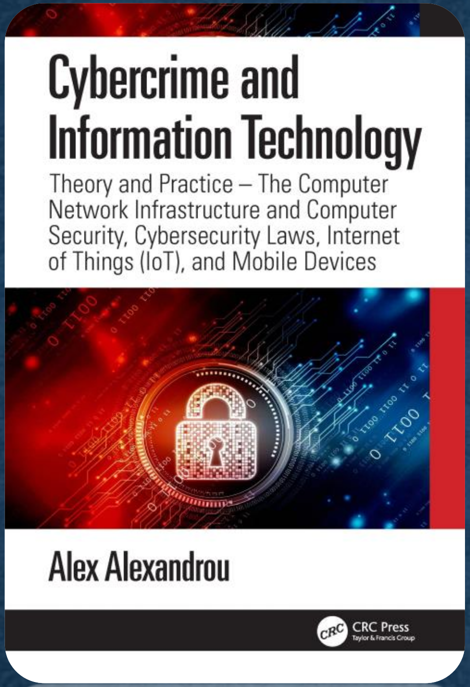


Cybercrime and Information Technology

Theory and Practice – The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices

Alex Alexandrou

CRC Press
Taylor & Francis Group

CYBERCRIME AND INFORMATION TECHNOLOGY: THEORY AND PRACTICE

The Computer Network Infostructure and Computer Security, Cybersecurity Laws,
Internet of Things (IoT), and Mobile Devices

INTERNET OF THINGS (IOTS)

CHAPTER 7, LECTURE 1

YOUR NAME

OBJECTIVES

- After completing this chapter, the student will be able to:
- Understand the Internet of Things (IoTs) and the four different lead stages
- Understand real-world applications
- Understand industrial IoT and its relation to manufacturing
- Illustrate IoT architecture

OBJECTIVES

- Explain different types of IoT protocols and standards
- Describe the IoT ecosystem—bandwidth, interoperability, power usage, and range
- Understand the importance of security in IoT devices

THE INTERNET OF THINGS-AN INTRODUCTION

- The Industrial Revolution, which began around 1760 and led to the rapid transformation of our society, culture, and economy, the Internet has undoubtedly transformed our lives.

- As wireless technologies evolve, inexpensive data storage such as cloud computing has enabled the Internet of Things (IoTs) to flourish.

- IoTs are an important part of today's Internet, just as the steam engine, mass production, railroad, and telegraphy typify the Industrial Revolution.

- The phrase "Internet of Things" was coined by Kevin Ashton in 1999. Like most inventions, it began with a new solution to an old problem.

THE INTERNET OF THINGS-AN INTRODUCTION (CONT.)

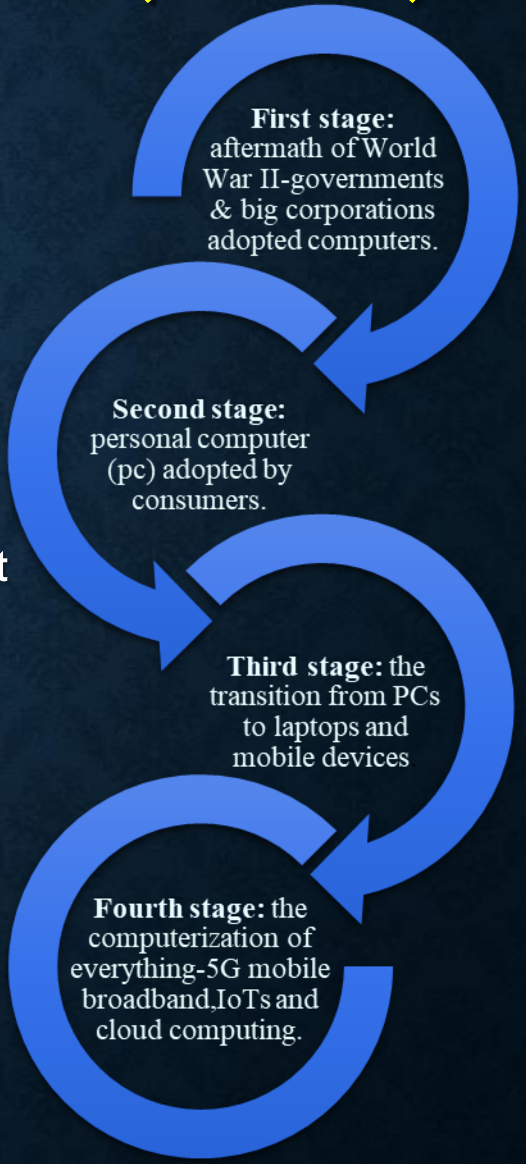
- Modern computing began after World War II when the aftermath of the war and the space program of the 1960s brought considerable changes to computing technologies.

- Their early adoption can be considered the first stage of modern computing.

- The second stage followed the introduction of microcomputers and the development of the personal computer (PC) in the early 1980s.

- The third stage is when computers became smaller and lighter, the transition to laptops and ultimately to mobile devices.

- The fourth stage is the gradual evolution of IoTs and the steady trend toward Internet-connected devices.



First stage: aftermath of World War II-governments & big corporations adopted computers.

Second stage: personal computer (pc) adopted by consumers.

Third stage: the transition from PCs to laptops and mobile devices

Fourth stage: the computerization of everything-5G mobile broadband,IoTs and cloud computing.

The four stages of modern computing adoption

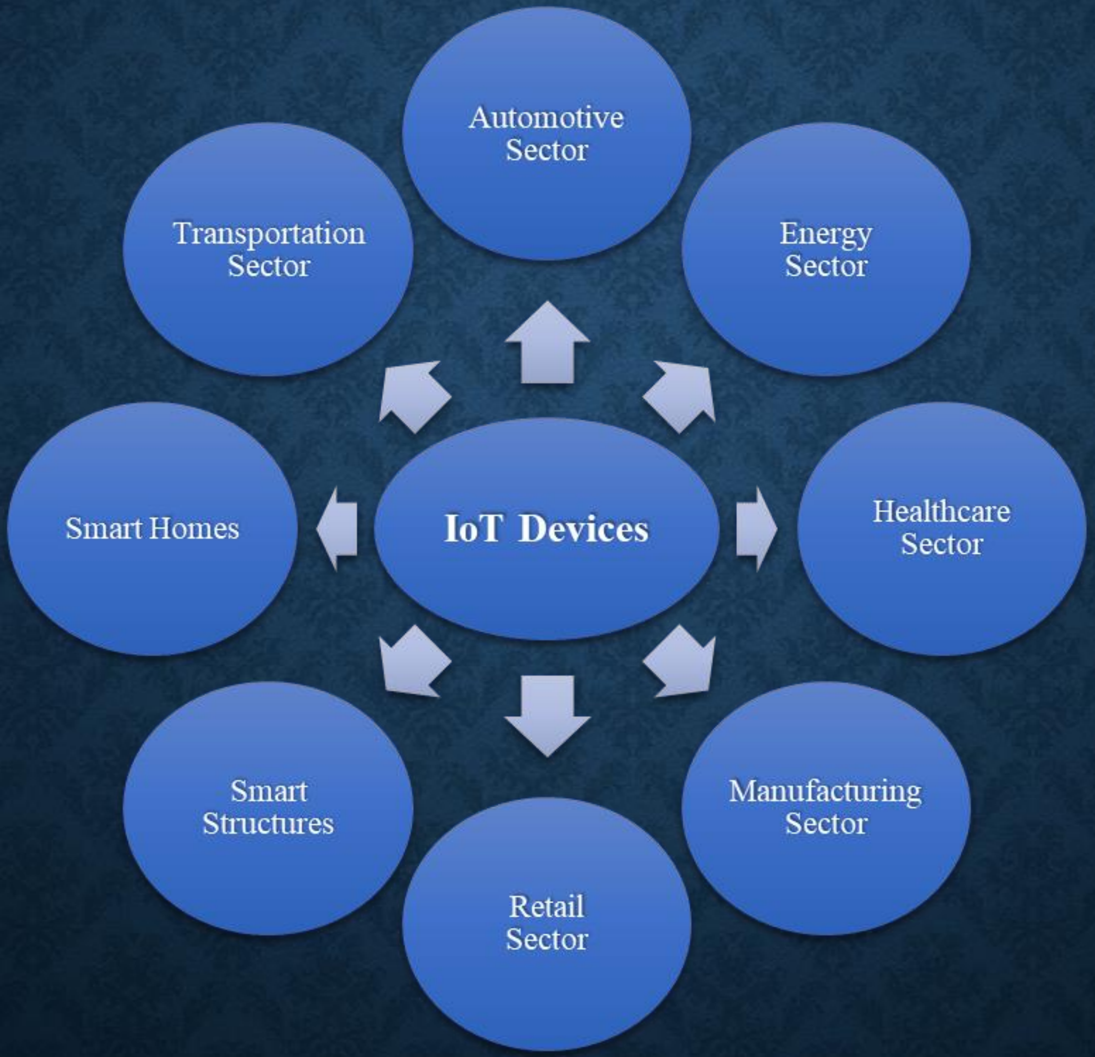
INTERNET OF THINGS (IOTS) DEFINITION (CONT.)

- Internet of Things as intelligent network-connected devices or systems, embedded in the physical environment, to improve the lives of people with minimal or no human intervention.

- The next generation of mobile networks, 5G, will enable the creation of a new wave of IoTs with higher bandwidth, greater reliability, and very high speed (up to 10 Gbps), which translates to low latency (the time needed for data to travel between two points).

- Example of IoTs devices include lightbulbs that can be controlled by an phone app, motion sensors, smart thermostats, smart locks, smart light switches, smoke alarms, doorbells, virtual assistants and speakers like Amazon Echo, and Google Home.

SUMMARY OF IOT APPLICATIONS



The range of IoT applications

SUMMARY OF IOT APPLICATIONS (CONT.)

- Automotive Sector
    - In the automotive industry, sensors collect enormous amounts of data that are processed, conceptualized into a visual format and streamed to the cloud.
        - The data can be accessed from any device via the internet. These sensory data are vital components of the automotive IoT environment.

- Energy Sector
    - IoT-enabled sensors and devices provide intelligence and detailed data analytics to energy companies and consumers.
        - Smart devices monitor and manage equipment, measure vibration and temperature, monitor wear, and improve maintenance schedules.
        - All these functions are performed remotely, without human intervention, reduce costs, and enable virtual troubleshooting.

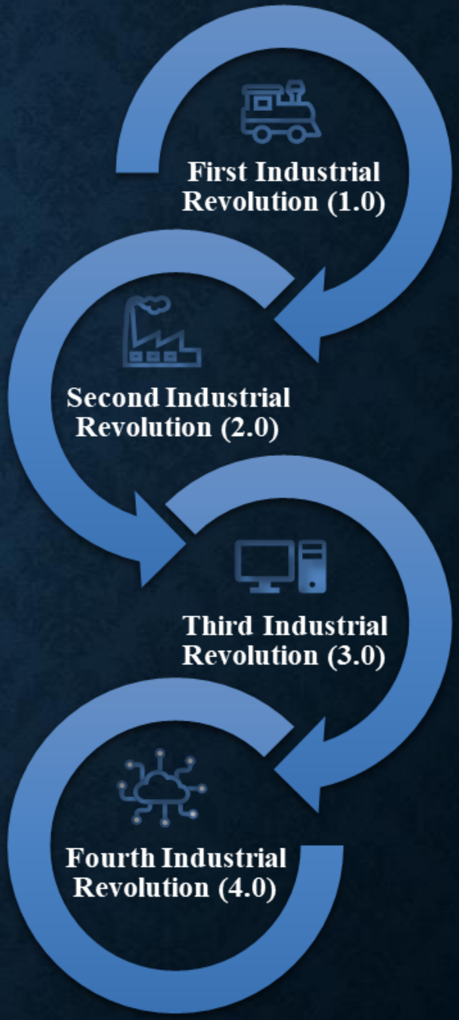
SUMMARY OF IOT APPLICATIONS (CONT.)

- Healthcare Sector
  - In the healthcare sector, IoT devices have been revolutionizing the diagnosis, treatment, and management of patient care.
    - These devices open up a world of possibilities for telemedicine and education paradigms for patients, providing data to help patients and healthcare professionals gain a deeper understanding of the human body.
    - Remote monitoring can reduce number of days patients stay in hospitals and empower their engagement and interaction with healthcare providers.

- Manufacturing Sector
  - In the manufacturing sector, IoT devices add intelligence to industrial manufacturing and are poised to transform equipment, processing, and management.
    - Industrial IoT devices, along with 5G mobile broadband, will improve productivity and product quality, and will reduce maintenance of manufacturing technologies through real-time data analytics.
    - This developing trend towards automation, smart factories, real-time data analysis and network connectivity is called the Fourth Industrial Revolution or Industry 4.0

SUMMARY OF IOT APPLICATIONS (CONT.)

- Manufacturing Sector (cont.)
  - Historically, near the end of the 18th century, the First Industrial Revolution was characterized by the steam engine, powered by coal.
  - The Second Industrial Revolution began in the late 19th century with the discovery of oil, and early innovations in manufacturing, such as Henry Ford's assembly line for mass production of automobiles, and the work of Frederick Winslow Taylor, the father of scientific management.
  - The Third Industrial Revolution began when manufacturing data moved from analogue and mechanical to digital in the 1970's.
  - The changes that Internet computers brought to automation bore a resemblance to the scale of those brought about by steam engine technology.
  - As we continue to move into the twenty-first century, interconnected IoT devices have been transforming the traditional manufacturing landscape with real-time connectivity, replacing traditional manufacturing processes.
  - Industry 4.0 has transformed the world's economic outlook and will continue to innovate and effect change.


First Industrial Revolution (1.0)
Second Industrial Revolution (2.0)
Third Industrial Revolution (3.0)
Fourth Industrial Revolution (4.0)

The four phases of the industrial revolution

SUMMARY OF IOT APPLICATIONS (CONT.)

- Retail Sector
  - In the retail sector, IoT devices will help customers make more informed decisions and will help retailers redefine the customer experience.
    - An example of a smart store is Amazon Go, in which shopping occurs without the need to stop and check out with a cashier.
    - Other examples include the ability to search for products, compare prices, provide feedback, and receive coupons for a relevant product while customers are still in the store.
- Smart Structures (Buildings, Roads and Bridges Sector)
  - Any structure that communicates wirelessly, or one that is wired and sends and receives autonomous responses, is considered a smart structure.
    - IoT devices that collect data, transmit and receive data between systems to provide air conditioning and heating temperature controls.
    - They can switch lights on or off and have security controls like motion detection and can show whether people are present or absent.
    - In the field of structural design technology, including roads, bridges, and tunnels, IoT devices serve as an early detection system.
    - Sensors monitor structural cracks, vibrations, temperature and acceleration, and when applied to machine learning models, can predict defects or quality deviations, ultimately saving lives.

SUMMARY OF IOT APPLICATIONS (CONT.)

- Smart Homes

  - Smart home automation, or the smart home ecosystem, refers to all internet-connected and integrated devices in our homes, such as appliances, smart light bulbs and switches, smart climate control systems, entertainment systems, and security systems like smart door locks, motion detectors and security cameras.

  - All these devices can be controlled through one home automation system, offered by tech companies such as Amazon, Apple, Google, Logitech, and others.

  - Smart home IoT devices can be remotely monitored anytime and from anywhere using the home network and a voice or remote-control command, or by an IoT-enabled application from any computing device.

SUMMARY OF IOT APPLICATIONS (CONT.)

Transportation Sector

- One of the basic functions of daily living in both urban and rural environments is transportation.
- The transportation sector consists of many different types of businesses that transport people and goods.
- Examples include airlines, railroads, marine, freight, public transportation, and the transportation infrastructure.

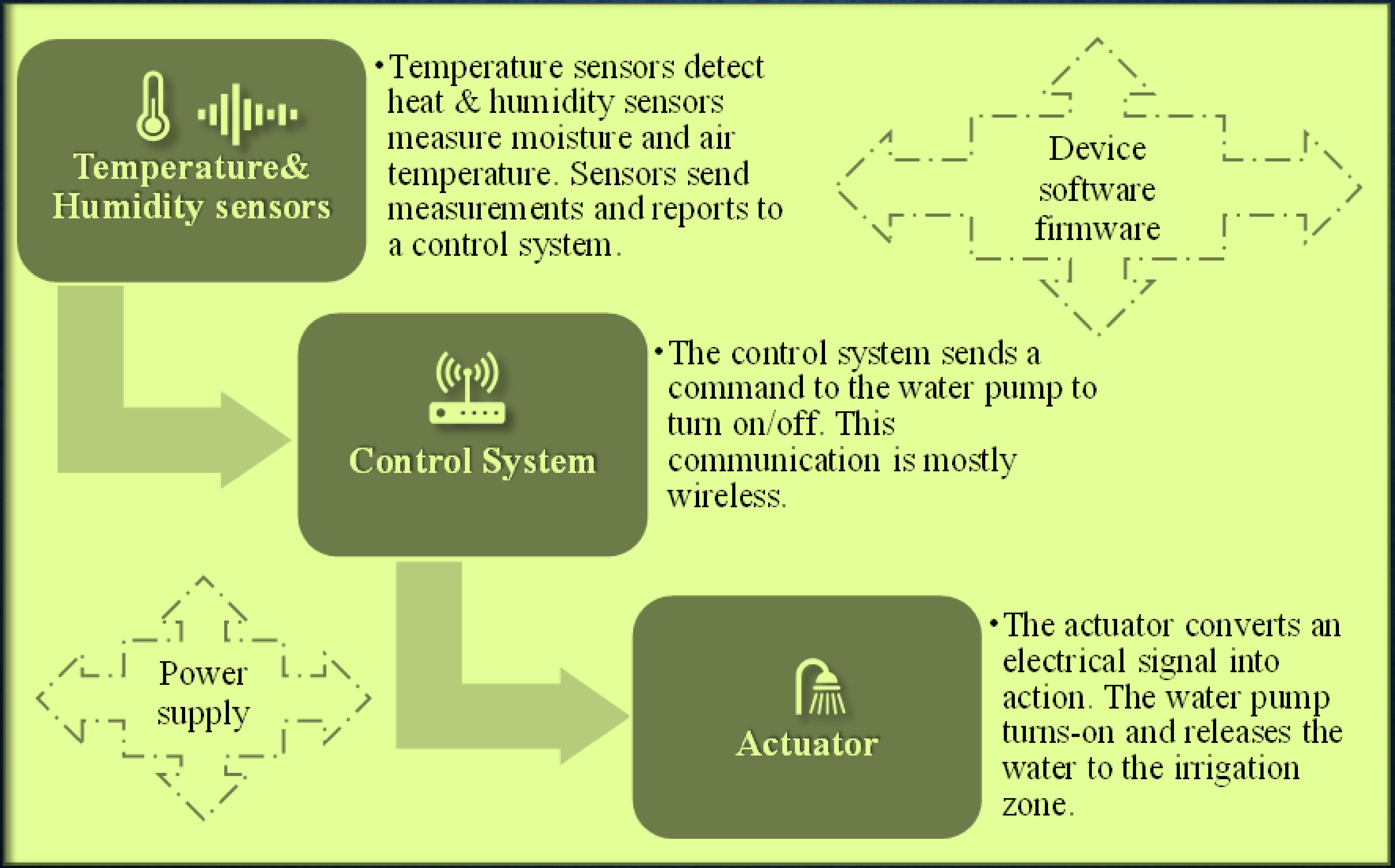
  - Improved travel with better communication.
  - Enhanced safety, including sensors to maintain train speeds, the condition of aircraft parts, and roadway safety for trucks and cars.
  - Environmental effects to reduce energy use, congestion control, including traffic patterns, control of traffic lights, monitoring CO2 emissions, location and speed control applications on buses and taxis, streetlights that automatically adjust to changing light conditions, pothole location and communication of accurate weather conditions.
  - Vehicle-tracking systems, enabling monitoring with GPS tracking and analysis, provision of fleet information, including maintenance, advanced engine diagnostics, etc.
  - For Maritime applications, IoT devices help by streamlining data operations across a fleet, tracking individual vessels, monitoring equipment and machinery in real time, forecasting maintenance needs, improving planning, reduction of fuel consumption, and safeguarding passengers and crews.

IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES

Basic Components and Data Processing

- IoT devices consist of a collection of various technologies that work together seamlessly. Basic IOT hardware includes a sensor, an actuator, A processor, a transceiver, and a power supply. New nanotechnology-enabled sensors convert physical characteristics into electrical signals. IoT devices are embedded with software and essential IoT hardware.
-
  - **The Sensor** captures physical characteristics. It first processes them into electrical signals and then interprets them to provide readable information.
  - **An Actuator** converts electrical signals into action. An actuator turns an electric signal into a motion, for example turning a furnace on or off.
  - **A processor**, processes and stores data within an application, on a server or in the cloud.
  - **A wireless communication transceiver** provides communication through wireless links, allowing people to monitor or configure IoT devices, and enabling interaction between the owner and the device.
  - **A Power supply** may be either Alternating current (AC) or Direct current (DC). All IoTs require power. The power supply must be reliable, affordable, efficient, and space-saving.

IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES (CONT.)



- Temperature sensors detect heat & humidity sensors measure moisture and air temperature. Sensors send measurements and reports to a control system.

- The control system sends a command to the water pump to turn on/off. This communication is mostly wireless.

- The actuator converts an electrical signal into action. The water pump turns-on and releases the water to the irrigation zone.

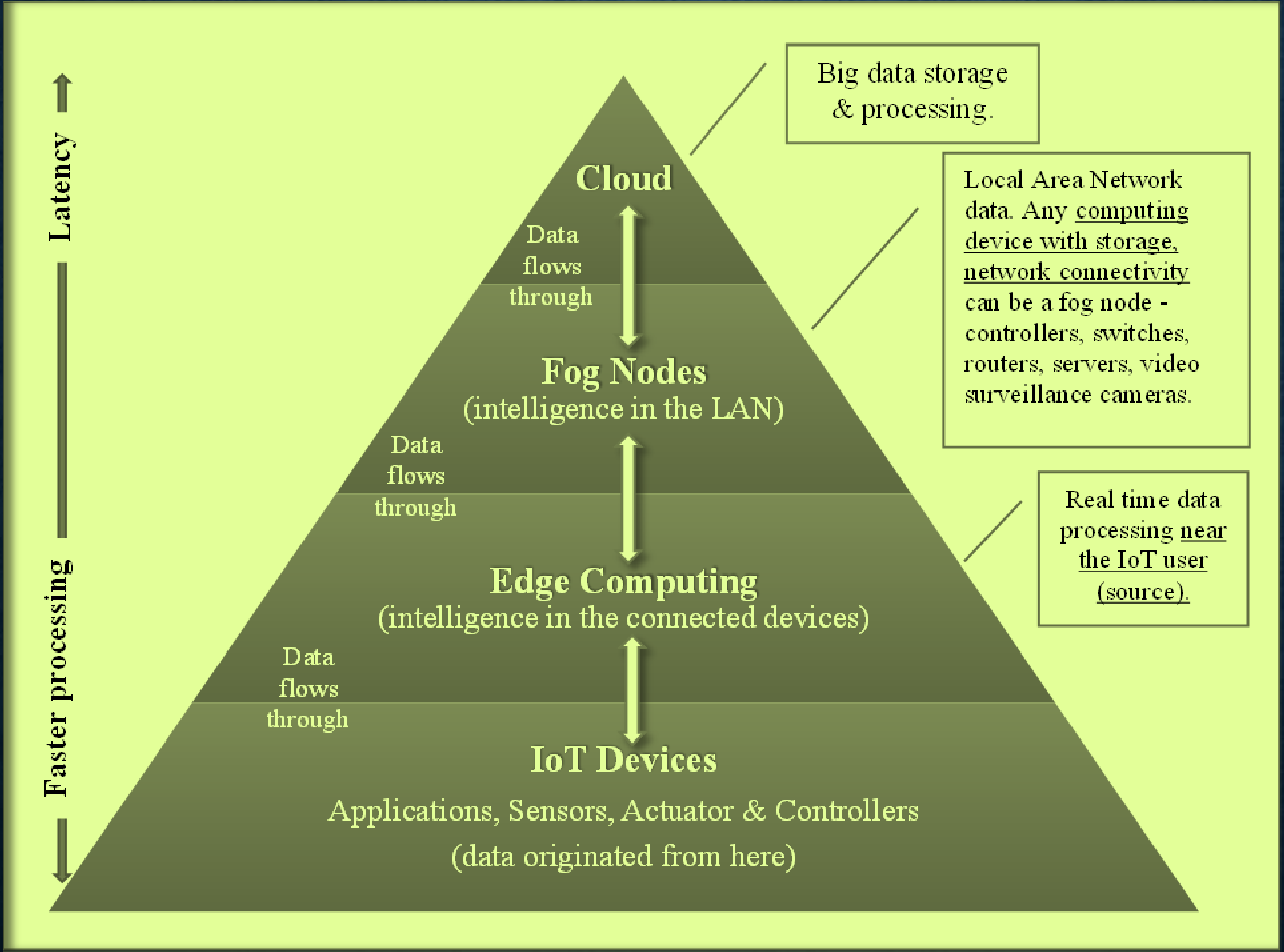
An example of how an IoT system works

IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES (CONT.)

Big data in IoT

- The increasing number of IoT devices and the vast amount of data being generated, along with the increasing use of processing power, together create delays and performance issues, especially when the centralized cloud computing model is used.
  - To address this, a paradigm called edge computing eliminates the centralized cloud servers and brings processing closer to the IoT device or data source.
  - Edge computing is making IoT devices more flexible, by removing the limits of centralized cloud servers, minimizing delays, and theoretically providing more security, since all data are not in the same place.
  - Data processing happens on the edge of the network, or nearer to the source of the data.
  - The edge computing paradigm allows processing in real time at a location closer to the user, resulting in shorter response time and more efficient processing.
- In addition to edge computing, a standard introduced by Cisco called fog computing, defines how edge computing should work.
  - The fog standard brings intelligence down to the Local Area Network (LAN) architecture and processes the data in a fog node.
  - They are called fog nodes because they can be implemented anywhere within a network connection (classrooms, factory floor, power poles, parks, streets, train tracks etc.).
  - In other words, a fog node can be any computing device with storage and network connectivity.
  - These devices include controllers, switches, routers, servers, video surveillance cameras and more.

IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES (CONT.)


Latency
Faster processing
Cloud
Data flows through
Fog Nodes
(intelligence in the LAN)
Data flows through
Edge Computing
(intelligence in the connected devices)
Data flows through
IoT Devices
Applications, Sensors, Actuator & Controllers
(data originated from here)

Big data storage & processing.

Local Area Network data. Any <u>computing device with storage, network connectivity</u> can be a fog node - controllers, switches, routers, servers, video surveillance cameras.

Real time data processing <u>near the IoT user (source).</u>

The edge and fog processing paradigms

IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES (CONT.)

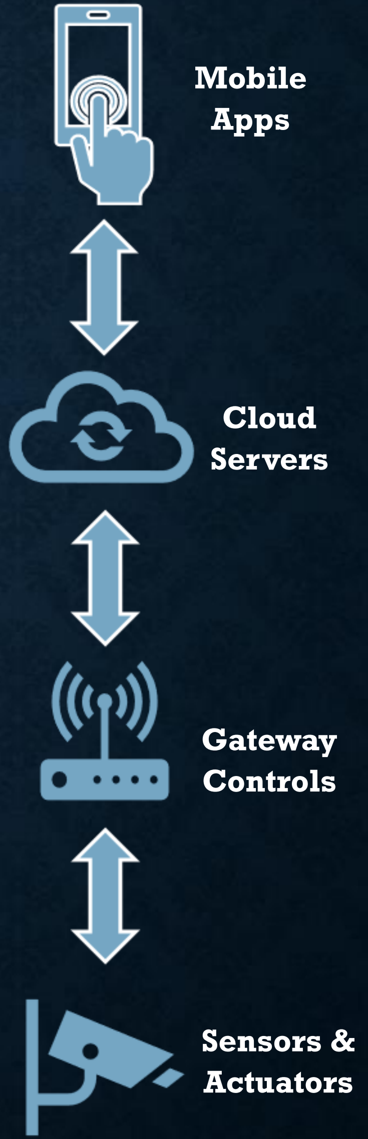
Architectures

- Although the IoT network comprises many interdependent components, its primary purpose is to provide a complete solution and work flawlessly.

- All components of an IoT system must be integrated and must follow rules that define the interface between hardware and software.

- Like any computing device, IoT architecture contains a set of rules or building blocks describing how each part functions, organizes, and integrates with the other parts.

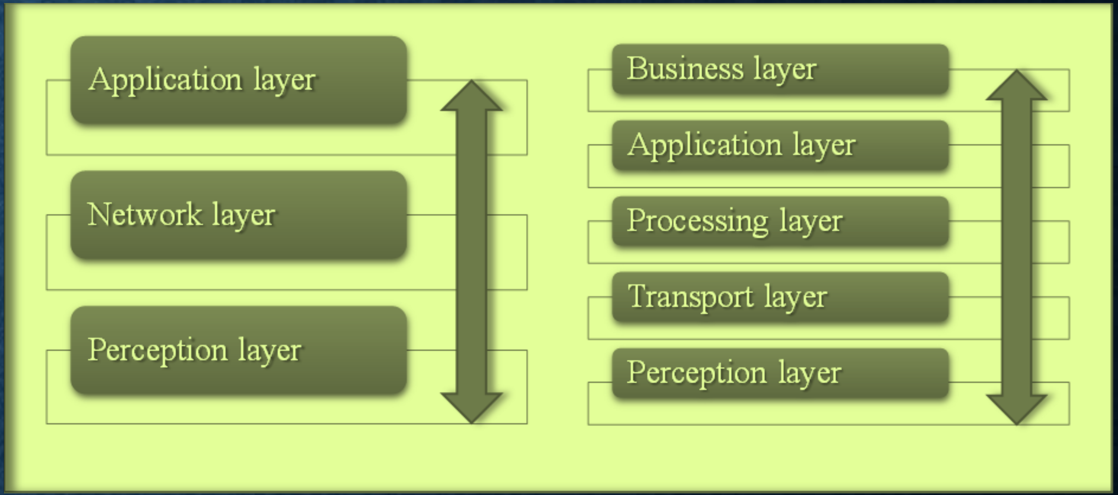
- There is no standard IoT architecture model. Researchers, however, have proposed different architecture models.



IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES (CONT.)

Architectures (cont.)

- The most common are the *three* and the *five-layer* architecture
- The basic three-layer architecture consists of the following:
  - The perception layer is the physical layer, where the collection, transfer and sending of data about the physical environment is accomplished, using sensors, networks-sensors & actuators, tags, Near Field Communication (NFC), and (RFID) Radio Frequency Identification.
  - In the network layer, IoT devices connect to other smart devices and network devices such as gateways, wireless access points, servers, routers, switches, hubs and repeaters.
  - The application layer is where the data are delivered to the IoT user.



The three and five-layer IoT architectures

IOT COMPONENTS, DATA PROCESSING AND ARCHITECTURES (CONT.)

Architectures (cont.)

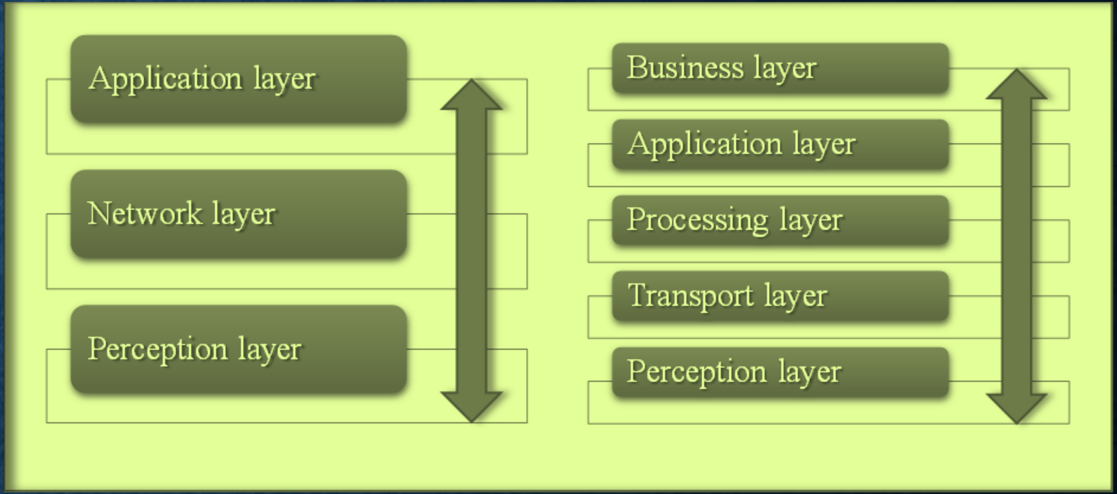
- The three-layer architecture has been expanded to contain three additional layers; the transport layer, the processing layer and the business layer.

  - The transport layer resembles the network layer, which is responsible for transmitting the data from the sensors of the perception layer to the processing layer across the network.

  - The processing or middleware layer is responsible for aggregating data, data storage (cloud computing and databases), processing data received from the transport layer, and protecting against security attacks.

  - The business layer functions as the manager of the IoT system.

  - This layer is responsible for operating the applications, user privacy, and managing how data is created, stored and used.



The three and five-layer IoT architectures

IOT PROTOCOLS

Protocols and Standards

- A **protocol** is a procedure or set of rules used by systems to communicate with one another. Well known examples include Transmission Control Protocol (TCP) and Hypertext Transfer Protocol Secure (HTTPS).

- A **standard,** in this context, is a set of rules followed by systems manufacturers that defines how devices communicate in different settings.
  - For example, Ethernet based networks are defined by IEEE 802.3 standards, issued by the Institute of Electrical and Electronics Engineers (IEEE), and Bluetooth devices are defined by Bluetooth Low Energy 5.1, which is a wireless technology standard for exchanging data over short distances,

Protocols and standards define how IoT devices are managed, and how data are transmitted via networks.

- Standards and protocols are developed by different regulatory organizations and industrial bodies.
  - Among the best known are the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the Organization for the Advancement of Structured Information Standards (OASIS), the International Telecommunication Union (ITU), and the NIST's (National Institute of Standards and Technology) recommendations for IoT device manufacturers (NISTIR 8259).

IOT PROTOCOLS (CONT.)

Protocols and Standards (cont.)

The IoT ecosystem is comprised of the following four layers: Network Access & Physical, Internet, Transport and Application.

I. Application layer (layers 5-7 in OSI): In this layer the user employs the interface given by the IoT to interact with the IoT device or other application.

Protocols used in this layer:

- AMQP
- CoAP
- DDS
- MQTT

II. Transport Layer (layer 4 in OSI): This layer enables host-to-host data communication between layers. Examples of transport protocols are TCP and UDP. Both transport protocols work on top of the IP (Internet Protocol) to send bits of data known as packets from an IoT device to different routers.

- DTLS
- UDP
- TCP

IOT PROTOCOLS (CONT.)

Protocols and Standards (cont.)

III. Internet Layer (layer 3 in OSI): In this layer routers transport packets of data between the source host and the destination host. The IoT device communicates with the router using logical IP addressing to deliver packets of information between different networks. Following are some of the protocols the routers use:

- IPv4
- Ipv6
- RPL
- 6LoWPAN

IV. Network Access Layer (layers 1-2 in OSI): This layer oversees how an IoT device is physically connected to the network through Ethernet wired cables or wireless radio wave technology, using Wi-Fi standards.

- In addition to this connection, the IoT device is connected to a Media Access Control (MAC) and its protocols.
- The MAC address is a unique identification number allocated for every device and is used to connect the device to the network. This address is burnt into every device's hardware by the manufacturer. Some of the protocols in this layer include the following:

- Bluetooth
- Cellular technology

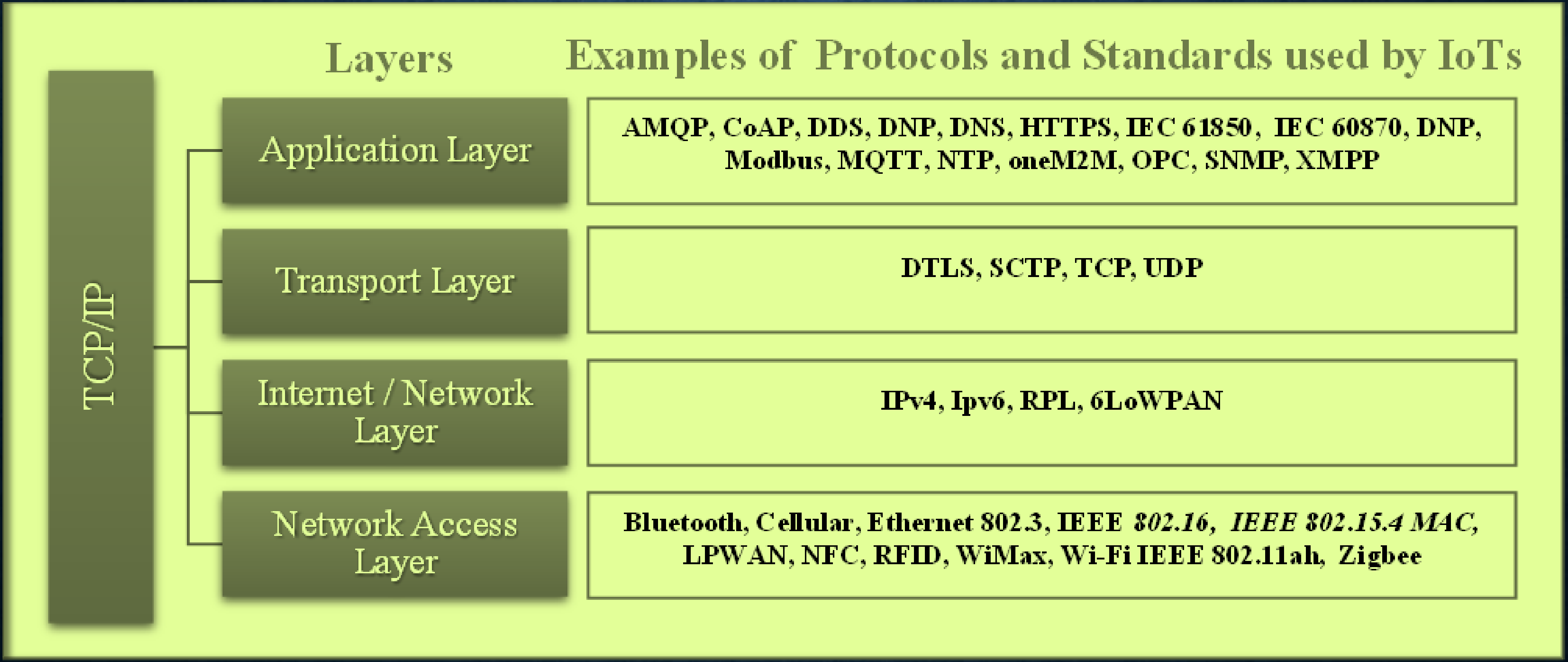
IOT PROTOCOLS (CONT.)

Protocols and Standards (cont.)

IV. Network Access Layer (layers 1-2 in OSI) (cont.)

- Dash7
- Ethernet IEEE 802.3
- NFC (Near Field Communication)
- RFID (Radio Frequency Identification)
- Wi-Fi IEEE 802.11
- ZigBee

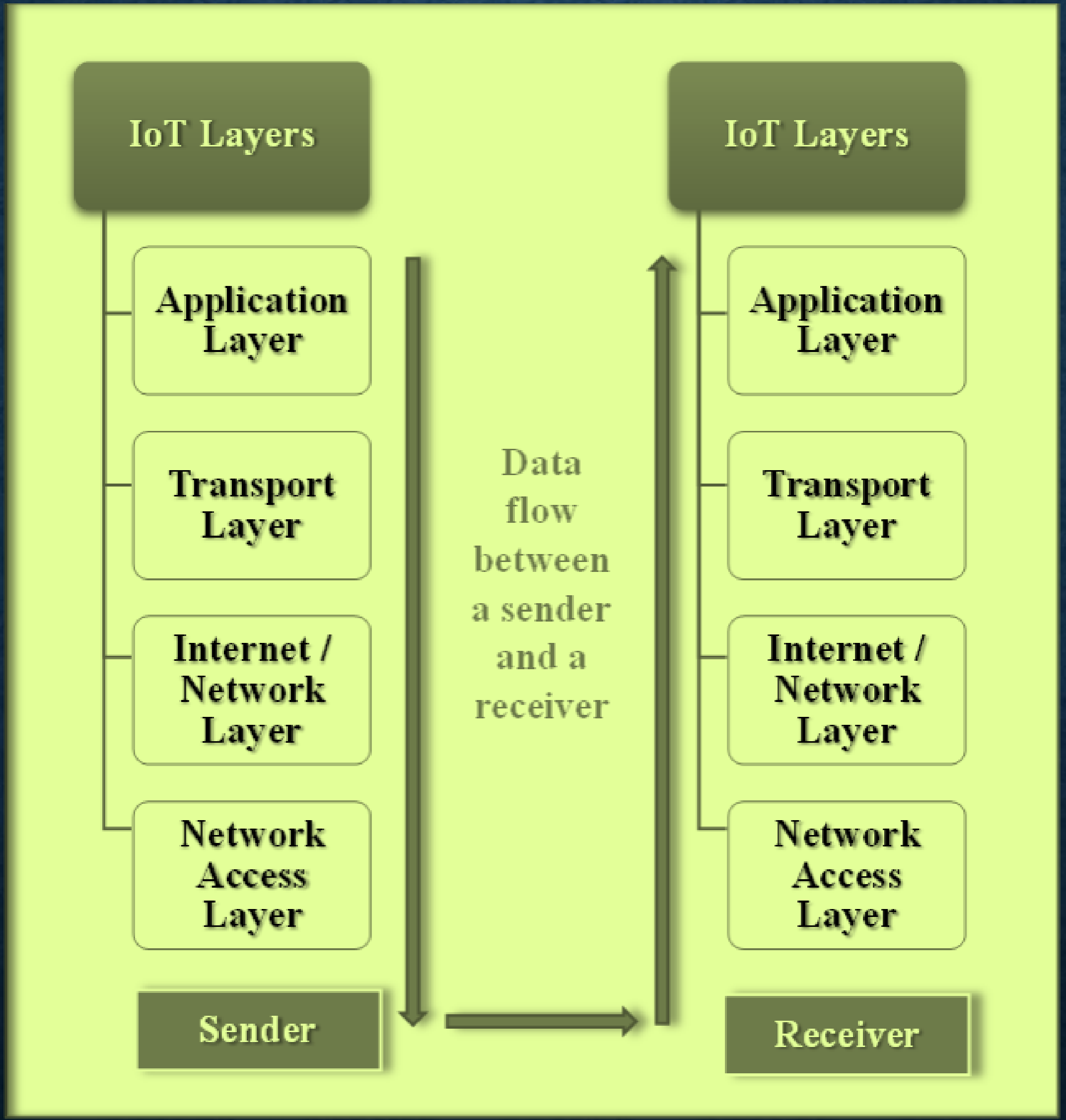
IOT PROTOCOLS (CONT.)



TCP/IP	Layers	Examples of Protocols and Standards used by IoTs
TCP/IP	Application Layer	AMQP, CoAP, DDS, DNP, DNS, HTTPS, IEC 61850, IEC 60870, DNP, Modbus, MQTT, NTP, oneM2M, OPC, SNMP, XMPP
	Transport Layer	DTLS, SCTP, TCP, UDP
	Internet / Network Layer	IPv4, Ipv6, RPL, 6LoWPAN
	Network Access Layer	Bluetooth, Cellular, Ethernet 802.3, IEEE *802.16, IEEE 802.15.4 MAC,* LPWAN, NFC, RFID, WiMax, Wi-Fi IEEE 802.11ah, Zigbee

TCP/IP model, protocols and standards used by IoTs

IOT PROTOCOLS (CONT.)



Data flow between a sender and a receiver

NETWORK CONSIDERATION FOR IOT DEVISES

In addition to protocols and standards, an IoT ecosystem requires bandwidth, interoperability, power usage, and range for successful deployment.

I. Bandwidth

- Bandwidth defines the maximum rate of data transmitted across a network path per unit of time.

- Bandwidth is measured in bits per second (bps), kbps (kilobits per second), mbps, (megabits per second), gbps (gigabits per second), or tbps (terabits per second).

  - Thus, bandwidth is affected by the number of physical devices deployed, the volume of data each device transmits and whether data should be processed or transmitted as raw data to the cloud.

NETWORK CONSIDERATION FOR IOT DEVISES (CONT.)

II. Interoperability

- Interoperability refers to the ability of IoT devices to work and interact well with other existing devices, such as equipment and systems utilizing standards and protocols.
- With the great number of different IoT ecosystems that can be connected, poor interoperability can cause serious issues.

III. Power usage

- Every IoT device requires power to process and transmit data.
- Most of these devices are small, contain limited battery power, and are "always connected" and transmitting data.

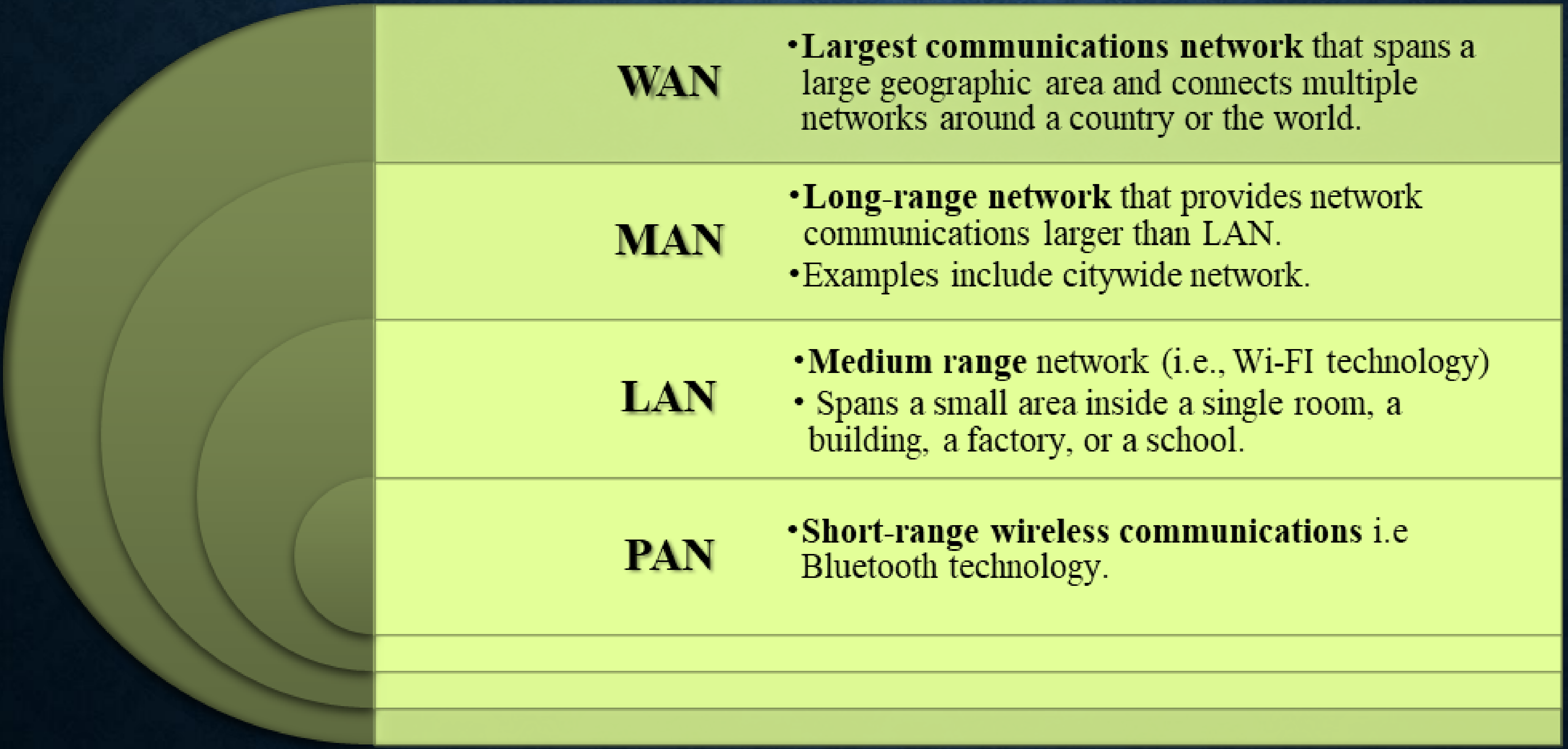
NETWORK CONSIDERATION FOR IOT DEVISES

IV. Range of Networks

Different types of networks can transfer IoT data from one system to another. Following are the types of networks over which data is usually transmitted by IoT devices.

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network) WAN (Wide Area Network)

IOT PROTOCOLS (CONT.)



WAN

- **Largest communications network** that spans a large geographic area and connects multiple networks around a country or the world.

MAN

- **Long-range network** that provides network communications larger than LAN.
- Examples include citywide network.

LAN

- **Medium range** network (i.e., Wi-FI technology)
- Spans a small area inside a single room, a building, a factory, or a school.

PAN

- **Short-range wireless communications** i.e Bluetooth technology.

The Different types of network connectivity for IoTs

NETWORK CONSIDERATION FOR IOT DEVISES

Security

- Security vulnerabilities continue to hound manufacturers and users in every layer of IoT architecture.
- One of the most infamous IoT security attacks occurred in 2016.
  - An IoT botnet malware called Mirai took advantage of unprotected IoT devices by using default usernames and passwords to log in and infect the IoT devices with malware. It then used the IoTs to issue massive distributed denial of service (DDoS) attacks.
  - IoT devices provide hackers with new targets, and more importantly can become part of a “botnet” army that delivers distributed denial of service (DDoS) attacks.

IOT PROTOCOLS (CONT.)

Security (cont.)

- The wide variety of IoT applications using different IoT frameworks, the many manufacturers that fail to implement adequate security measures, along with the lack of computing and battery power make it very difficult to implement a universal security solution.
- Some of the major security issues, limitations and challenges that face IoT devices are the following:
  - Device limitations:
    - IoT devices generally have short battery lifetimes and limitations in memory and processing power. As a result, they cannot handle all the requirements for advanced cryptography algorithms that would protect them from security threats.
  - The lack of security by IoT device manufactures:
    - Manufacturers are profit driven, and rush to produce the latest IoT device, often ignoring the lack of appropriate legislation and other security considerations such as insecure software or firmware. In addition, security software updates have often been largely ignored by device manufacturers.

IOT PROTOCOLS (CONT.)

Security (cont.)

- Physical attacks, Network attacks, Software and Encryption attacks:
  - Physical attack performed in proximity of the IoT device (i.e., attacker is close enough to the device to analyze electrical signals such as electromagnetic waves emitted, and can gather sensitive information.
  - Network attacks occur when an attacker accesses, manipulates or intercepts an IoT network system remotely and causes damage (a DoS attack, Malware, breach, man-in-the-middle attack (MITM), routing information or traffic attack, RFID Spoofing).
  - Software attacks, including Phishing attacks, malware, virus, worms, trojan horse, spyware, and adware.
  - Encryption attacks. These occur when an attacker tries to break the encryption scheme and obtain the private key to the device. These types of attacks include cryptanalysis attacks, side channel attacks, MITM attacks, sleep deprivation attacks, eavesdropping and interference.

ANY QUESTIONS ?