ECE 442/510
Internet of Things and Cyber Physical Systems

Lecture 1: Introduction to IoT and CPS
Summer 2022

Jafar Saniie & Won-Jae Yi

Definition of IoT

A dynamic global network infrastructure with **self-configuring** capabilities based on **standard and interoperable communication protocols** where physical and virtual "things" have **identities**, physical attributes, and virtual personalities and use intelligent interfaces, and are **seamlessly integrated into the information network**, often communicate data associated with users and their environments.

Ch2. Internet of Things – Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7

IoT Data, Information, Knowledge

DATA

Raw and unprocessed data obtained from IoT devices/systems

INFORMATION

Information is inferred from data by filtering, processing, categorizing, condensing and contextualizing data

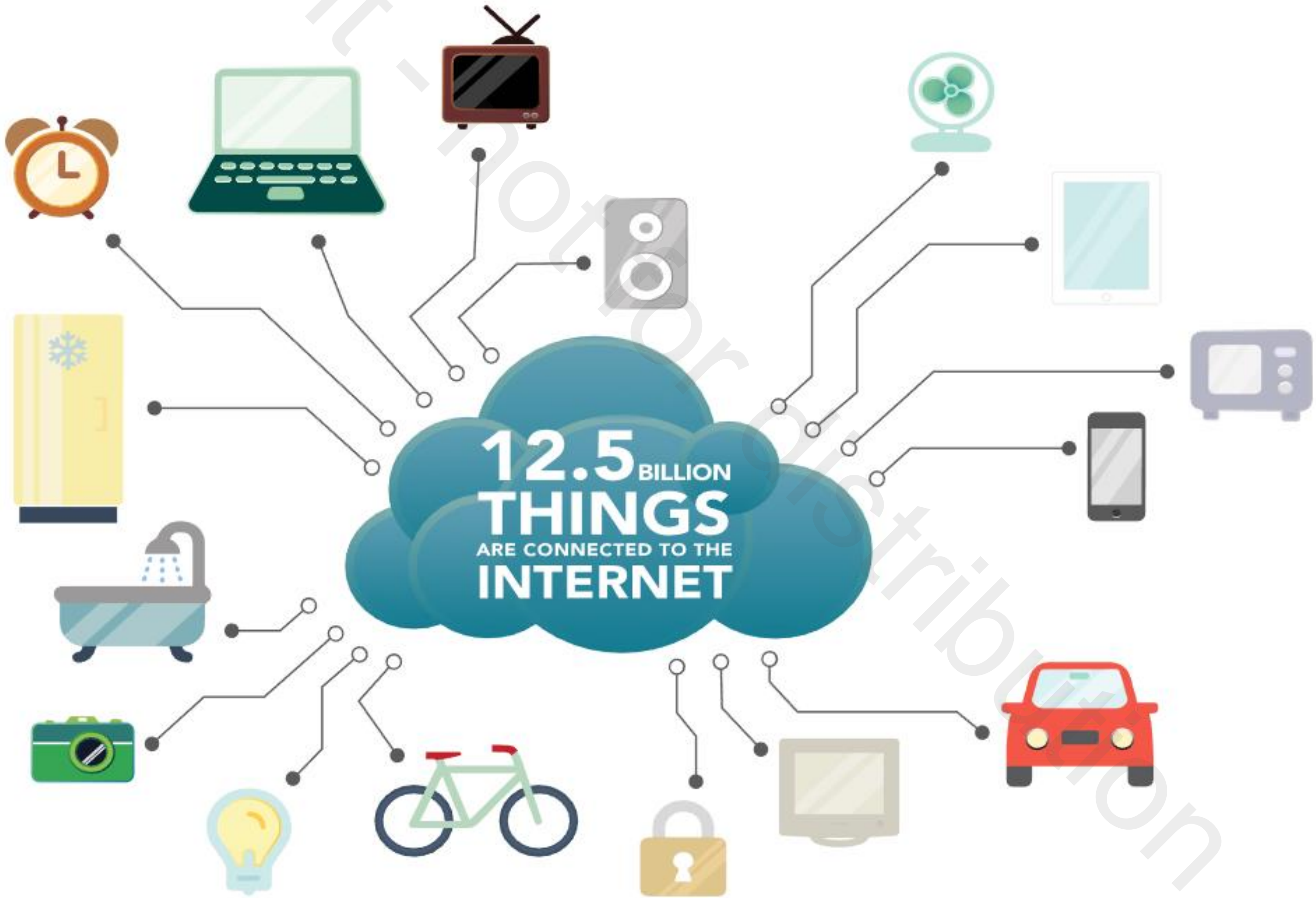
KNOWLEDGE

Knowledge is inferred from information by organizing and structuring information and is put into action to achieve specific objectives

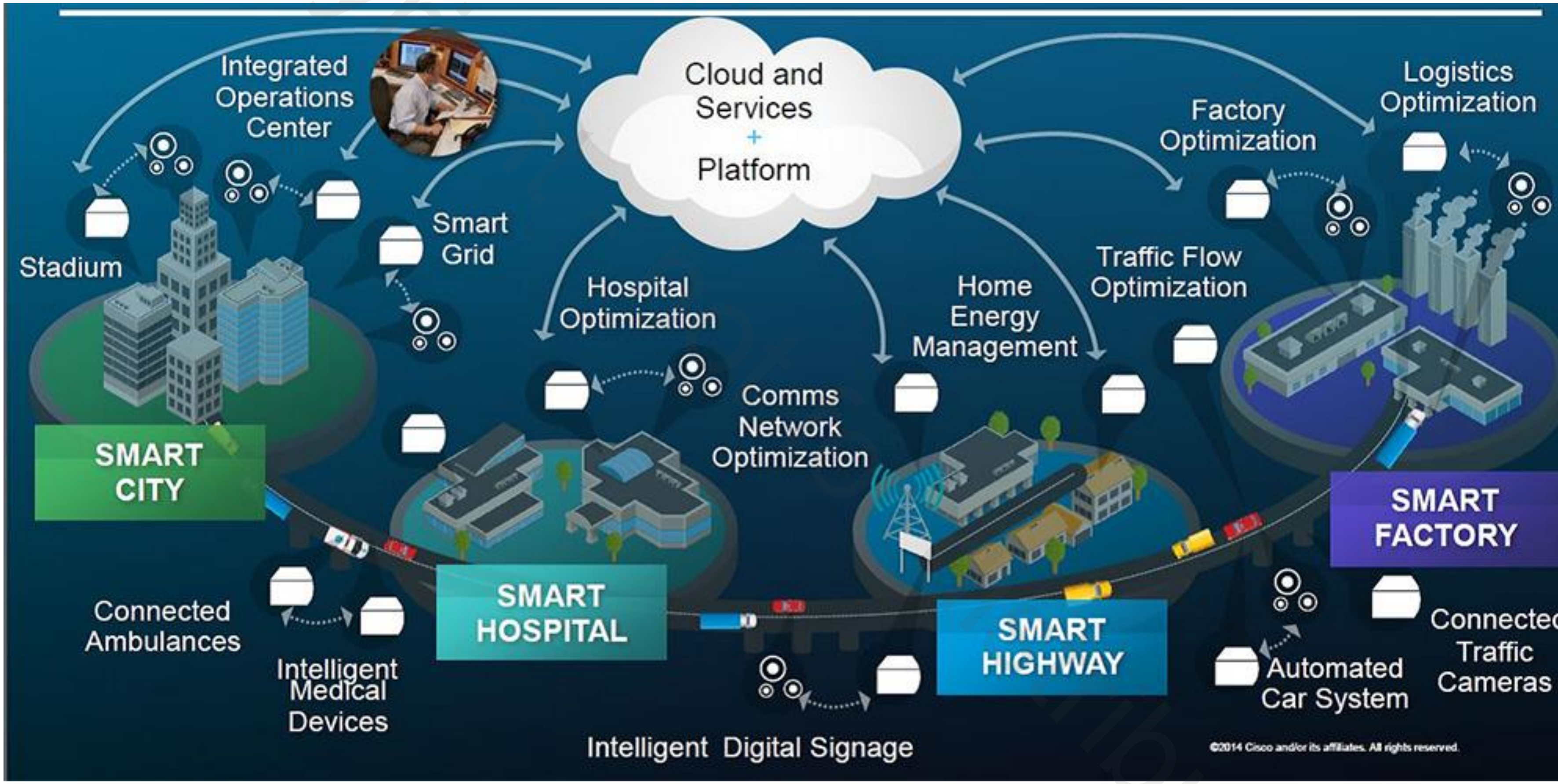
Inferring Information and Knowledge from Data

Internet of Things

- A phenomenon that connects a variety of things
- Things?? Everything with communication capability

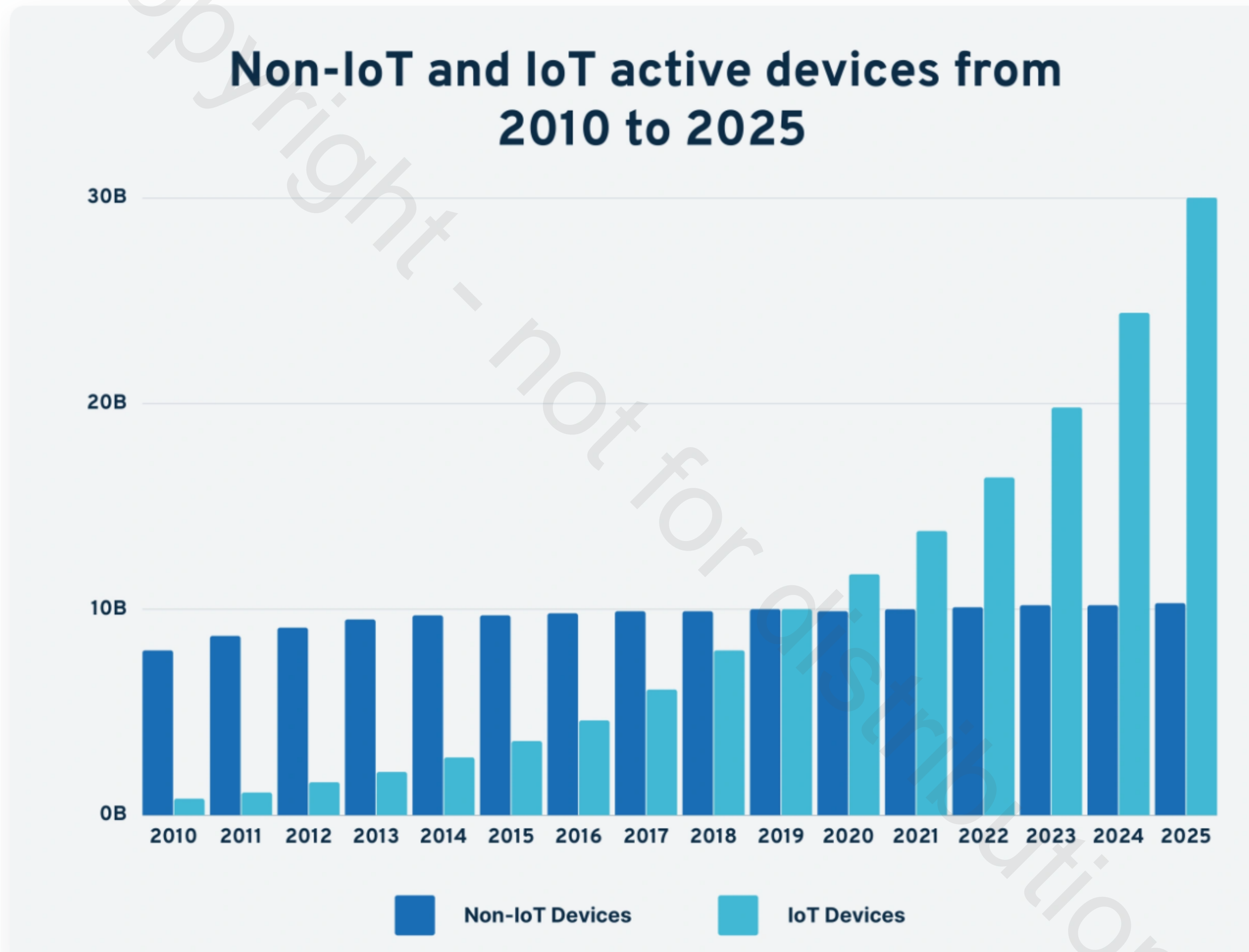


Internet of Things



Applications of IoT

- **Home**
  - Smart Lighting, Smart Appliances
  - Intrusion Detection
  - Smoke/Gas Detectors
- **Cities**
  - Smart Parking, Smart Roads
  - Structural Health Monitoring
  - Emergency Response
- **Environment**
  - Weather, Air Pollution Monitoring
  - Noise Pollution Monitoring
  - Forest Fire Detection
- **Energy**
  - Smart Grids, Prognostics
  - Renewable Energy Systems
- **Retail**
  - Inventory Management
  - Smart Payments, Smart Vending Machines
- **Logistics**
  - Route Generation & Scheduling
  - Fleet Tracking, Shipment Monitoring
  - Remote Vehicle Diagnostics
- **Agricultures**
  - Smart Irrigation, Green House Control
- **Industry**
  - Machine Diagnosis & Prognosis
  - Indoor Air Quality Monitoring
- **Health & Lifestyle**
  - Health & Fitness Monitoring
  - Wearable Electronics
  - Remote Health Patient Monitoring



Non-IoT and IoT active devices from 2010 to 2025
30B
20B
10B
0B
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Non-IoT Devices
IoT Devices

Trending Internet of Things Statistics for 2022:

- The internet of things market revenue is $212 billion worldwide
- Google Home will have the largest IoT devices market share by 2021, at 48%.
- The average number of connected devices per household in 2020 will be 50.
- By 2021, 35 billion IoT devices will be installed around the world.

1. **Households have ten connected devices on average and will rise to 50 in 2021**
2. **Worldwide IoT spending surpassed $1 trillion in 2020 alone**
3. **Spending on IoT Endpoint Security solutions will reach $631M in 2021**
4. **Every second, 127 devices hook up to the internet for the first time.**
5. **There Will Be 1.9 Billion 5G Cellular Subscriptions by 2024**
6. **Revenue for 2020 is expected to be $212 billion worldwide.**
7. **Hardware currently accounts for around 35% of the market's value.**
8. **The number of cellular IoT connections is expected to reach 3.5 billion in 2023**
9. **Companies could invest up to $15 trillion in IoT by 2025**
10. **Smart factories in North America are predicted to be worth more than $500 billion in 2022**
11. **The IoT market is predicted to be worth $4 trillion by 2025**
12. **North America is expected to own 29% of the world's self-driving fleet by 2035**
13. **The Smart Home IoT market will grow to $53.45 billion by 2022**

Internet of Things Smart City Stats

- 14. The Smart Home IoT market will grow to $53.45 billion by 2022
- 15. The top 600 smart cities will account for 60% of the global GDP in 2025

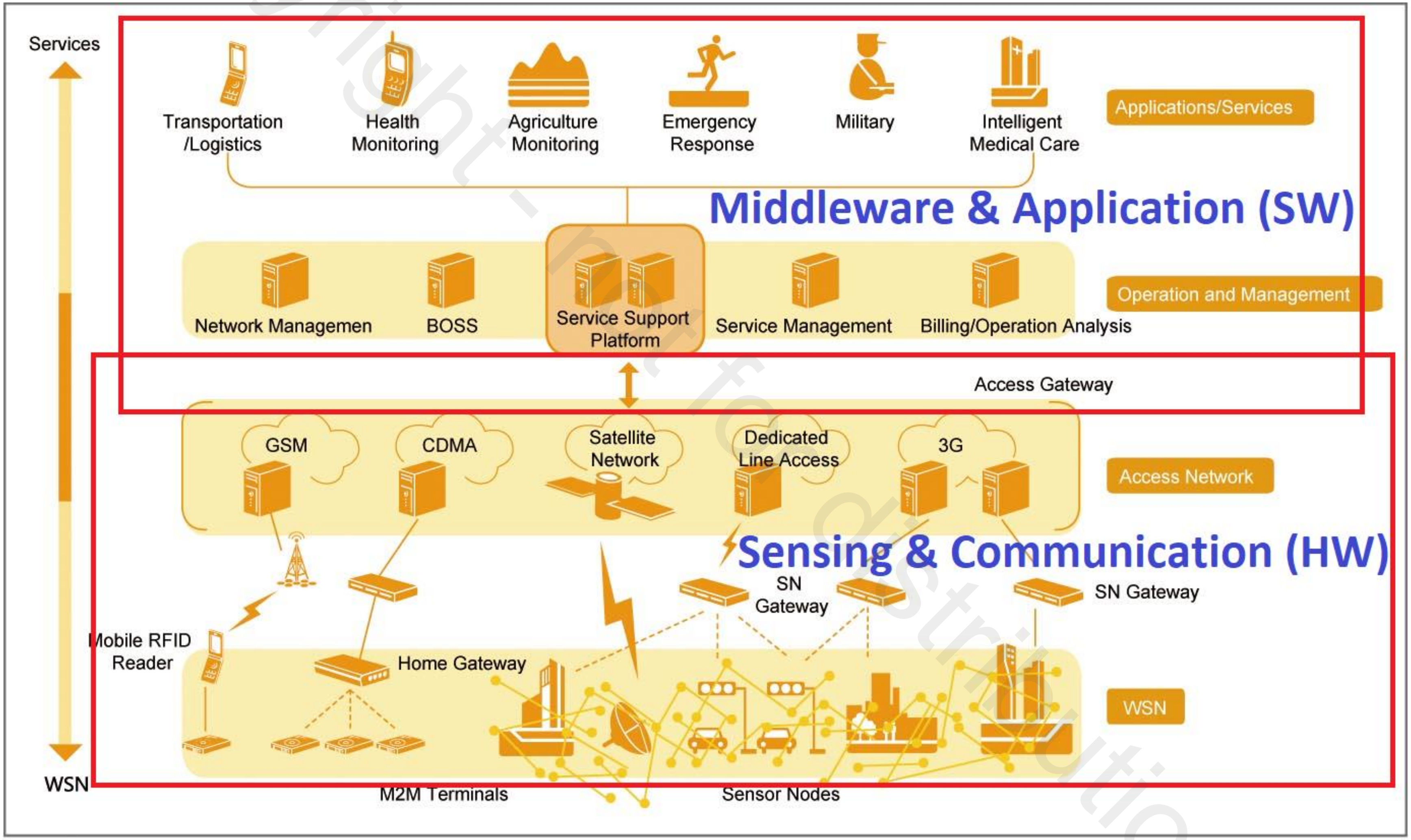
IoT Technology Statistics

- 17. IoT devices will generate 79.4 zettabytes of data by 2025

Security of IoT Devices Statistics

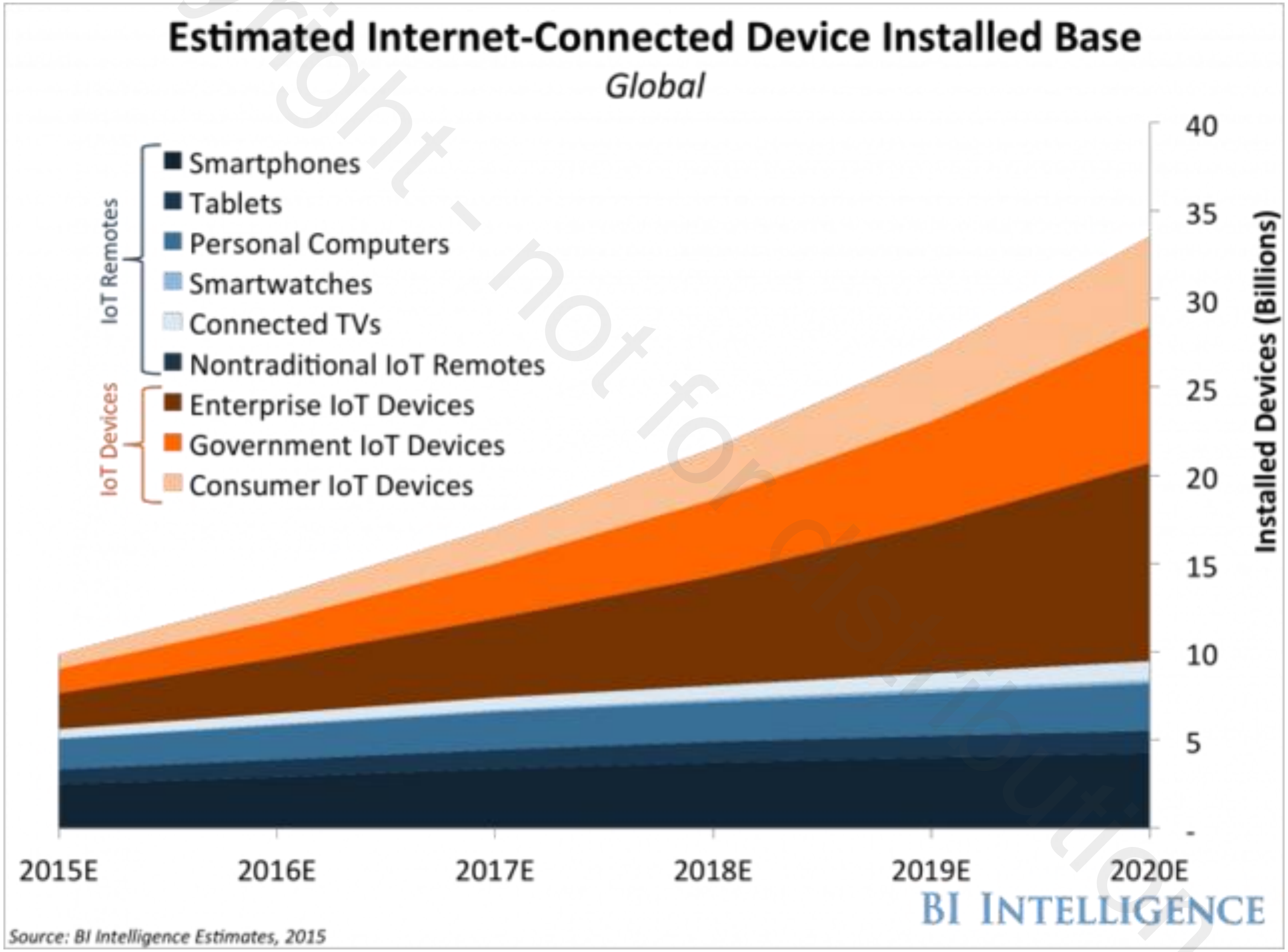
- 18. Annual spending on IoT security measures will increase to $631 million by 2021.
- 19. IoT devices are typically attacked within five minutes of connecting to the internet.
- 20. 75% of cyberattack cases are carried out through routers
- 21. 74% of global consumers worry about losing their civil rights because of IoT
- 22. 48% of businesses admit they are unable to detect IoT security breaches on their network.

Internet of Things

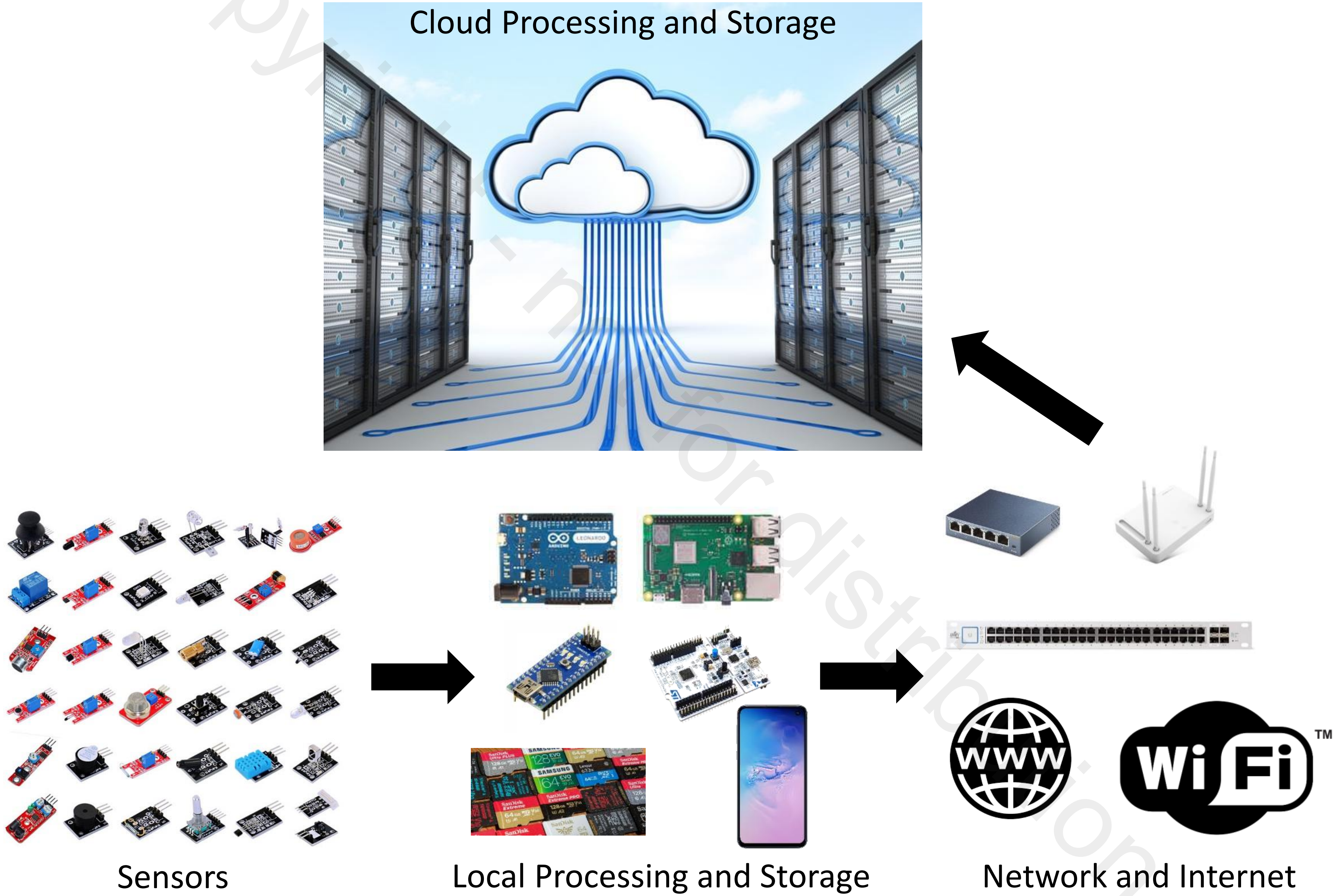


"Opportunities, Challenges and Practices of the Internet of Things, Fan Wanpeng and Li Yu, ZTE Technologies

IoT Trend Forecast



Internet of Things



Internet of Things

- **Sensors & Actuators**
  - Transforms analog data (environment sensing) to digital data
  - No/minimum data processing
  - Consume low power, operates on batteries for a long time
  - Industry, agriculture, homes, transportation or smartphones
- **Local Processing and storage devices**
  - Microcontrollers/embedded systems handling data retrieval
  - Send some data to *"Edge/Fog Computing"* → *devices are on the 'edge' of the cloud*
- **Network and Internet**
  - Dedicated hardware connects to the local devices
  - Pulls out data, sends it to the cloud to be stored
- **Cloud**
  - Aggregation of data from Edge/Fog
  - Making predictions based on the stored information
  - Further processing of collected data, used for "heavy lifting"

Fog computing vs Edge computing in a nutshell

- In a nutshell, edge computing is data computation that happens at the network's edge, in close proximity to the physical location creating the data.
- On the other hand, fog computing acts as a mediator between the edge and the cloud for various purposes, such as data filtering.

Sensors and Actuators

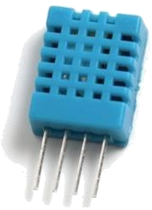
Sensors	Functionality
Accelerometer /gyroscope	Movement, orientation, position detection
Camera	Capturing images
Strain gauge	Force, pressure, tension, weight detection
Microphone	Capturing sounds
Barometer	Measuring air pressure
Radar/LIDAR	Object detection

Actuators	Functionality
Servomotor	Rotary actuator for accurate angular/linear position, velocity and acceleration
Solenoids	Actuates valve/switch via electromagnetics
LED/LCD displays	Displays information
Speakers	Generates sounds
Valves	Open/close

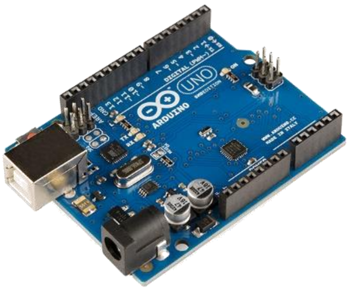
Design Consideration

- Noise
- Vibration
- Bias
- Faults
- Physical dynamics
- Sampling rates

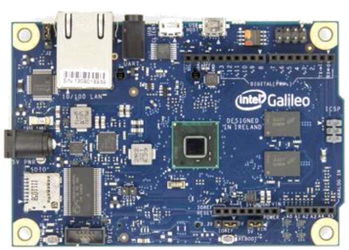
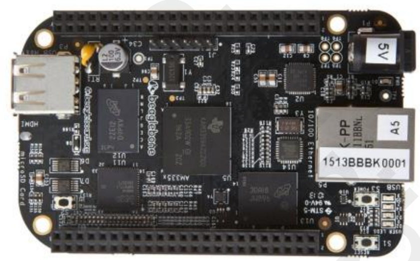
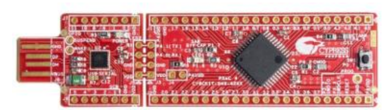
Internet of Things – Medical Sensors

			
ECG Sensor	EEG Sensor	EMG Sensor	SpO_2 Pulse Oximeter
			
Blood Pressure	Temperature & Humidity	Air Flow (Breathing)	Accelerometer

Internet of Things – Local Device

			
Smartphone	Tablet	Single-board Computer	Desktop
		• Wireless connectivity • Computation Power • Flexibility in Wireless Protocols • Easily reconfigurable hardware/software	
FPGA	Single-board microcontroller		

Internet of Things – Local Device

			
Arduino	Raspberry Pi	TI Launchpad	STM32 Nucleo
			
Intel Galileo	Intel Edison	Beaglebone Black	Cypress PSoC 4

Cyber Physical Systems (CPS)

- Cyber Physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components

US National Science Foundation (tinyurl.com/ya9nqh6s)

- CPS integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other

CPS Virtual Organization

- CPS are smart systems that include engineered interacting networks of physical and computational components.

CPS Public Working Group (NIST) (tinyurl.com/yczudlx5)

- In such technical systems, which are often called CPS, real-time computing elements and physical systems interact tightly. …The merging of IoT and CPS into closed-loop, real-time IoT-enabled cyber-physical systems is seen as an important future challenge.

PICASSO Project Opportunity Report (tinyurl.com/yczudlx5)

IoT: Examples of Current Definitions

- An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

  ISO/IEC JTC1, 2015 (tinyurl.com/y7leyljg)

- The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 as 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-TY.400/Y.2060 (tinyurl.com/yaung7uf)

- IoT refers to any systems of interconnected people, physical objects, and IT platforms, as well as any technology to better build, operate, and manage the physical world via pervasive data collection, smart networking, predictive analytics, and deep optimization.

  IEEE-SA IoT Ecosystem Study 2015 (tinyurl.com/y9vmtam8)

Cyber Physical Systems Paradox

Design Considerations

- Cyber environment and Physical environment
- Computational Powers and Dynamics of the System
- Data Security, Privacy and Safety

Paradox System Requirements

- System Adaptability vs Repeatability
- High connectivity vs Security and Privacy
- High performance vs Low energy
- Asynchrony vs Coordination/Cooperation
- Scalability vs Reliability and Predictability
- Laws and Regulations vs Technical Possibilities
- Economies of scale(cloud) vs Locality (fog or edge)
- Open vs Proprietary
- Algorithms vs Dynamics

∴ Innovative New Engineering and Modeling Methods Required for establishing CPS

Relationship between CPS and IoT

- In most academic and project activities, the difference between “Internet of Things” and “Cyber-Physical Systems” is not made clear and it is difficult to find a source that draws a clear-cut distinction… Yet, identified objects in an IoT system can still be networked together so as to control a certain scenario in a coordinated way, in which case an IoT system can be considered to grow to the level of a CPS.

  IEEE Towards a Definition of the Internet of Things (tinyurl.com/yckrfolc)

Advances that will transform life, business, and the global economy…

Disruptive technology is an innovation that significantly alters the way that consumers, industries, or businesses operate.

Twelve potentially economically disruptive technologies

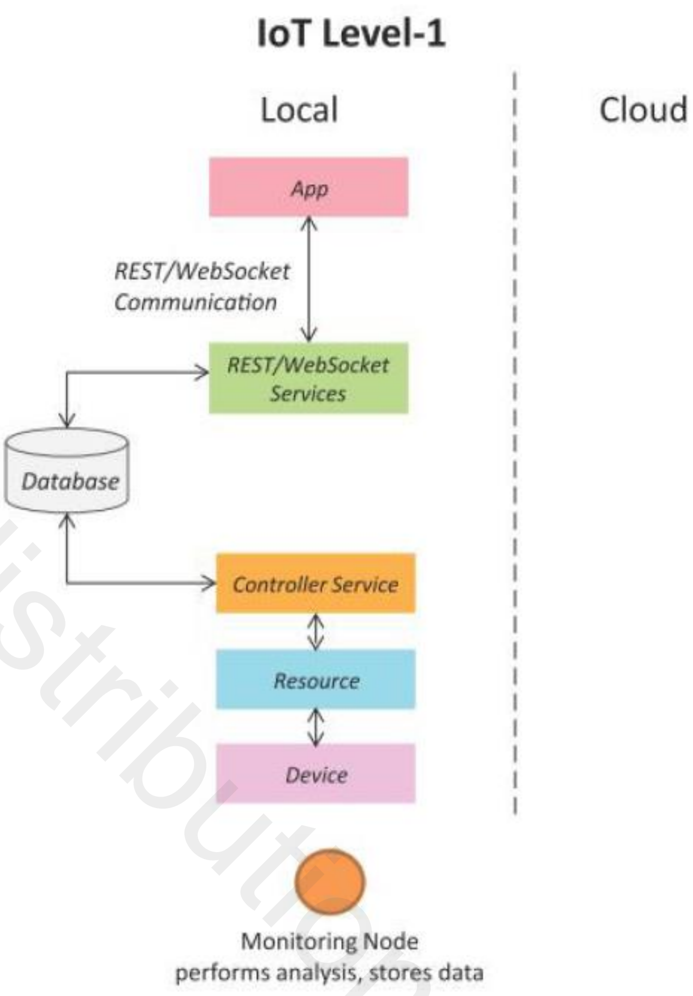
Mobile Internet	Increasingly inexpensive and capable mobile computing devices and Internet connectivity
Automation of knowledge work	Intelligent software systems that can perform knowledge work tasks involving unstructured commands and subtle judgments
The Internet of Things	Networks of low-cost sensors and actuators for data collection, monitoring, decision making, and process optimization
Cloud technology	Use of computer hardware and software resources delivered over a network or the Internet, often as a service
Advanced robotics	Increasingly capable robots with enhanced senses, dexterity, and intelligence used to automate tasks or augment humans
Autonomous and near-autonomous vehicles	Vehicles that can navigate and operate with reduced or no human intervention
Next-generation genomics	Fast, low-cost gene sequencing, advanced big data analytics, and synthetic biology ("writing" DNA)
Energy storage	Devices or systems that store energy for later use, including batteries
3D printing	Additive manufacturing techniques to create objects by printing layers of material based on digital models
Advanced materials	Materials designed to have superior characteristics (e.g., strength, weight, conductivity) or functionality
Advanced oil and gas exploration and recovery	Exploration and recovery techniques that make extraction of unconventional oil and gas economical
Renewable energy	Generation of electricity from renewable sources with reduced harmful climate impact

Courtesy of Lee, Berkeley

IoT Levels & Deployment

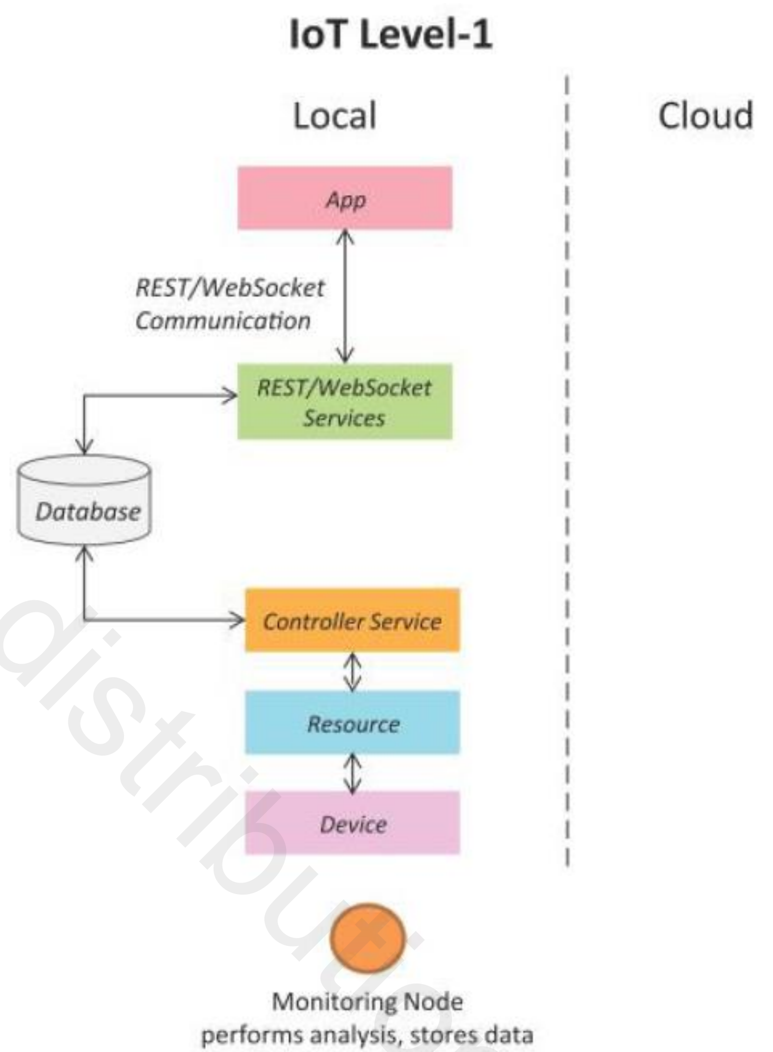
IoT Levels & Deployment Templates

- An IoT system comprises of the following components:
  - **Device**: An IoT device allows identification, remote sensing, actuating and remote monitoring capabilities.
  - **Resource**: Resources are software components on the IoT device for accessing, processing, and storing sensor information, or controlling actuators connected to the device. Resources also include the software components that enable network access for the device.
  - **Controller Service**: Controller service is native service that runs on the IoT device and interacts with the web services. Controller service sends data from the device to the web service and receives commands from the application (via web services) for controlling the device.



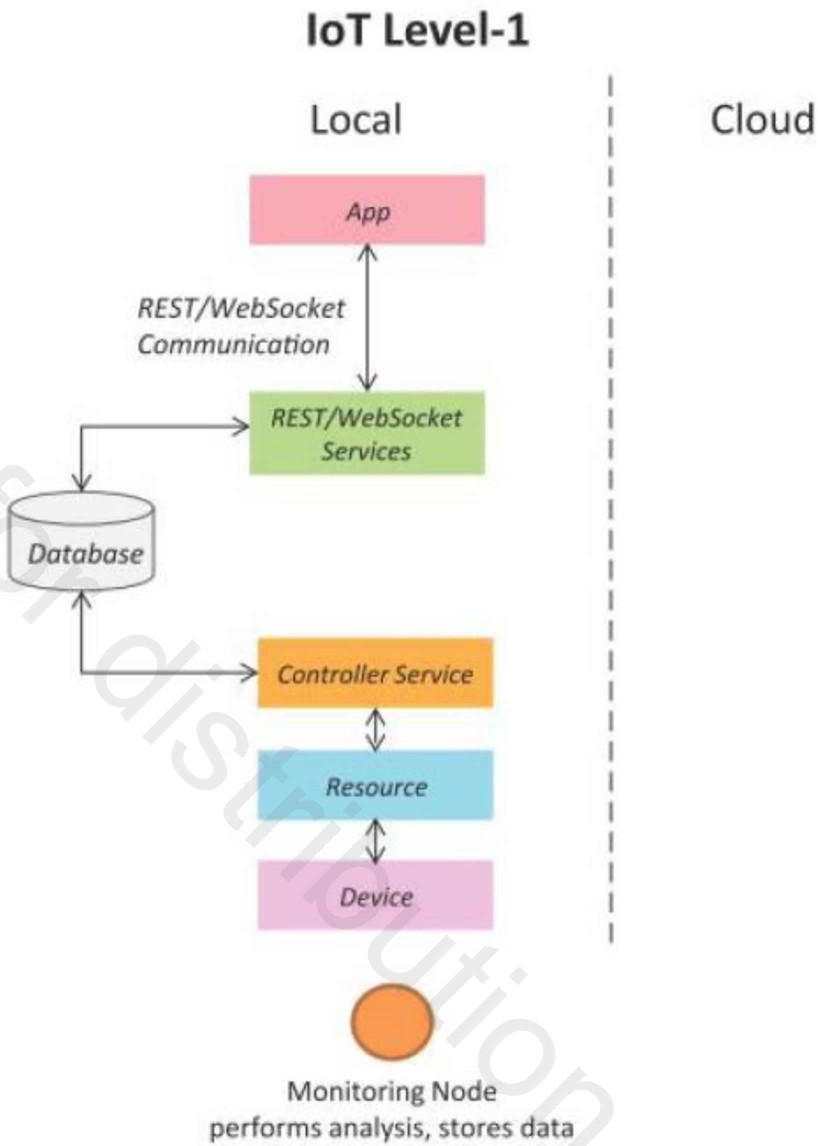
IoT Levels & Deployment Templates

- **Database**: Database can be either local or in the cloud and stores the data generated by the IoT device
- **Web Service**: Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).
- **Analysis Component**: The Analysis Component is responsible for analyzing the IoT data and generate results in a form which are easy for the user to understand.
- **Application:** IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view the processed data.



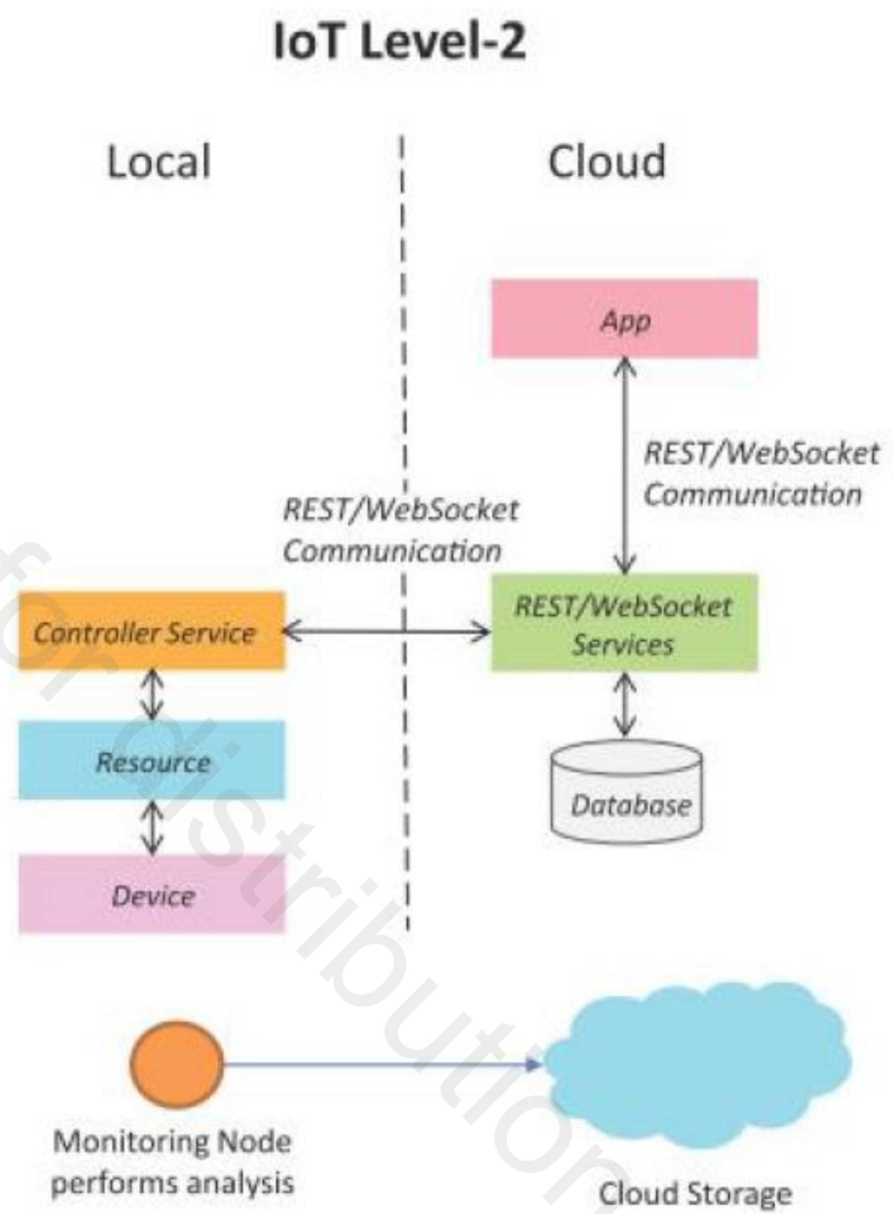
IoT Level-1

- A level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application
- Level-1 IoT systems are suitable for modeling low-cost and low-complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive.



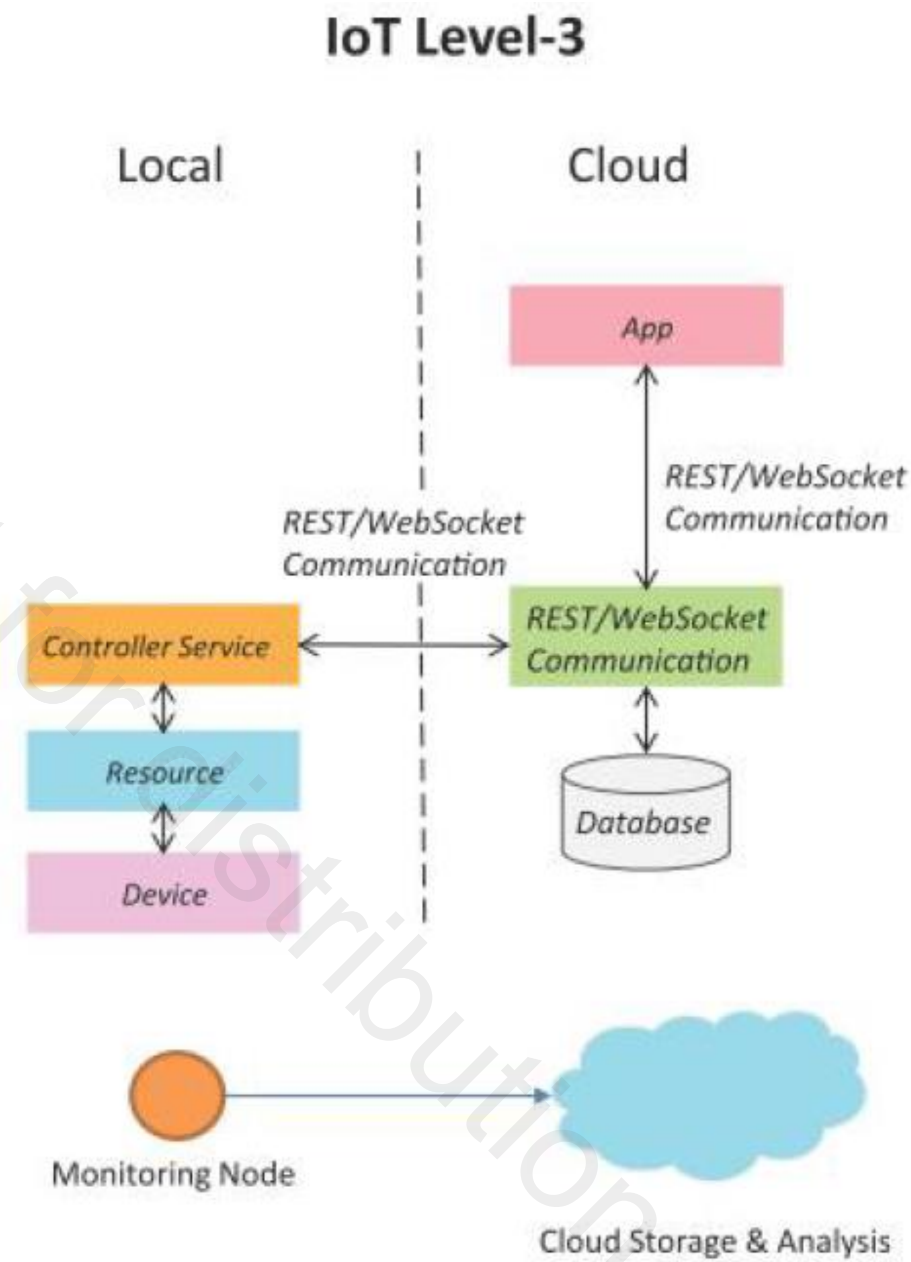
IoT Level-2

- A level-2 IoT system has a single node that performs sensing and/or actuation and local analysis.
- Data is stored in the cloud and application is usually cloud-based
- Level-2 IoT systems are suitable for solutions where the data involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself.



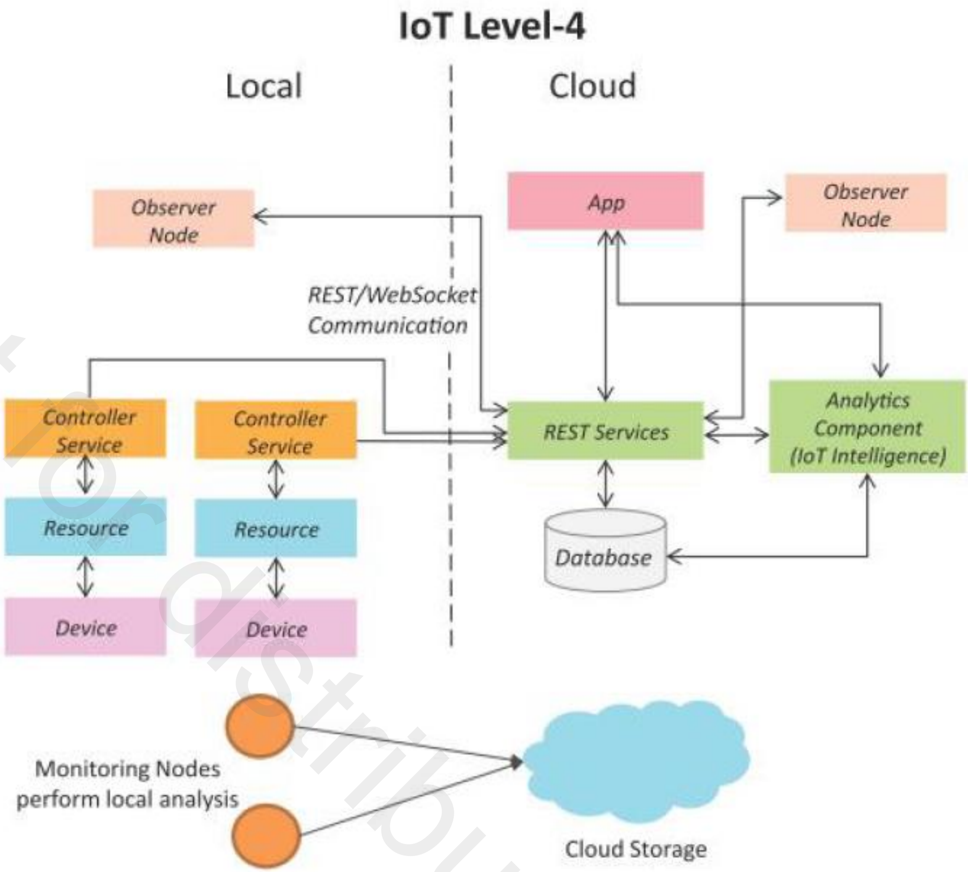
IoT Level-3

- A level-3 IoT system has a single node. Data is stored and analyzed in the cloud and application is cloud-based.
- Level-3 IoT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive and are done at the cloud



IoT Level-4

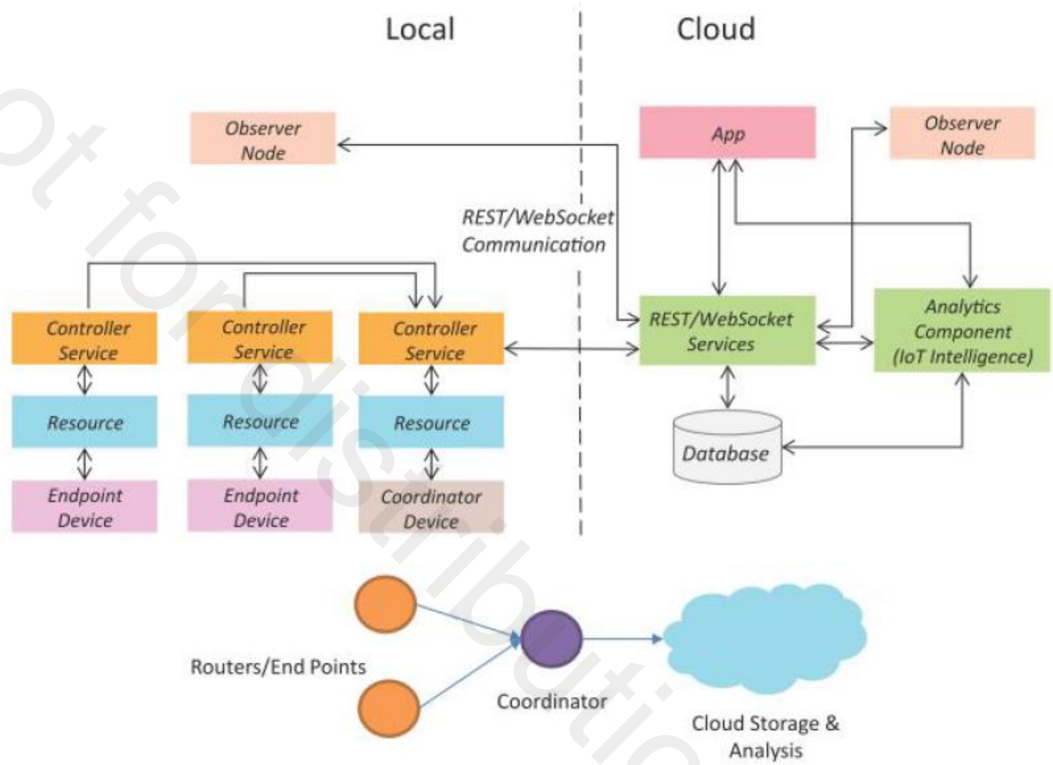
- A level-4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud-based.
- Level-4 contains local and cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices.
- Level-4 IoT systems are suitable for solutions where multiple nodes are required, and the data involved is big.



IoT Level-5

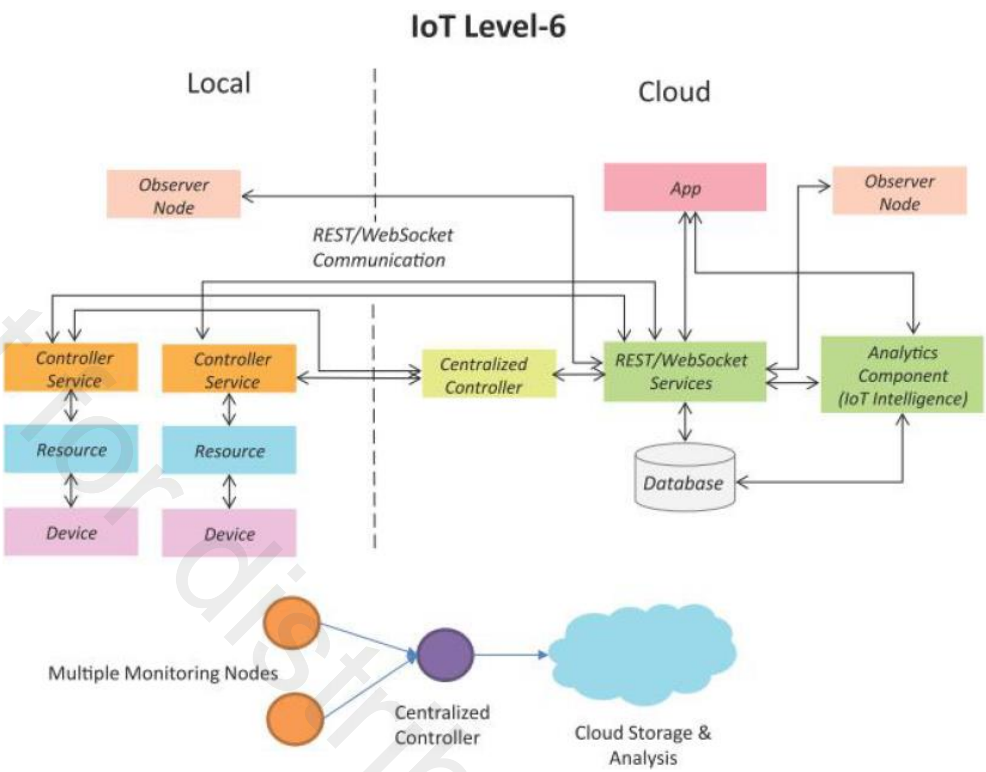
- A level-5 IoT system has multiple end nodes and one coordinator node.
- The end nodes that perform sensing and/or actuation.
- Coordinator node collects data from the end nodes and sends to the cloud.
- Data is stored and analyzed in the cloud and application is cloud-based.
- Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive

IoT Level-5



IoT Level-6

- A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud
- Data is stored in the cloud and application is cloud-based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud-based application.
- The centralization controller is aware of the status of all the end nodes and sends control commands to the nodes.



Characteristics of IoT

- **Dynamic & Self-Adapting**
  - Capability to dynamically adapt with the changing contexts
  - Take actions based on their operating conditions, user's context, sensed environment
- **Self-Configuring**
  - Allowing a large number of devices to work together to provide certain functionality (e.g., weather monitoring)
  - Ability to configure themselves (in association with the IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual/user intervention

Characteristics of IoT

- **Interoperable Communication Protocols**
  - Support a number of interoperable communication protocols
  - Communicate with other devices and also with the infrastructure
- **Unique Identity**
  - Each IoT device has a unique identity and a unique identifier

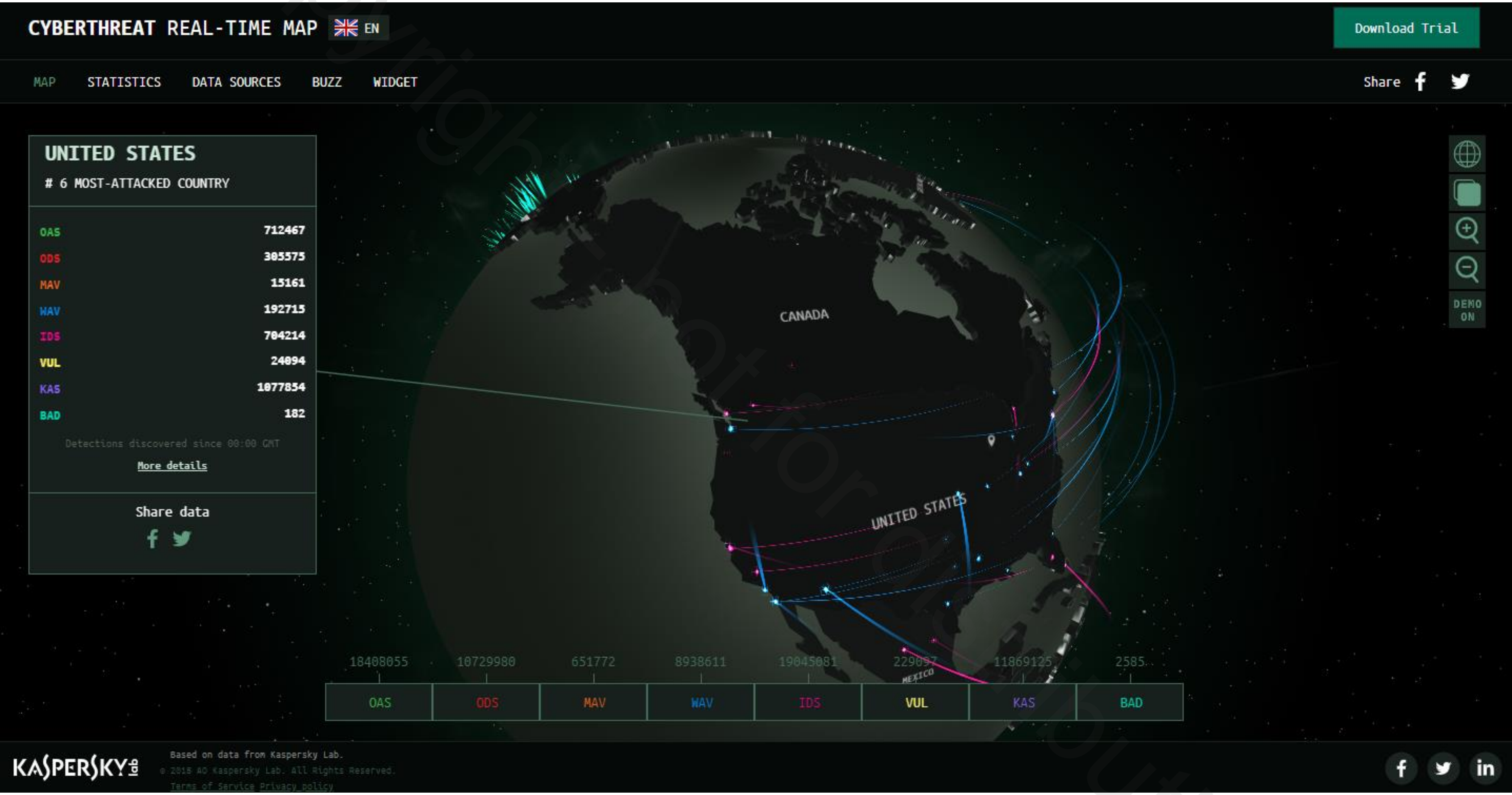
    (IP: **Internet Protocol** or URI: **Uniform Resource Identifier**)
  - Intelligent interfaces which adapt based on the context, allow communicating with users and the environmental contexts
  - IoT device interfaces allow users to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure

Characteristics of IoT

- **Integrated into Information Network**
  - Usually integrated into the information network that allows them to communicate and exchange data with other devices and systems
  - IoT devices can be dynamically discovered in the network, by other devices and/or the network, and have the capability to describe themselves (and their characteristics) to other devices or user applications
  - Integration into the information network helps in making IoT system “smarter”
  - Collective intelligence of the individual devices in collaboration with the infrastructure
  - Data aggregation and analysis from a large number of connected IoT nodes

IoT and Security

IoT Vulnerabilities



https://cybermap.kaspersky.com/

Security in IoT

Impacts everyone's day-to-day life

- Millions of compromised computers, millions of stolen passwords, stolen money

It's important for our

- Physical safety and safety of our possessions
- Confidentiality of data/privacy
- Functionality

Safety

Adversaries can affect our safety by tampering with pacemakers, planes, vehicles

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

JULIE BORT

Jan. 16, 2014, 1:36 PM 195,469 39

FBI probe of alleged plane hack sparks worries over flight safety

Courtesy of Ada Popa, Berkeley

Privacy/Confidentiality

Adversaries get access to medical, financial, personal user data, or sensitive corporate data

91% OF HEALTHCARE ORGANIZATIONS HAVE REPORTED A DATA BREACH IN THE LAST FIVE YEARS.

DON'T LET THE DOOR HIT YOU... —

After huge Equifax breach, CEO "retires"

Board is "deeply concerned about and totally focused on the cybersecurity incident."

CYRUS FARIVAR - 9/26/2017, 6:42 AM

140 million records breached (containing SSN, names, credit cards)

- Pretty much any major company collecting user data has been hacked

EVERYDAY MONEY IDENTITY THEFT

Data Breach Tracker: All the Major Companies That Have Been Hacked

Courtesy of Ada Popa, Berkeley

Why is IoT Security behind?

Security on Desktop/Mobile

- Massive security investments over past 20 years, in response to growing adversarial pressure
- Consumers’ security actively managed by O.S., platform, and browser vendors
  - Automatic updates applied without user intervention
  - Defaults assume users uninformed, need developers’ protection
- Applications are constrained by security requirements
- Small number of popular, homogeneous platforms to protect

Why is IoT Security behind?

Security in IoT

- Still don’t want to believe that the network is evil and wants to kill you
- Massive underinvestment in security. Viewed as an obstacle or as somebody else’s problem
- Consumers must manage security themselves. In practice, it’s managed by no one
  - Updates are rarely or never applied, if they’re available at all
  - Defaults throw users to the wolves. If they don’t lock things down, it’s their down fault.
- Applications completely unconstrained
- Massive number of heterogeneous systems to protect

Physical and Functional Design of IoT Network

Physical Design of IoT Network

- The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.
- IoT devices can
  - Exchange data with other connected devices and applications (directly or indirectly)
  - Collect data from other devices and process the data locally
  - Send the data to centralized servers or cloud-based application back-ends for processing the data
  - Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints

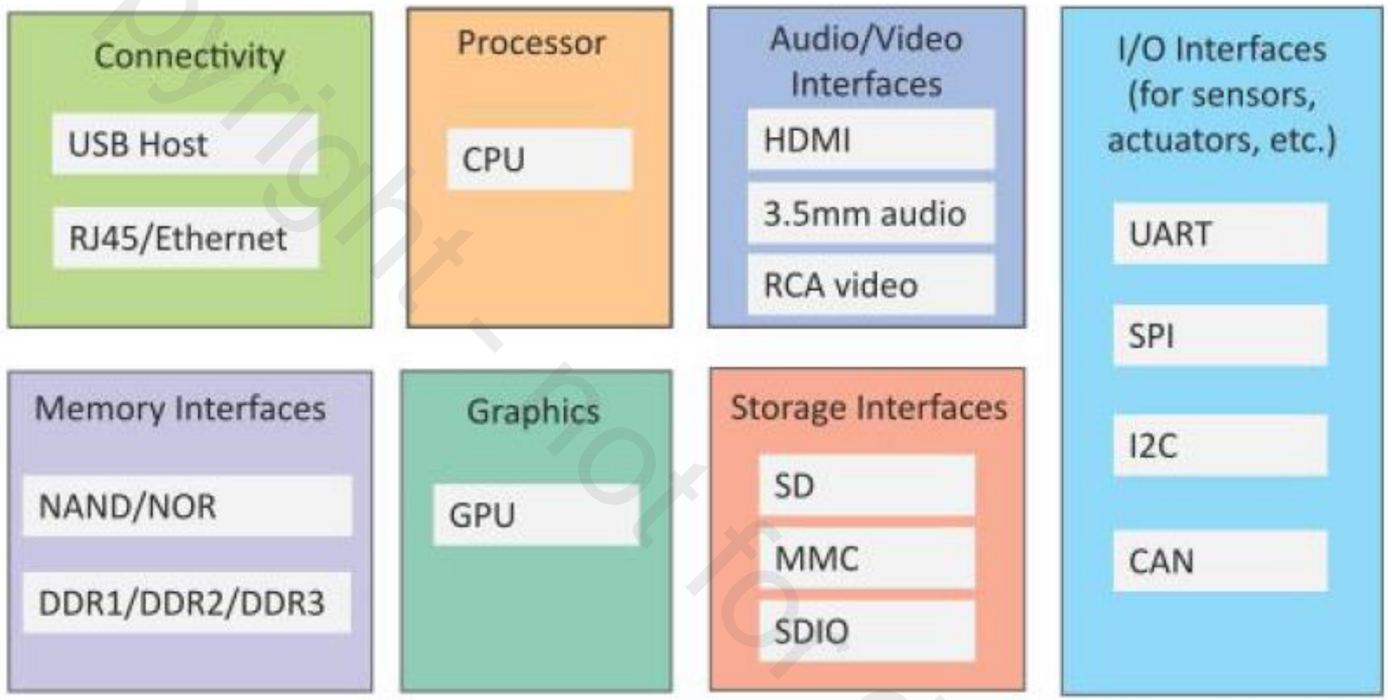
Acronyms

Acronym	Meaning	Acronym	Meaning
6LoWPAN	IPv6 over Low power Wireless Personal Area Network	HTTPS	Hypertext Transfer Protocol Secure
AMQP	Advanced Messaging Queuing Protocol	GSM	Global System for Mobile Communication
API	Application Programming Interface	CDMA	Code Division Multiple Access
LTE	Long Term Evolution	UMTS	Universal Mobile Telecommunications Service
CoAP	Constrained Application Protocol	NR	New Radio
DDS	Data Distribution Service	LR-WPAN	Low-rate Wireless Personal Area Network
SMTP	Simple Mail Transfer Protocol	XML	Extensible Markup Language

Acronyms

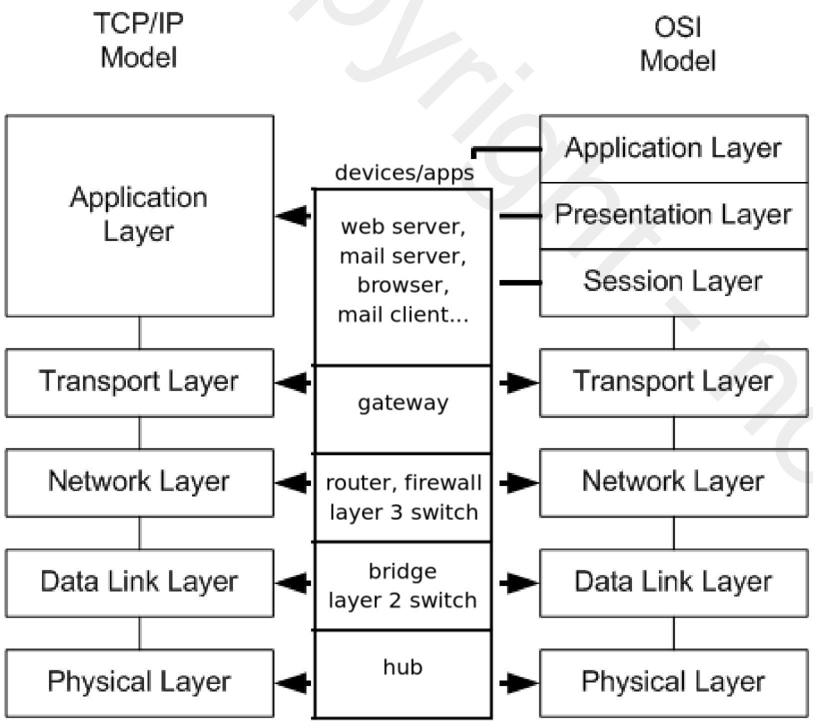
Acronym	Meaning	Acronym	Meaning
MMC	MultiMedia Card	UID	Unique Identifier
MQTT	Message Query Telemetry Transport	URI	Uniform Resource Identifier
NFC	Near Field Communication	WISP	Wireless Internet Service Provider
RFID	Radio-Frequency Identification	WLAN	Wireless Local Area Network
SDIO	Secure Digital Input Output	WPAN	Wireless Personal Area Network
TCP	Transmission Control Protocol	WWAN	Wireless Wide Area Network
UDP	User Datagram Protocol	XMPP	Extensible Messaging and Presence Protocol

IoT Device



- An IoT device may consist of several interfaces for connections to other devices, both wired and wireless
  - I/O interfaces for sensors
  - Interfaces for Internet connectivity
  - Memory and storage interfaces
  - Audio/video interfaces

Data Encapsulation (OSI Layer, TCP/IP Layer)



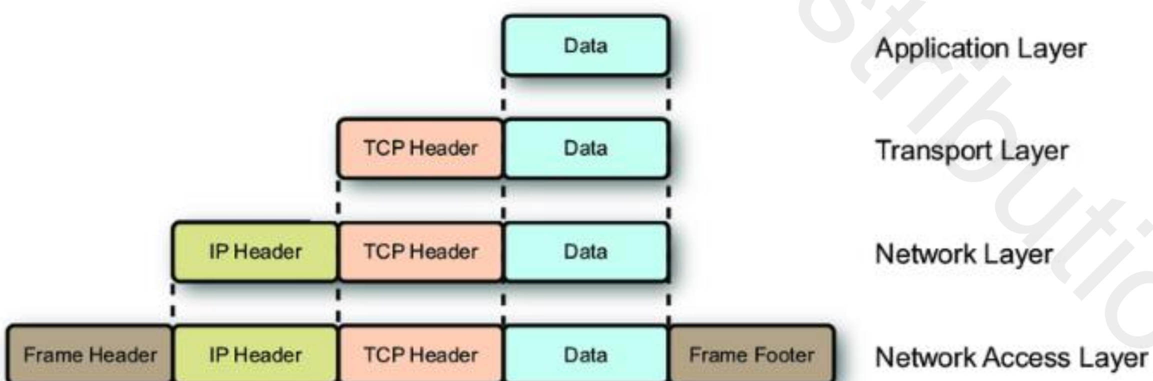
Presents data to the users, encoding and session control, data translation with protocols (e.g., HTTPs, FTP, DNS, DHCP)

Support end-to-end connection establishment of data segments and delivery with error control by TCP/UDP protocols

Logical addressing and routing of data packet from source to destination by identifying neighbors

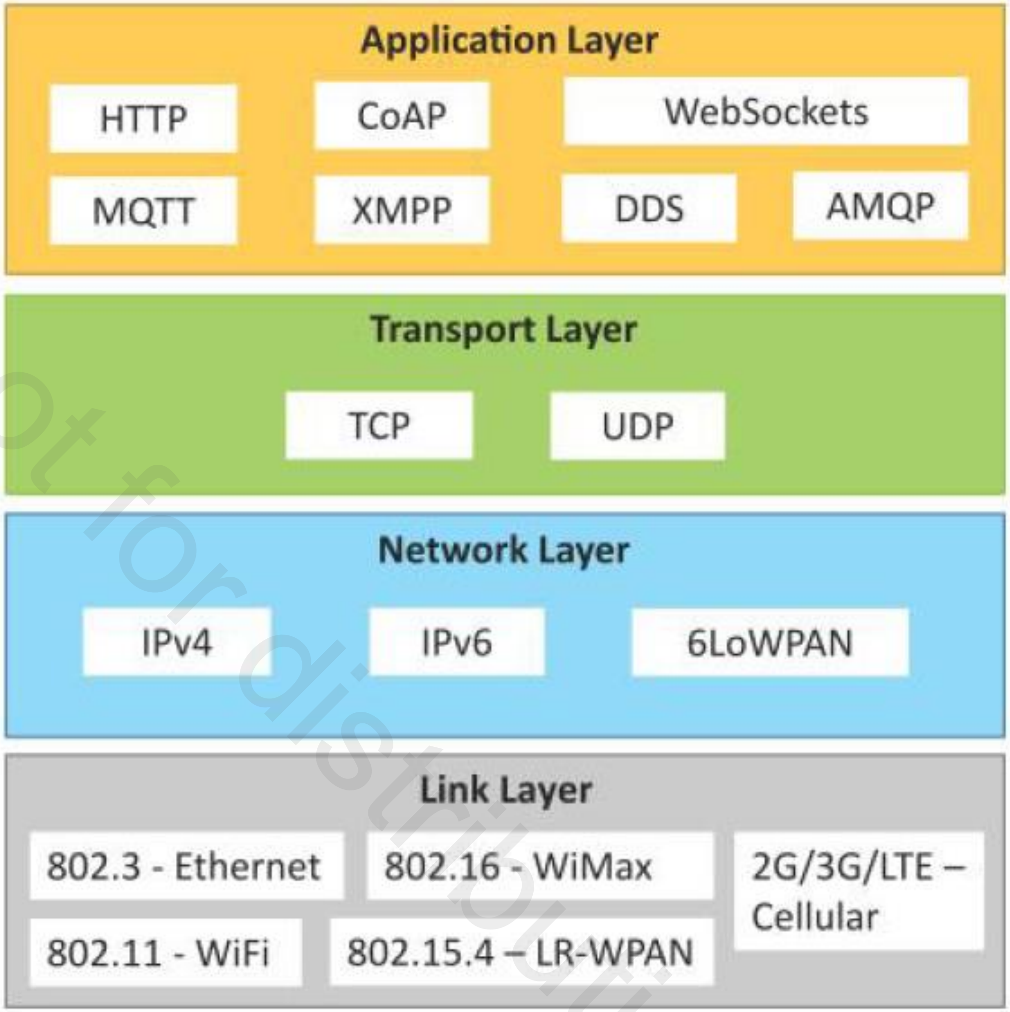
Combine raw data into frames, error recovery and retransmissions

Provide the physical interface for the data transmission



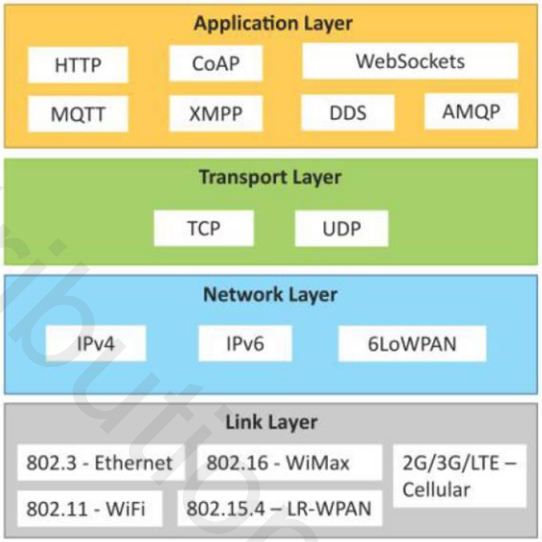
IoT Protocols

- Link Layer
  - 802.3 – Ethernet
  - 802.11 – Wi-Fi
  - 802.16 – Wi-Max
  - 802.15.4 – LR-WPAN
  - 2G/3G/4G/5G
- Network Layer
  - IPv4, IPv6
  - 6LoWPAN
- Transport Layer
  - TCP, UDP
- Application Layer
  - HTTP
  - CoAP
  - WebSocket
  - MQTT
  - XMPP
  - DDS
  - AMQP



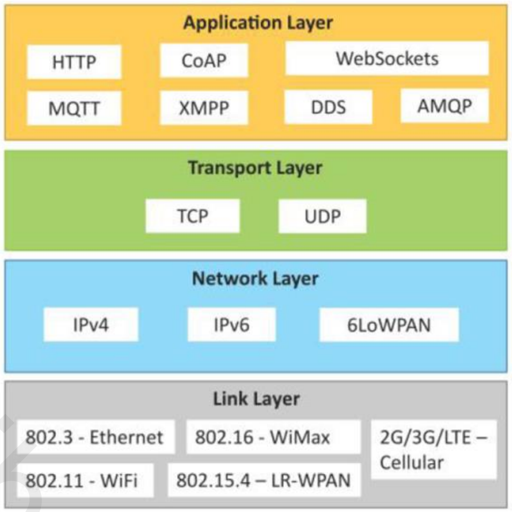
IoT Protocols – Link Layer

- Determines how the data is physically sent over the network's physical layer/medium
- Determines how the packets are coded and signaled by the hardware device over the medium
- **802.3** – Ethernet (10 Mb/s to 40 Gb/s)
  - 802.3 : 10BASE5 Ethernet (coaxial cable)
  - 802.3.i : 10BASE-T Ethernet (copper twisted-pair connections)
  - 802.3.j: 10BASE-T Ethernet (fiber optic connections)
  - 802.3ae: 10 Gbit/s Ethernet over fiber
- **802.11** – Wi-Fi (1 Mb/s to 6.75 Gb/s)
  - Standards: 802.11a/b/g/n/ac/ad
  - Operating frequency bands: 2.4 GHz, 5 GHz, 60 GHz
- **802.16** – Wi-Max (1.5 Mb/s to 1 Gb/s)



IoT Protocols – Link Layer

- **802.15.4** – LR-WPAN (low-rate wireless personal area network)
  - Data rates: 40 Kb/s to 250 Kb/s
  - Low-cost, low-speed communication for power constrained device
- **2G/3G/4G/5G** – Mobile Communication
  - Communication over cellular network
  - 2G: GSM and CDMA
  - 3G: UMTS, CDMA2000
  - 4G: LTE & NB-IoT
  - 5G: NR

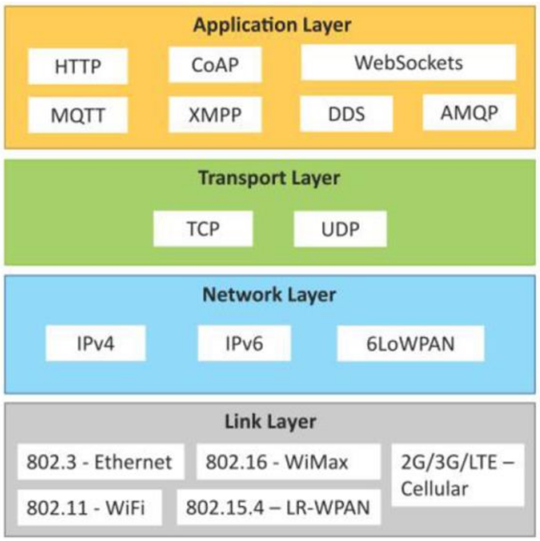


5G bands

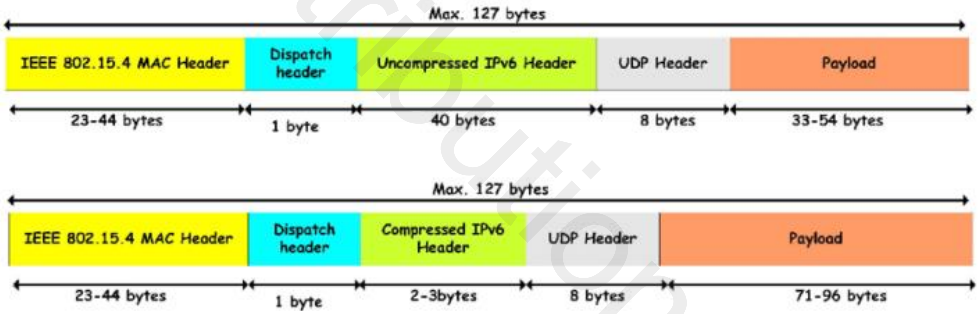
- **Low-bands**: 600, 800, 900 MHz (long range, 20% faster than LTE)
- **Mid-bands**: 2.5, 3.5, 3.7-4.2 GHz (mid range, 6x faster than LTE)
  - Airports and 5G (signal interference) – LINK 1
- **High-bands**: 24, 28 ,37, 39, 47 GHz (short range, 10x faster than LTE)
  - Need repeaters in short ranges – LINK 2
  - mmWave (~300 GHz): absorbed by plants, rain, cannot penetrate building, etc..

IoT Protocols – Network Layer

- Responsible for sending of IP datagrams from the source network to the destination network
- Performs host addressing and packet routing
- Datagrams contain the source and destination addresses which are used to route them from the source to destination across multiple networks



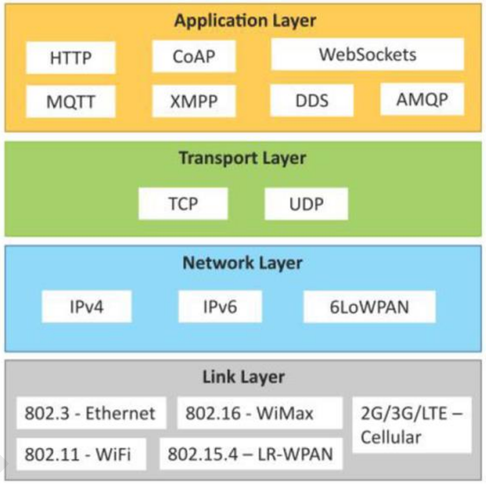
- **IPv4**: 32-bit address scheme (e.g., 192.168.0.1)
- **IPv6**: 128-bit address scheme (e.g., 2001:0077:AC10:FE01:0000:0000:0000:0000)
- **6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)**
  - Operating in 2.4 GHz, data rate of 250 Kb/s
  - Works with the 802.15.4 link layer protocol
  - Enables IPv6 datagrams over IEEE 802.15.4-based networks



6LoWPAN frames without and with IPv6 header compression.

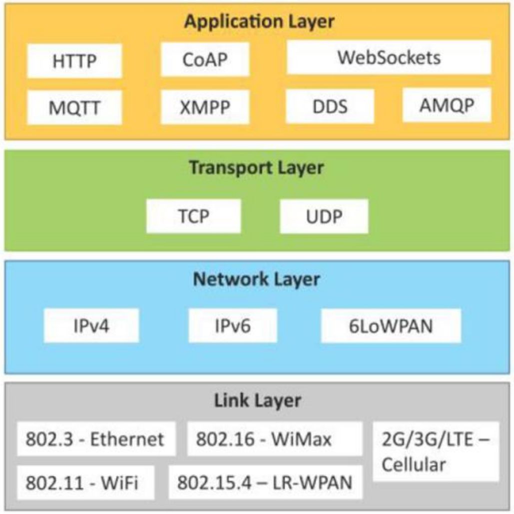
IoT Protocols – Transport Layer

- Provide end-to-end message transfer capability independent of the underlying network
- Provides functions such as error control, segmentation, flow control and congestion control
- **TCP (Transmission Control Protocol)**
  - Most widely used transport layer protocol in web browsers (along with HTTP, HTTPS application layer protocols), email programs (SMTP application layer protocols), file transfer (FTP)
  - Connection oriented and stateful protocol. Ensures reliable transmission of packets in-order
  - Provides error detection capability, lost packets are retransmitted
  - Flow control, congestion control
- **UDP (User Datagram Protocol)**
  - Connectionless protocol, useful for time-sensitive applications with very small data units
  - Transaction oriented and stateless protocol. Doesn't provide guaranteed delivery, ordering of messages and duplicate elimination
  - Higher levels of protocols can ensure reliable delivery



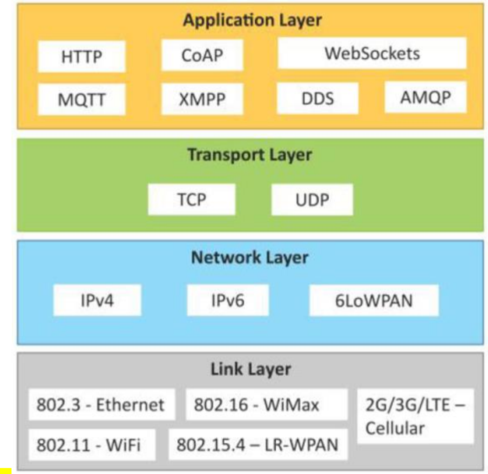
IoT Protocols – Application Layer

- Application layer protocol defines how the applications interface with the lower layer protocols to send the data over the network.
- Application data is encoded by the application layer protocol and encapsulated in the transport layer protocol, providing connection/transaction-oriented communication over the network
- **HTTP (Hypertext Transfer Protocol)**
    - Forms the foundation of the WWW (World Wide Web)
    - Includes commands such as GET, PUT, POST, DELETE, HEAD, TRACE, OPTIONS, etc. → RESTful (REpresentational State Transfer) API
    - Follows a request-response model where a client sends requests to a server using the HTTP commands
    - Stateless protocol, each HTTP request is independent of the other requests
    - An HTTP client can be a browser, an application
- **CoAP (Constrained Application Protocol)**
    - For Machine to Machine (M2M) applications, meant for constrained environments (low power/lossy network)
    - A Web transfer protocol, uses a request-response model, runs on top of UDP
    - Uses a client-server architecture (clients communicate with servers through connectionless datagrams)



IoT Protocols – Application Layer

- **WebSocket**
  - Allows full-duplex communication over a single socket connection for sending messages between client and server
  - Based on TCP, allows streams of messages to be sent back and forth while keeping TCP connection open
  - Client can be a browser, a mobile application, or an IoT device
- **MQTT (Message Queue Telemetry Transport)**
  - A light-weight messaging protocol based on the publish-subscribe model
  - Uses a client-server architecture where the client (IoT device) connects to the server (MQTT broker), and publishes messages to topics on the server
  - Brokers forwards the messages to the clients subscribed to topics.
  - Well suited for constrained environments with limited processing and memory resources, and low bandwidth network
- **XMPP (Extensible Messaging and Presence Protocol)**
  - For real-time communication and streaming XML data between network entities.
  - Instant Messaging, presence, data syndication, gaming, multi-party chat, voice/video calls
  - Decentralized protocol and uses a client-server/server-server architecture



Server advertises resource binding feature to client:

```
<stream:stream
xmlns='jabber:client'
xmlns:stream='http://etherx.jabber.org/
streams'
id='c2s_345'
from='example.com'
version='1.0'>
<stream:features>
<bind
xmlns='urn:ietf:params:xml:ns:xmpp-
bind'>
</stream:features>
```

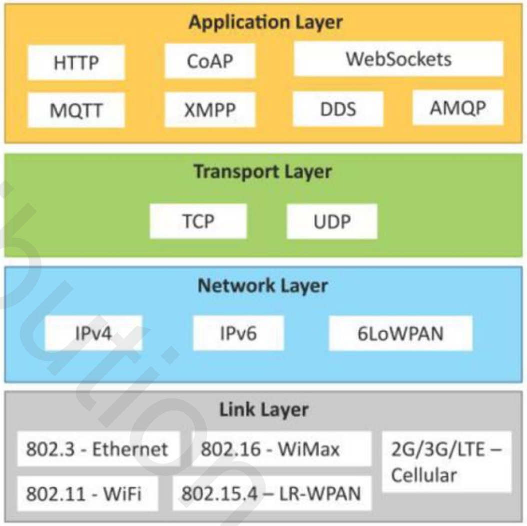
Client asks server to bind a resource:

```
<iq type='set' id='bind_1'>
<bind
xmlns='urn:ietf:params:xml:ns:xmpp-
bind'/>
</iq>
```

IoT Protocols – Application Layer

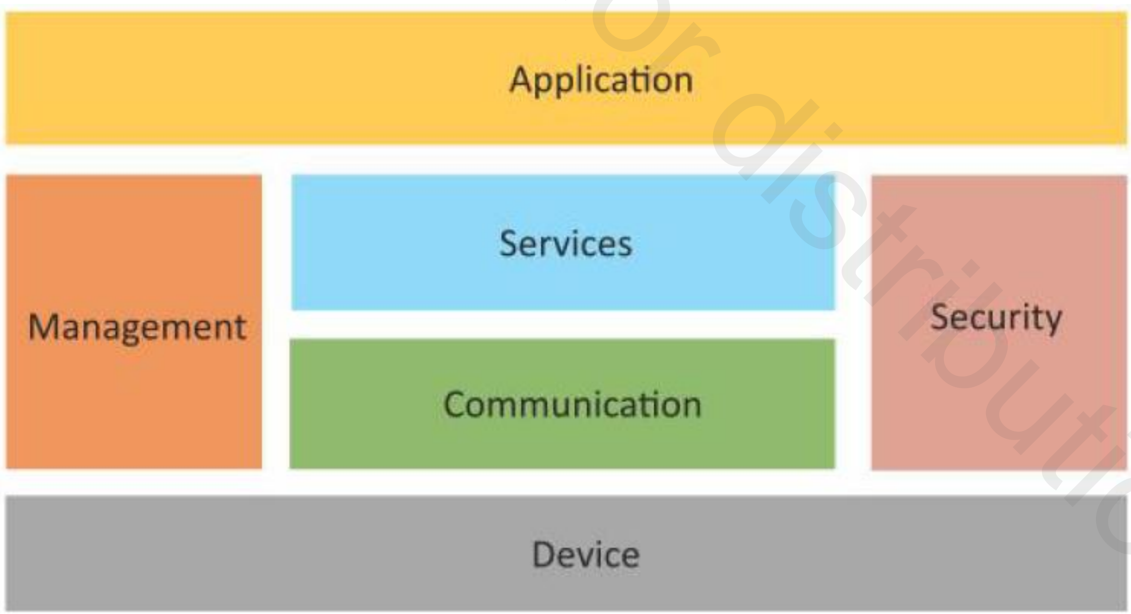
- **DDS (Data Distribution Service)**
  - A data-centric middleware standard for device-to-device or machine-to-machine communication
  - Uses a publish-subscribe model where publishers create topics to which subscribers can subscribe
  - Publisher is an object responsible for data distribution
  - Subscriber is responsible for receiving published data
  - Provides QoS (quality-of-service) protocol and configurable reliability
    - Defining device priority: durability, history, reliability, ownership deadline, resource limitation

- **AMQP (Advanced Message Queuing Protocol)**
  - Open application layer protocol for business messaging
  - Supports both Point-to-Point (P2P) and publisher/subscriber models, routing and queuing
  - AMQP brokers receive messages from publishers and route them over connections to consumers
  - Messages are either delivered by the broker to the consumers, or the consumers can pull the messages from the queues



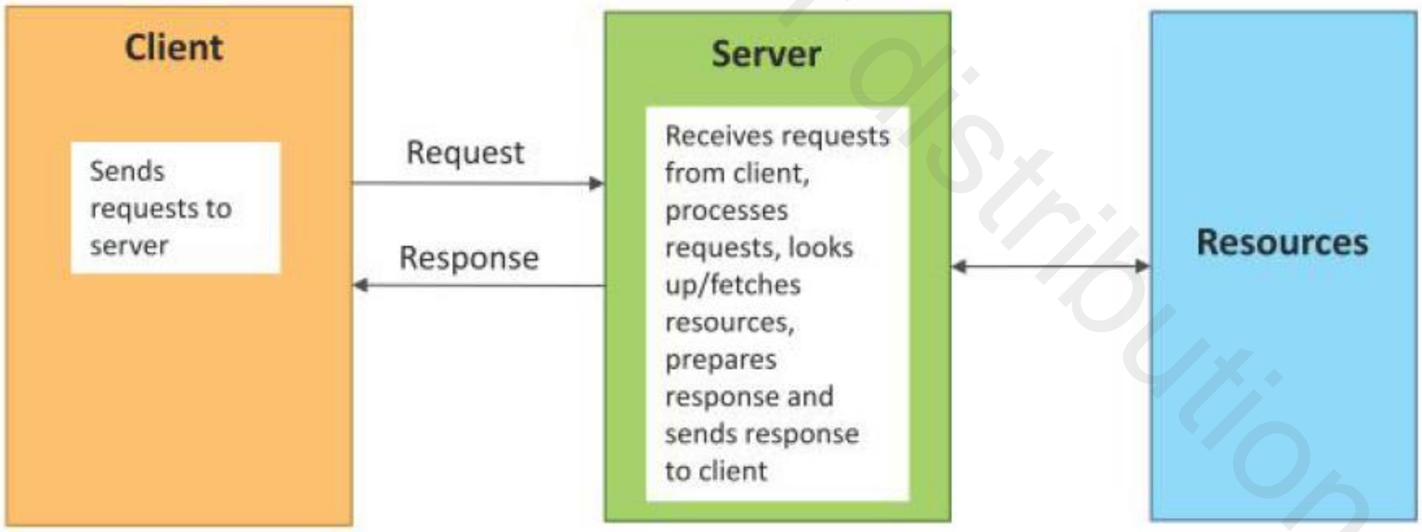
Functional Design of IoT Network

- Functional design of an IoT network refers to an abstract representation of the entities and processes without going into the low-level specifics of the implementation.
- An IoT system comprises of a number of **functional blocks** that provide the system the capabilities for identification, sensing, actuation, communication and management



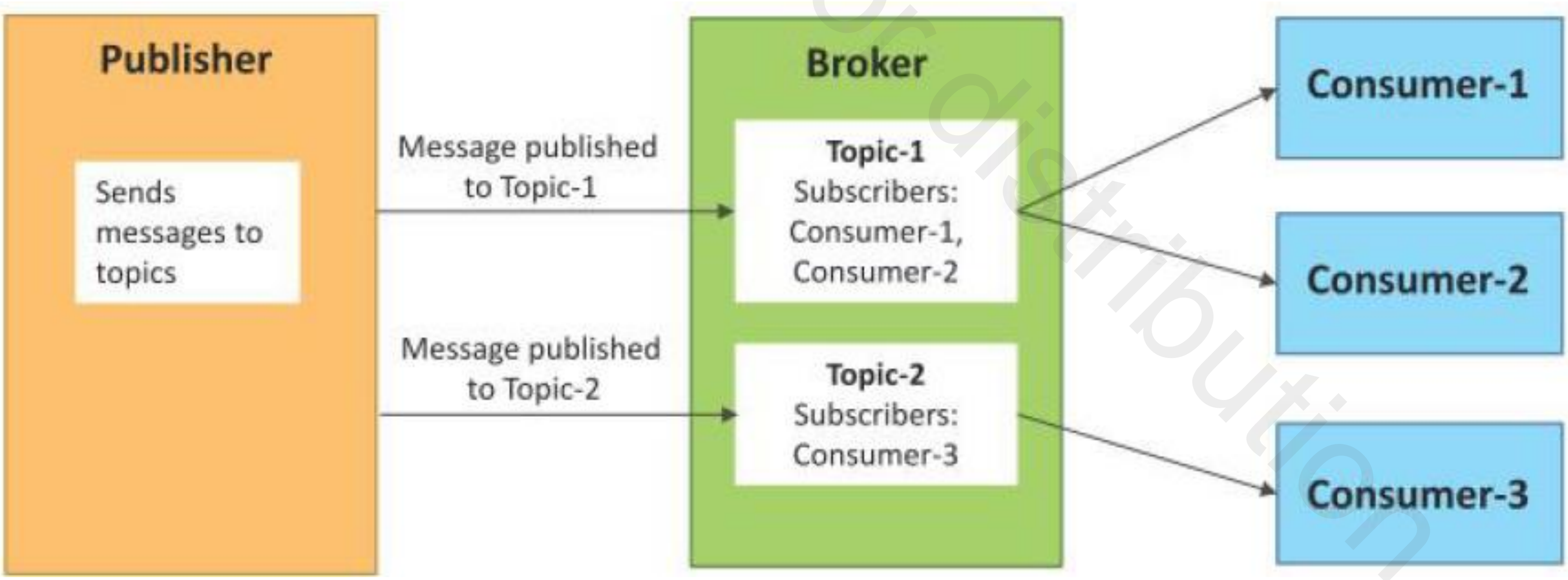
Request-Response Communication Model (HTTP, CoAP)

- Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests.
- When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.



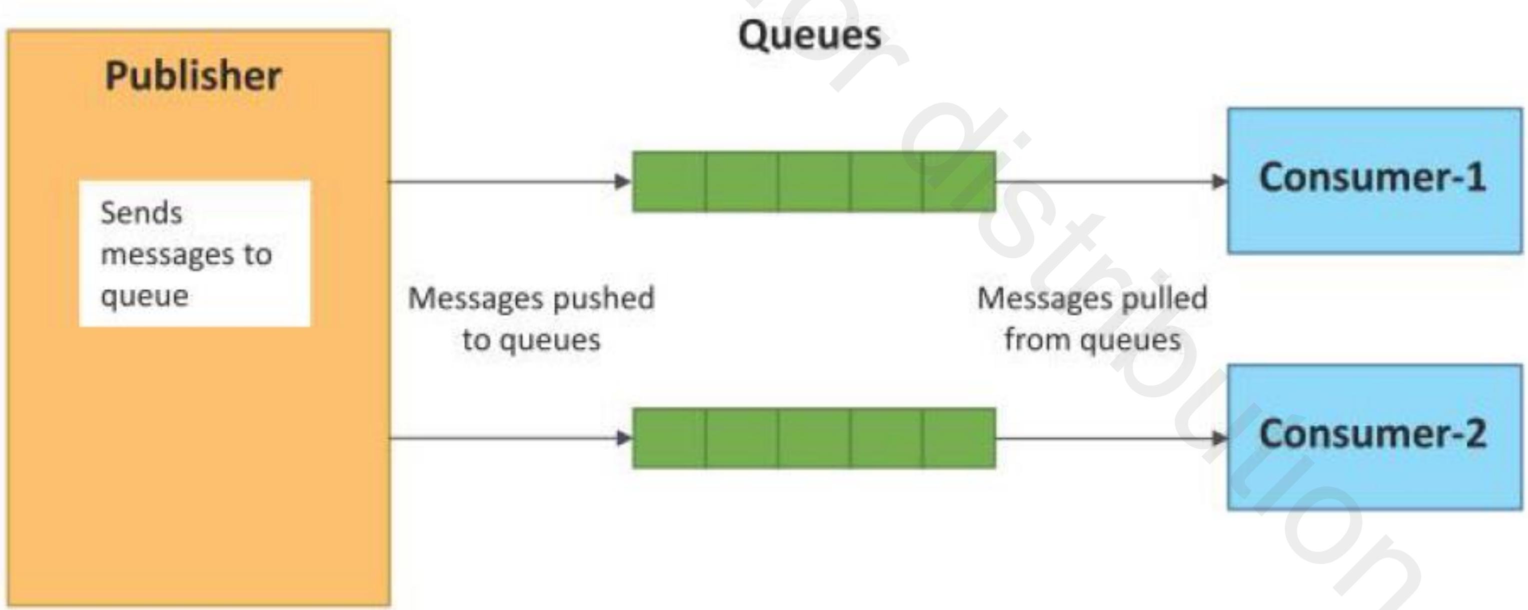
Publish-Subscribe Communication Model (MQTT, BLE, DDS, AMQP)

- Publish-Subscribe is a communication model that involves publishers, brokers and consumers
- Publishers are the source of data. Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers.
- Consumers subscribe to the topics which are managed by the broker.
- When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.



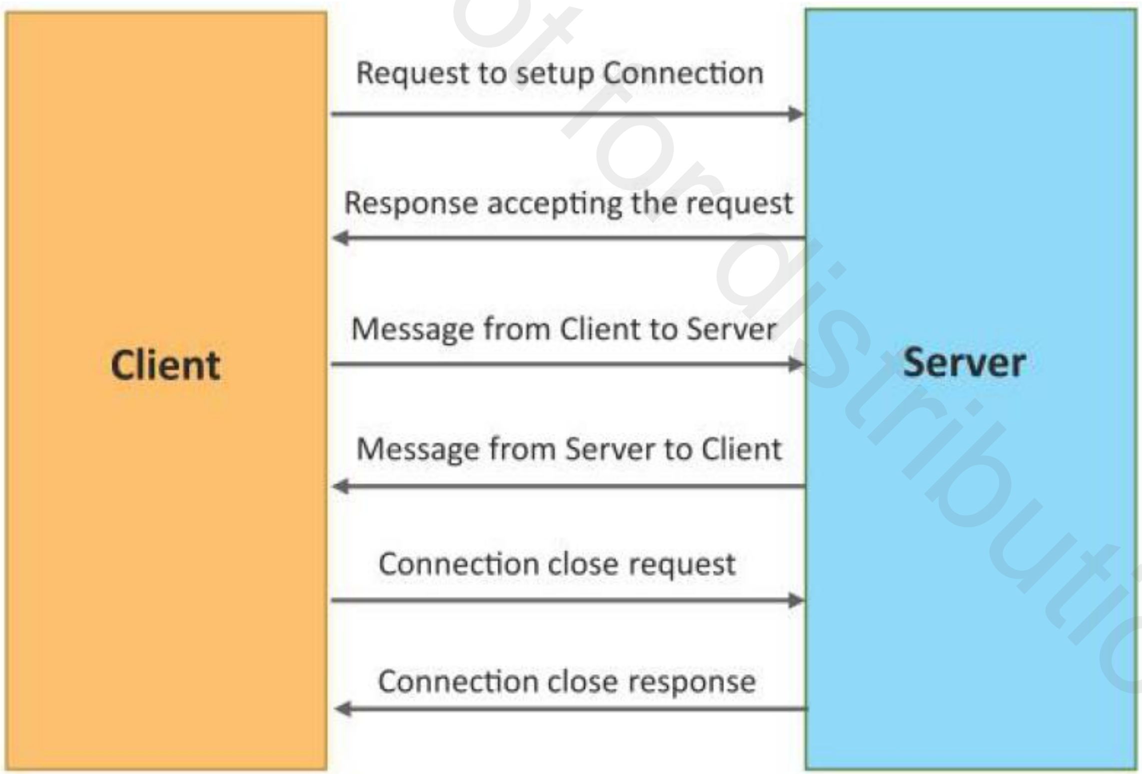
Push-Pull Communication Model

- Push-Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues. Producers do not need to be aware of the consumers.
- Queues help in decoupling the messaging between the producers and consumers.
- Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the produces push data and the rate at which the consumers pull data

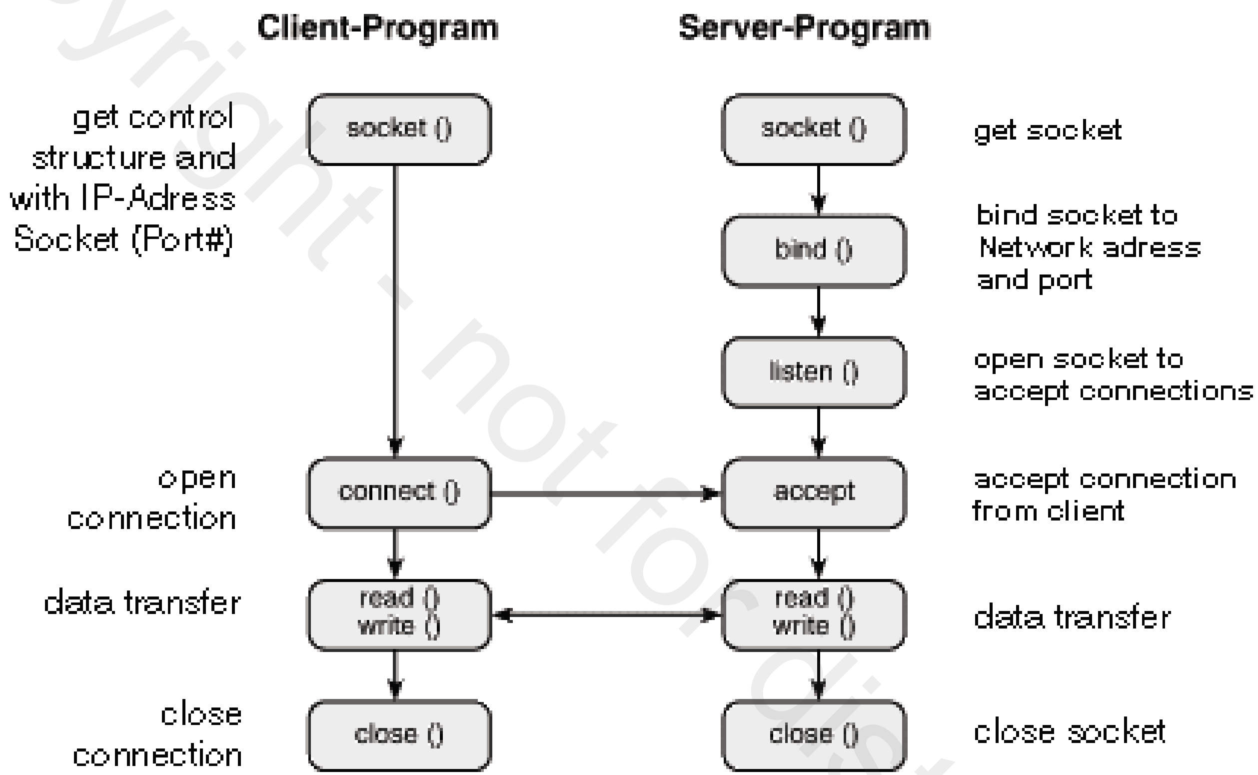


Exclusive Pair Communication Model (WebSocket)

- Exclusive Pair is a bi-directional, fully duplex communication model that uses a persistent connection between the client and server.
- Once the connection is setup, it remains open until the client sends a request to close the connection.
- Client and server can send messages to each other after connection setup



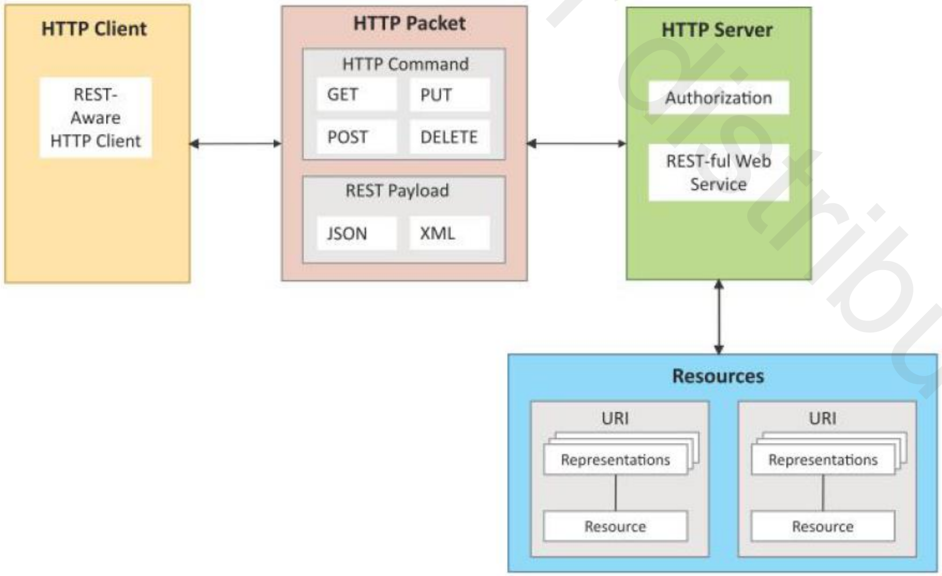
Client-Server Socket Programming



- Applies to Lab 2 Experiment, connecting Raspberry Pi to your computer
- Does not need to match programming language, but follow above procedure
  - Python, C++, C#, JAVA, Visual Basic, etc. will have functions/libraries

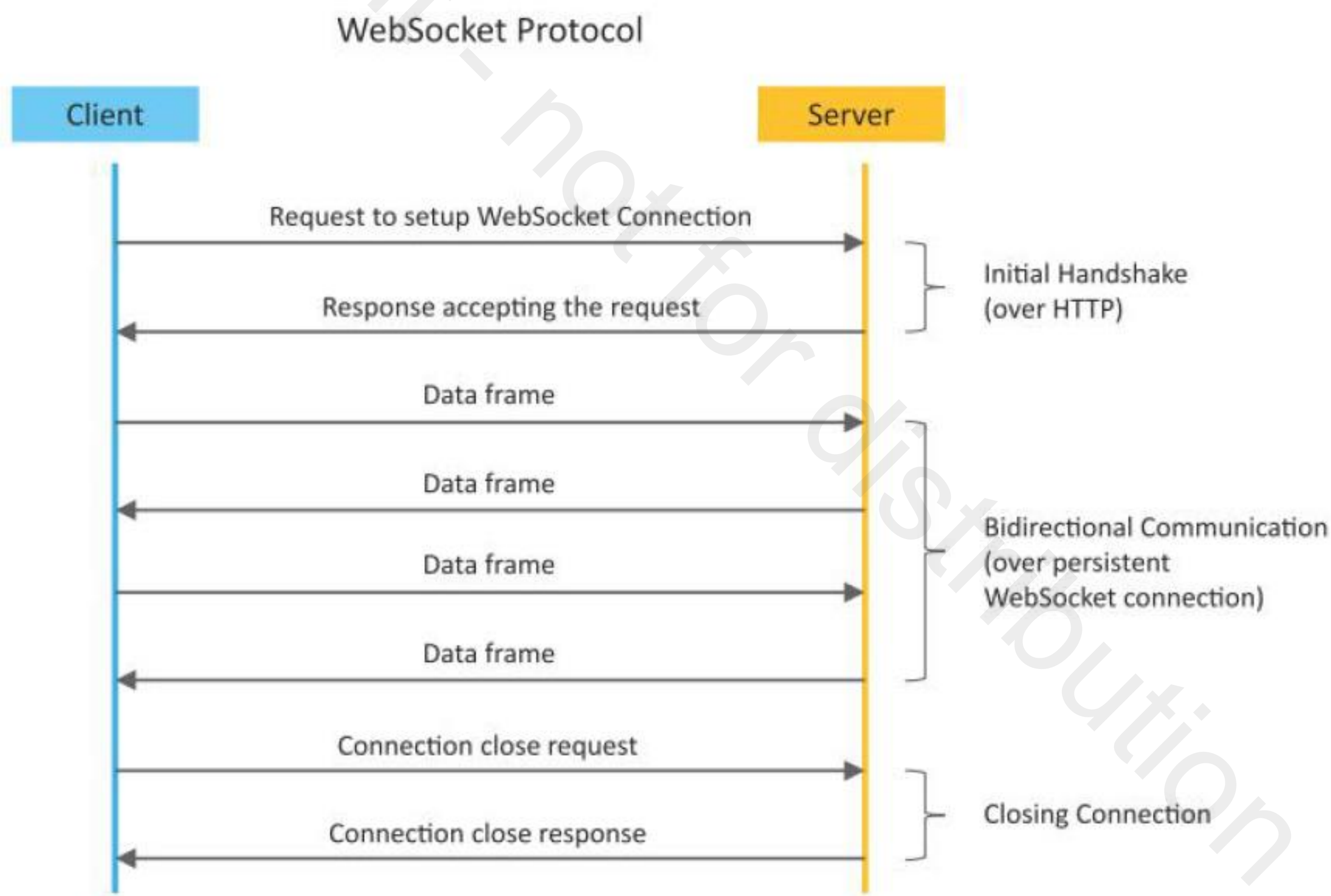
REST-based Communication APIs

- Representational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred.
- REST APIs follow the request-response communication model.
- The REST architectural constraints apply to the components, connectors, and data elements, within a distributed hypermedia system.
- **Let's use HTTP for SIMPLICITY**



WebSocket-based Communication APIs

- WebSocket APIs allow bi-directional, full duplex communication between clients and servers.
- WebSocket APIs follow the exclusive pair communication



Acronyms

Acronym	Meaning	Acronym	Meaning
6LoWPAN	IPv6 over Low power Wireless Personal Area Network	HTTPS	Hypertext Transfer Protocol Secure
AMQP	Advanced Messaging Queuing Protocol	GSM	Global System for Mobile Communication
API	Application Programming Interface	CDMA	Code Division Multiple Access
LTE	Long Term Evolution	UMTS	Universal Mobile Telecommunications Service
CoAP	Constrained Application Protocol	NR	New Radio
DDS	Data Distribution Service	LR-WPAN	Low-rate Wireless Personal Area Network
SMTP	Simple Mail Transfer Protocol	XML	Extensible Markup Language

Acronyms

Acronym	Meaning	Acronym	Meaning
MMC	MultiMedia Card	UID	Unique Identifier
MQTT	Message Query Telemetry Transport	URI	Uniform Resource Identifier
NFC	Near Field Communication	WISP	Wireless Internet Service Provider
RFID	Radio-Frequency Identification	WLAN	Wireless Local Area Network
SDIO	Secure Digital Input Output	WPAN	Wireless Personal Area Network
TCP	Transmission Control Protocol	WWAN	Wireless Wide Area Network
UDP	User Datagram Protocol	XMPP	Extensible Messaging and Presence Protocol