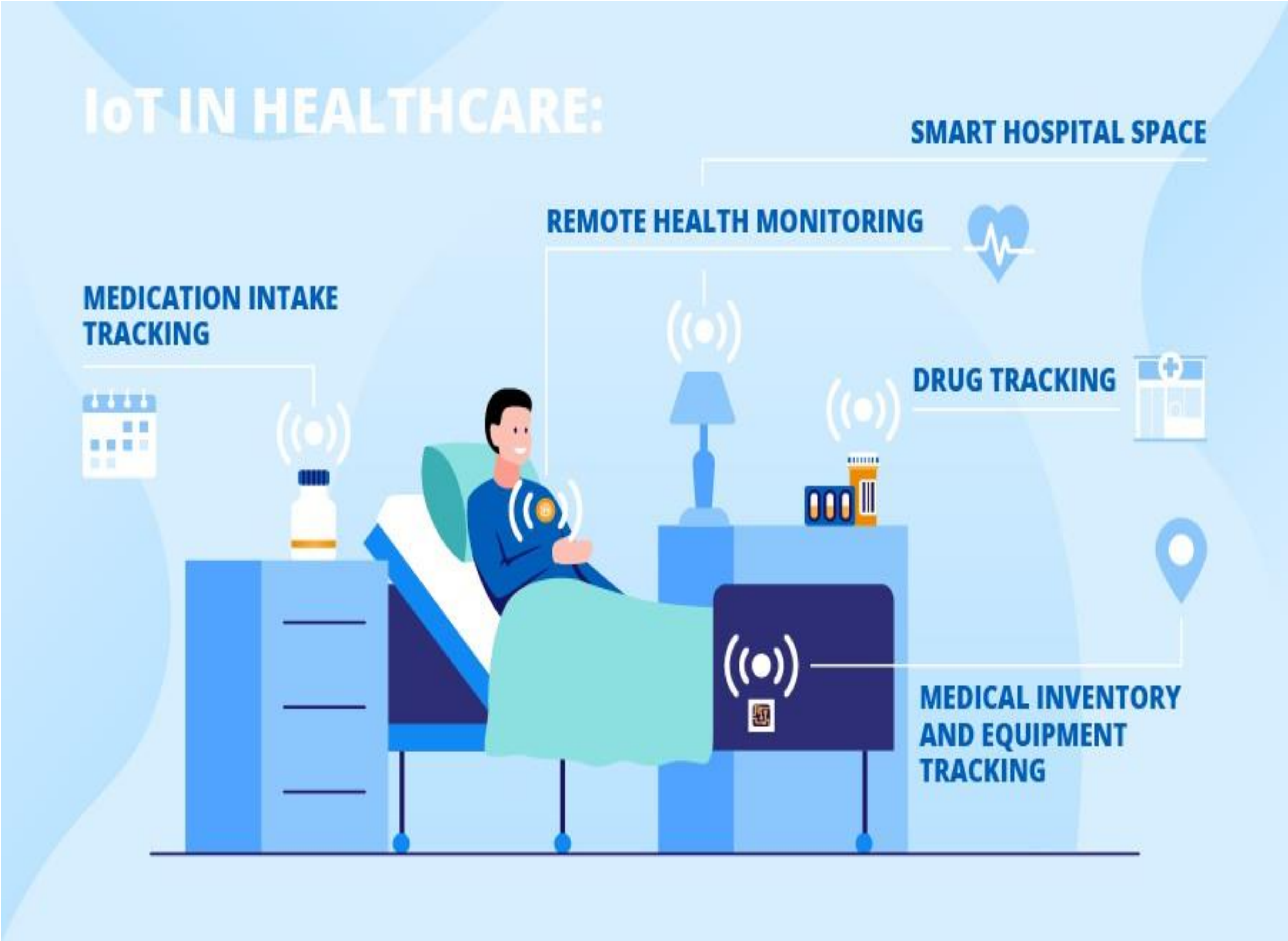
Statistical Data: Various statistics are provided, such as a percentage of smartphone users who plan to use their devices while shopping, the preference for personalized offers, and engagement rates with in-store marketing campaigns.

Retail Benefits: Specific examples include Carrefour's beacon-based marketing results and Urban Outfitters' in-store push messaging success.

Centralized Information: Central to IoT in retail is the collection and centralized processing of data, which allows for instant customer feedback and appropriate retail action.



Co-funded by the European Union

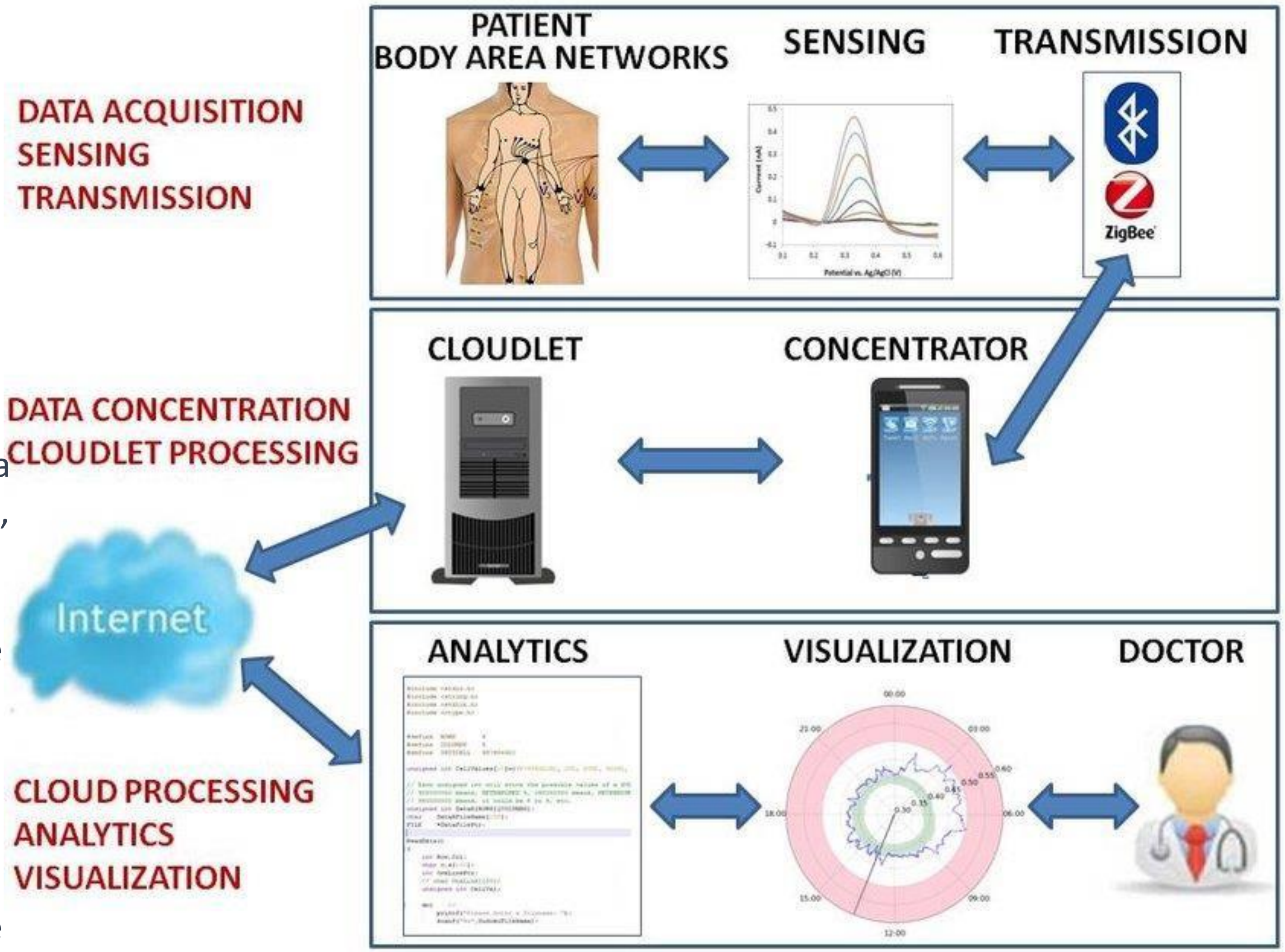


- The image illustrates the use of IoT in healthcare, specifically within a smart hospital setting.
- **Medication Intake Tracking**: Utilizing IoT to monitor patient medication schedules.
- **Remote Health Monitoring**: Implementing IoT devices for patient monitoring outside of traditional healthcare settings.
- **Drug Tracking**: Leveraging IoT for managing drug supplies within the hospital.
- **Medical Inventory and Equipment Tracking**: Using IoT for real-time tracking of hospital inventory and medical equipment.

Co-funded by the European Union

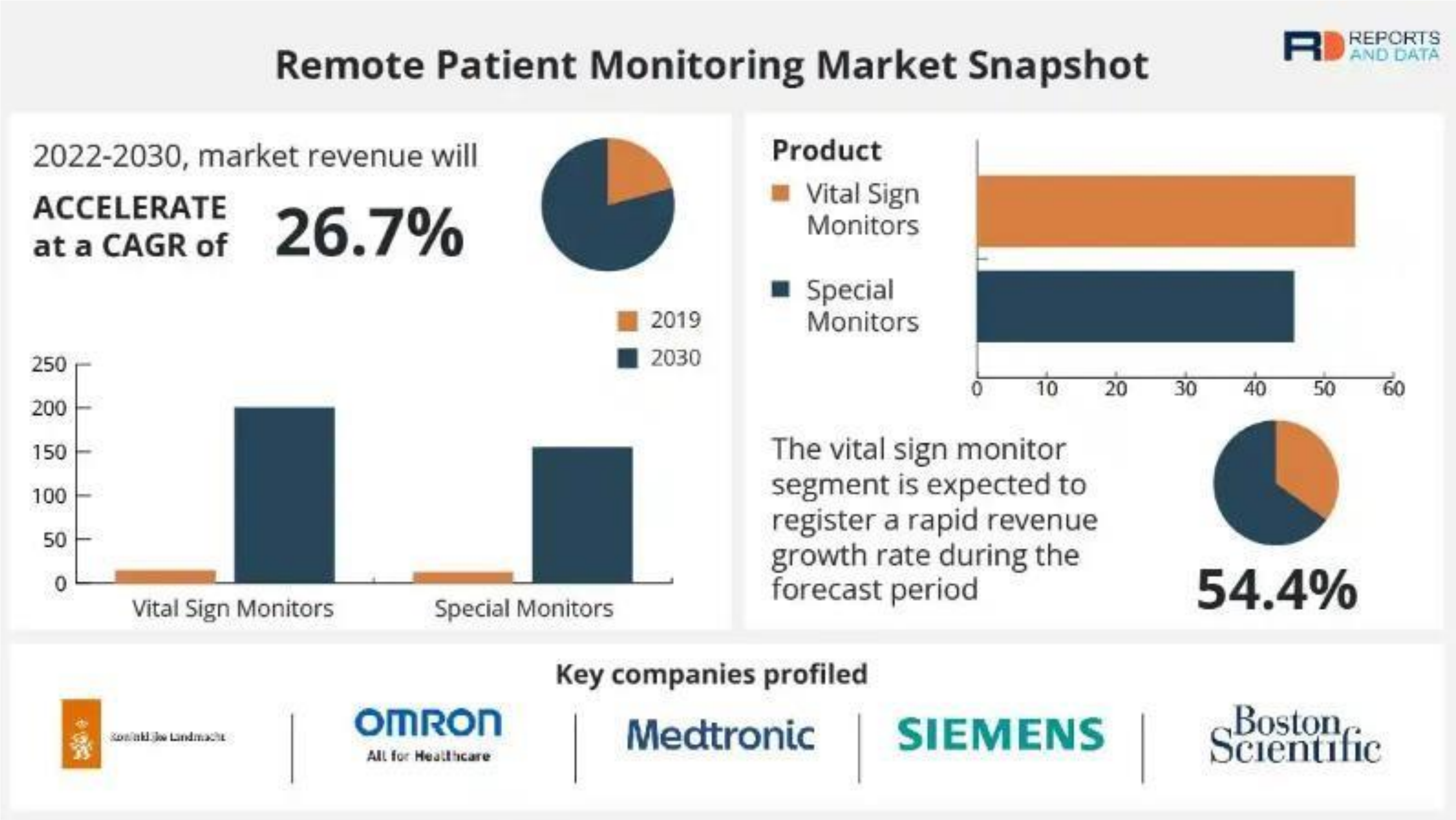
IoT in Healthcare

Data Acquisition: Patient's health data is collected through sensors attached to the body, known as Body Area Networks (BAN).
Sensing: The sensors collect various health metrics, which are then represented in graphical form.
Transmission: This collected data is transmitted using wireless technology such as ZigBee.
Data Concentration: A concentrator device, such as a smartphone, receives the transmitted data.
Cloudlet Processing: The data is processed locally or in a nearby 'cloudlet', which is a small-scale cloud datacenter, before being sent to the central cloud.
Cloud Processing: Further processing of the data takes place in the cloud, where more powerful analytics can be performed.
Analytics and Visualization: The analyzed data is then visualized in a format that is useful for medical professionals.
Doctor: Finally, a doctor or healthcare provider reviews the visualized data to make informed decisions about the patient's care.



Co-funded by the
European Union

IoT in Healthcare – Wearables



- Vital Sign Monitors
  - Pulse Oximeter
  - Temperature Monitor
  - Brain Monitoring (EEG)
  - Blood Pressure Monitor
  - Heart Rate Monitor (ECG)
  - Respiratory Rate Monitor
- Special Monitors
  - Blood Glucose Monitor
  - Respiratory Monitor
  - Cardiac Rhythm Monitor
  - Multi-Parameter Monitor (MPM)

Co-funded by the European Union

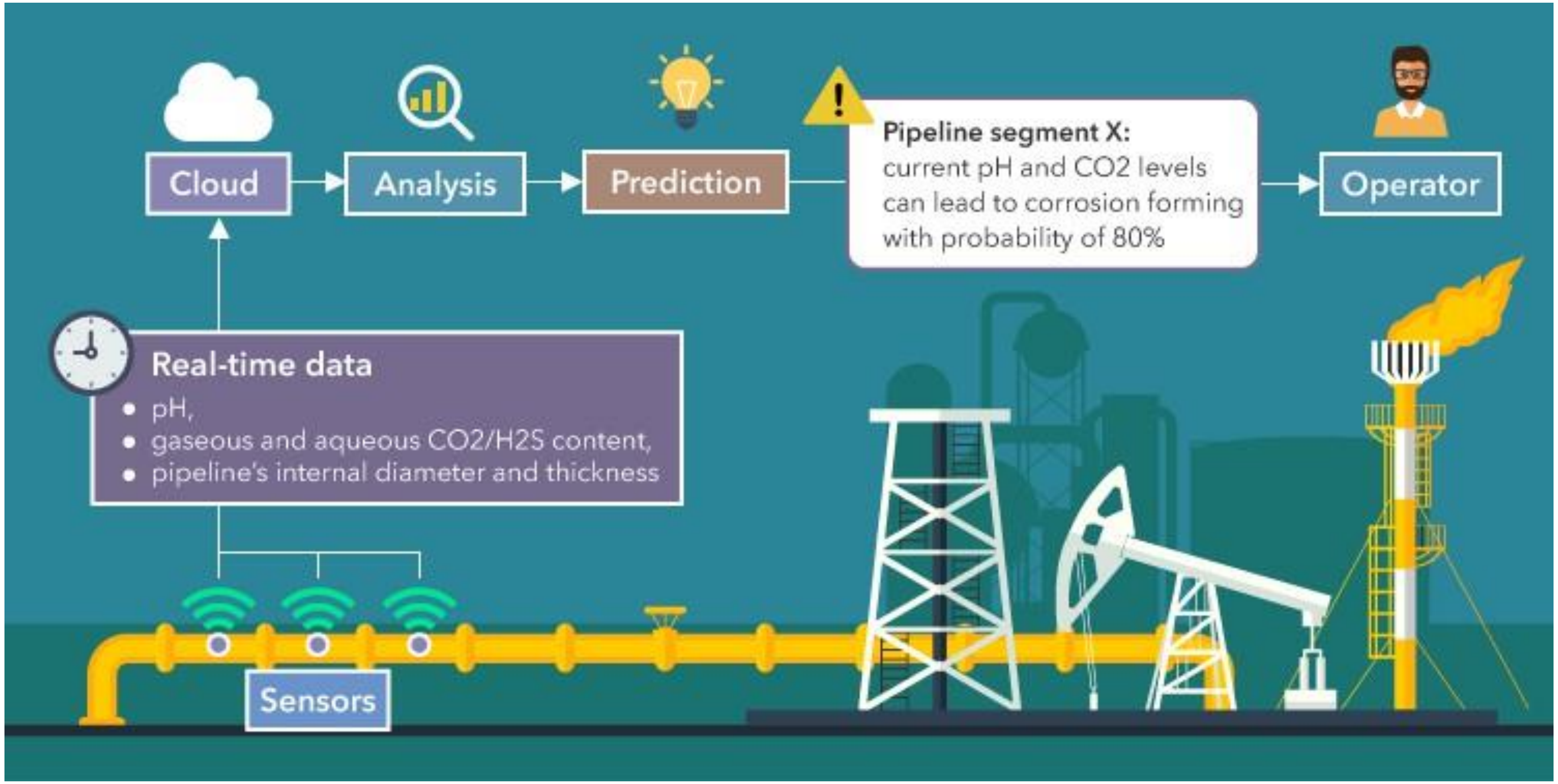
Industrial Internet of Things (IIoT) technologies are becoming pervasive across organizations and industry sectors, driving operational effectiveness in an array of industrial environments.

Co-funded by the European Union

IoT in Manufacturing (IIoT)

- The diagram provides a snapshot of IoT's role in streamlining the supply chain:
- **Supplier**: Enhances asset management and tracking.
- **Manufacturer**: Implements equipment monitoring for predictive maintenance.
- **Logistics**: Optimizes routing and real-time asset tracking.
- **Warehouse**: Employs intelligent inventory and storage management.
- **Retail**: Innovates with smart packaging and autonomous checkouts.
- **Consumer**: Offers dynamic product performance monitoring and support.
- This IoT-driven approach results in a responsive, efficient, and consumer-focused product journey from creation to end-user.

IoT in Manufacturing (IIoT) - example

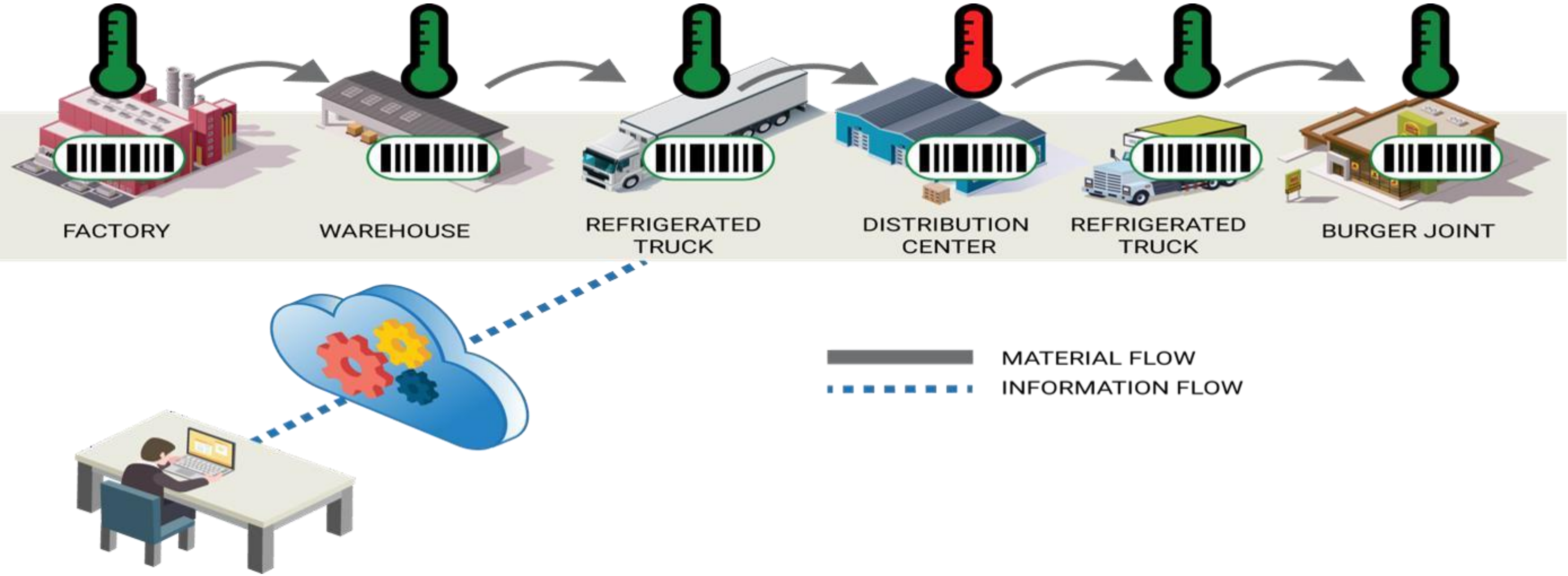


- Sensors collect real-time pipeline data: pH levels, gas content, diameter, thickness.
- Data is uploaded to the cloud for processing.
- Analysis performed in the cloud generates predictions.
- Prediction includes an 80% chance of corrosion in pipeline segment X.
- Operator is alerted about potential risks for proactive maintenance.

Co-funded by the European Union

IoT in Manufacturing (IIoT)

- Example: Supply chain for the food industry

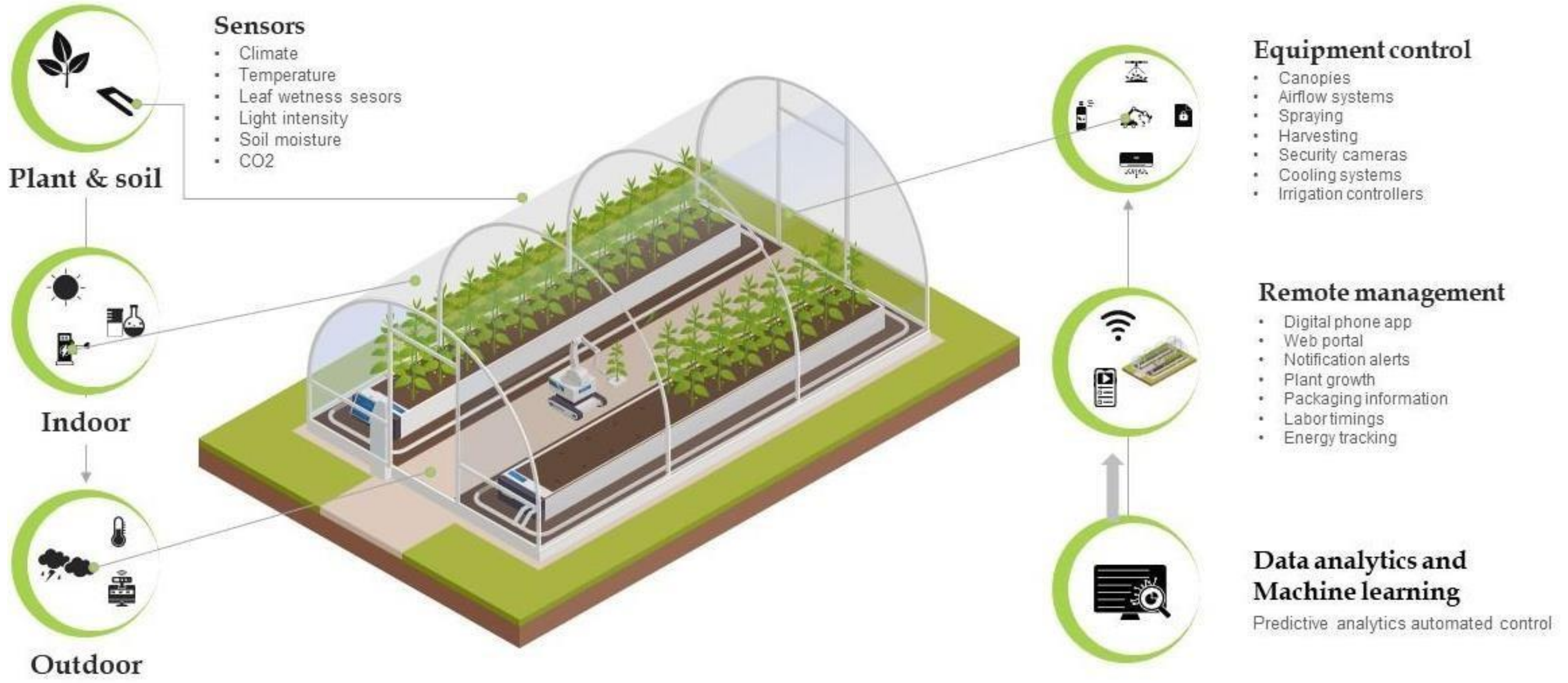


Co-funded by the European Union

IoT in Agriculture

- Greenhouse monitoring

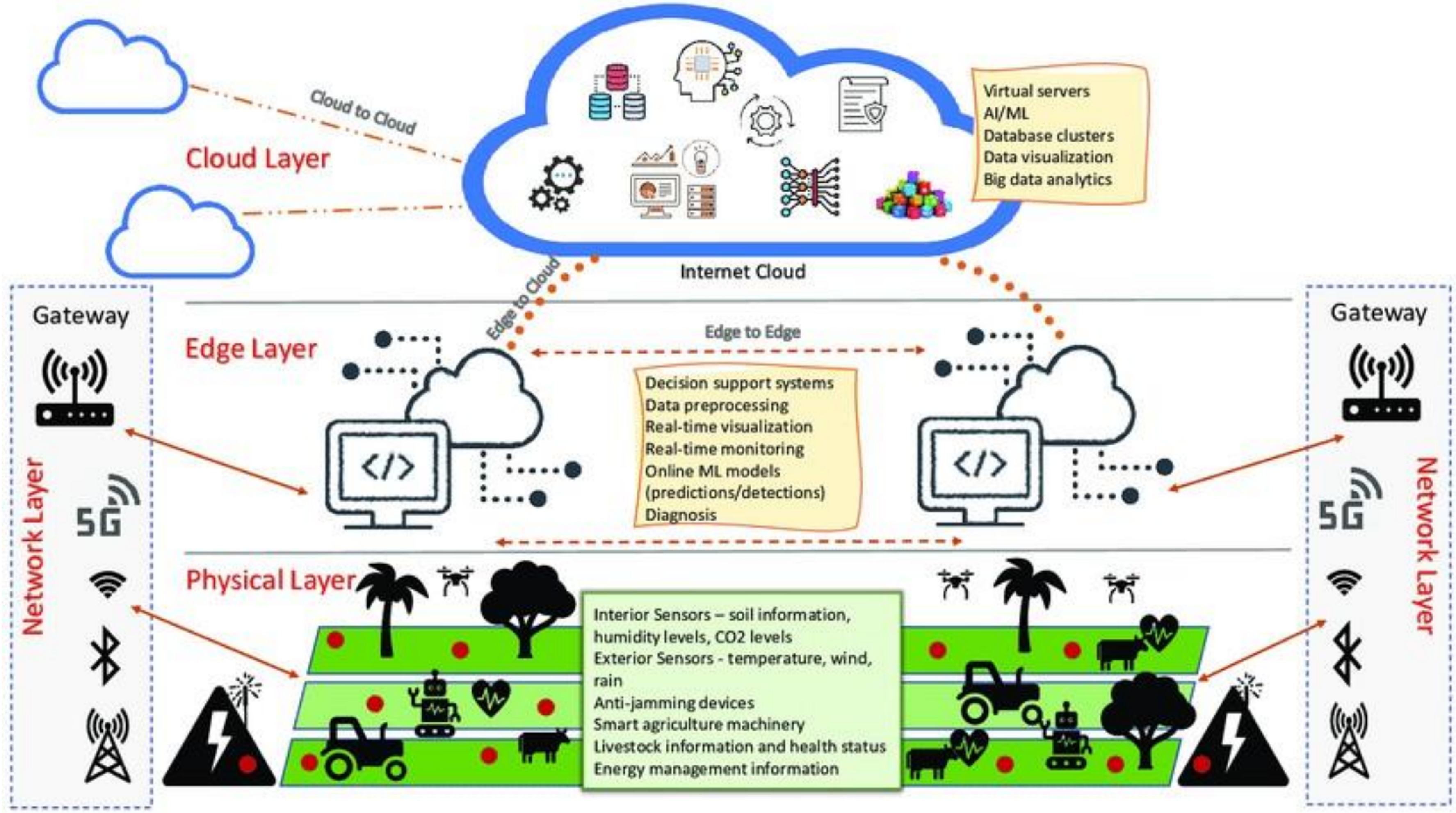
- **Plant & Soil Monitoring**: Utilizes sensors for climate, temperature, leaf wetness, light intensity, soil moisture, and CO2 levels.
- **Indoor and Outdoor Settings**: Differentiates between sensor applications and control mechanisms tailored for indoor facilities like greenhouses and outdoor environments.
- **Equipment Control**: Automated control systems for canopies, airflow, spraying, harvesting, security, cooling, and irrigation.
- **Remote Management**: Management via digital phone apps, web portals, and notifications for plant growth, packaging information, labor timings, and energy usage tracking.
- **Data Analytics and Machine Learning**: Employs predictive analytics and automated control based on machine learning algorithms for enhanced agricultural decision-making.



This smart farming approach integrates advanced technology to optimize growth conditions, improve resource management, and increase overall production efficiency.

Co-funded by the European Union

IoT in Agriculture



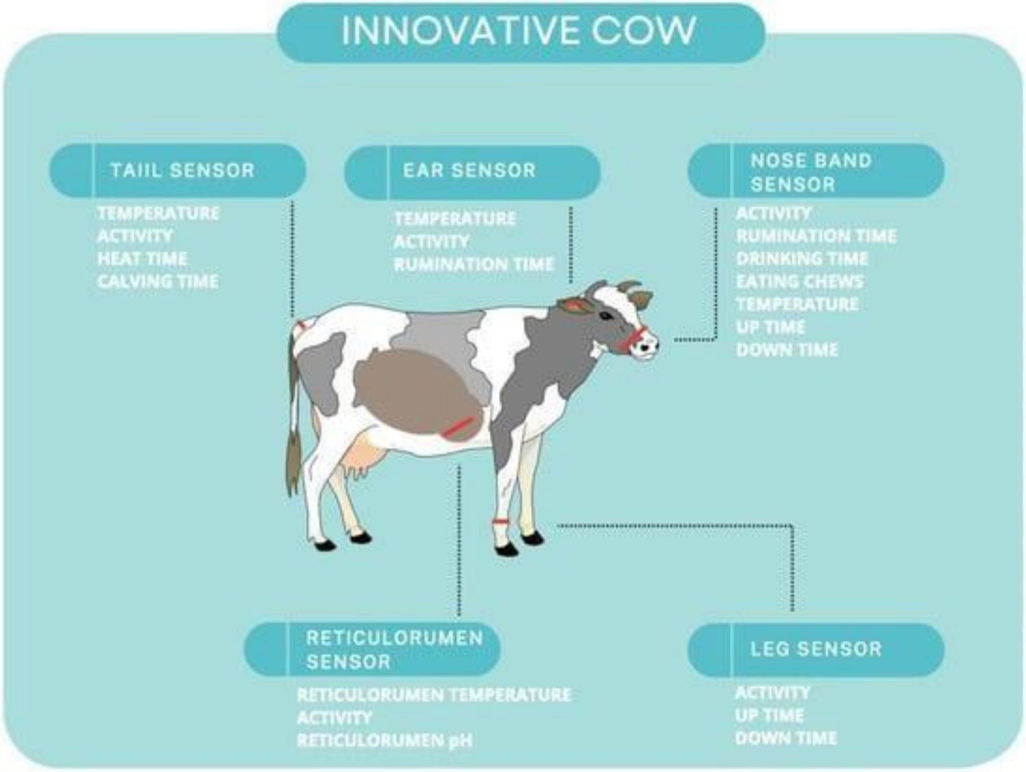
- Soil Information
- Humidity levels
- Weather conditions
- Temperature
- Wind
- Solar radiation

- 5G/4G/ Cellular network
- Wifi
- Lorawan
- Nb-IoT

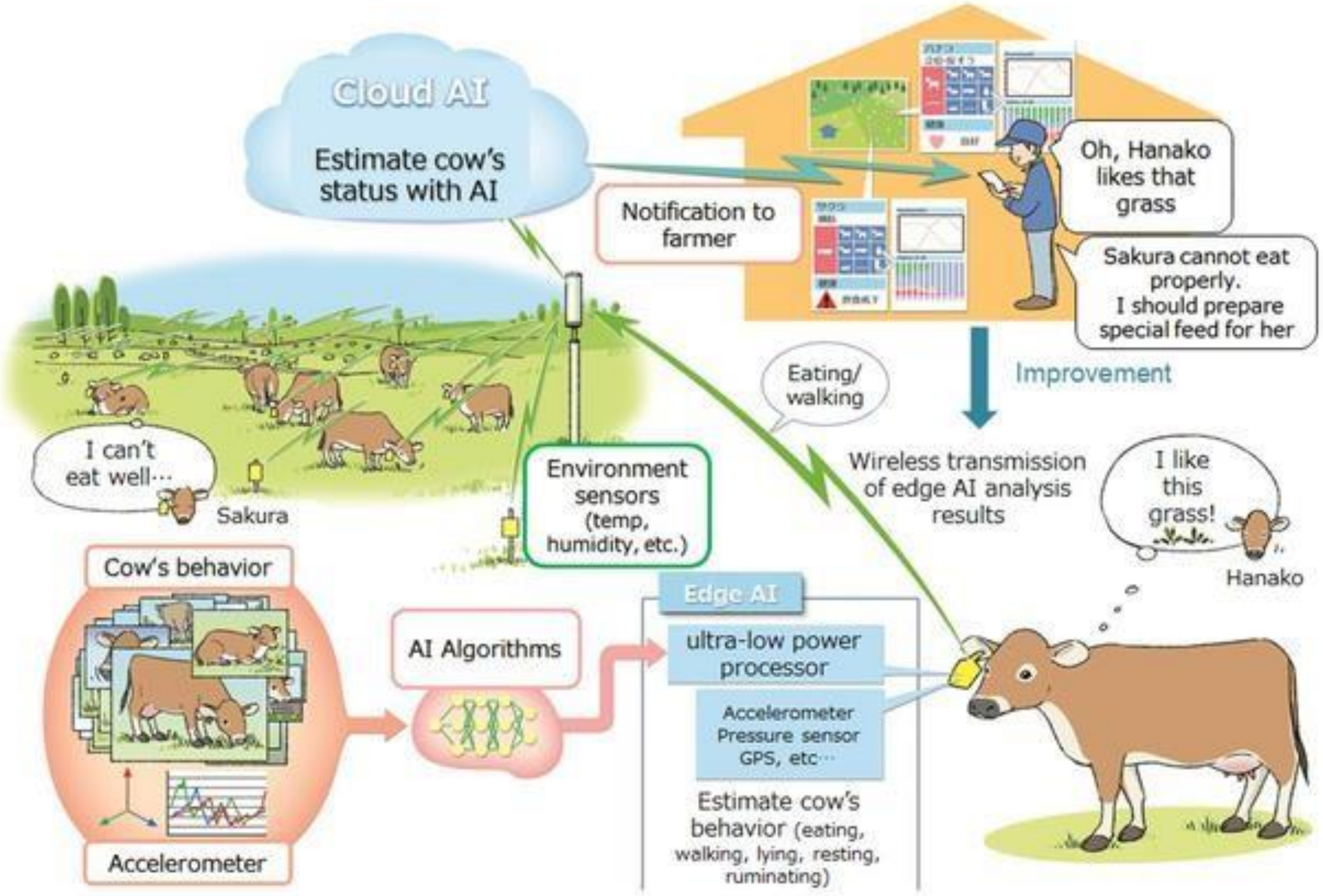
IoT in Agriculture / Livestock

These sensors monitor a variety of health and behavioral indicators to help farmers manage the well-being and productivity of their cattle. The sensors and their respective data points might include:

- **Tail Sensor**: Monitors temperature, activity, estrus cycles (heat), and potentially calving timing.
- **Ear Sensor**: Tracks temperature, general activity, and cud-chewing patterns (rumination time), which are indicators of health and digestion.
- **Nose Band Sensor**: Observes eating behavior, including rumination time, drinking patterns, the number of chews, and could also monitor temperature and rest patterns (up and down time).
- **Reticulorumen Sensor**: Measures temperature within the rumen, activity levels, and pH levels, which are critical for monitoring digestion and metabolic health.
- **Leg Sensor**: Keeps track of physical activity and rest periods by noting when the cow is standing (up time) and lying down (down time).



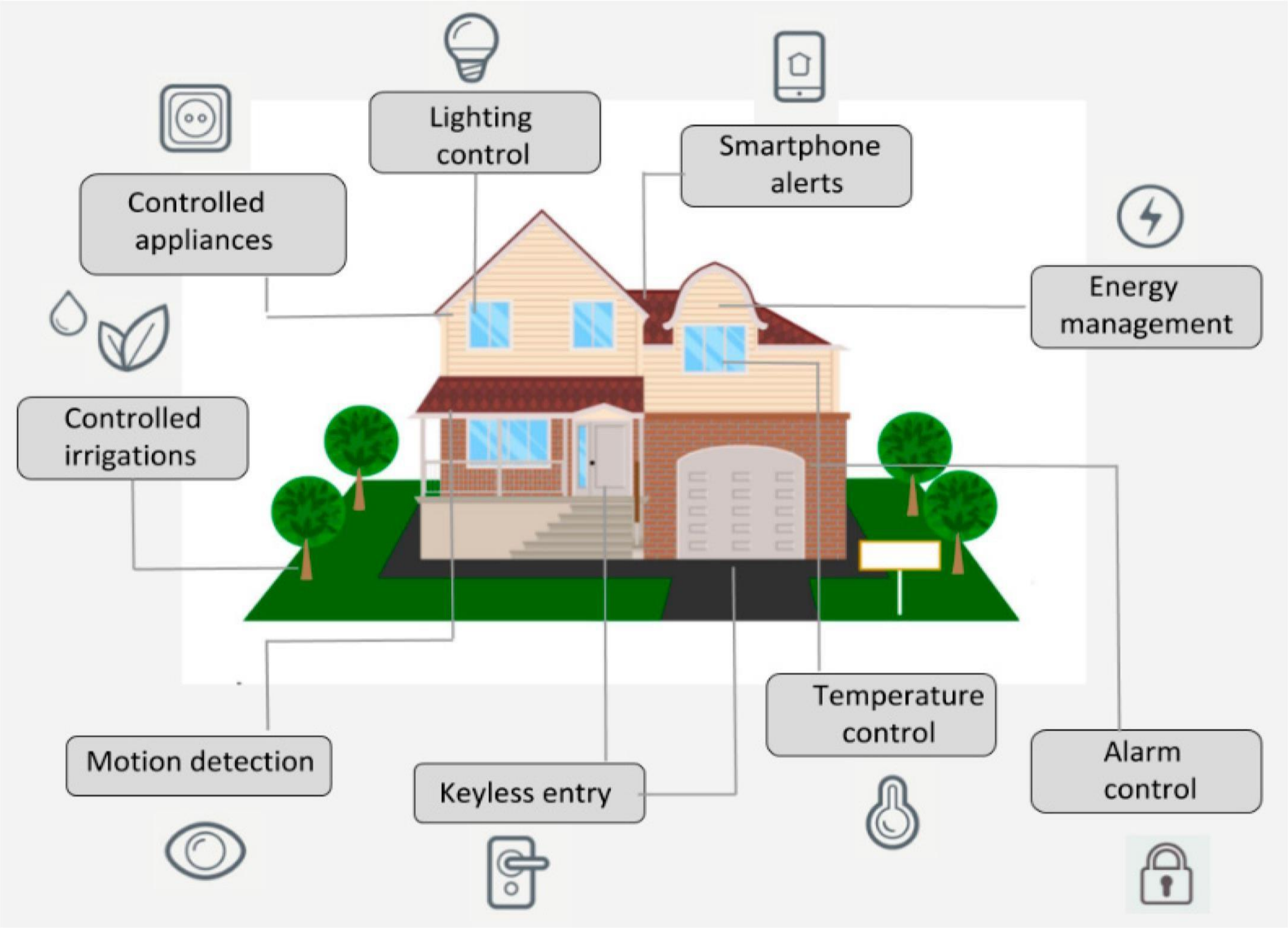
Co-funded by the European Union



- Livestock monitoring and management

Co-funded by the European Union

IoT in Smart Homes



The image illustrate a smart home ecosystem, detailing various IoT-enabled features for home automation. Here's a summary in bullet points:

- **Lighting Control**: Automated systems to manage home lighting for efficiency and convenience.
- **Smartphone Alerts**: Notifications sent to a mobile device regarding home status or security.
- **Energy Management**: System to optimize the use of electricity and reduce costs.
- **Controlled Appliances**: IoT-enabled household appliances that can be monitored and managed remotely.
- **Temperature Control**: Automated regulation of home temperature for comfort and energy savings.
- **Alarm Control**: Security systems that can be armed or disarmed remotely.
- **Keyless Entry**: Electronic lock systems that allow entry without traditional keys.
- **Motion Detection**: Security feature that detects movement around the property.
- **Controlled Irrigations**: Automated watering systems for gardens and lawns, optimizing water usage.

Co-funded by the European Union

IoT in Transportation

Wireless Mesh Cellular 3G/LTE: This indicates the use of a wireless network for communication between devices, which could include both short-range mesh networking and longer-range cellular networks.

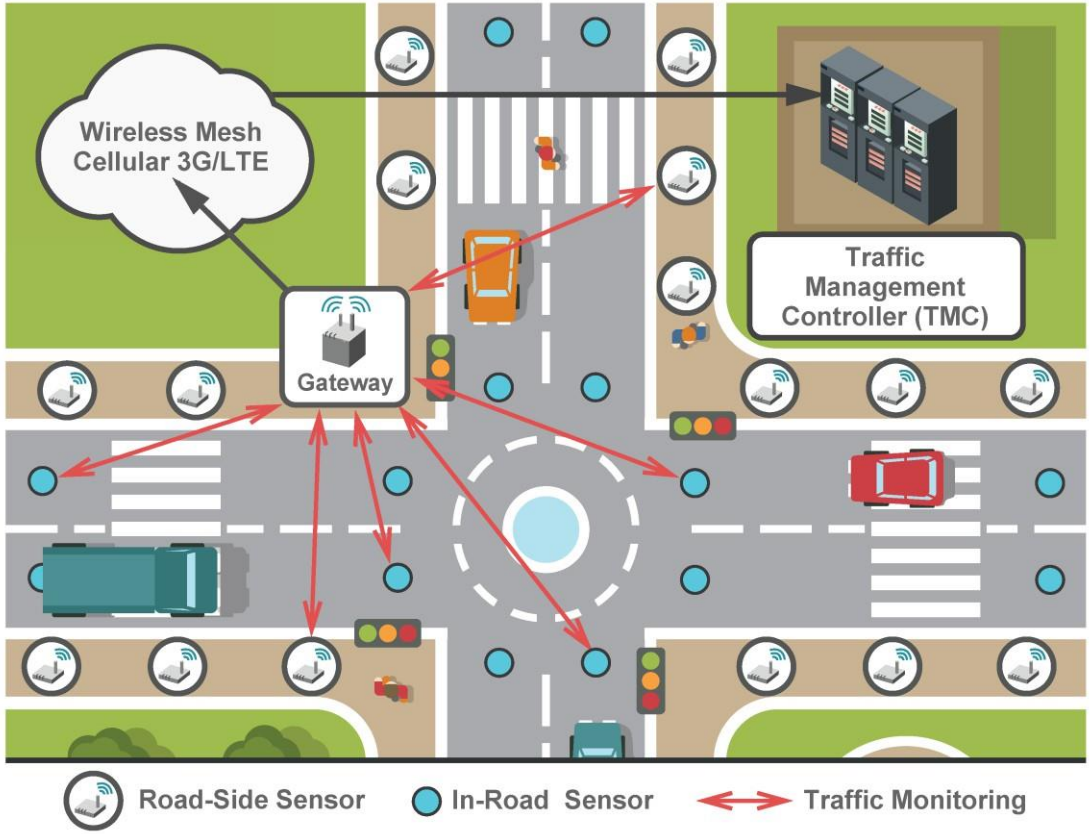
Gateway: Acts as a bridge between the sensors and the larger network, collecting sensor data and forwarding it to the traffic management system.

Road-Side Sensor: Positioned alongside roads to gather data on traffic conditions, vehicle counts, and other environmental factors.

In-Road Sensor: Embedded in the road surface to detect the presence and speed of passing vehicles, contributing to traffic flow analysis.

Traffic Management Controller (TMC): Central system that processes input from various sensors to manage traffic lights, electronic road signs, and other control mechanisms to optimize traffic flow.

Traffic Monitoring: Refers to the overall process of gathering, analyzing, and responding to real-time traffic data to improve efficiency and reduce congestion.



Smart traffic management system that utilizes various types of sensors and connectivity technologies to monitor and control traffic flow

IoT in Transportation

The image illustrates various IoT applications in the field of transportation logistics, particularly for a trucking fleet. Key IoT components and their functionalities might include:

Tyre Pressure: Monitoring for optimal fuel efficiency and safety.

GPS: Real-time vehicle tracking for navigation and fleet management.

Tachograph: Recording driving time, speed, and distance for compliance and safety.

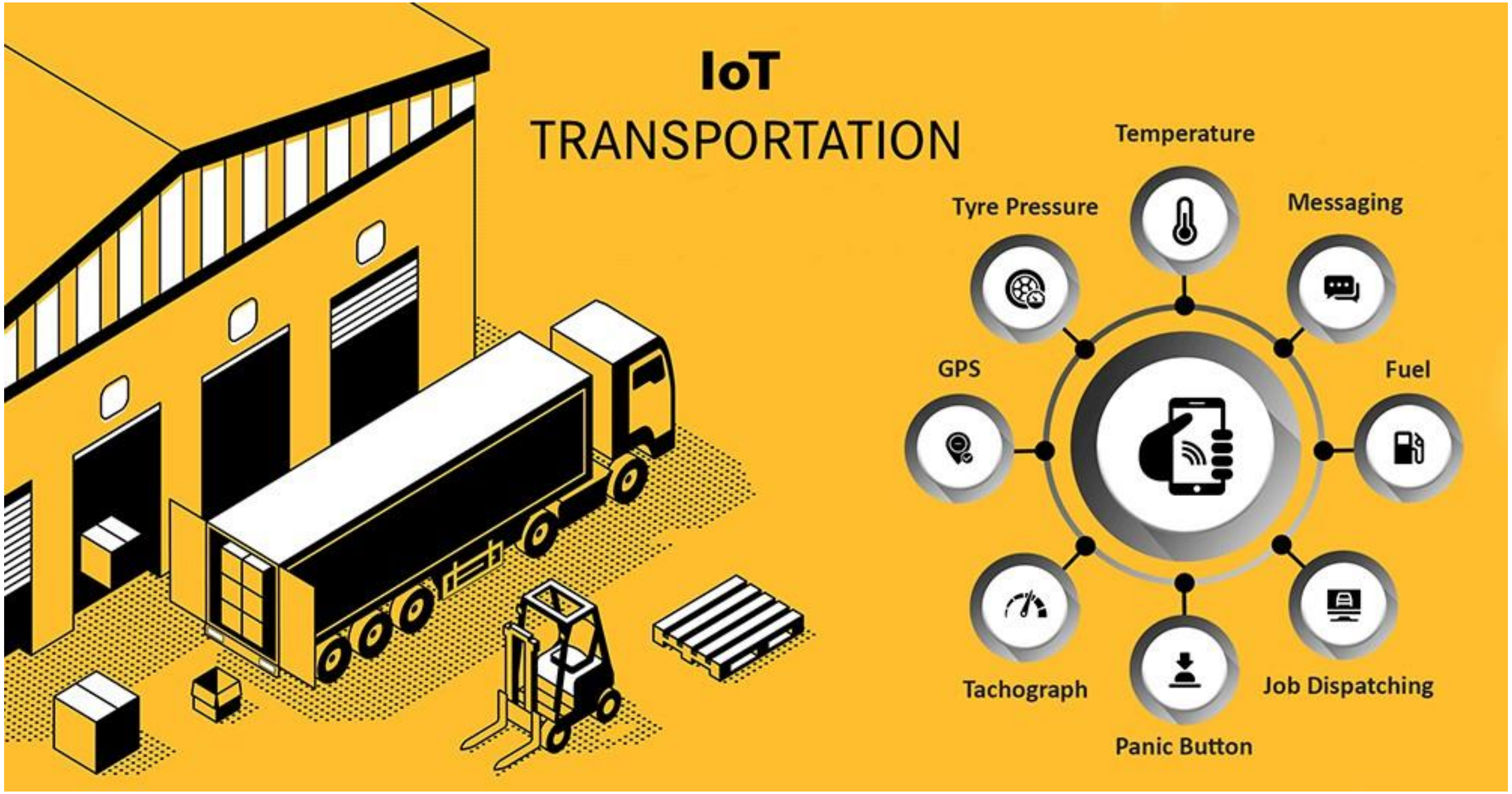
Panic Button: For emergency situations, allowing drivers to alert the central system.

Temperature: Ensuring the proper climate for temperature-sensitive cargo.

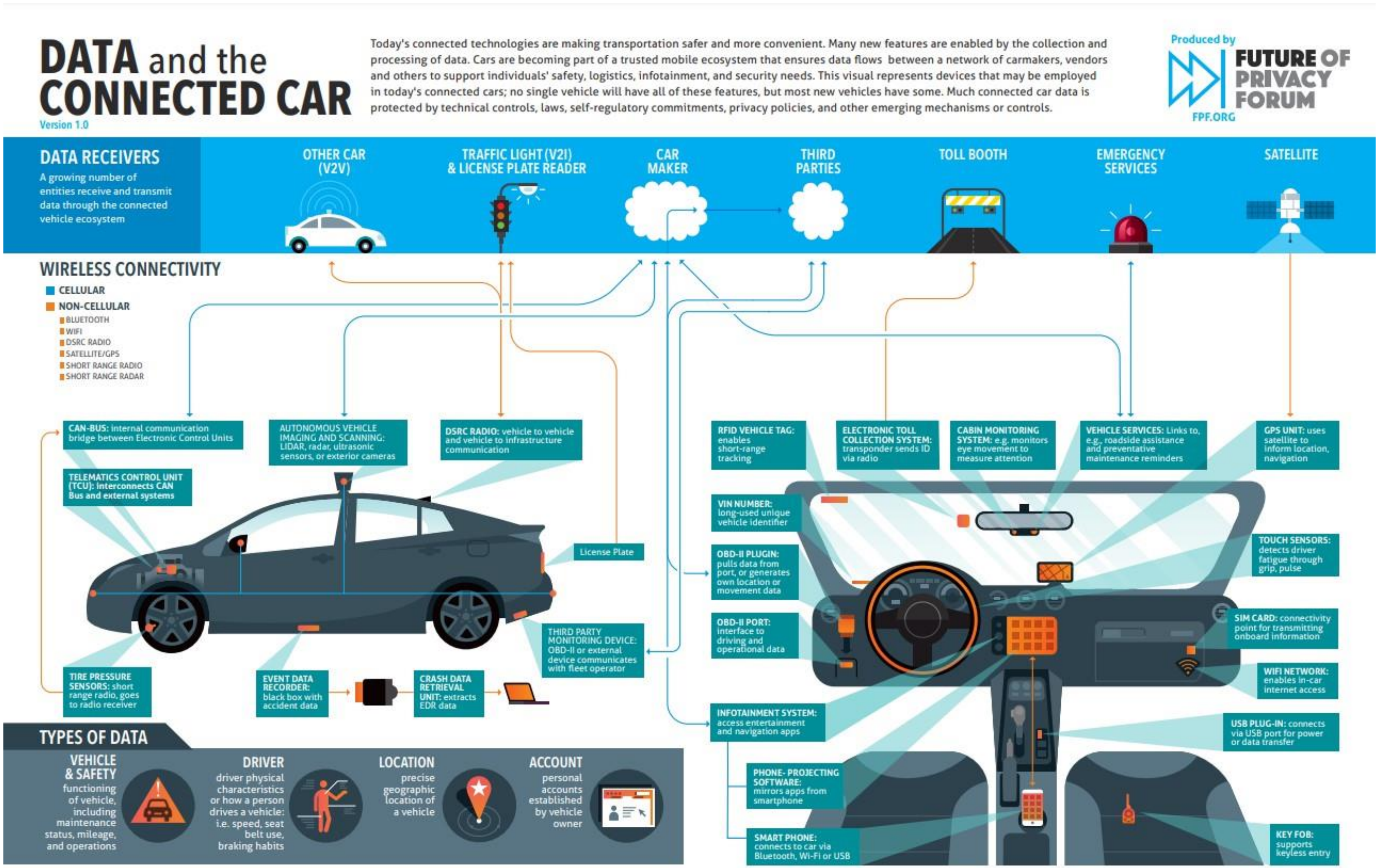
Messaging: Communication between the driver and dispatch.

Fuel: Monitoring fuel consumption and optimizing routes.

Job Dispatching: Assigning and managing delivery tasks electronically.

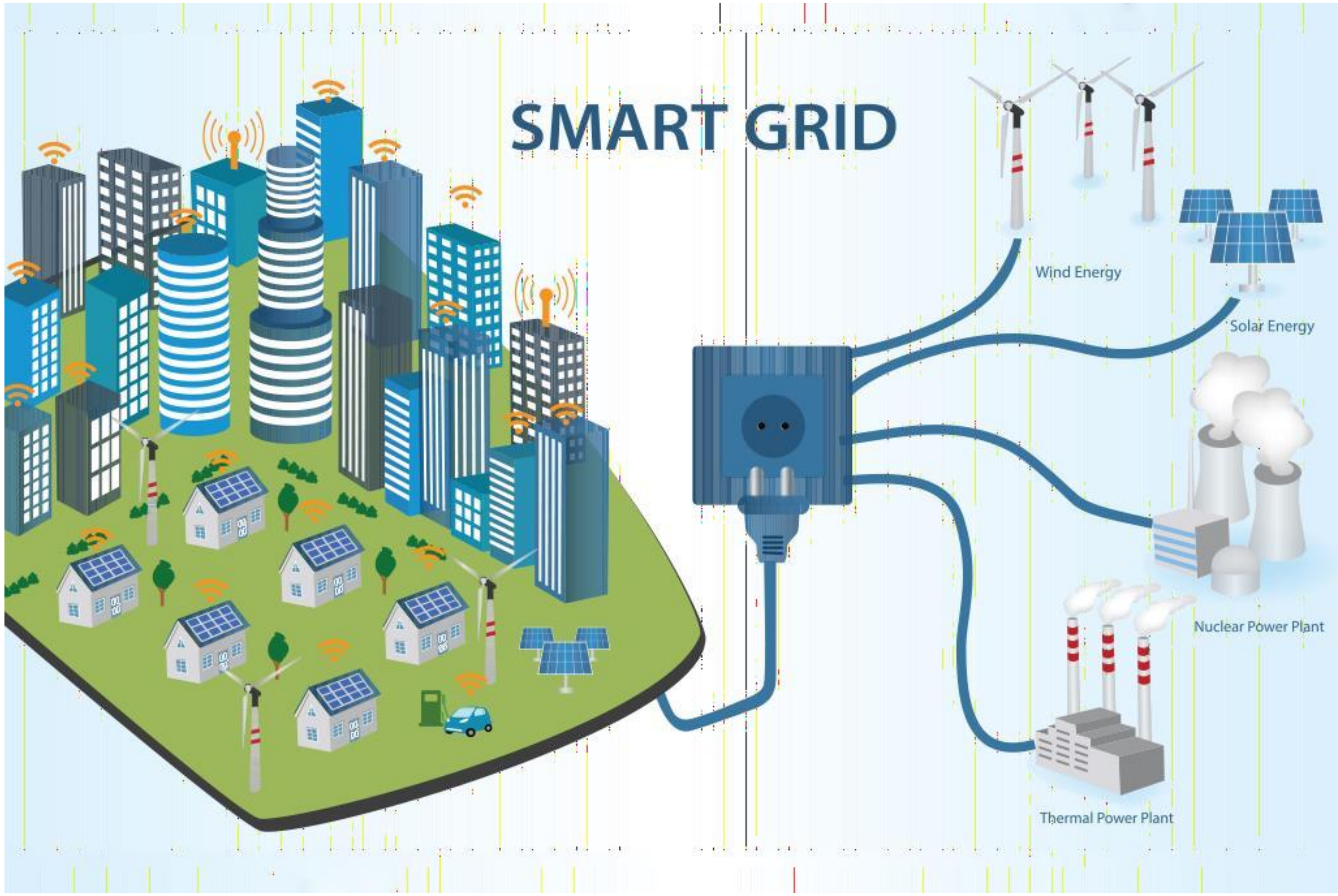


Co-funded by the European Union



Co-funded by the European Union

IoT in Energy Management



Smart grid technology

Smart grid allows a power company to assess system health in significantly more detail than was previously possible.

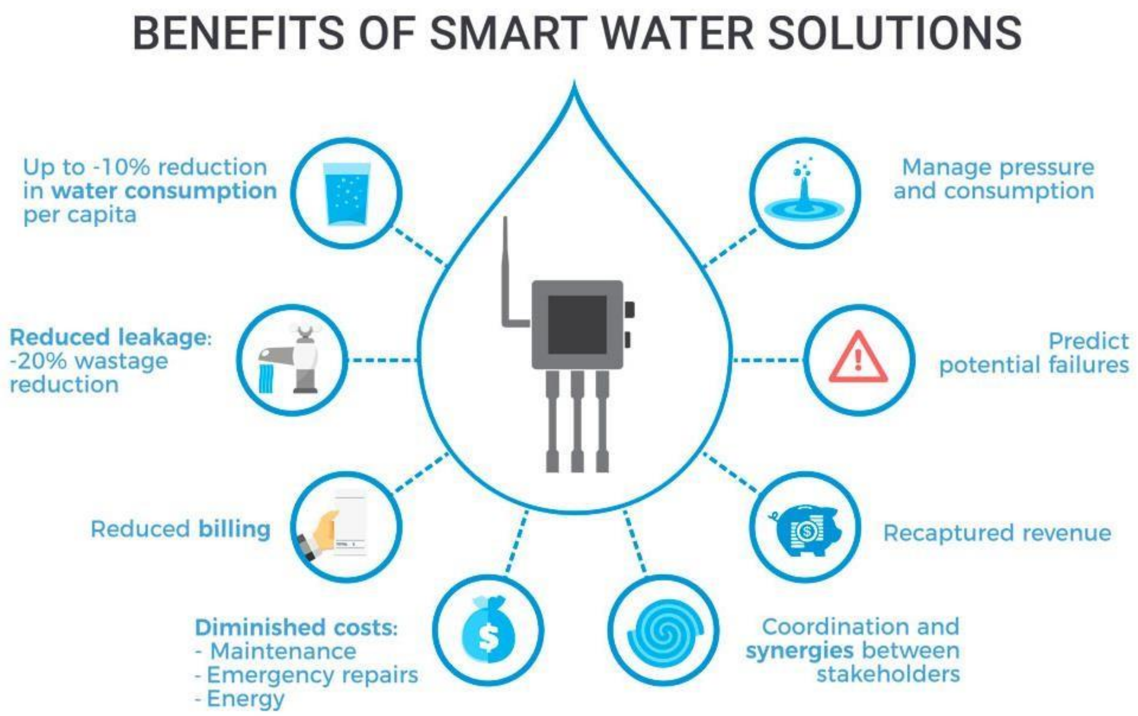
For instance, with smart meters the power company can discover real time power demands with a granularity and accuracy that is simply not possible with older technology.

This can allow them to better predict and respond to sudden increases in demand, which can help to prevent blackouts.

Co-funded by the European Union

Water supply

Consumption Efficiency: Smart water solutions can lead to up to a 10% reduction in water consumption per capita, indicating significant savings and more sustainable usage patterns.
Leakage Reduction: There's a potential for a 20% reduction in water wastage due to decreased leakage, which can be achieved through more precise monitoring and rapid response capabilities.
Cost Savings: Reduced billing for consumers and diminished operational costs for providers are expected, including savings on maintenance, emergency repairs, and energy.
Operational Management: Management of pressure and consumption is improved, which helps in preserving the integrity of water supply systems and ensuring optimal delivery.
Revenue Protection: The ability to recapture lost revenue, likely through more accurate metering and billing practices.
Predictive Maintenance: Advanced systems can predict potential failures before they occur, which minimizes downtime and prevents large-scale disruptions.
Stakeholder Collaboration: Enhanced coordination and synergies between stakeholders, such as utility companies, regulatory bodies, and consumers, leading to improved service delivery.



Co-funded by the European Union

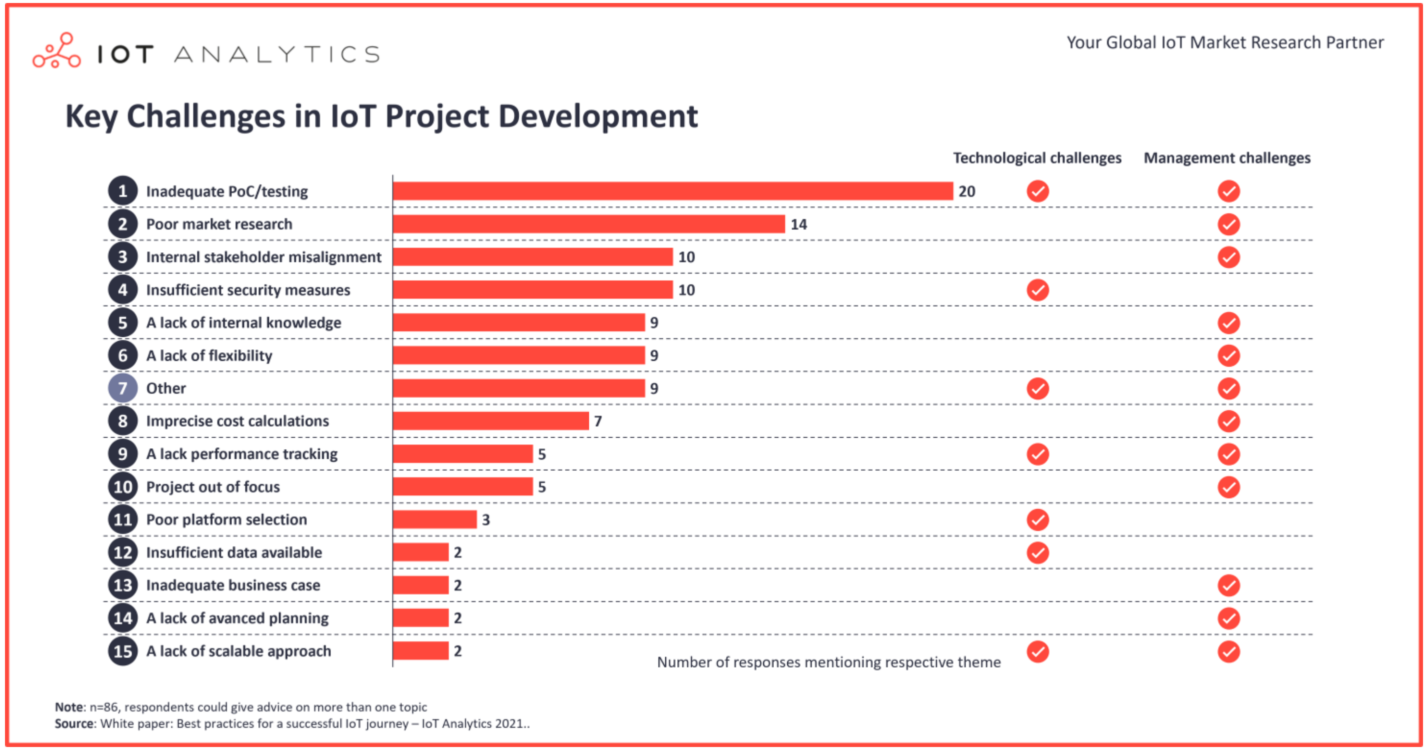
Impact on Business Operations

Smart Solutions: IoT aids in launching new smart products that offer added value compared to standard solutions.
Simpler Automation: IoT enables two-way communication between devices, streamlining business processes and enhancing user experiences with automation.
Lower Downtime: IoT adoption can lead to decreased downtime costs by improving predictive maintenance and the longevity of devices.
Environmental Sustainability: IoT contributes to sustainability through systems that monitor and aim to reduce energy consumption by significant percentages.
Better Assets Tracking: The impact of IoT on businesses includes improved asset tracking, providing real-time location data and usage insights.
Accelerated Cloud Development: IoT solutions demand accelerated development in cloud technologies to ensure adequate support for data storage and management.

Co-funded by the European Union

Challenges in IoT for Business

In IoT project development, key challenges highlighted include inadequate testing, misalignment among internal stakeholders, and poor market research. Security and knowledge gaps within the team are critical areas needing attention. Furthermore, maintaining project focus, precise cost estimation, performance tracking, and ensuring a scalable approach are essential for project success. Addressing these technological and management challenges is vital to the effective deployment of IoT solutions.



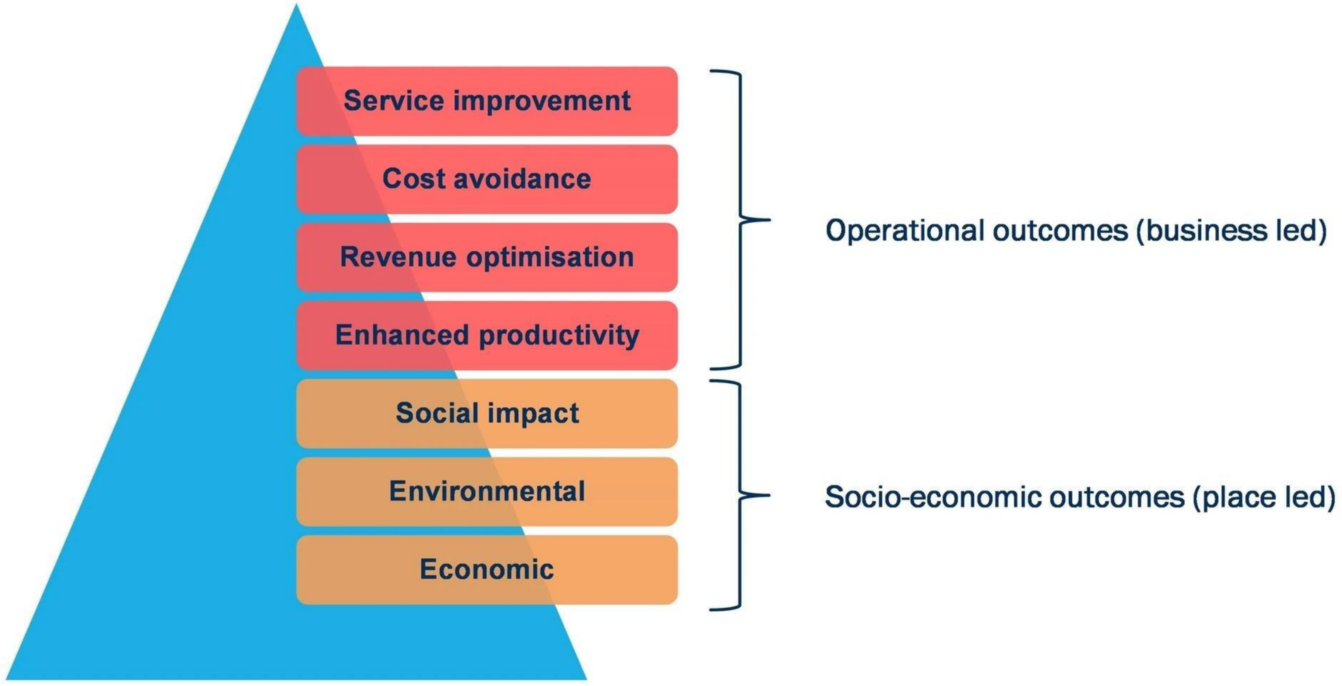
Co-funded by the European Union

IoT and Corporate Responsibility

Social Impact: IoT projects should be assessed for their impact on communities, ensuring they contribute positively and do not exacerbate social inequalities.

Environmental: Corporate responsibility includes environmental stewardship, where IoT can play a significant role in monitoring and reducing a company's carbon footprint.

Economic: Beyond immediate business benefits, IoT projects should bolster the broader economy, creating jobs, and promoting economic development in a responsible manner.



Co-funded by the European Union

Discover Technologies, expand opportunities!

Thank you!

For more information:

www.betesproject.eu

www.facebook.com/BETESproject

ecect.projects@gmail.com

+ 357 96520112 (Cyprus)

Co-funded by the European Union