Introduction

Thanasis Papaioannou

Introduction to IoT Systems and Technologies

MSc on Modern Communication Systems and Internet of Things

University of Thessaly, Larisa, Greece

Fall ’23

Quick who-is-who

- Assistant Professor in Cloud Computing, Dept. of Digital Industrial Technologies, National and Kapodistrian University of Athens
- 20+ years experience in programming and research
  - ✓ JAVA, C, C++, MATLAB, Python, Javascript…
- Taught in University of Thessaly, EPFL, Athens University of Economics and Business
  - Distributed Systems, Programming, IoT Data Management and Analytics, Computer Networks and Security, Software Design, Data Privacy
- Researcher since 1998
  - ✓ More than 80 publications, more than 2000 citations
- E-mail: atpapaioannou@uth.gr

Course Outline

- IoT Definitions – IoT Architecture
- Sensors/Actuators
- Arduino
- Introduction to Python
- IoT Basic Communication Protocols
- IoT Basic Networking
- Raspberry Pi
- IoT Data Storage
- IoT Data Visualization – Grafana
- IoT Middleware
- And more…

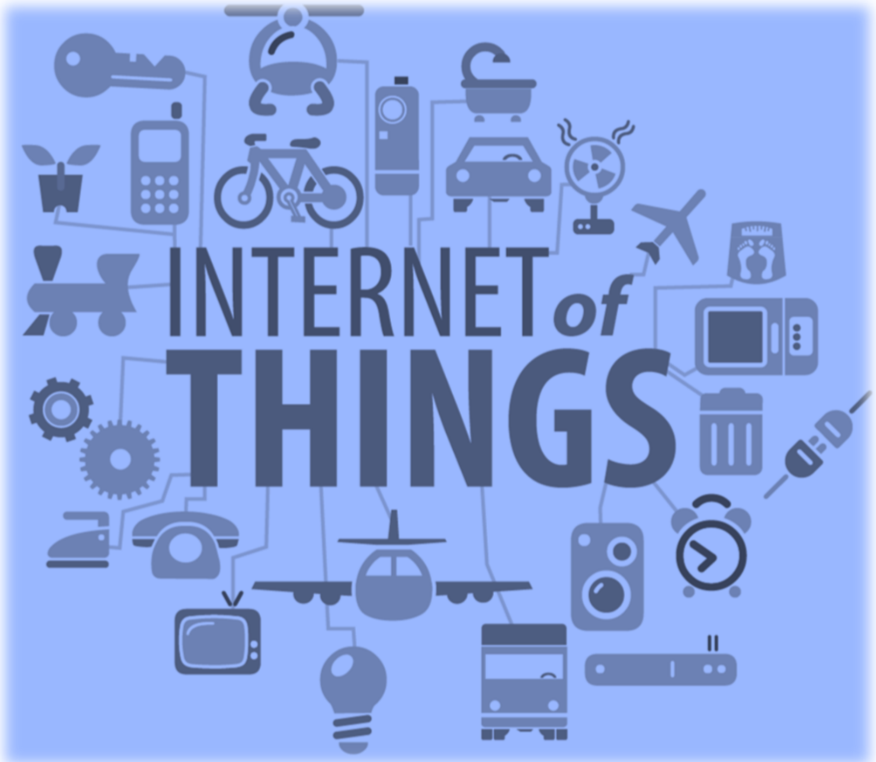
Course Grading

- Exercises/projects (30%)
- Final exam (70%)

Hardware

- Arduino UNO (or better)
- Raspberry PI 3 (or more)

What is IoT?



IoT is…. (According to EU)

A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities

IoT is.... (According to ITU)

A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies [ITU-T Y.2060]

IoT is.... (According to IETF)

IoT is a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols

IoT is.... (According to IEEE)

A network of items each embedded with sensors which are connected to the Internet.

IoT is.... (According to Wikipedia)

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions.

Internet of Things - IoT

- Internet technology connecting devices, machines and tools to the Internet by means of wireless technologies
- Over 9.7 billion of “things” connected to the Internet, as of now (2020). **Source**: Statista.com
- “Things” connected to the Internet project to more than 29 billion in 2030. **Source**: Statista.com
- Unification of technologies such as low power and embedded systems, cloud computing, big data, machine learning, and networking

Origin of Technology

- In the 2000s, we are heading into a new era of ubiquity, where the "users" of the Internet will be counted in billions and where humans may become the minority as generators and receivers of traffic

- Instead, most of the traffic will flow between devices and all kinds of "things", thereby creating a much wider and more complex Internet of Things

Source: "Internet of Things", ITU Internet Report 2005

Origins

- The title of the report was “Internet of Things”
- Discussed the possibility of Internet-connected M2M connectivity networks, extending to common household devices
- Some areas identified as IoT enablers:
  - RFID
  - Nanotechnology
  - Sensors
  - Smart Networks

Source: “Internet of Things”, ITU Internet Report 2005

Alternate Definition

“The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment”

Gartner Research

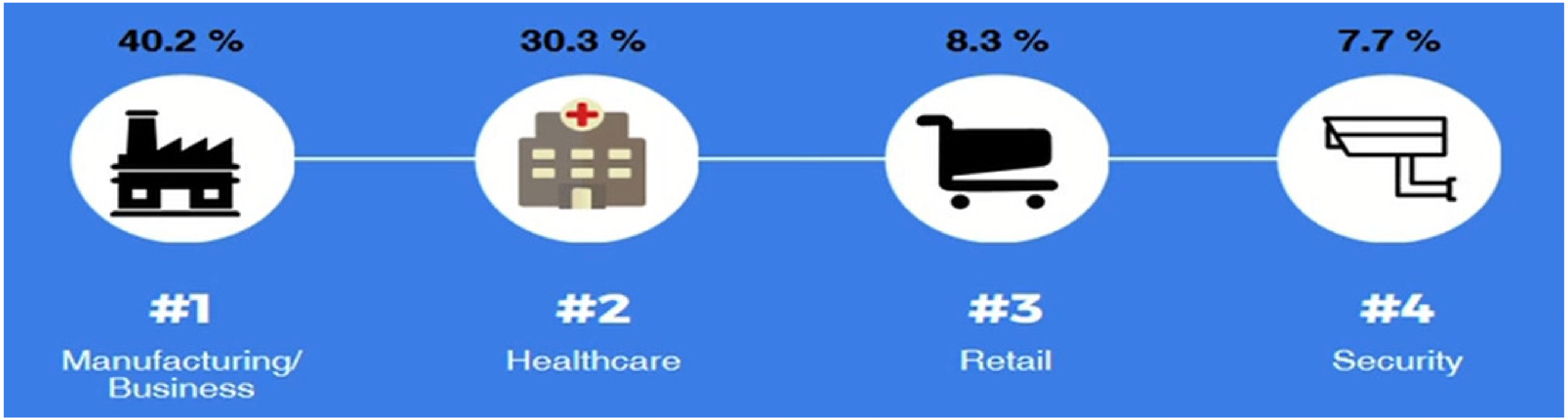
http://www.gartner.com/it-glossary/internet-of-things

Characteristics

- Efficient, scalable and associated architecture
- Unambiguous naming and addressing
- Abundance of sleeping nodes, mobile and non-IP devices
- Intermittent connectivity

Source: T. Savolainen, J. Soininen, and B. Silverajan. "IPv6 Addressing Strategies for IoT", IEEE Sensors, vol. 13, no. 10, Oct. 2013

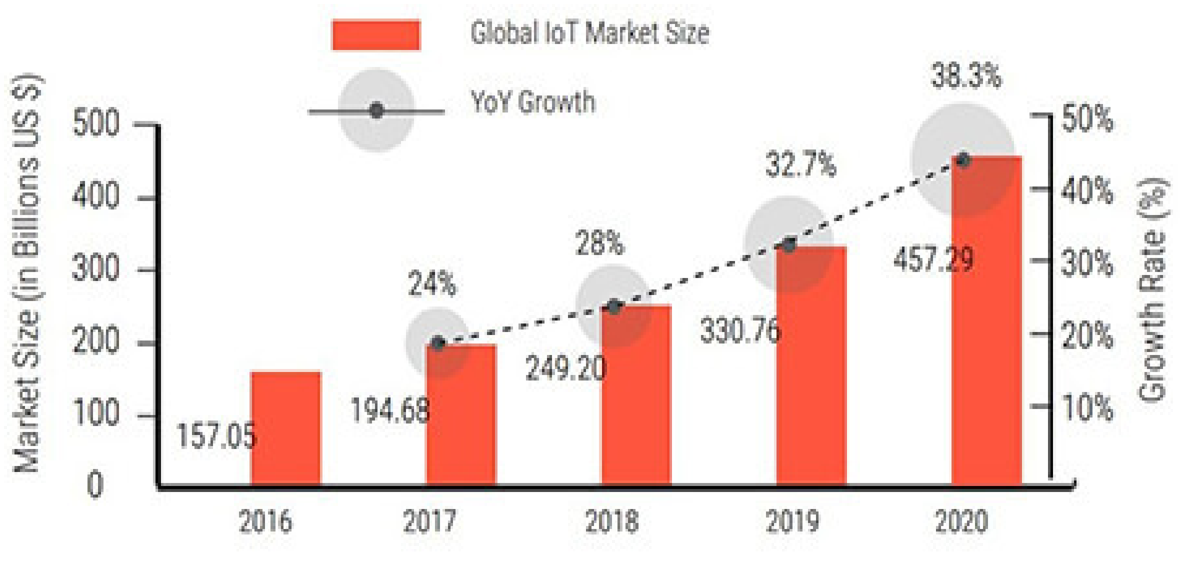
IoT Market Share



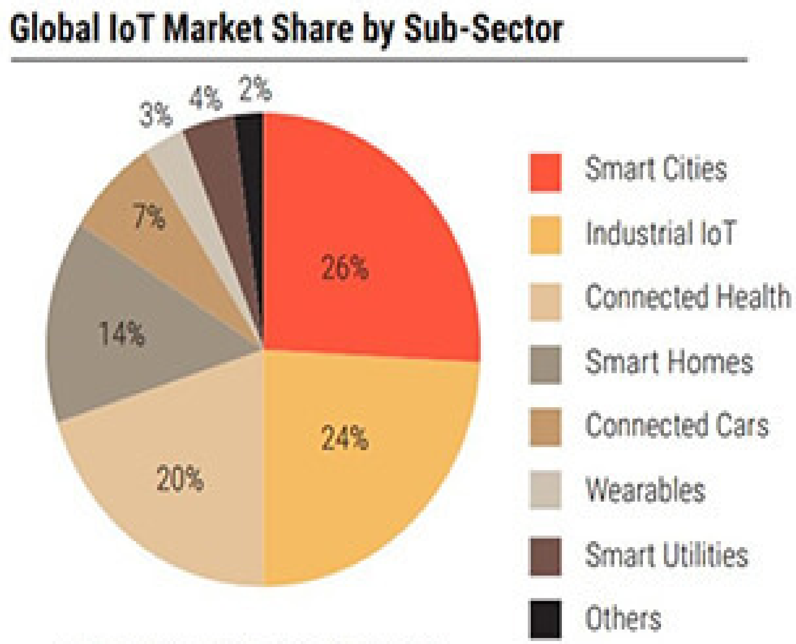
Verticals

- Business manufacturing
  - Real-time analytics of supply chains and equipment, robotic machinery
- Healthcare
  - Portable health monitoring, electronic record keeping, pharmaceutical safeguards
- Retail
  - Inventory tracking, smartphone purchasing, anonymous analytics of consumer choices
- Security
  - Biometric and facial recognition locks, remote sensors

Global Scenario IoT Market

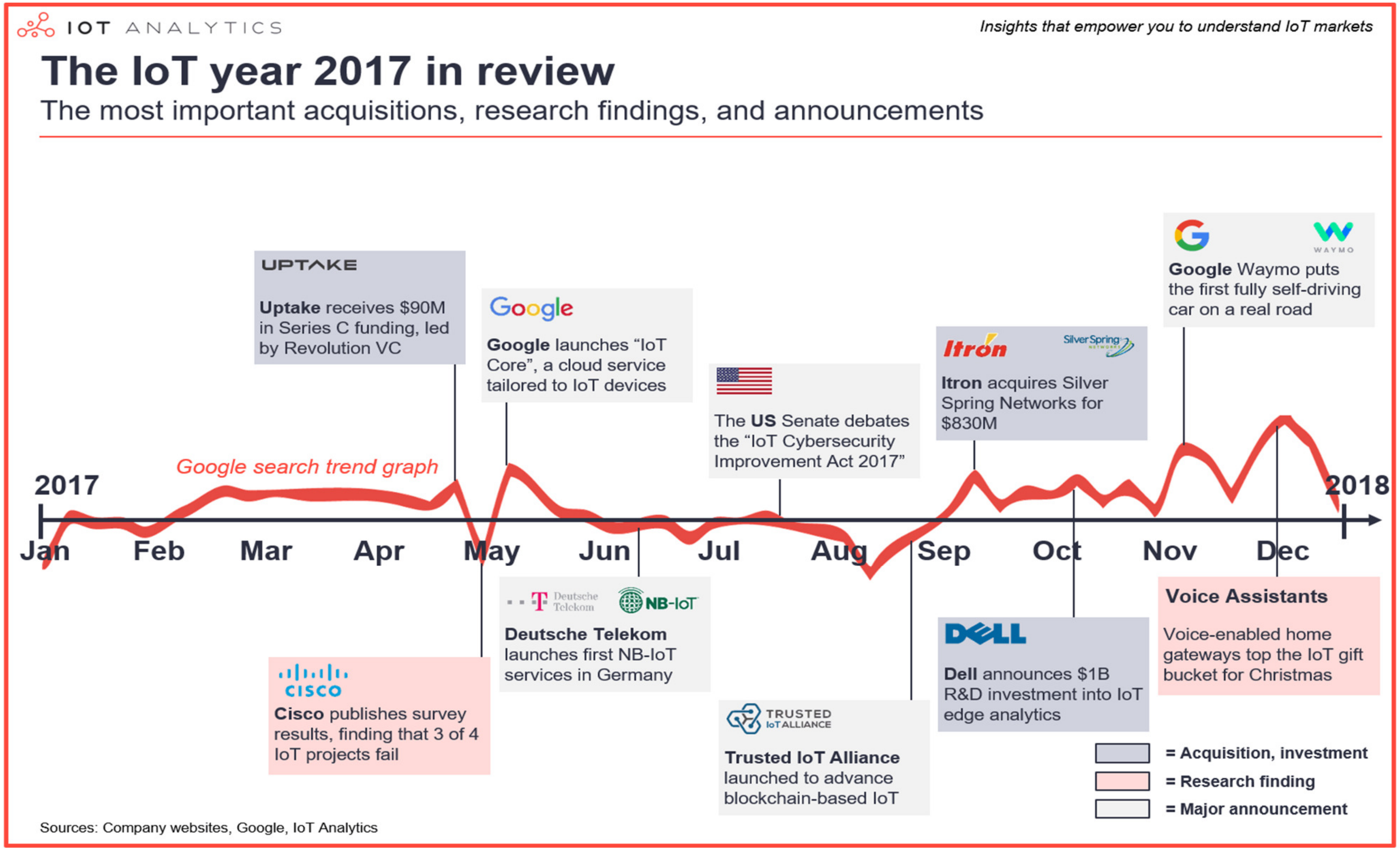


[Sources: GrowthEnabler Analysis/MarketsandMarkets]



[Source: GrowthEnabler Analysis]

Global Scenario IoT Market



Evolution of connected devices

History of Connected Devices

- ATM
  - These ubiquitous money dispensers went online for the first-time way back in 1974
- Web
  - World Wide Web made its debut in 1991 to revolutionize computing and communications
- Smart Meters
  - The first power meters communicate remotely with the grid were installed in the early 2000s
- Digital Locks
  - Smartphones can be used to lock and unlock doors remotely, and business owners can change key codes rapidly to grant or restrict access to employees and guests

History of Connected Devices

- Smart Healthcare
  - Devices connect to hospitals, doctors and relatives to alert them of medical emergencies and take preventive measures
- Smart Vehicles
  - Vehicles save themselves and alert owners about system failures
- Smart Cities
  - City-wide infrastructure communicating amongst themselves for unified and synchronized operations and information dissemination
- Smart Dust
  - Computers smaller than a grain of sand can be sprayed or injected almost anywhere to measure chemicals in the soil or to diagnose problems in the human body

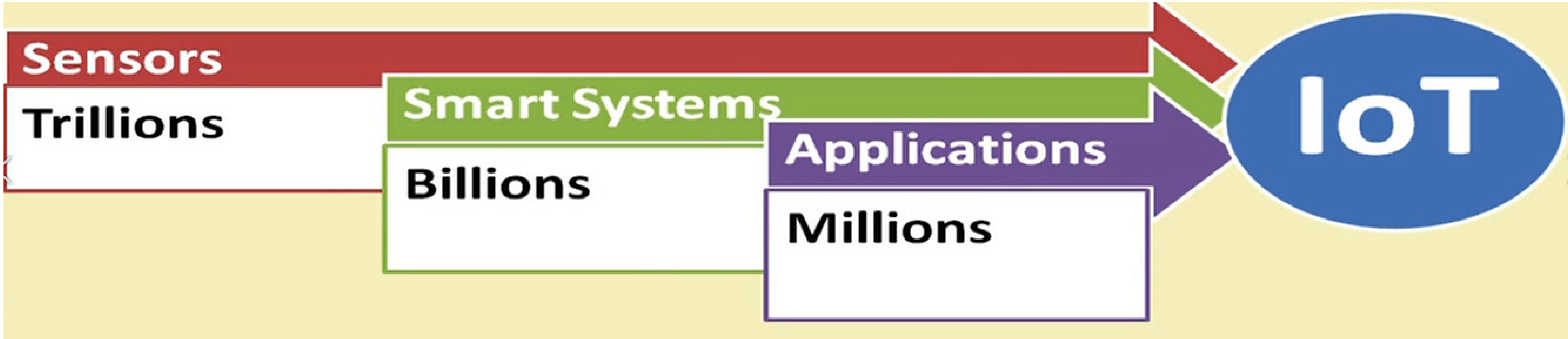
Modern Day IoT Applications

- Smart parking
- Structural health
- Noise urban maps
- Smartphone detection
- Traffic congestion
- Smart lighting
- Waste management
- Smart roads
- River floods
- Smart Grid
- Fuel tank level
- Photovoltaic installations
- Water flow
- Silos stock calculation
- Perimeter access control
- Liquid presence

Modern Day Applications

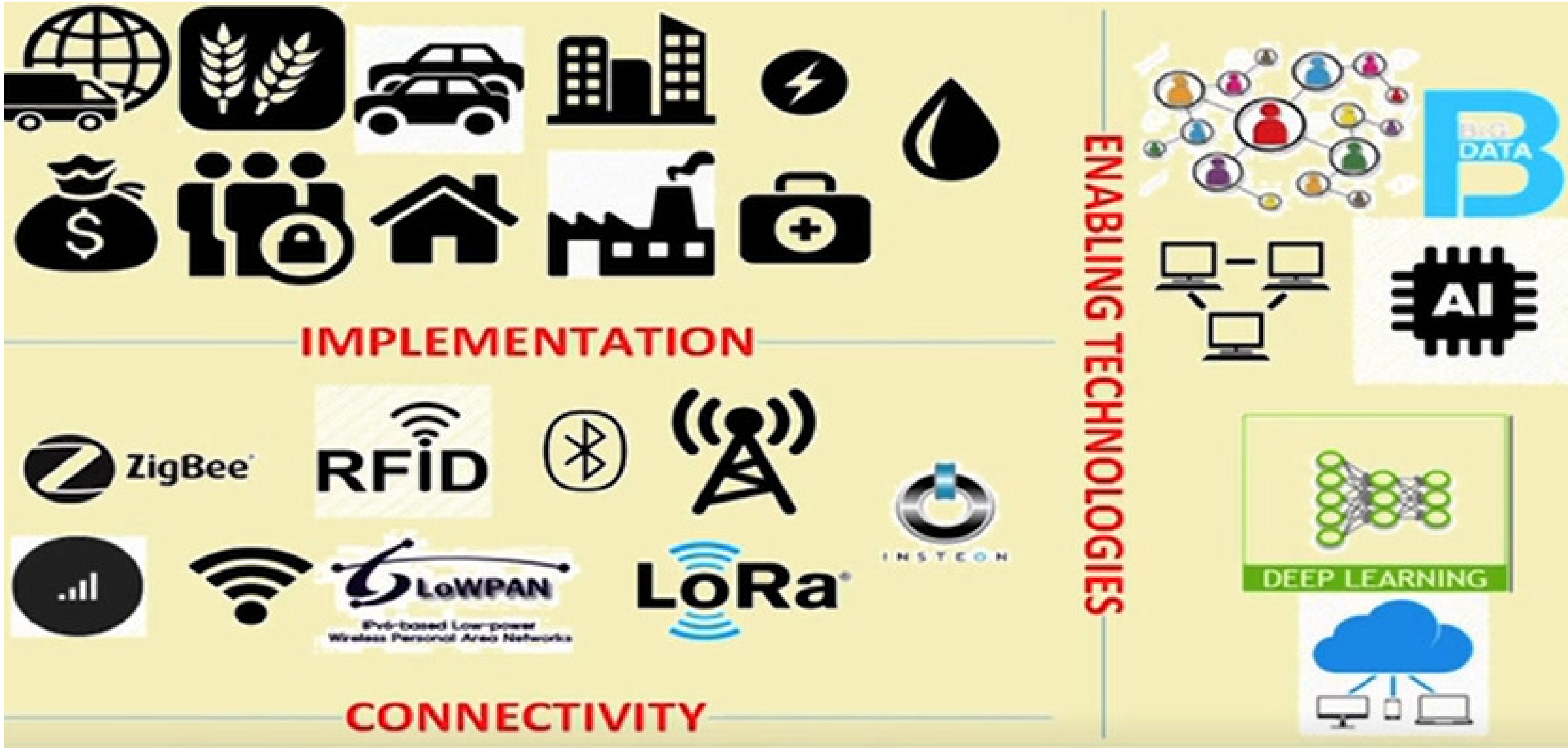
- Forest fire detection
- Air pollution monitoring
- Snow level monitoring
- Landslide and avalanche prevention
- Earthquake early detection
- Water leakages
- Radiation levels
- Explosive and hazardous gases
- Supply chain control
- NFC payment
- Intelligence shopping applications
- Smart product management

Expected



Sensors
Trillions
Smart Systems
Billions
Applications
Millions
IoT

IoT Enablers



Connectivity Layers

Baseline Technologies

- A number of technologies that are very closely related to IoT include
  - machine to machine (M2M) communications
  - cyber physical systems (CPS)
  - web of things (WoT)

Machine to Machine Communication (M2M)

- Data communication among the physical things which do not need human interaction
- Examples:
  - Data communication between things and a server
  - Thing-to-thing communication either directly or over a network

M2M Communication – Key Elements

M2M Device

- Device capable of replying to request for data contained within those devices or capable of transmitting data autonomously.

M2M Area Network (Device Domain)

- Provide connectivity between M2M Devices and M2M Gateways, e.g. personal area network.

M2M Gateway

- Uses M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.

M2M Communication Networks (Network Domain)

- Communications between the M2M Gateway(s) and M2M application(s), e.g. xDSL, LTE, WiMAX, and WLAN.

M2M Applications

- Contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.

IoT vs M2M

- M2M refers to communications and interactions between machines and devices
- Such interactions can occur via cloud computing infrastructure
- M2M offers the means for managing devices and devices interaction, while also collecting machine and/or sensor data
- M2M is a term introduced by telecommunications service providers and pays emphasis on machine interactions via one or more telecom/communication networks (e.g., 3G, 4G, 5G, satellite, public networks)

IoT vs M2M

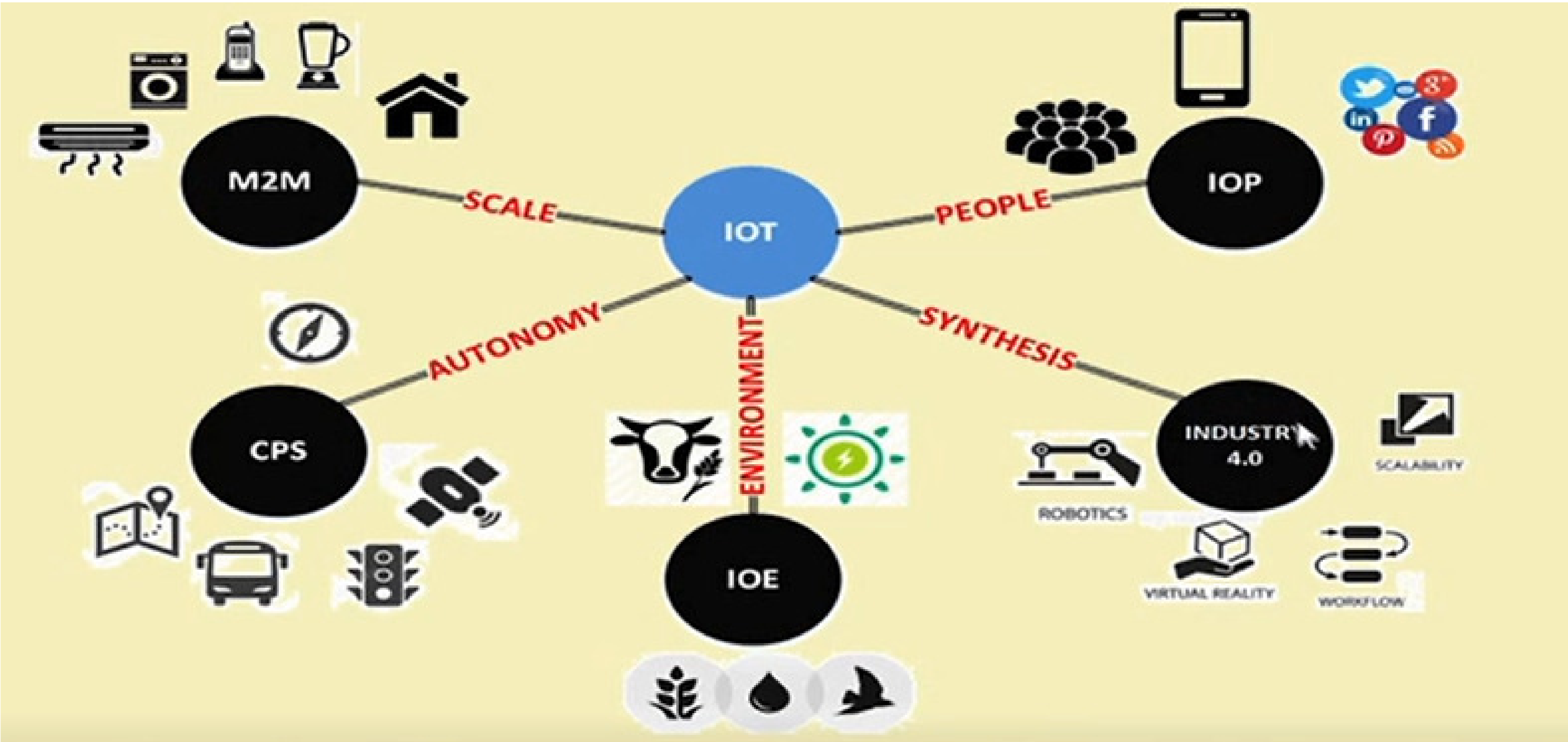
- **M2M is part of the IoT**, while M2M standards have a prominent place in the IoT standards landscape
  - However, IoT has a broader scope than M2M since it comprises a broader range of interactions including interactions between devices/things, things and people, things with applications, and people with applications
  - IoT also enables the compositions of workflows comprising all of the above interactions
- IoT includes the notion of Internet connectivity (which is provided in most of the networks outlined above) but is not necessarily focused on the use of telecom networks

IoT vs Web-of-Things (WoT)

- Web of Things (WoT) describes a set of standards by the World Wide Web Consortium (W3C) for the interoperability of different Internet of things (IoT) platforms and application domains.
  - https://www.w3.org/TR/wot-thing-description/

- From a developer's perspective, the WoT enables access and control over IoT resources and applications using mainstream web technologies, such as HTML5.0, JavaScript, Ajax, PHP , Ruby n' Rails etc.
  - The approach to building WoT is therefore based on RESTful principle and REST APIs, which enable both developers and employers to benefit from the popularity and maturity of web technologies
  - Still, building in the WoT has various scalability, security, etc. challenges, especially as part of a roadmap towards a global WoT

Technological Interdependence

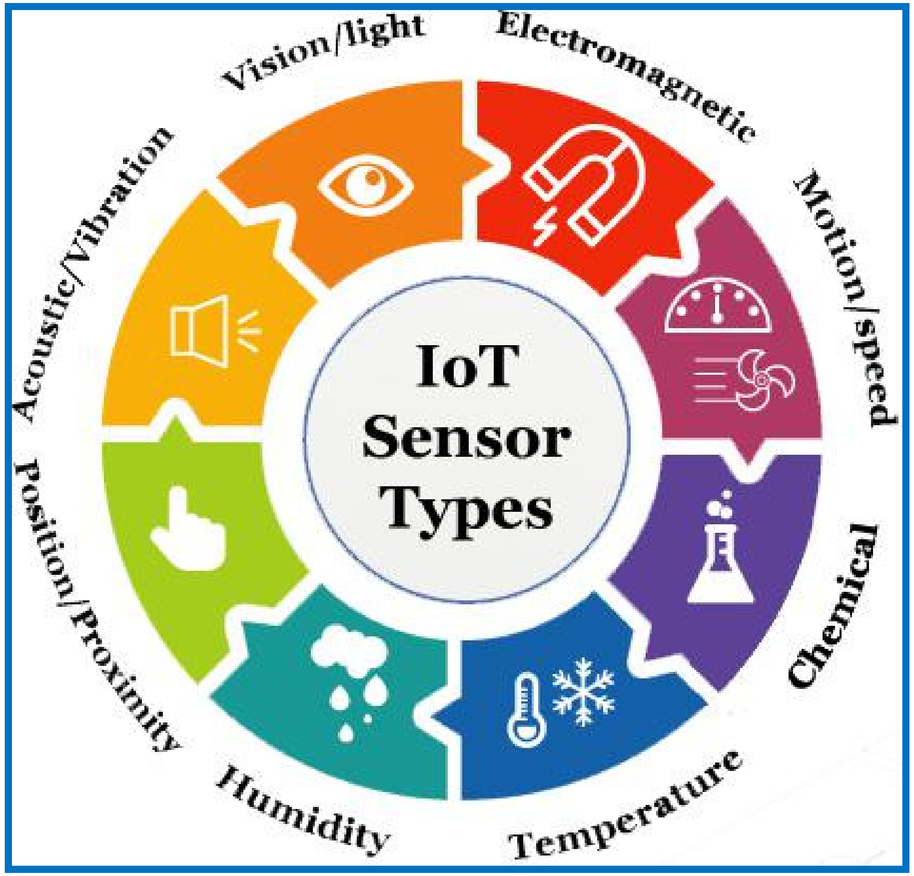


Building blocks of IoT

- End Devices / Nodes
- Gateways / Local Processing Nodes
- Connectivity
- Cloud Based Application and Storage

Building blocks of IoT

- End Devices / Nodes
  - Sensors
  - Objects
  - RFID Tags
  - Actuators

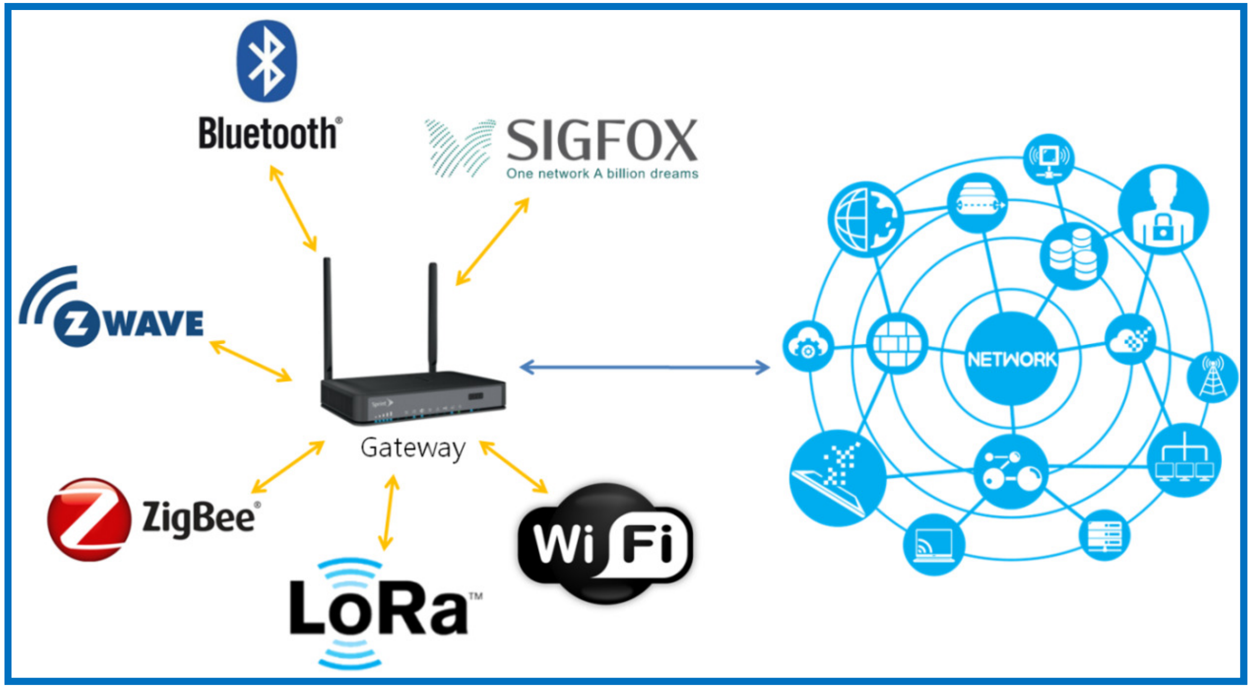


Building blocks of IoT

- Gateways / Local Processing Unit
  - Middleware
  - IoT Readers
  - Signal Receivers
  - Transceivers

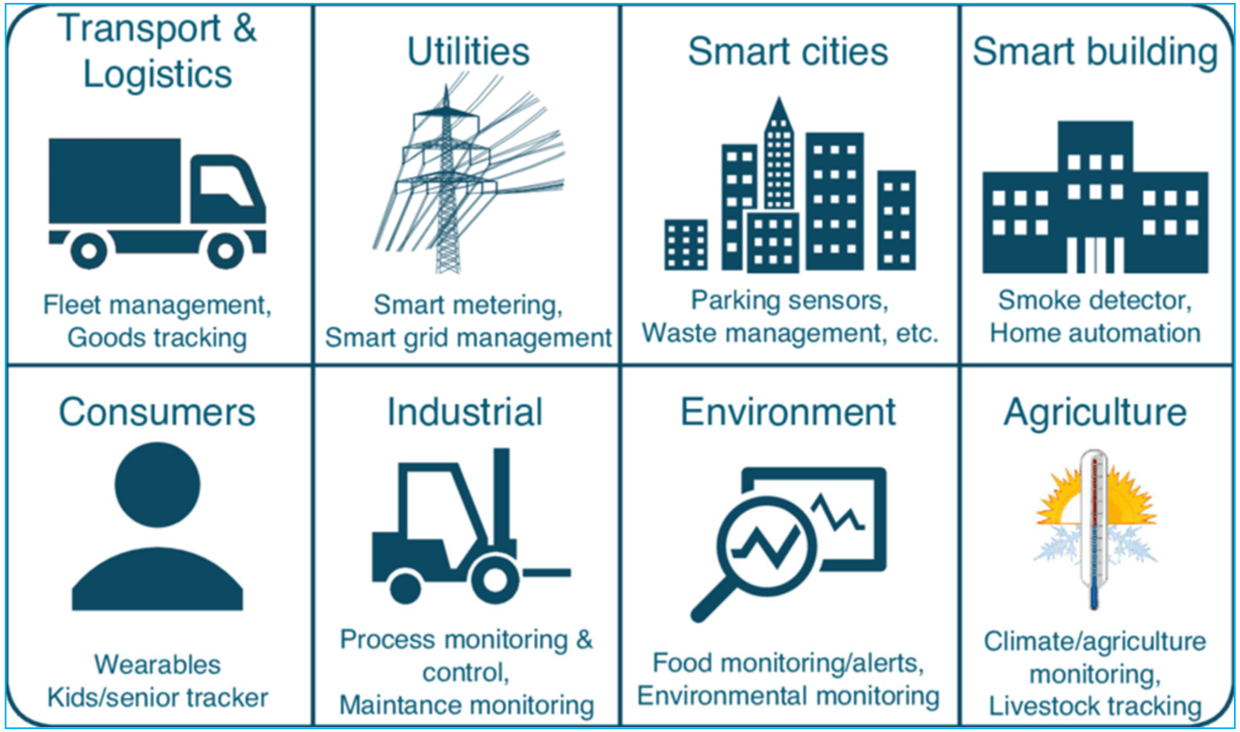
Building blocks of IoT

- Network (Connectivity)
  - WiFi
  - Bluetooth
  - ZigBee
  - LoRa

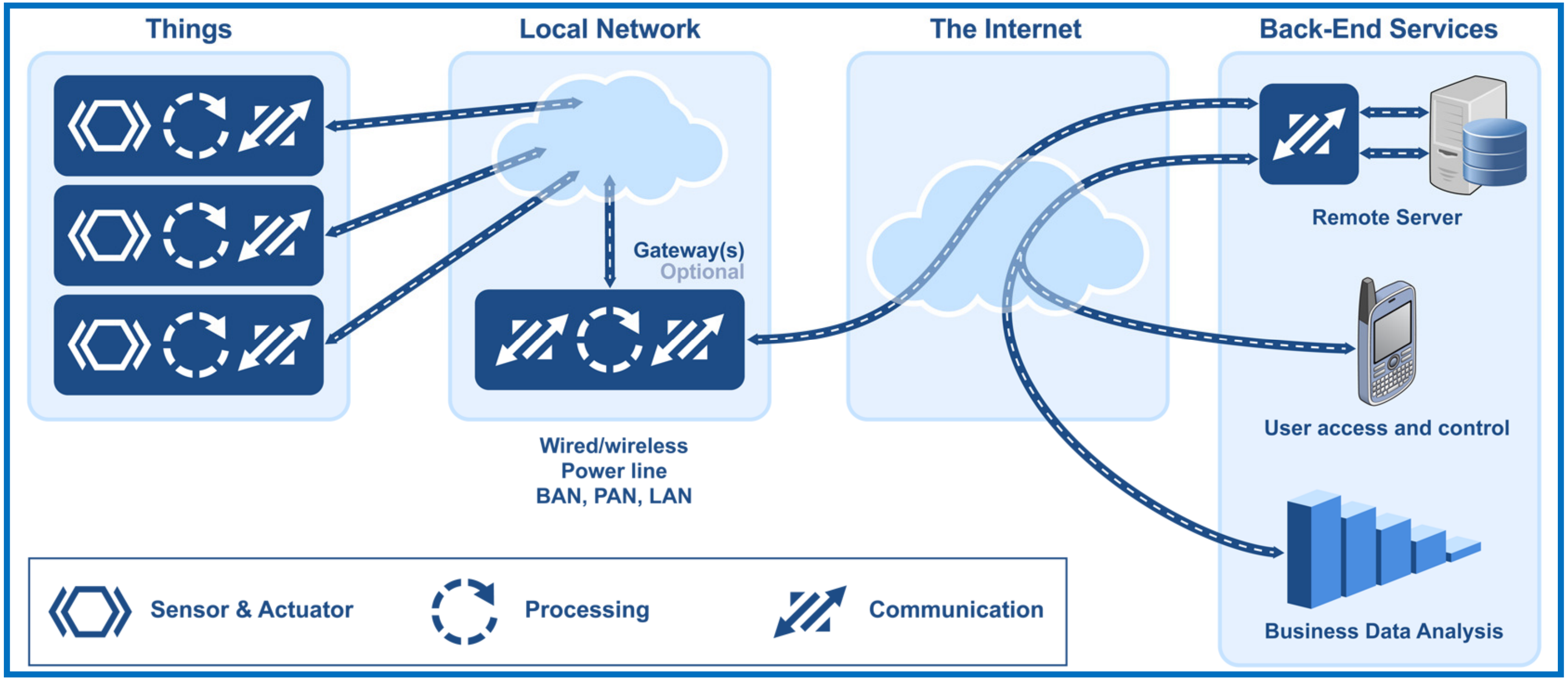


Building blocks of IoT

- Cloud-based IoT Application and Storage
  - Health
  - Agriculture
  - Traffic
  - Smart City



Building blocks of IoT



Layers of IoT

Applications Layer

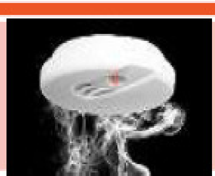
- Industrial Applications: Aerospace, Heavy Machinery, Oil & Gas, Healthcare, Process Industries
- Consumer Applications: Smart home, Retail, Appliance, Wearables etc.

Management Layer

- Analytics, Data Management, BI, Visualization, Security, OSS/BSS, BRM/BPM
- Analysis of the data, decision making and business analytics as well as logical representation

Communication Layer

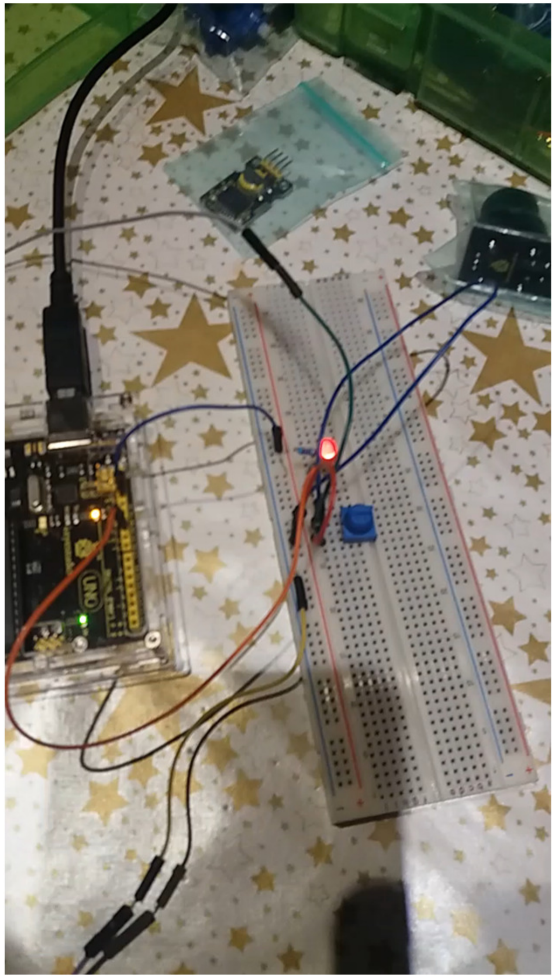
- Gateways: Encryption, SIM Module, Microcontroller, Signal Processors etc.
- Connectivity: Sensor network (LAN / PAN) Gateway Network (LAN / WAN)

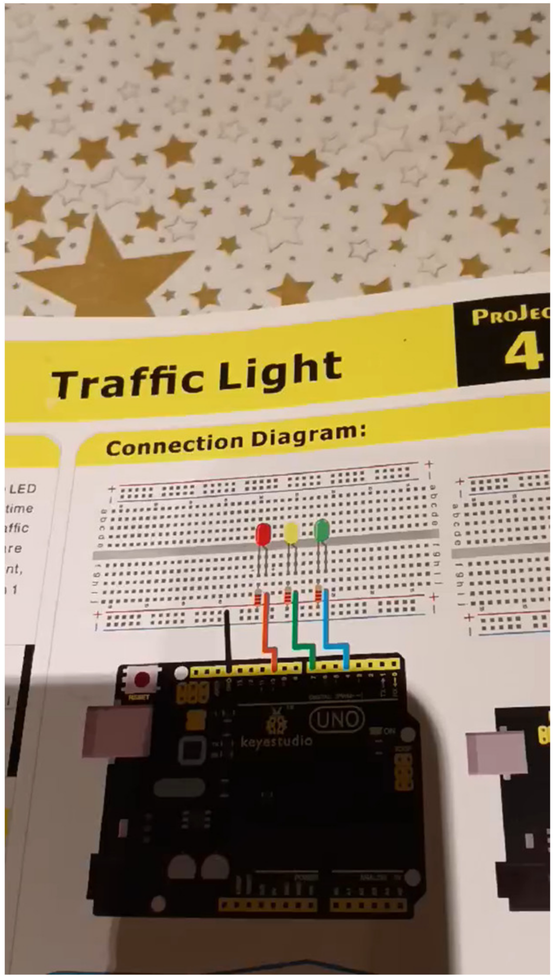


Sensing Layer

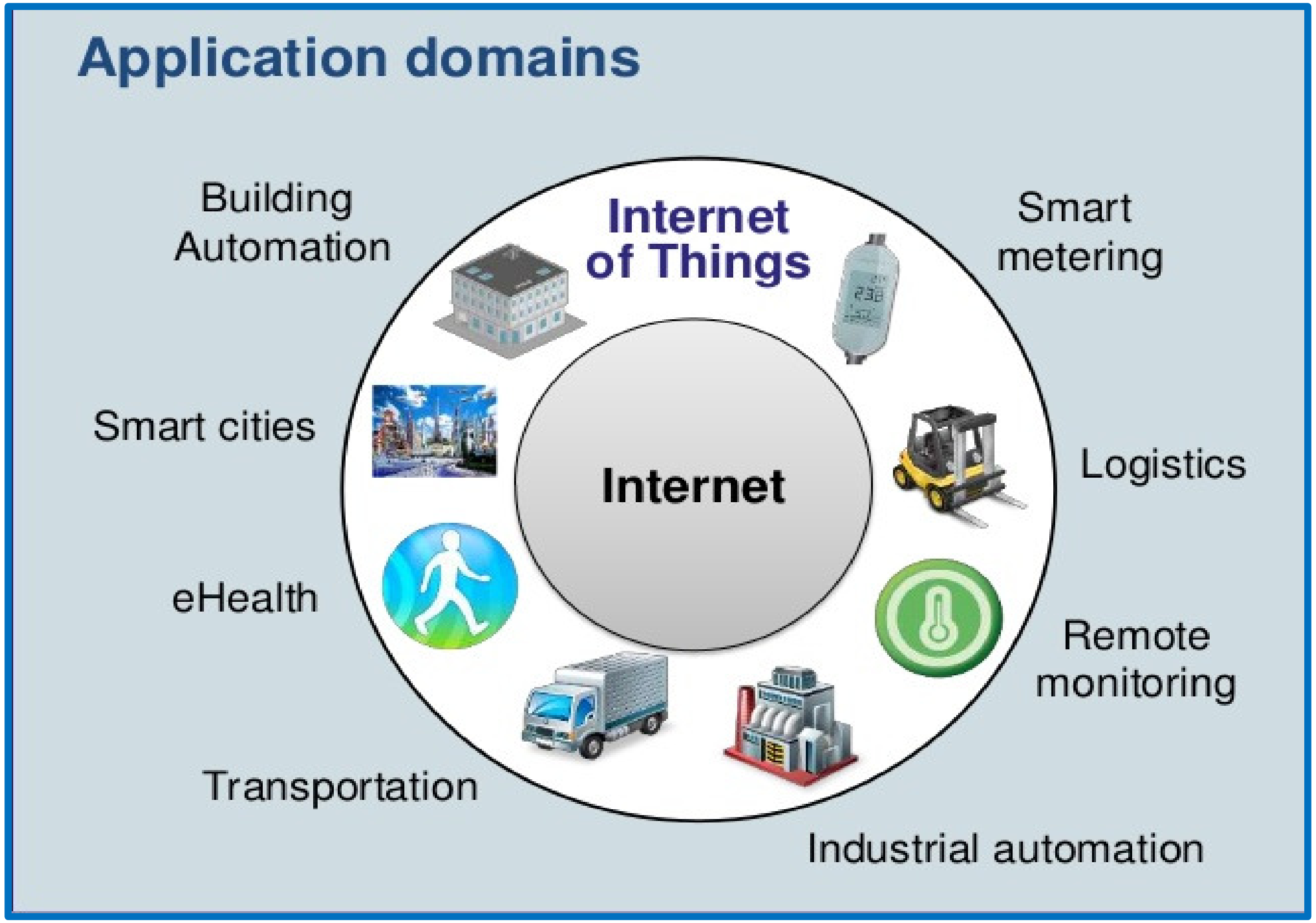
- Measure, collect and process physical quantities in real time
- Gyroscope, GPS, IR, RFID, Solid State, Accelerometer etc.

Sensing Layer: Arduino examples

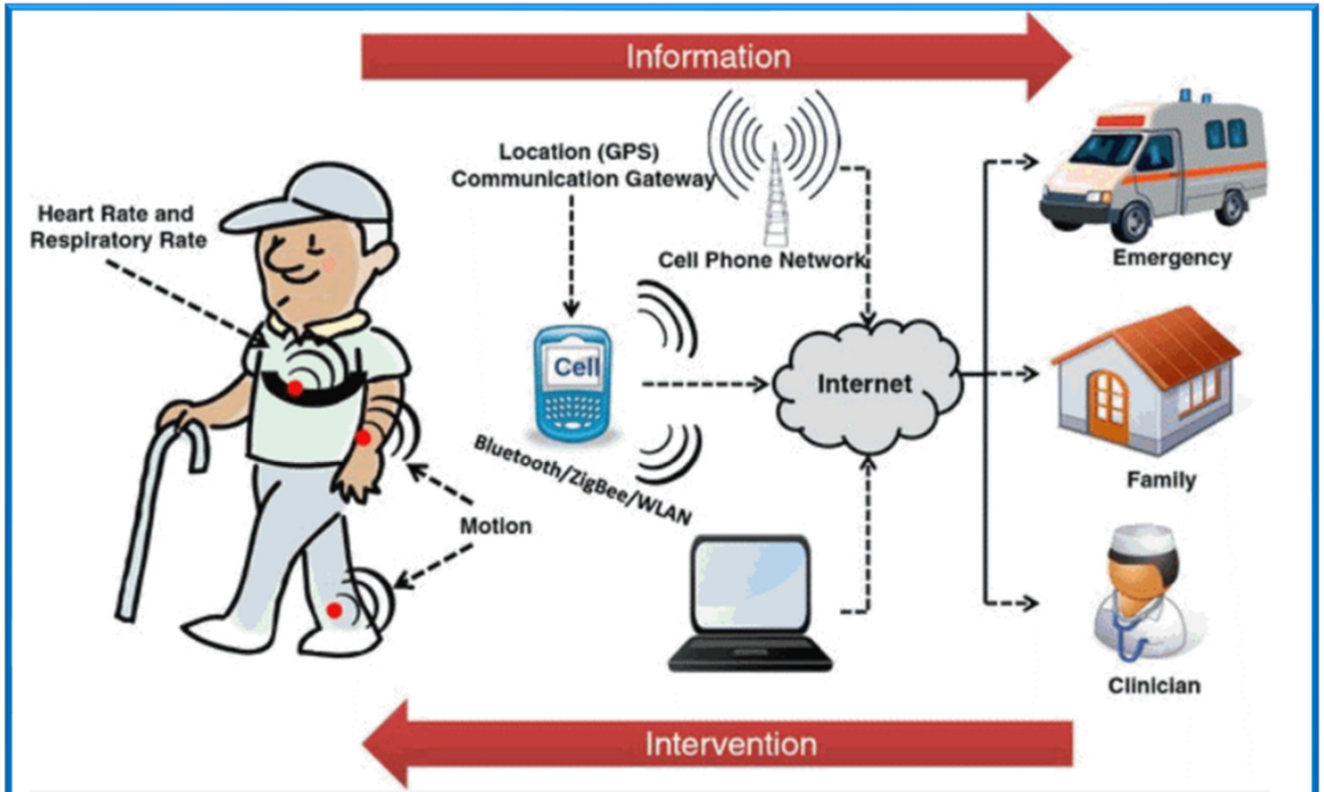




Applications of IoT

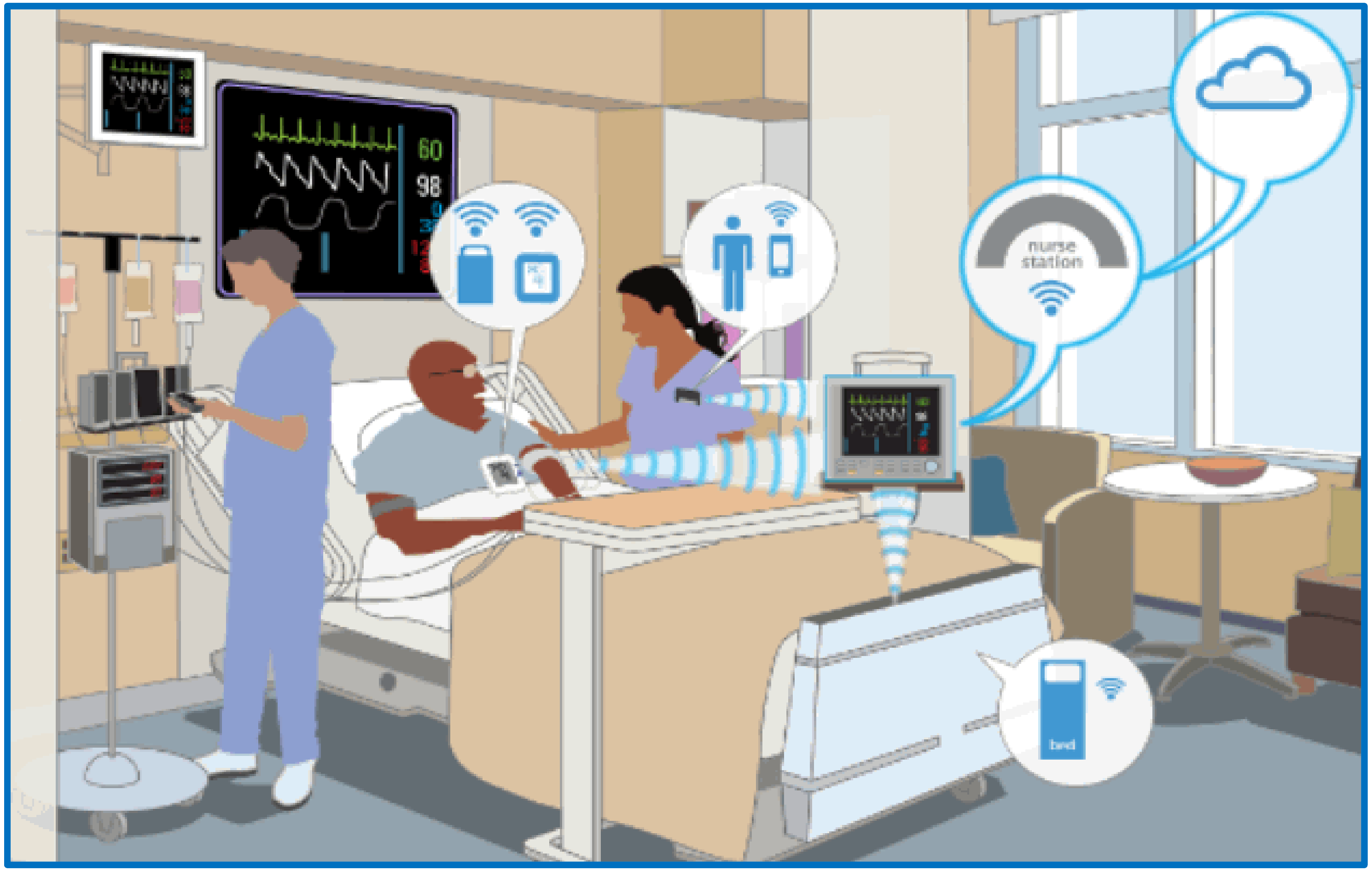


IoT in Health

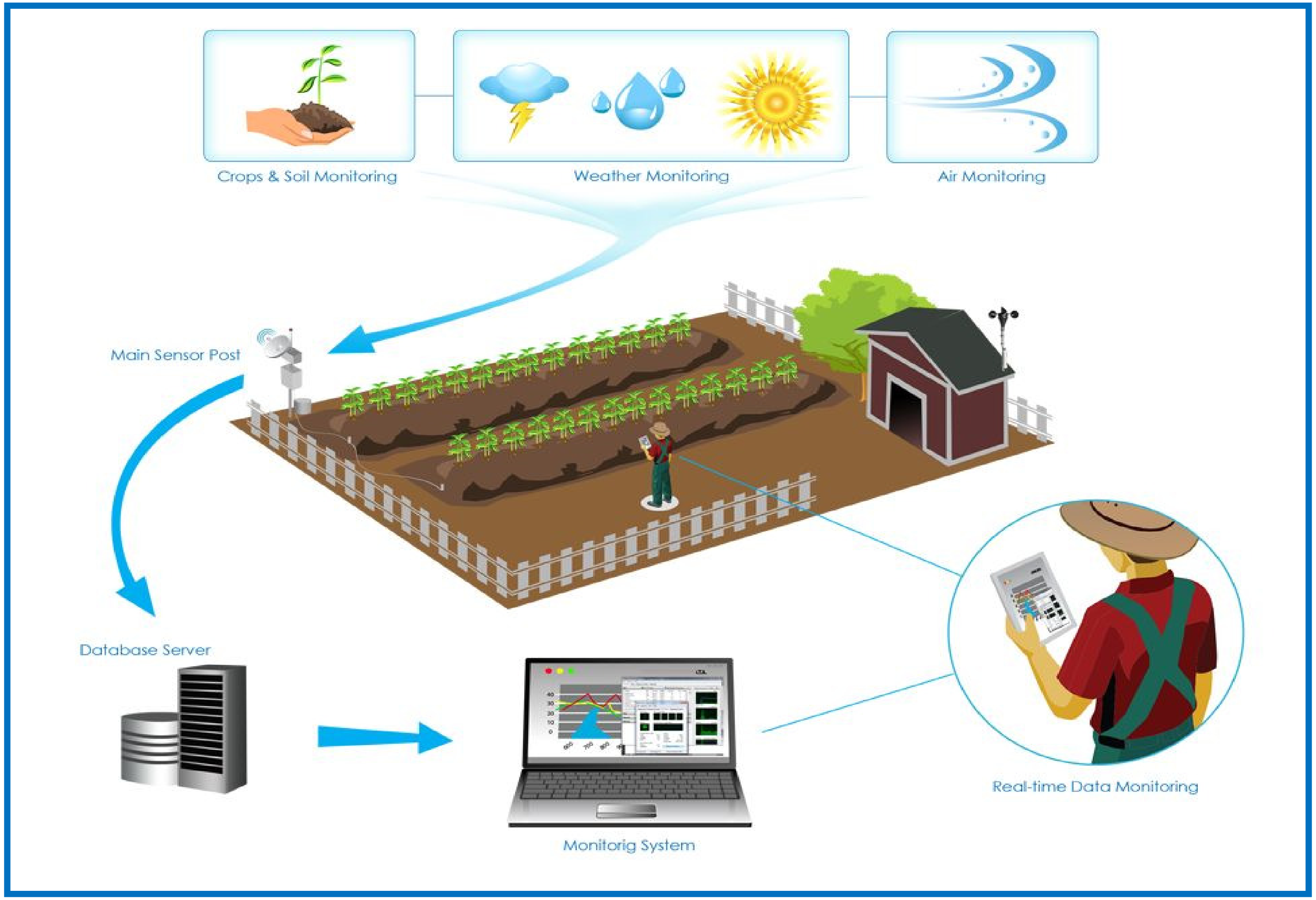


IoT in Remote Health Monitoring

IoT in Health

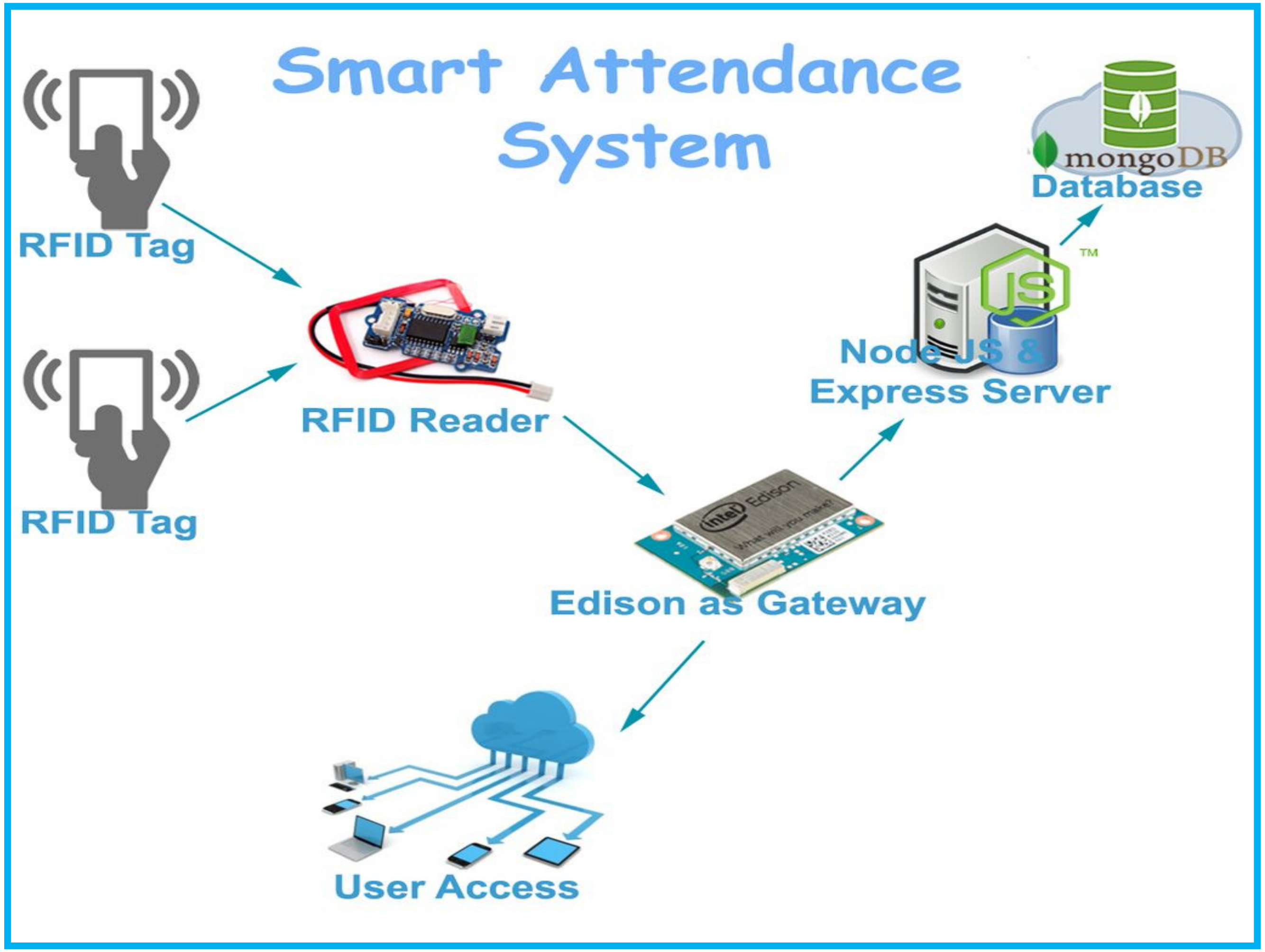


IoT in Agriculture



IoT in Agriculture

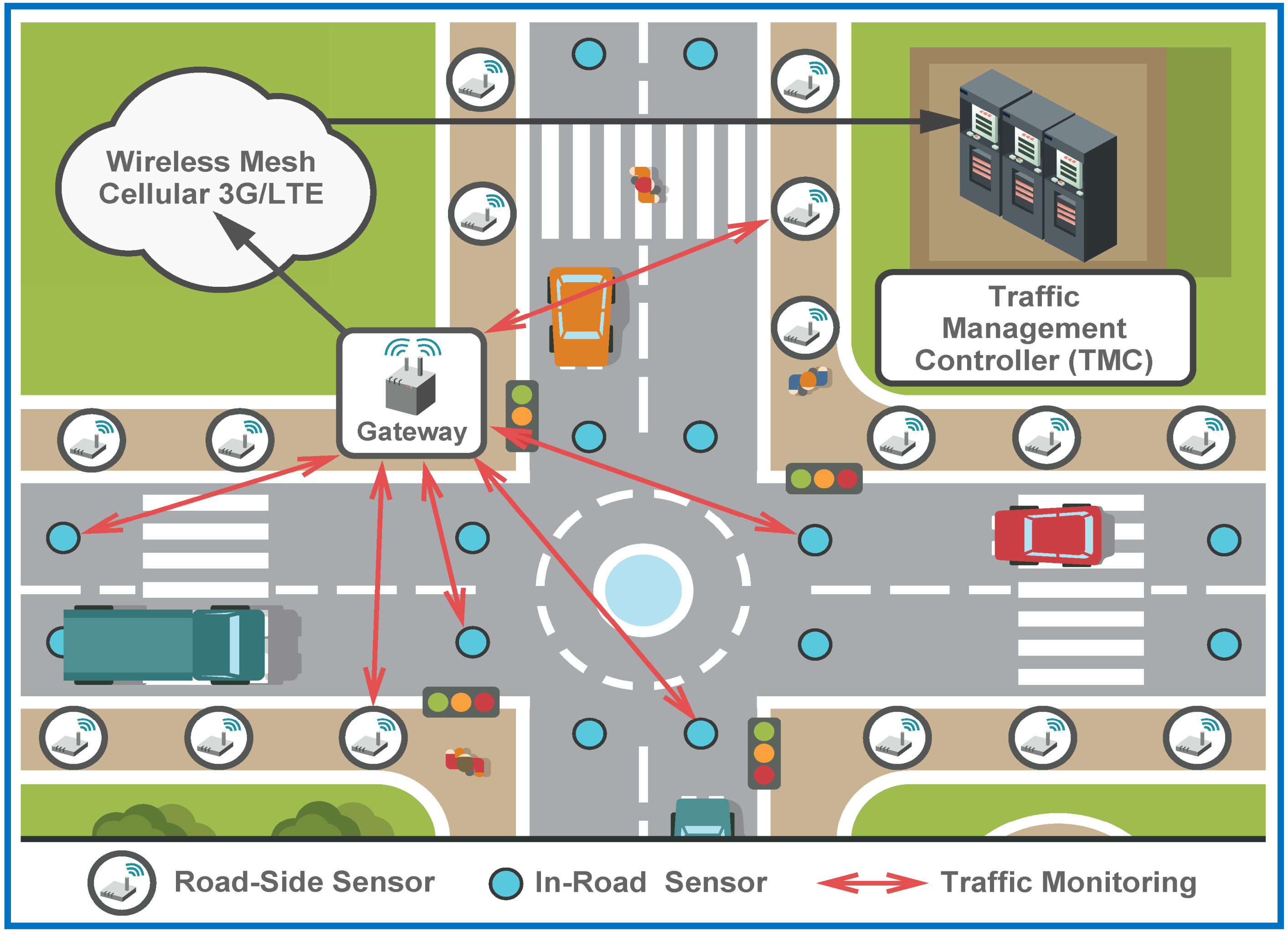
IoT in Education



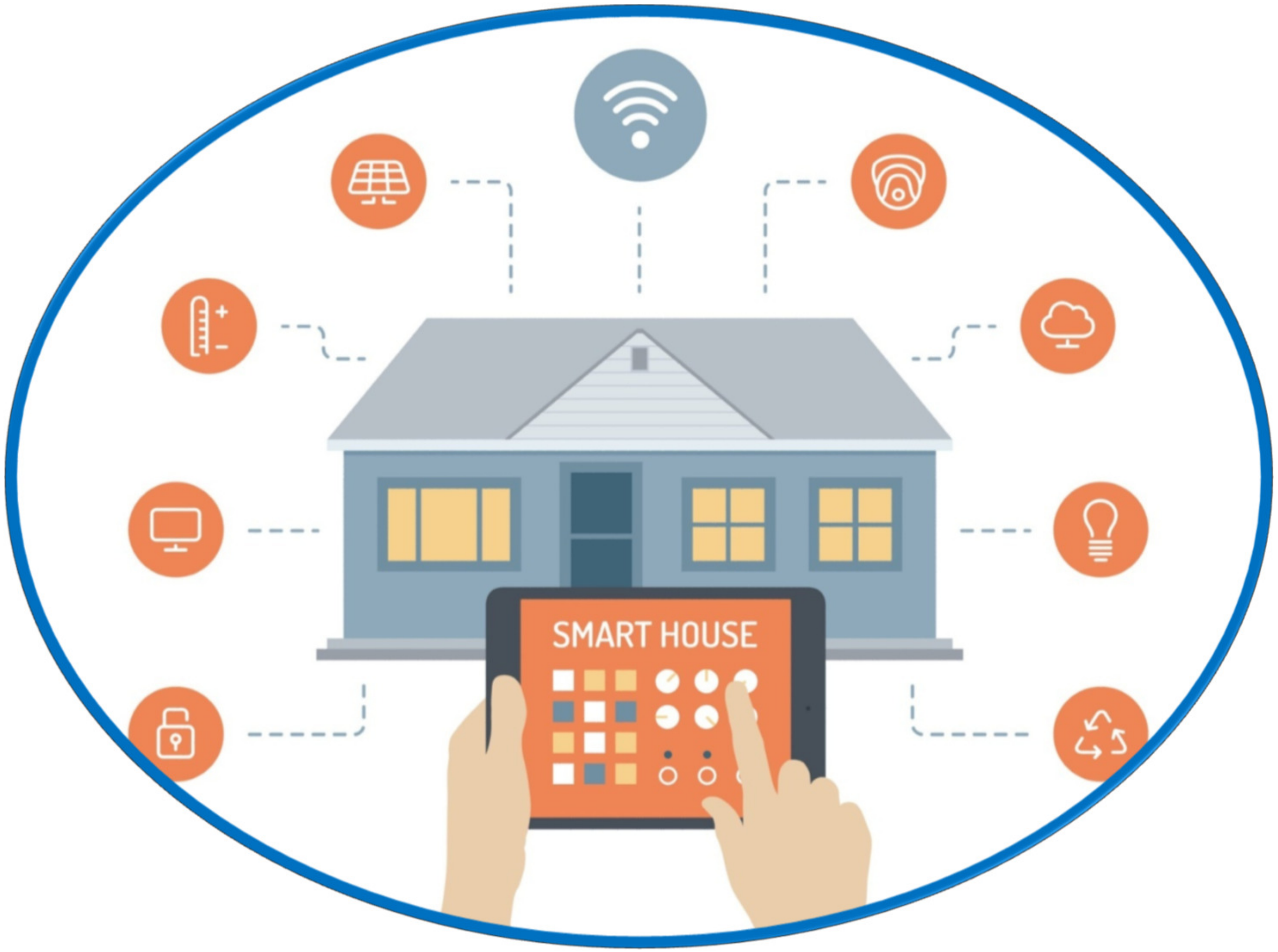
IoT in Education

IoT in Traffic

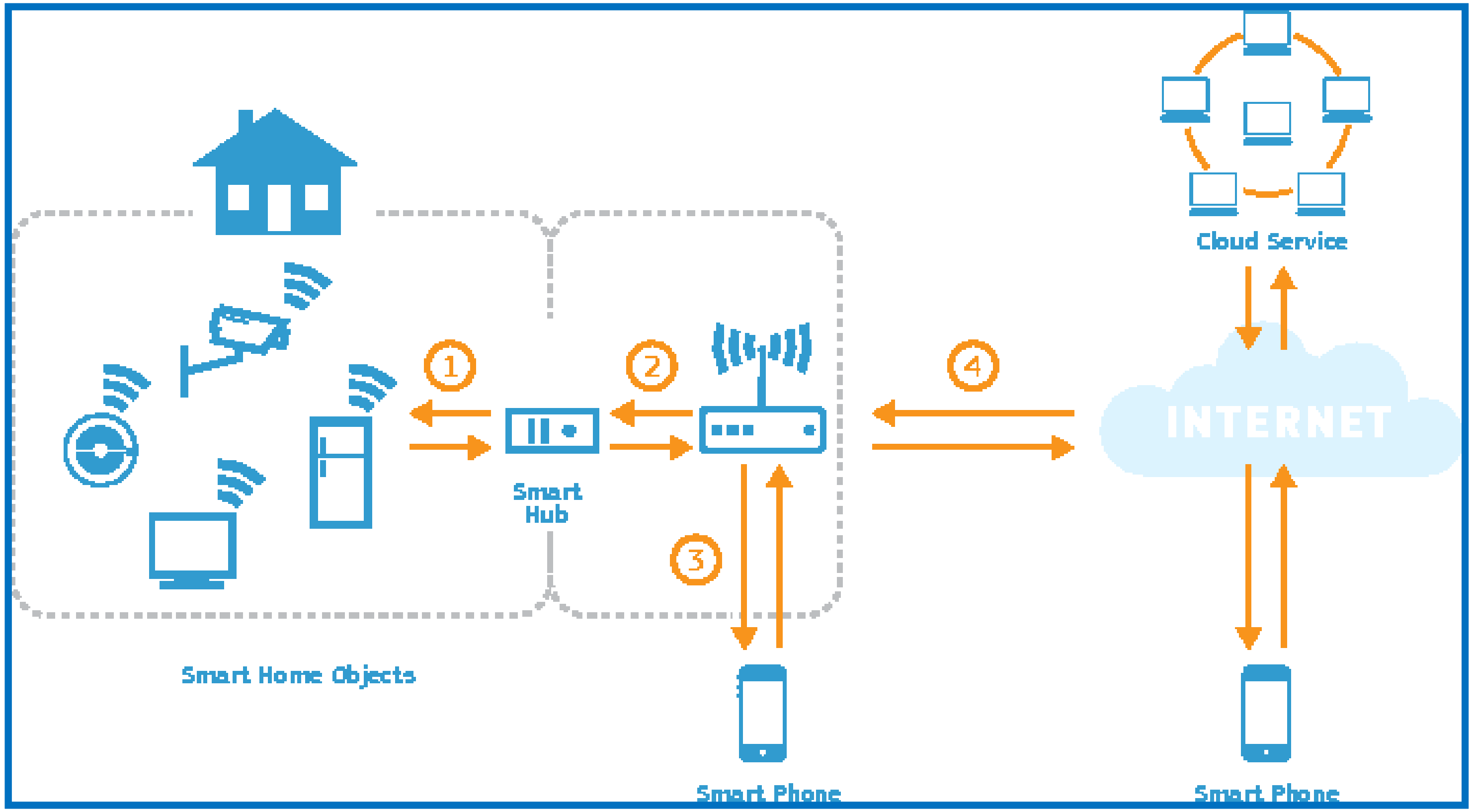
IoT in Traffic



IoT in Smart Home

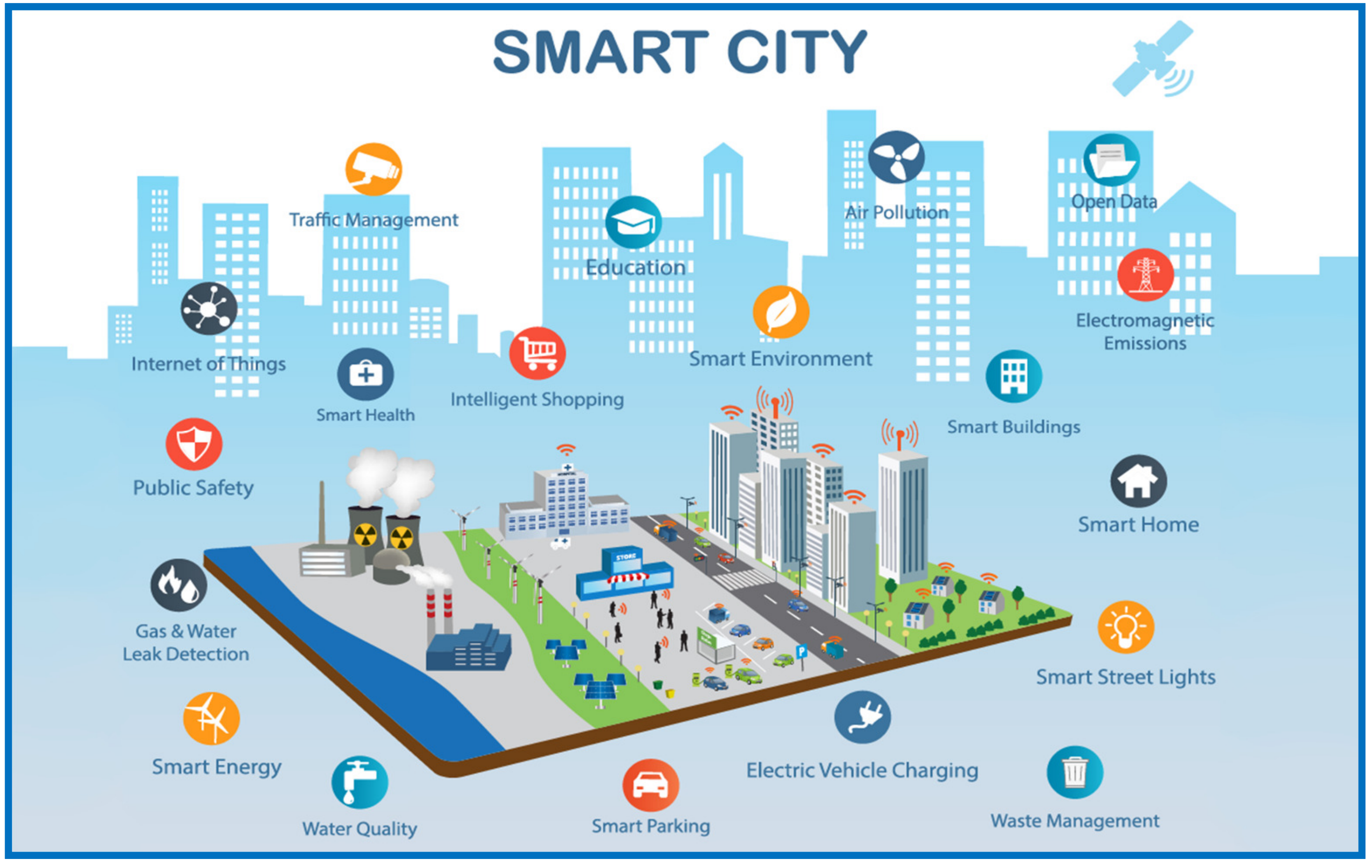


IoT in Smart Home



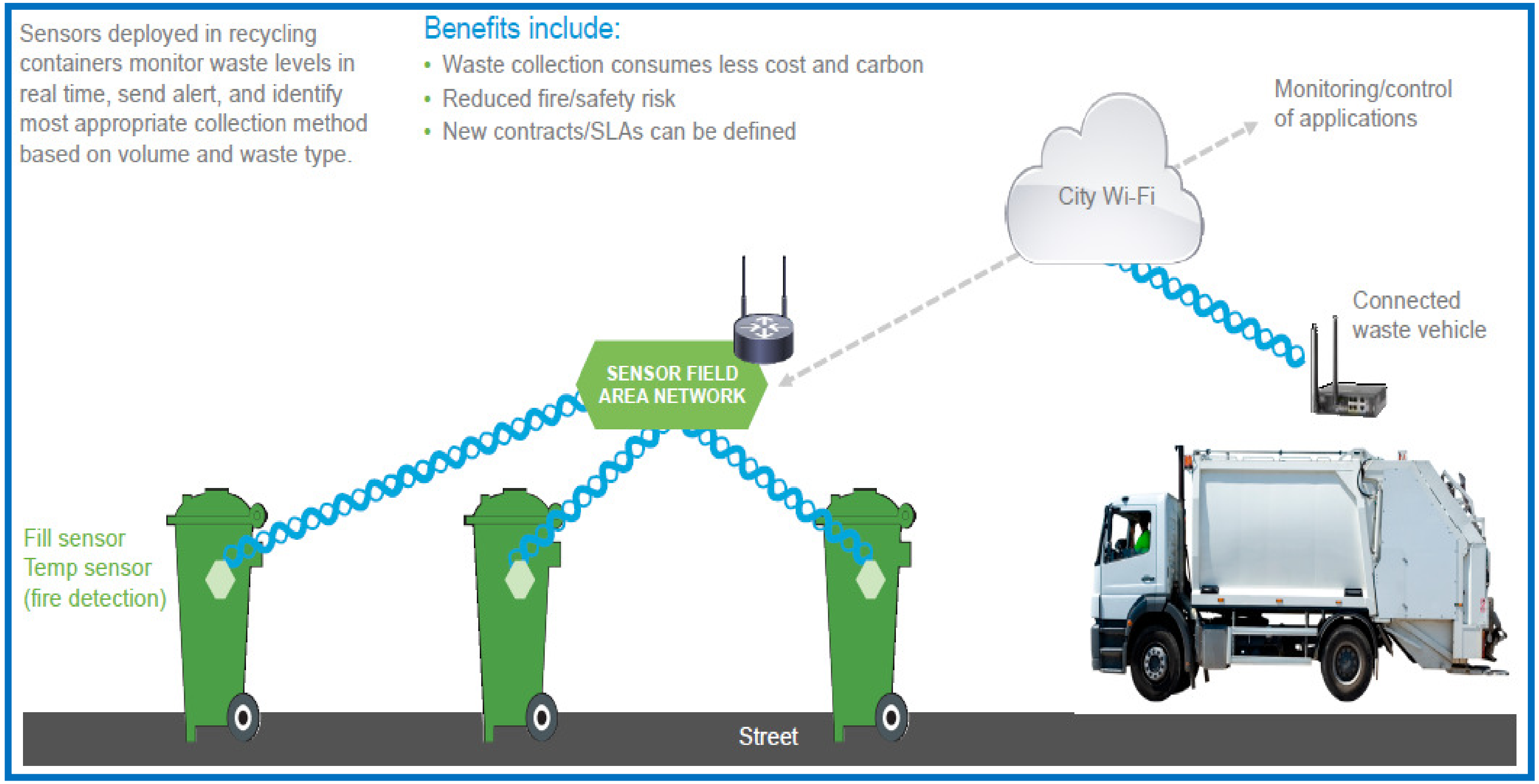
IoT in Retails

IoT in Smart Cities



IoT in Smart Cities

IoT Based Waste Collection

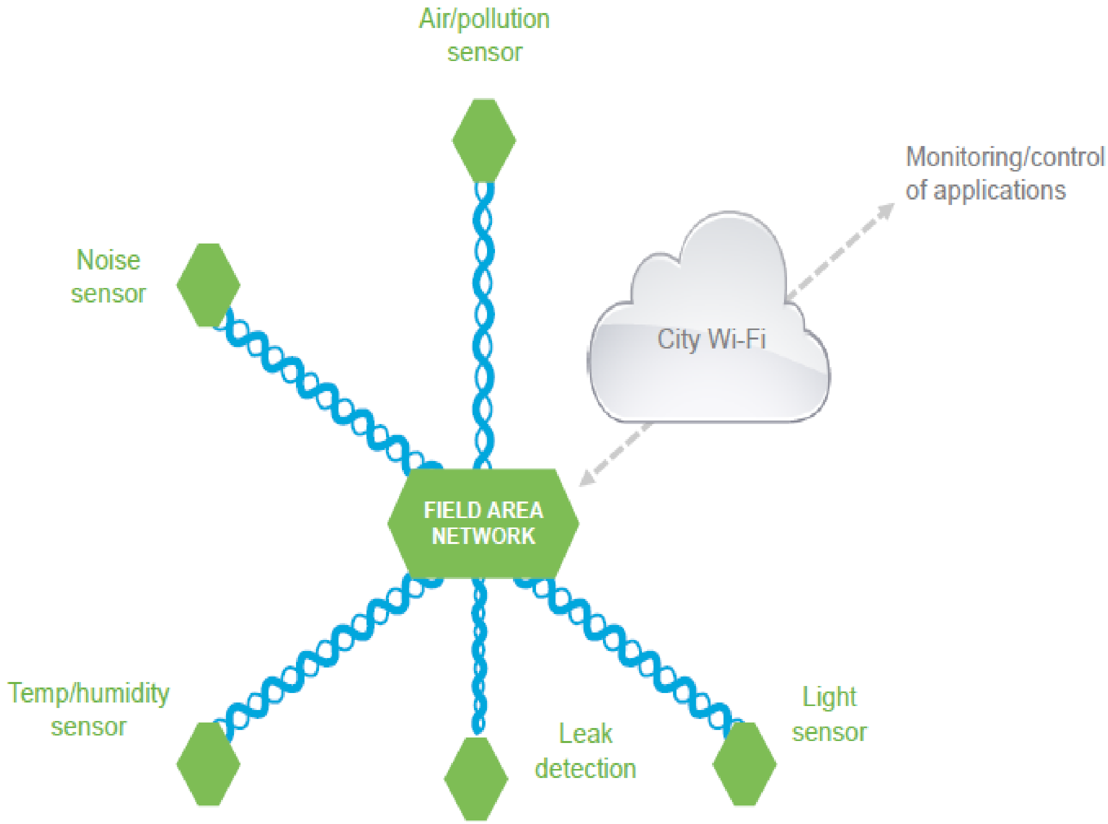


IoT Based Pollution Control

Installation of environment sensors:
air, light, humidity, noise, etc.

Benefits include:

- Leverages parking sensor infrastructure
- Provides valuable data for improving analytics applications and forecasting



Challenges of IoT

- Object Naming
- Data Conversion
- Privacy
- Interoperability
- Security
- Quality of Service
- Data Encryption and Key Management
- Network Issues (Traffic Congestion)

IoT Resulting in Address Crunch

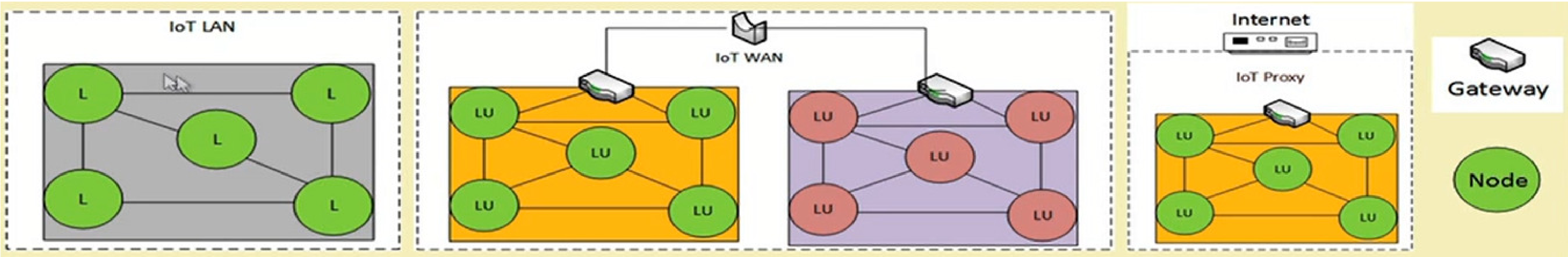
- Recall that more than 9.7 billion devices now, more than 29 billion in 2030
- Reason is the integration of existing devices smart devices as well as constrained nodes in a singular framework
- Integration of various connectivity features such as cellular, Wi-Fi, Ethernet with upcoming ones, such as Bluetooth Low Energy (BLE), DASH7, Insteon, IEEE 802.15.4, etc.
- The ITU vision is approaching reality as in the present day networked devices have outnumbered humans on Earth

Source: Cisco Systems (2011), The Internet of Things How the Next Evolution of the Internet is Changing Everything [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Connectivity Terminology

IoT LAN	• Local, Short range Comm, May or may not connect to Internet, Building or Organization wide
IoT WAN	• Connection of various network segments, Organizationally and geographically wide, Connects to the internet
IoT Node	• Connected to other nodes inside a LAN via the IoT LAN, May be sometimes connected to the internet through a WAN directly
IoT Gateway	• A router connecting the IoT LAN to a WAN to the Internet, Can implement several LAN and WAN, Forwards packets between LAN and WAN on the IP layer
IoT Proxy	• Performs active application layer functions between IoT nodes and other entities

IoT Network Configurations



L: local link addresses or **LU**: Local link addresses which are unique locally

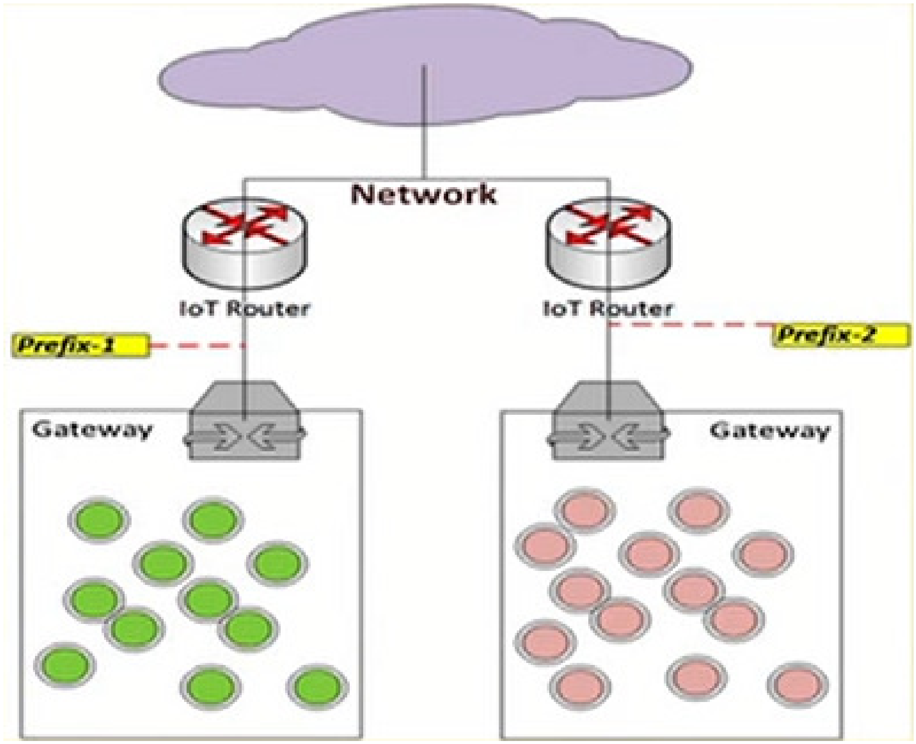
Source: T. Savolainen, J. Soininen, and B. Silverajan. “IPv6 Addressing Strategies for IoT”, IEEE Sensors, vol. 13, no. 10, Oct. 2013

Connectivity

- Some of the IoT network configurations restricted to local areas analogous to normal LANs, WANs and proxy
- Nodes within a gateway's jurisdiction have addresses that are <u>valid within the gateway’s domain only</u>
    - The same addresses may be repeated in the domain of another gateway. The gateway has a unique network prefix which can be used to identify them globally
    - This strategy saves a lot of unnecessary address wastage. Although, the nodes have to communicate to the Internet via the gateway

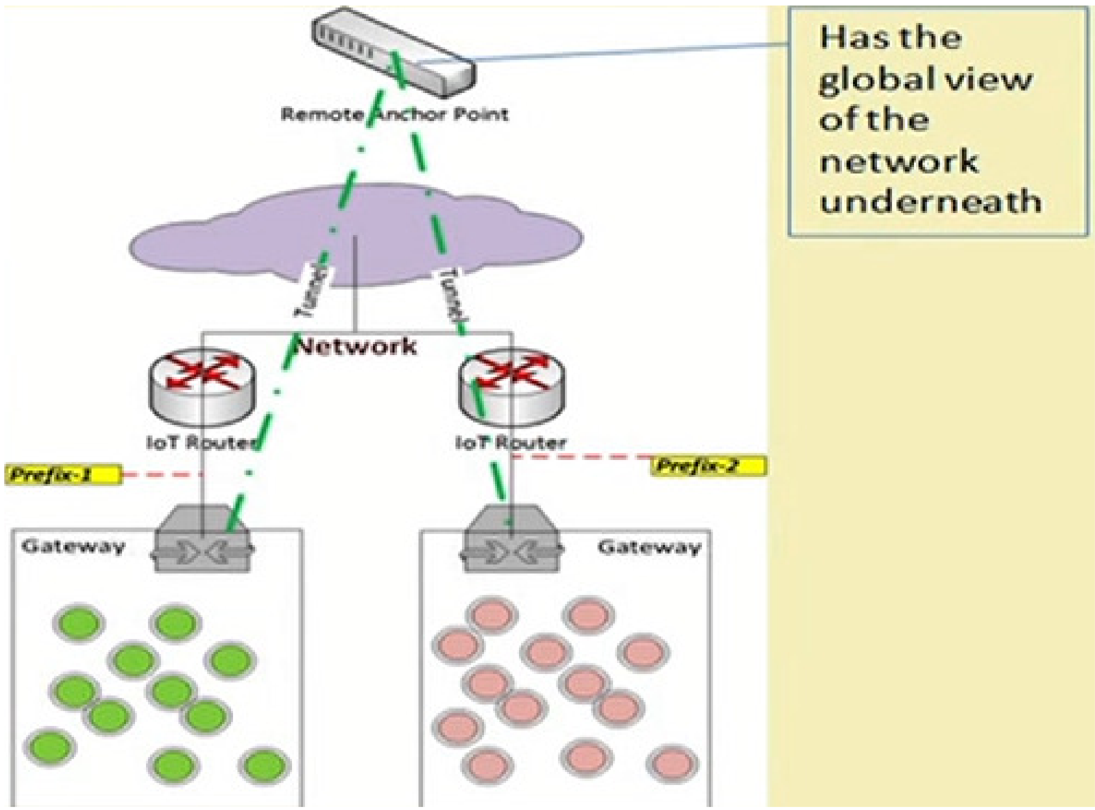
Gateway Prefix Allotment

- One of the strategies of address conservation in IoT is to use local addresses which exist uniquely within the domain of the gateway. These are represented by circles in this slide
- The network connected to the Internet has routers with their set of addresses and ranges
- These routers have multiple gateways connected to them which can forward packets from the nodes to the Internet
  - These routers assign prefixes to gateways under them, so that the gateways can be identified with them



Impact of Mobility on Addressing

- The network prefix changes from one to two due to movement, making the IoT LAN safe from changes due to movements
- IoT gateway WAN address changes without change in LAN address. This is achieved using ULA



Cont.

- The gateway is assigned with prefixes, which are attached to a remote anchor point by using various protocols such as Mobile IPv6, and are immune to changes of network prefixes
- This is achieved using LU. The address of the nodes within the gateways remain **unchanged** as the gateway provide them with local unique addresses and the change in gateways network prefix doesn't affect them
- Sometimes, there is a need for the nodes to communicate directly to the Internet. This is achieved by tunneling, where the nodes communicate to a remote anchor point instead of channeling their packets through their router which is achieved by using tunneling protocols such as IKEv2: Internet Key Exchange v2

Gateways

- IoT Gateways without proxies responsible mainly for:
  - Internet connectivity
  - IoT LAN intra-connectivity
- Upstream address prefixes or obtained using mechanisms like DHCPv6 and delegated to the nodes using SLAAC (stateless addressing)
- LU addresses are maintained independently of globally routable addresses, in cases where internal address stability is of prime concern

Source: T. Savolainen, J. Soininen, and B. Silverajan. “IPv6 Addressing Strategies for IoT”, IEEE Sensors, vol. 13, no. 10, Oct. 2013

Cont.

- Despite providing address stability, LU cannot communicate directly with the Internet or the upper layers, which is solved by implementing an **application layer proxy**
  - Application layer proxies may be additionally configured to process data rather than just passing it
  - In nodes with no support for computationally intensive tasks, IoT proxy gathers data sent to the link-local multicast address and routes them globally

Cont.

- Presently, the Internet is mainly IPv4-based with little or no IPv6 uplink facilities of support
- Due to the lack of a universal transition solution to IPv6, lots of suboptimal solutions are being used for IoT deployment
- This makes IT solutions mainly address
  - IPv6 to IPv4 translation
  - IPv6 tunneling over IPv4
  - Application layer proxies (e.g., data relaying)

Multi-homing

- A node/network connected to multiple networks for improved reliability
- In cases of small IoT LANs, where allotment of address prefixes is not feasible and possible, a proxy-based approach is used to manage multiple IP addresses and map them to link local addresses
- In other cases, gateway-based approach is used for assigning link local addresses to the nodes under it

Source: T. Savolainen, J. Soininen, and B. Silverajan. "IPv6 Addressing Strategies for IoT", IEEE Sensors, vol. 13, no. 10, Oct. 2013

Cont.

- Providing source addresses, destination addresses and routing information to the multi-home nodes is the real challenge in multi-homing networks
- In case the destination and source addresses originate from the same prefix, routing between gateways can be employed for IoT gateway selection
- Presently, IETF is still trying to standardize this issue

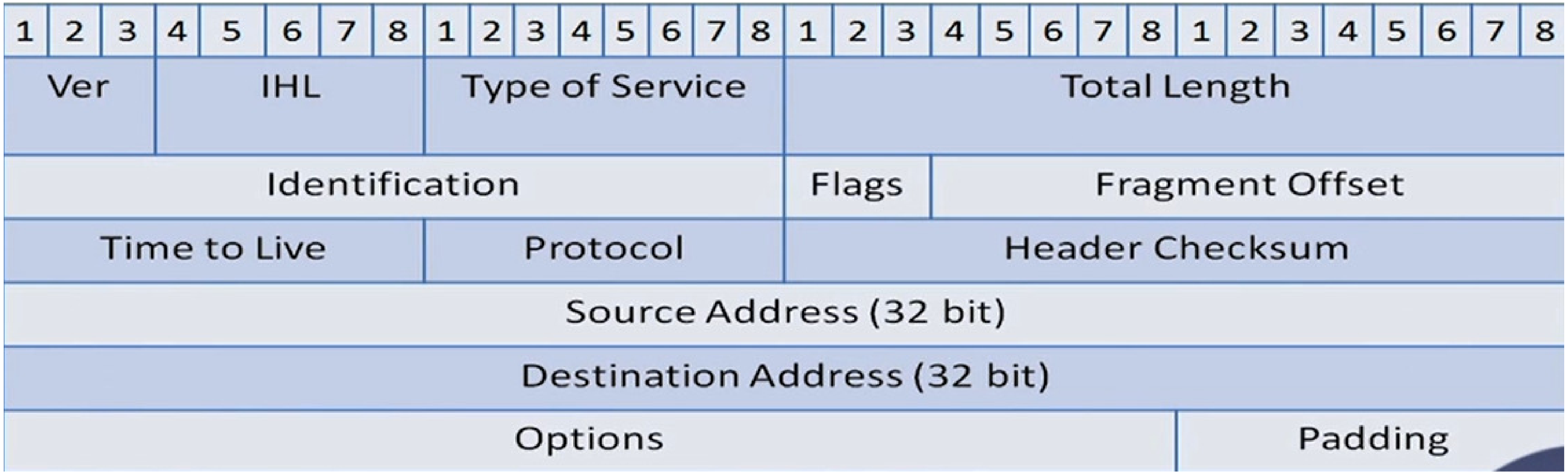
IPv4 vs IPv6

	IPv4	IPv6
Developed	IETF 1974	IETF 1998
Length (bits)	32	128
No. of Addresses	2^32	2^128
Notation	Dotted Decimal	Hexadecimal
Dynamic Allocation of addresses	DHCP	SLAAC/ DHCPv6
IPSec	Optional	Compulsory

IPv4 vs IPv6

	IPv4	IPv6
Header Size	Variable	Fixed
Header Checksum	Yes	No
Header Options	Yes	No
Broadcast Addresses	Yes	No
Multicast Address	No	Yes

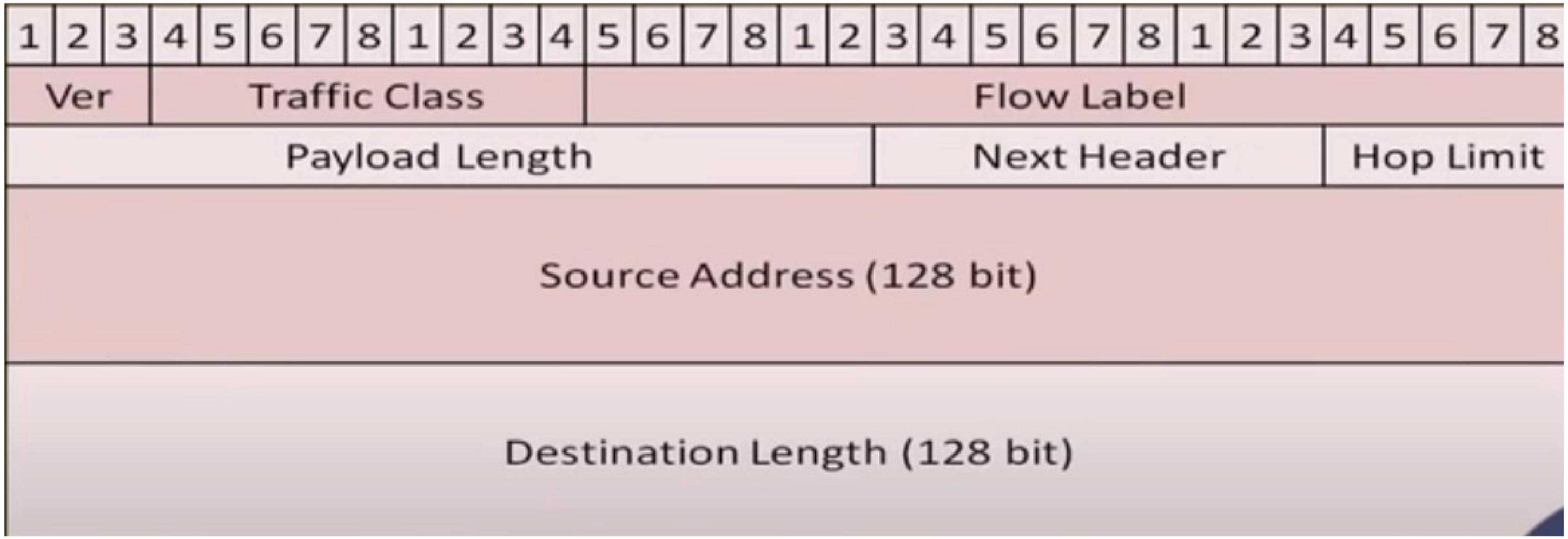
IPv4 Header Format



IPv4

- The IPv4 emphasizes more on reliable transmission, as is evident by fields such as type of service, total length, id, offset, TTL, checksum

IPv6 Header Format



IPv6

- The IPv6 header structure is simpler as it mainly focuses on the addressing part of the source and the destination
  - Rather than on reliability of the data delivery

Any questions?