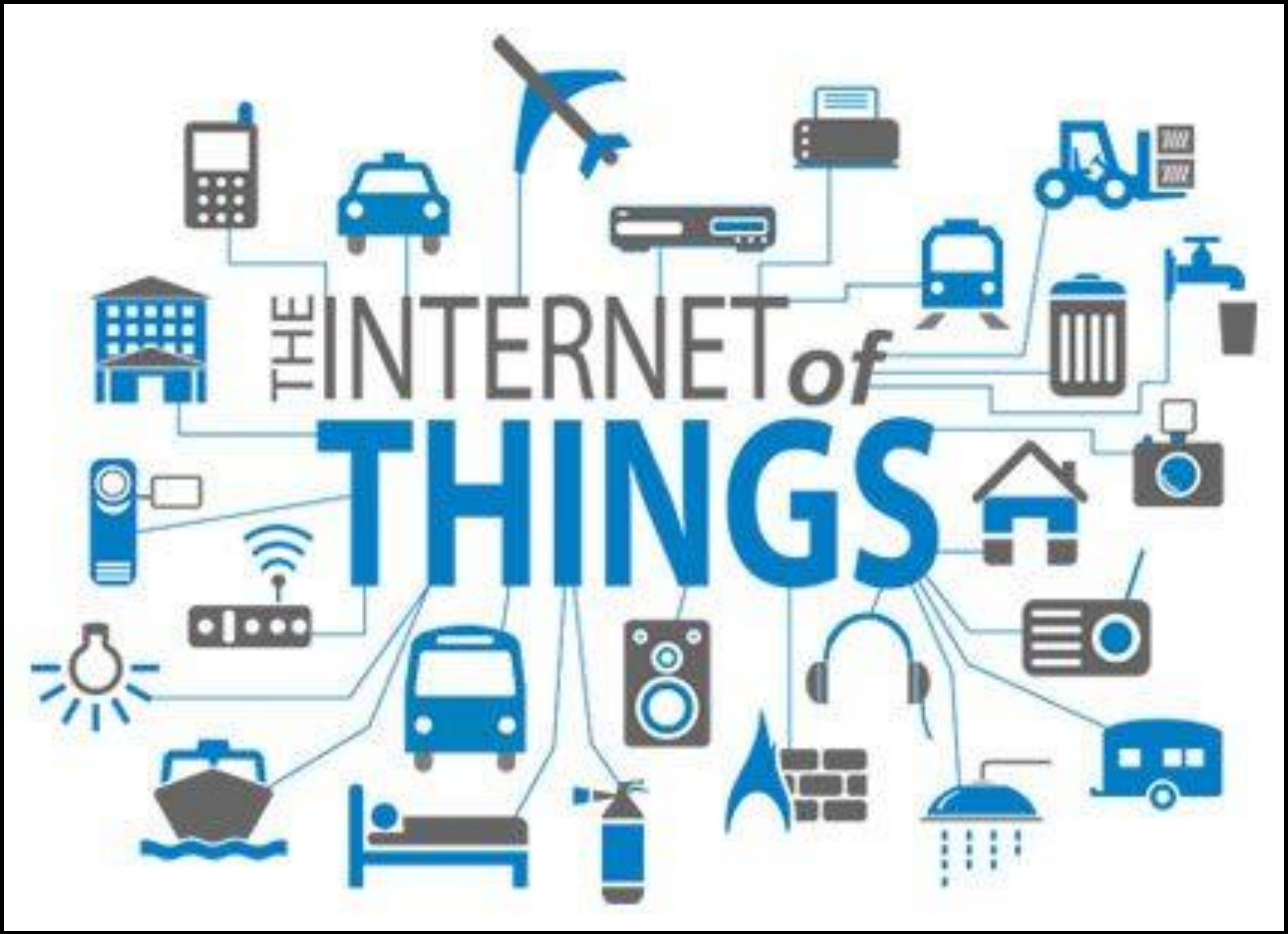


Internet of Things (IoT)

What is IoT?

Definition: The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.

"**Things**," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist fire-fighters in search and rescue operations.

These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.

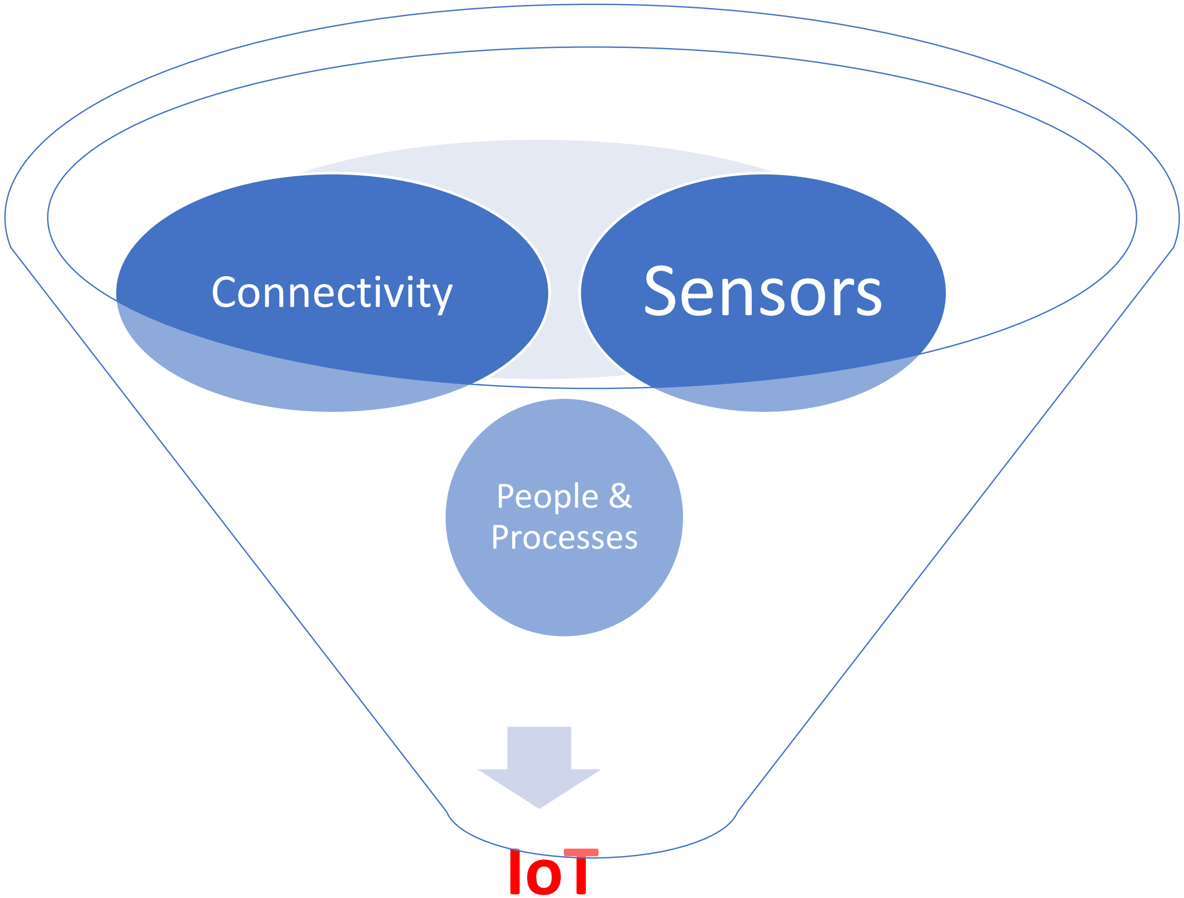
History of IoT

The concept of the Internet of Things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications.

Radio-frequency identification (RFID) was seen as a prerequisite for the IoT at that point. If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, **the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes, bluetooth, and digital watermarking.**

Components of IoT

- Sensors
- Connectivity
- People and Processes



How IoT Works?

Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

- ***Communication and cooperation***
- ***Addressability***
- ***Identification***
- ***Sensing***
- ***Actuation***
- ***Embedded information processing***
- ***Localization***
- ***User interfaces***

How IoT Works? Example

RFID

To identify and track the data of things

Sensor

To collect and process the data to detect the changes in the physical status of things

Smart Tech

To enhance the power of the network by devolving processing capabilities to different part of the network.

Nano Tech

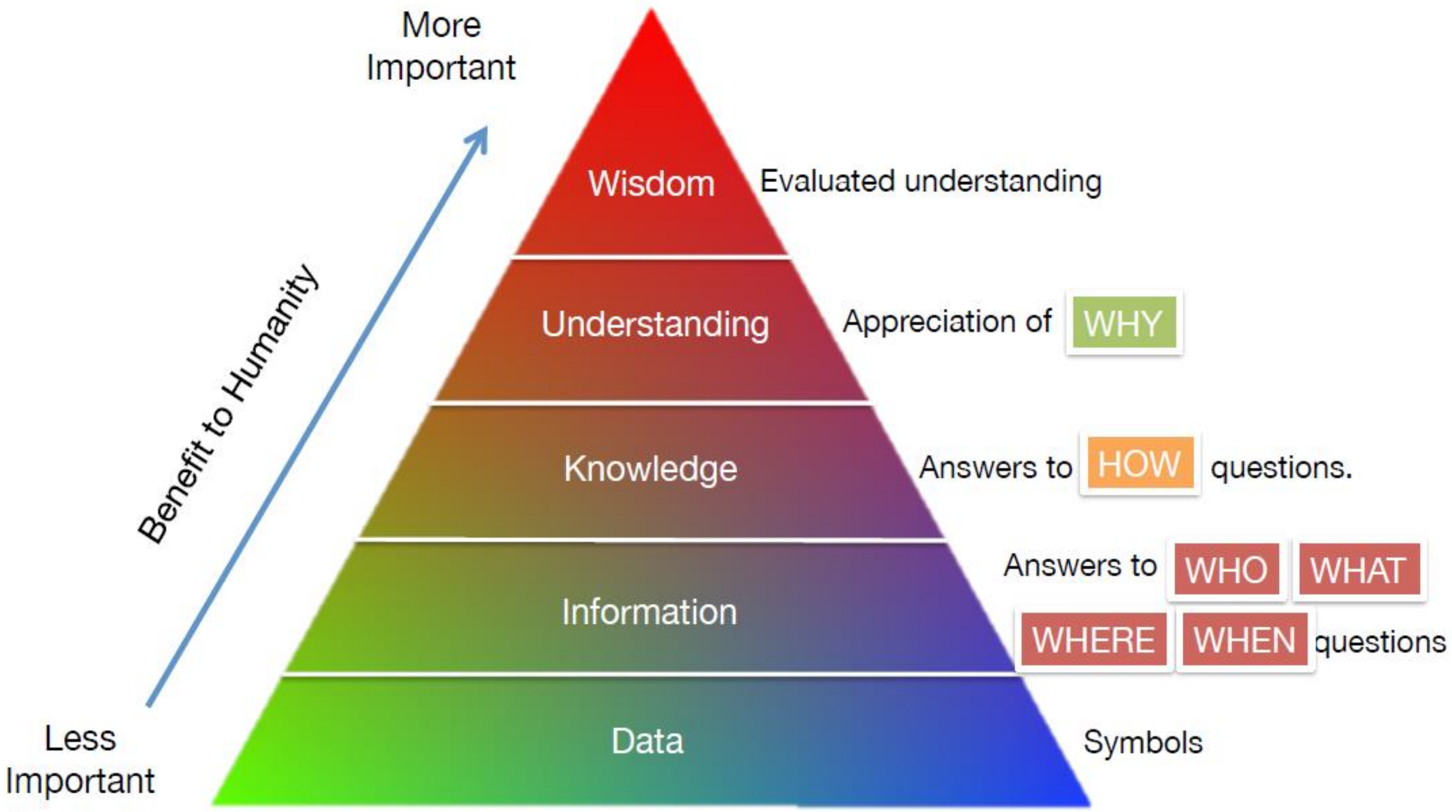
To make the smaller and smaller things have the ability to connect and interact.

The Structure of IoT

The IoT can be viewed as a gigantic network consisting of networks of devices and computers connected through a series of intermediate technologies where numerous technologies like RFIDs, wireless connections may act as enablers of this connectivity.

- ***Tagging Things :*** Real-time item traceability and addressability by ***RFID***s.
- ***Feeling Things : Sensors*** act as primary devices to collect data from the environment.
- ***Shrinking Things :*** *M*iniaturization and ***Nanotechnology*** has provoked the ability of smaller things to interact and connect within the "things" or "smart devices."
- ***Thinking Things : Embedded intelligence*** in devices through sensors has formed the network connection to the Internet. It can make the "things" realizing the intelligent control.

Knowledge Management –
Turning Data into Wisdom



The more data that is created, the better understanding and wisdom people can obtain.

Applications of IoT

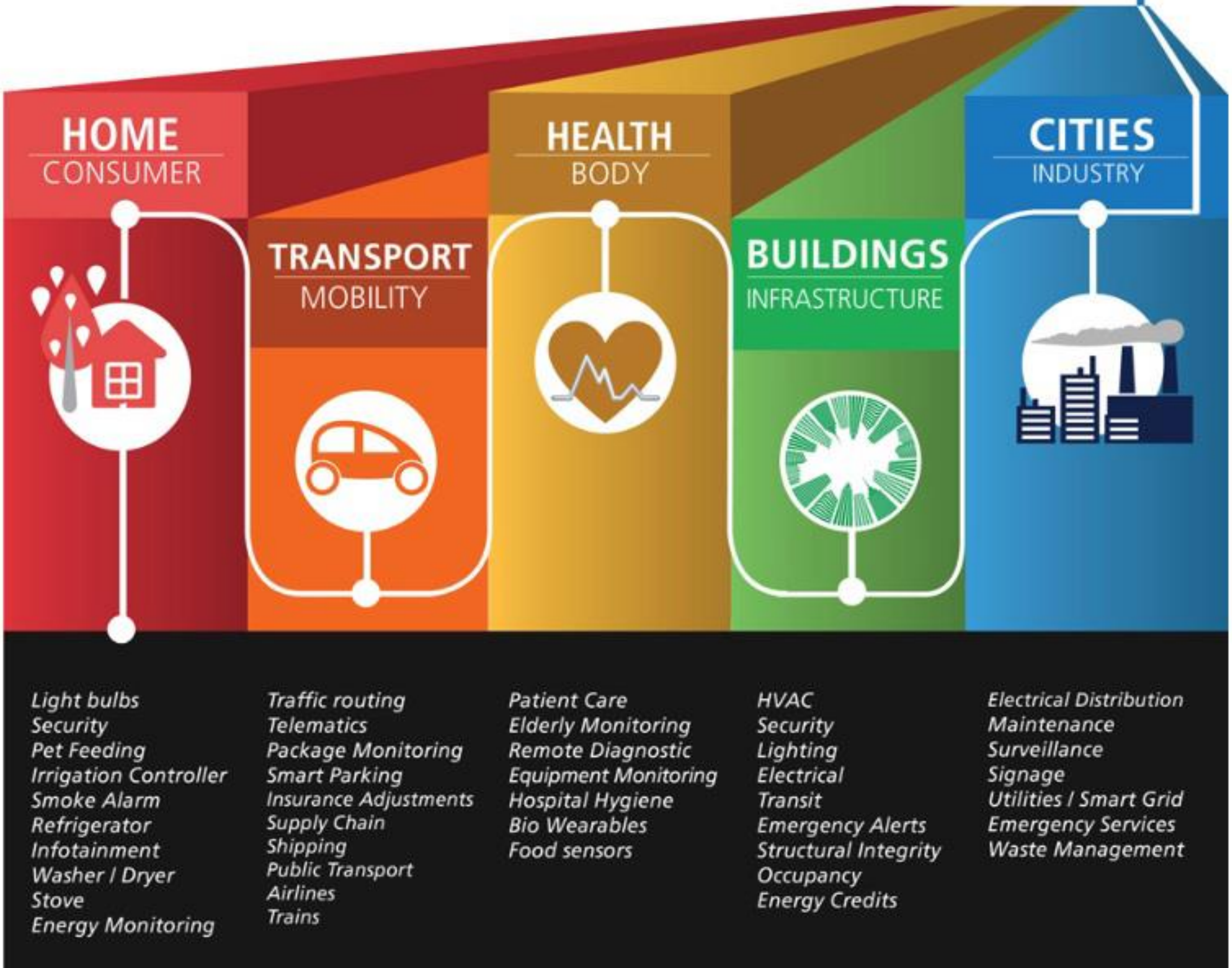
"The Ultimate Goal of IOT is to Automate Human Life."

Few Other Applications of IoT

- ✓ Building and Home automation
- ✓ Manufacturing
- ✓ Medical and Healthcare systems
- ✓ Media
- ✓ Environmental monitoring
- ✓ Infrastructure management
- ✓ Energy management
- ✓ Transportation
- ✓ Better quality of life for elderly
- ✓ … … …

You name it, and you will have it in IoT!

TO DIVERSE APPLICATIONS



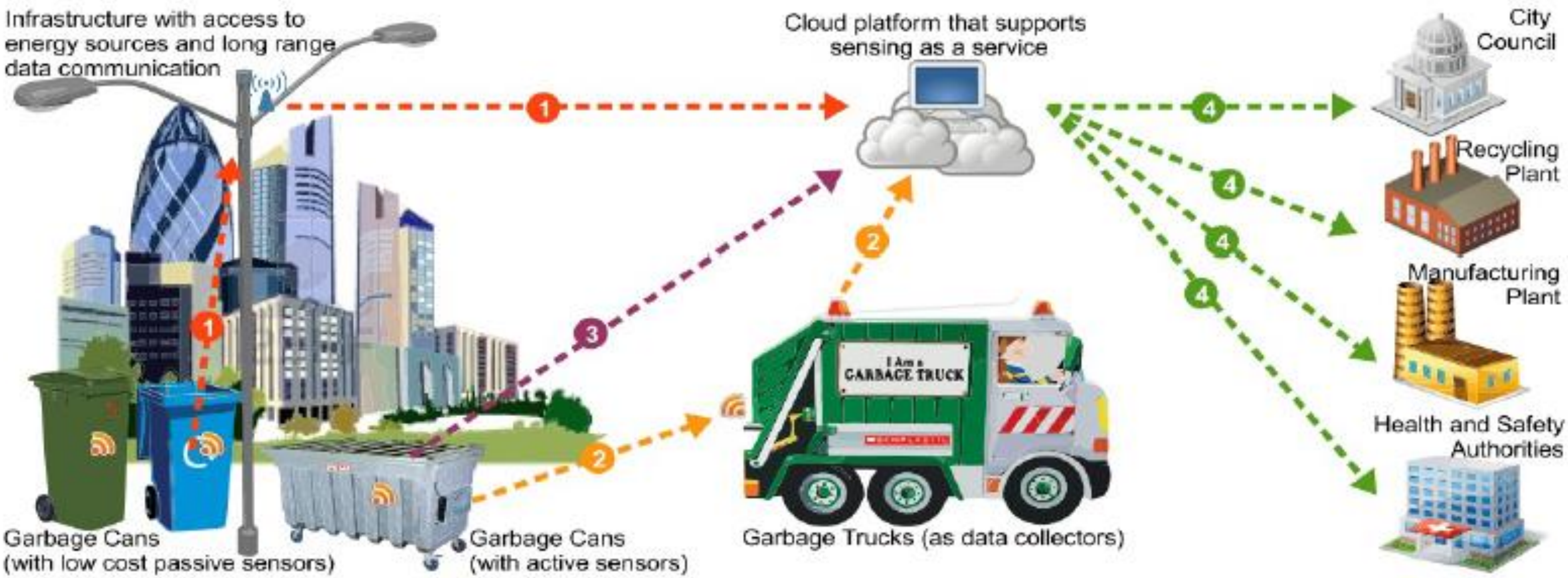
Smart Parking

Create **USD 41Billion** by providing visibility into the availability of parking spaces across the city.

Residents can identify and reserve the closest available space, traffic wardens can identify non-compliant usage, and municipalities can introduce demand-based pricing.

[Source: http://www.telecomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/]

Efficient Waste Management in Smart Cities Supported by the Sensing-as-a-Service



[Source: "Sensing as a Service Model for Smart Cities Supported by Internet of Things", Charith Perera et. al., Transactions on Emerging Telecommunications Technology, 2014]

Sensors in even the holy cow!

In the world of IoT, even the cows will be connected and monitored. Sensors are implanted in the ears of cattle. This allows farmers to monitor cows' health and track their movements, ensuring a healthier, more plentiful supply of milk and meat for people to consume. On average, each cow generates about 200 MB of information per year.

IOT Application Scenario - Shopping

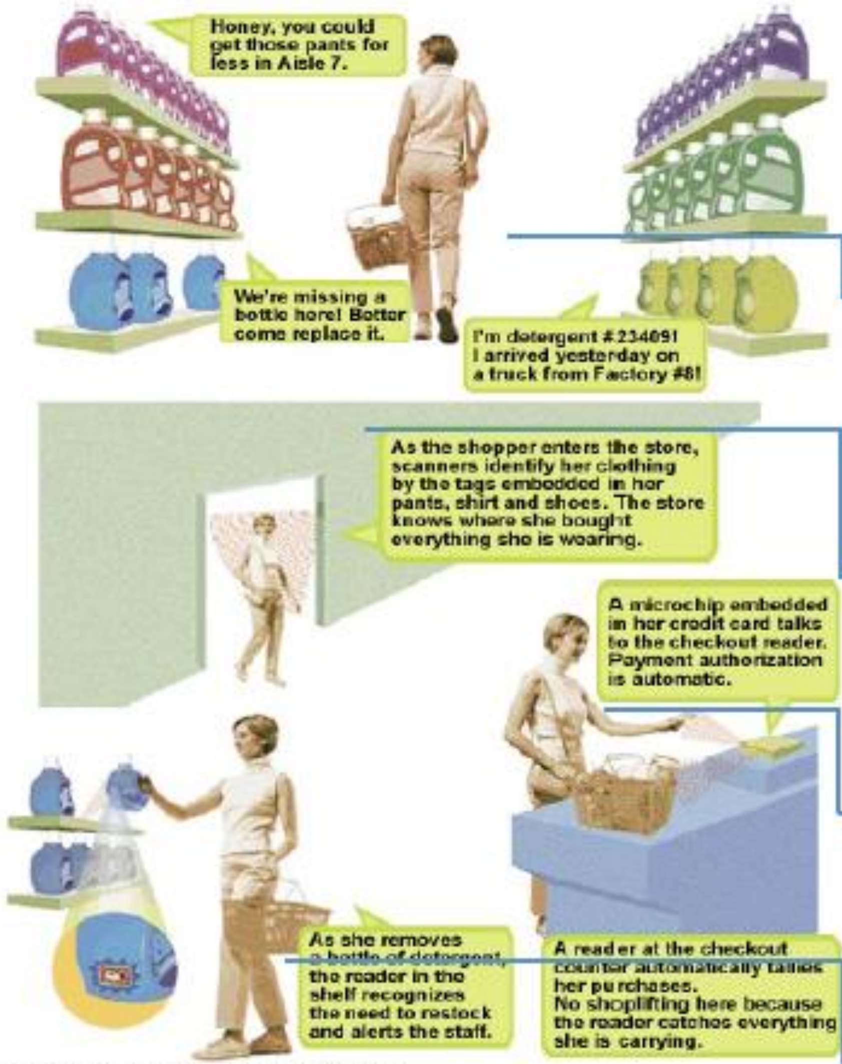


Illustration by Lisa Knouse Braiman for Forbes

(2) When shopping in the market, the goods will introduce themselves.

(1) When entering the doors, scanners will identify the tags on her clothing.

(4) When paying for the goods, the microchip of the credit card will communicate with checkout reader.

(3) When moving the goods, the reader will tell the staff to put a new one.

Thought Controlled Computing

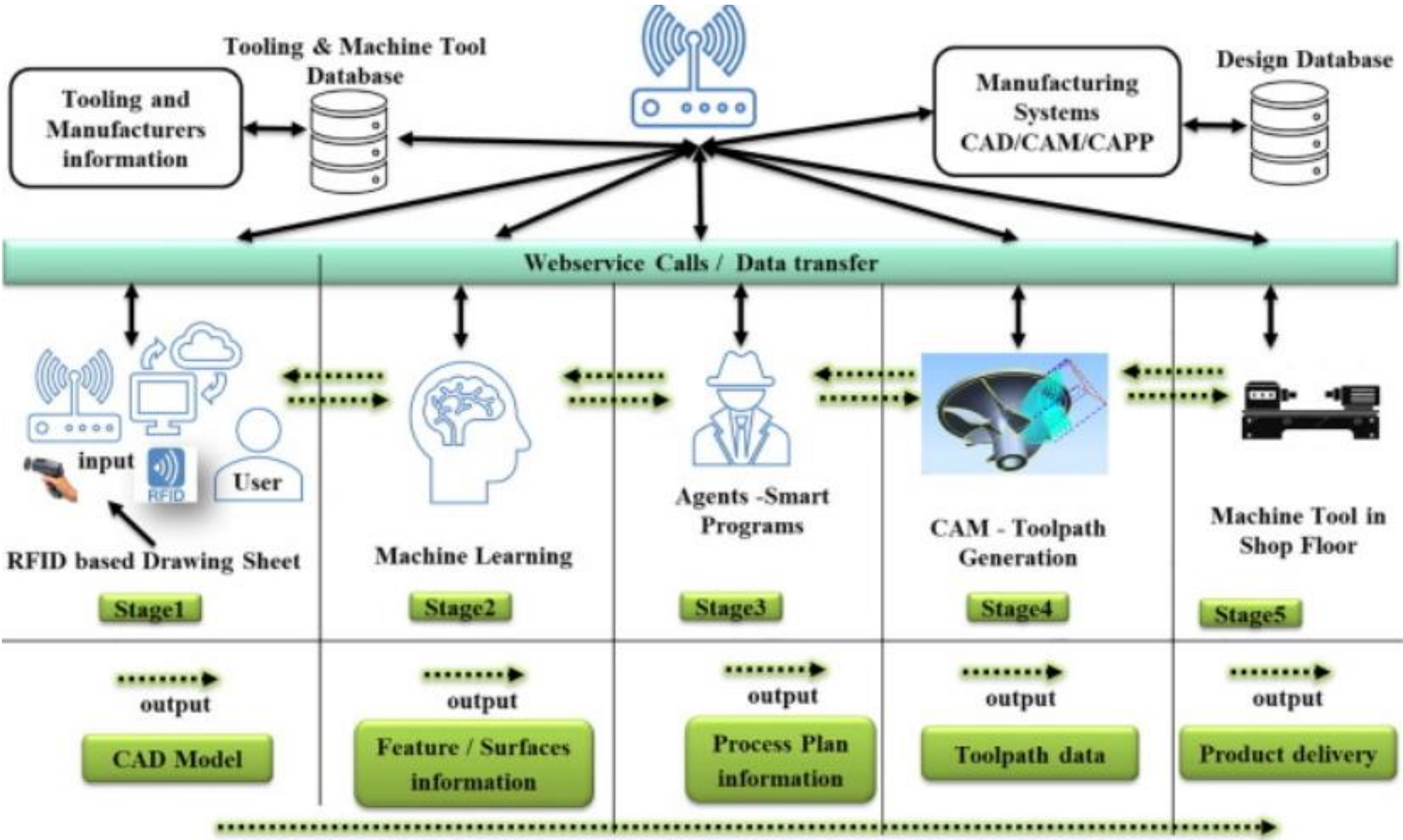
The flagship product, MindWave, is a headset that can log into your computer using just your thoughts. Researchers recently used the EEG headset to develop a toy car that can be driven forward with thought.

NeuroSky's smart sensors can also track your heart rate and other bodily metrics and can be embedded in the next generation of wearable devices.

"We make it possible for millions of consumers to capture and quantify critical health and wellness data," Yang (CEO of Softbank) said. Softbank is the funder.

[Source: http://venturebeat.com/2013/11/04/next-step-for-wearables-neurosky-brings-its-smart-sensors-to-health-fitness/]

Industry 4.0 and IoT Together



CHARACTERSTICS OF IoT

- **Dynamic & Self-Adapting:-** IoT devices and systems may have the capability to dynamic adapt with the changing contexts and take actions based on their operating conditions, user's context, or sensed environment.
- **Self-Configuring:-** IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality.
- **Interoperable Communication Protocols:-** IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.

CHARACTERSTICS OF IoT (Contd.)

- **Unique Identity:-** Each IoT device has a unique identity and a unique identifier. IoT device interfaces allow user to query the device, monitor their status, and control them remotely.
- **Integrated into Information Network:-** IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

TECHNOLOGICAL CHALLENGES OF IoT

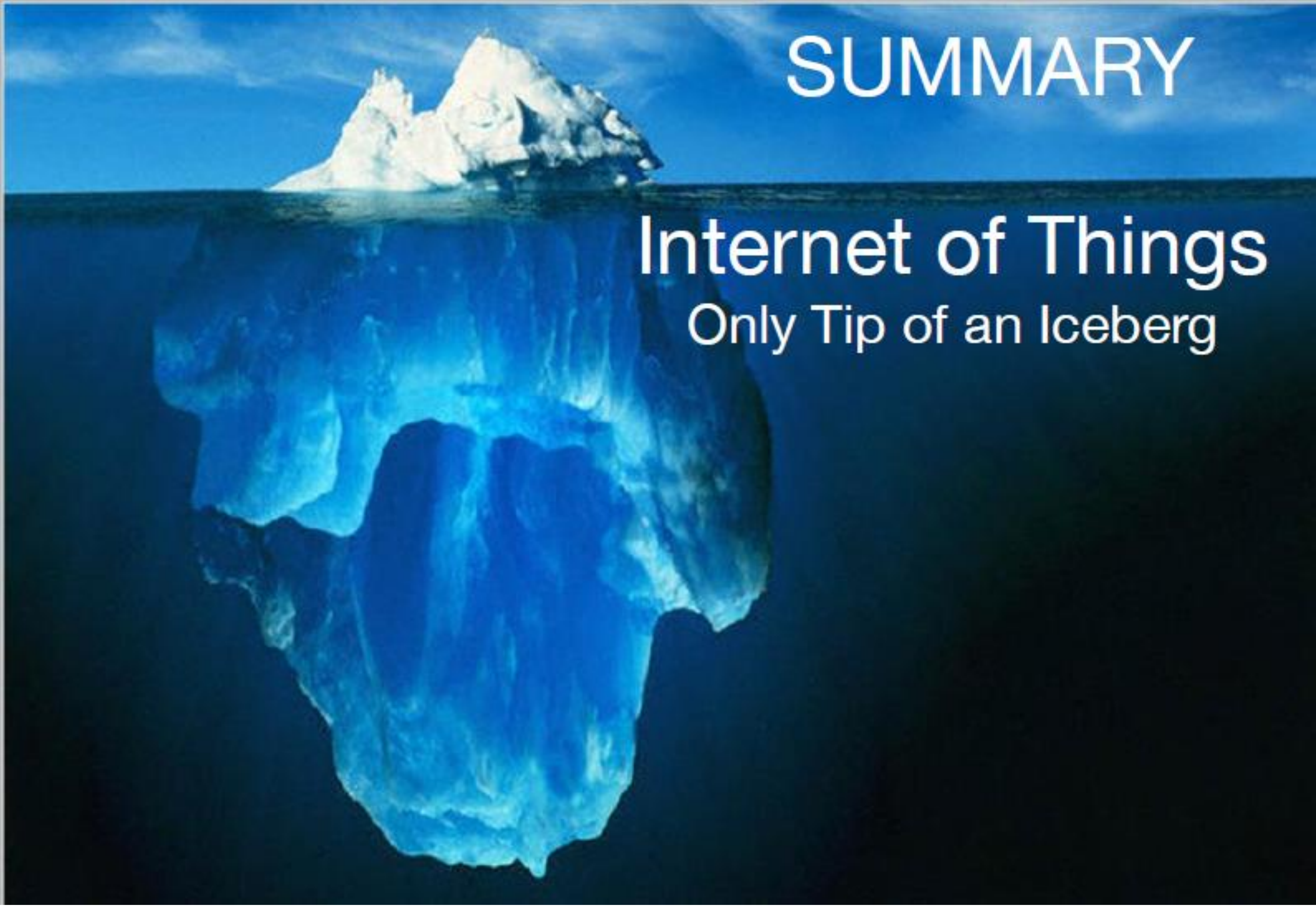
At present IoT is faced with many challenges, such as:

- Scalability
- Technological Standardization
- Inter operability
- Discovery
- Software complexity
- Data volumes and interpretation
- Power Supply
- Interaction and short range communication
- Wireless communication
- Fault tolerance

Criticisms and Controversies of IoT

Scholars and social observers and pessimists have doubts about the promises of the ubiquitous computing revolution, in the areas as:

- Privacy
- Security
- Autonomy and Control
- Social control
- Design
- Environmental impact
- Influences human moral decision-making

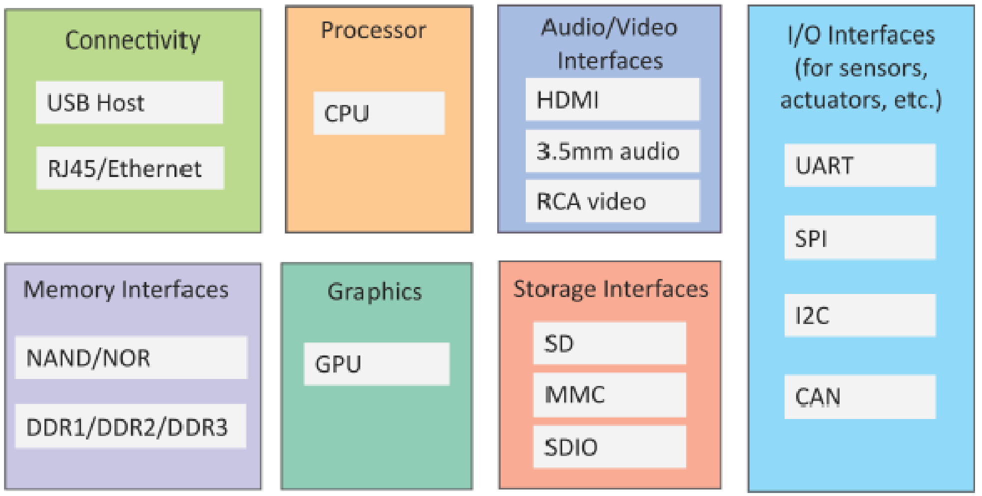

SUMMARY
Internet of Things
Only Tip of an Iceberg

Module-1

Generic Block Diagram of an IoT Device

Generic Block Diagram of an 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



Notations:

- Serial Peripheral Interface (SPI)
- I^{2}C (Inter-Integrated Circuit)
- Controller Area Network (CAN)
- Universal Asynchronous Receiver/Transmitter (UART)
- Secure Digital (SD)
- Multi Media Card (MMC)
- Secure Digital Input Output (SDIO)

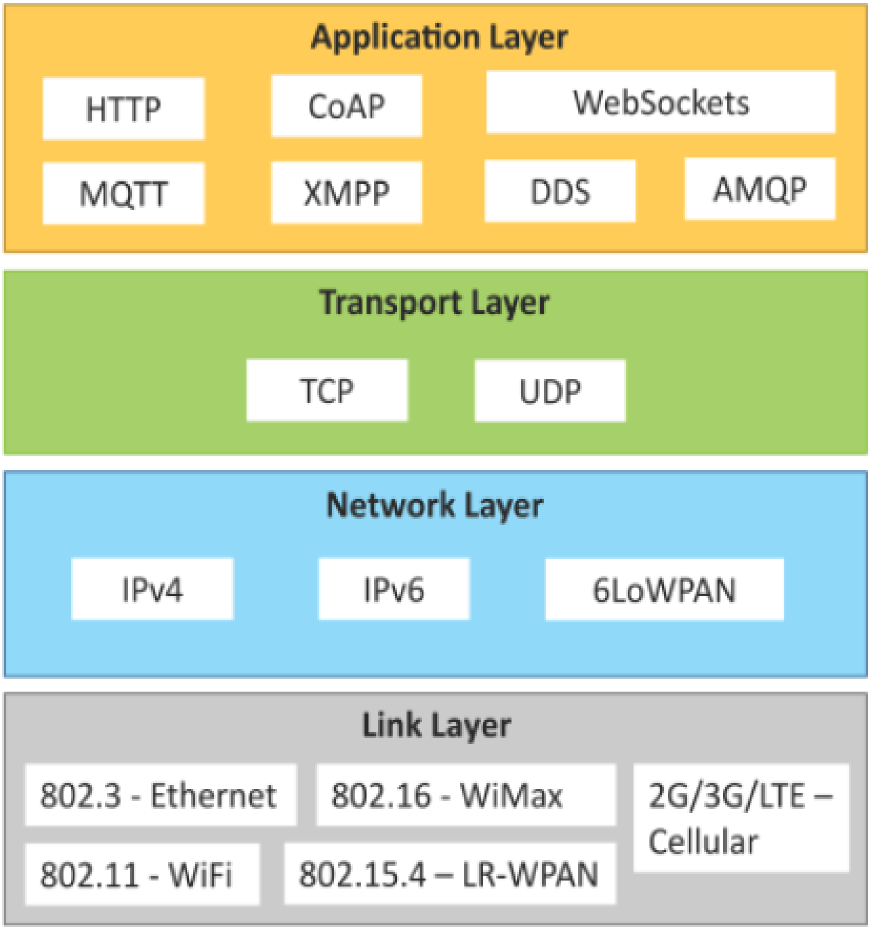
Open Systems Interconnection (OSI) Model

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

IoT Protocols

Pre-requisite: OSI model
Open Systems Interconnection (OSI)

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



Notations:

Low-Rate Wireless Personal Area Network (LR-WPAN)
WiMax: Worldwide Interoperability for Microwave Access
6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)
Hypertext Transfer Protocol (HTTP)
COAP: Common Offer Acceptance Portal
MQTT (Message Queuing Telemetry Transport)
XMPP: Extensible Messaging and Presence Protocol
Data Distribution Service (DDS)
Advanced Message Queuing Protocol (AMQP)

IoT Protocols…Link Layer…

- Link layer protocols determine how the data is physically sent over the network's physical layer or medium (e.g. copper wire, coaxial cable).
- The scope of the link layer is the local network connection to which host is attached.
- Hosts on the same link exchange data packets over the link layer using link layer protocol.
- Link layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached.

IoT Protocols…Link Layer…Ethernet

Sr.No	Standard	Shared medium
1	802.3	Coaxial Cable…10BASE5
2	802.3.i	Copper Twisted pair …..10BASE-T
3	802.3.j	Fiber Optic……10BASE-F
4	802.3.ae	Fiber…..10Gbits/s

Data Rates are provided from 10Gbit/s to 40Gb/s and higher

IoT Protocols…Link Layer…WiFi

Sr.No	Standard	Operates in
1	802.11a	5 GHz band
2	802.11b and 802.11g	2.4GHz band
3	802.11.n	2.4/5 GHz bands
4	802.11.ac	5GHz band
5	802.11.ad	60Hz band

- Collection of Wireless LAN
- Data Rates from 1Mb/s to 6.75 Gb/s

IoT Protocols...Link Layer...WiMax

Sr.No	Standard	Data Rate
1	802.16m	100Mb/s for mobile stations 1Gb/s for fixed stations

- Collection of Wireless Broadband standards
- Data Rates from 1.5Mb/s to 1 Gb/s

WiMax stands for Worldwide Inter-operability for Microwave Access. This technology is based on IEEE 802.16. It is used to provide higher data rates with increased coverage. It is based on MAN (Metropolitan Area Network) technology. Its range is upto 50 Km.

IoT Protocols…Link Layer…LR-WPAN

- Collection of standards for low-rate wireless personal area networks
- Basis for high level communication protocols such as Zigbee
- Data Rates from 40Kb/s to 250Kb/s
- Provide low-cost and low-speed communication for power constrained devices
- **868.0–868.6 MHz: Europe, allows one communication channel**
- **902–928 MHz: North America, originally allowed up to ten channels (2003), but since has been extended to thirty (2006)**
- **2400–2483.5 MHz: worldwide use, up to sixteen channels (2003, 2006)**

IoT Protocols…Link Layer…2G/3G/4G –Mobile Communication

Sr.No	Standard	Operates in
1	2G	GSM-CDMA
2	3G	UMTS and CDMA 2000
3	4G	LTE

- Data Rates from 9.6Kb/s (for 2G) to up to 100Mb/s (for 4G)

IoT Protocols…Network/Internet Layer

- Responsible for sending of IP datagrams from source to destination network
- Performs the host addressing and packet routing
- Host identification is done using hierarchical IP addressing schemes such as IPV4 or IPV6

IoT Protocols...Network Layer

- IPV4
  - Used to identify the devices on a network using hierarchical addressing scheme
  - Uses 32-bit address scheme
- IPV6
  - Uses 128-bit address scheme
- 6LoWPAN (IPV6 over Low power Wireless Personal Area Network)
  - Used for devices with limited processing capacity
  - Operates in 2.4 Ghz
  - Data Rates of 250Kb/s

IoT Protocols…Transport Layer

- Provide end-to-end message transfer capability independent of the underlying network
- It provides functions such as error control, segmentation, flow-control and congestion control

(Transport Layer)

IoT Protocols…TCP

- Transmission Control Protocol
- Connection Oriented
- Ensures Reliable transmission
- Provides Error Detection Capability to ensure no duplicacy of packets and retransmit lost packets
- Flow Control capability to ensure the sending data rate is not too high for the receiver process
- Congestion control capability helps in avoiding congestion which leads to degradation of n/w performance

(Transport Layer)

IoT Protocols…UDP

- User Datagram Protocol
- Connectionless
- Does not ensures Reliable transmission
- Does not do connection before transmitting
- Does not provide proper ordering of messages
- Transaction oriented and stateless

Question: What is the difference between TCP and UDP?

IoT Protocols...Application Layer...Hyper Transfer Protocol

- Forms foundation of World Wide Web(WWW)
- Includes commands such as GET,PUT, POST, HEAD, OPTIONS, TRACE..etc
- Follows a request-response model
- Uses Universal Resource Identifiers(URIs) to identify HTTP resources

A Uniform Resource Identifier (URI) is a unique sequence of characters that identifies a logical or physical resource used by web technologies.

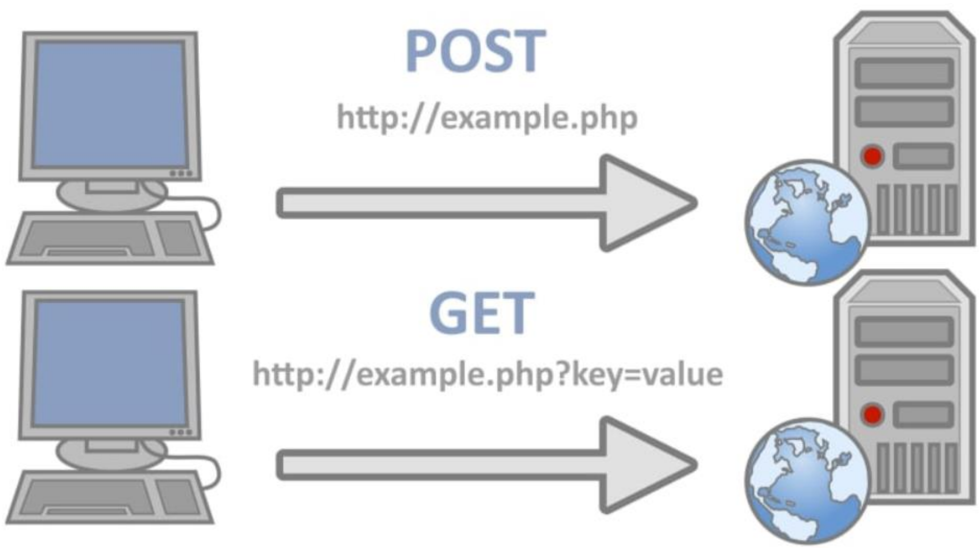
A Uniform Resource Identifier (URI) is a unique sequence of characters that identifies a logical or physical resource used by web technologies.

Example: GET Method

https://www.google.com/search?q=uri+in+internet

POST Method:

In this example, When a user fills out an HTML form and clicks the submit button, the browser sends a POST request to the server at the specified URL, which is mentioned in the form's action attribute.



IoT Protocols…Application Layer…CoAP

- Constrained Application Protocol
- Used for Machine to machine (M2M) applications meant for constrained devices and n/w's
- Web transfer protocol for IoT and uses request-response model
- Uses client –server architecture
- Supports methods such as GET,POST, PUT and DELETE

IoT Protocols…Application Layer…WebSocket

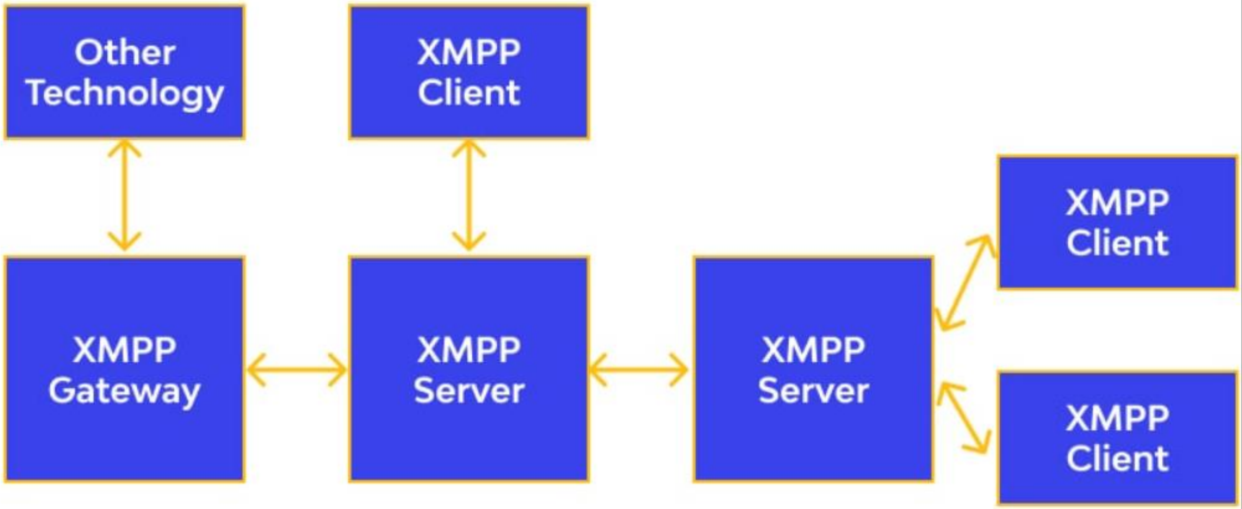
- Allows full-duplex communication over single socket
- Based on TCP
- Client can be a browser, IoT device or mobile application

IoT Protocols…Application Layer…MQTT

- Message Queue Telemetry Transport , light-weight messaging protocol
- Based on publish-subscribe model
- Well suited for constrained environments where devices have limited processing, low memory and n/w bandwith requirement

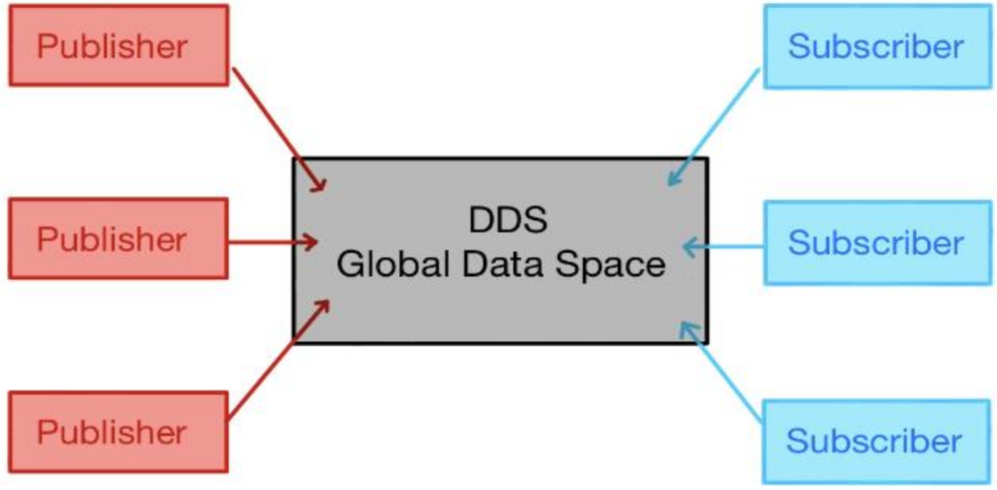
IoT Protocols…Application Layer…XMPP

- Extensible messaging and presence protocol
- For Real time communication and streaming XML data between n/w entities
- Used for Applications such as Multi-party chat and voice/video calls.
- Decentralized protocol and uses client server architecture.



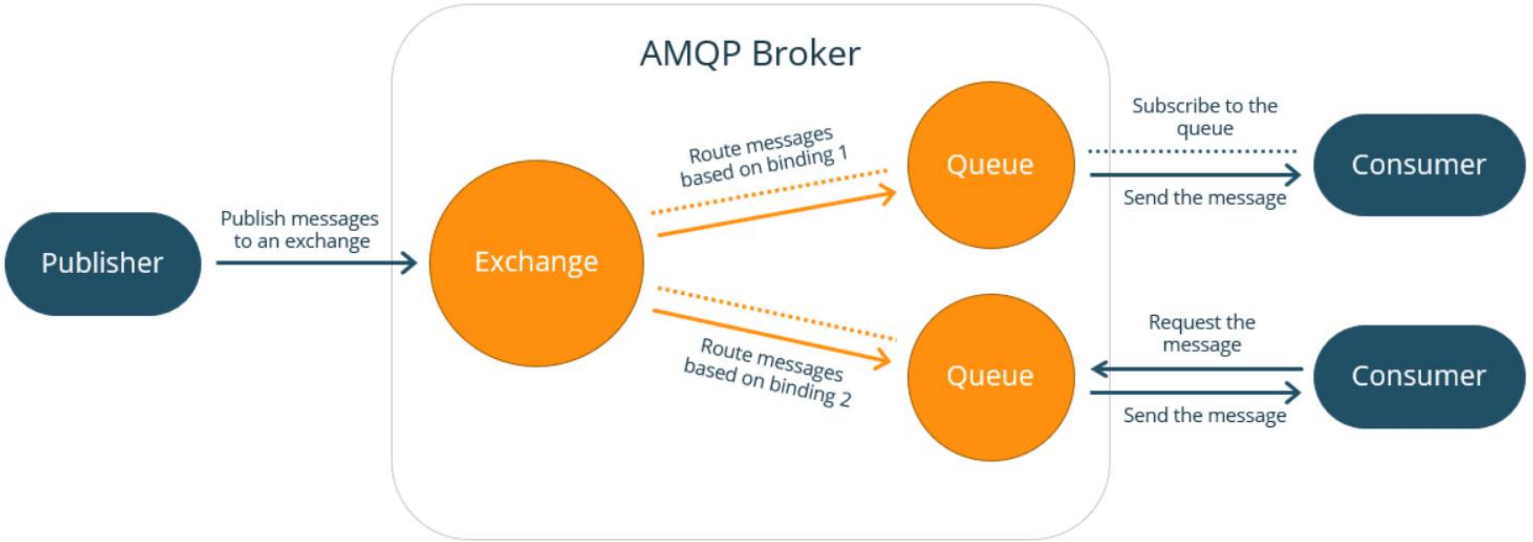
IoT Protocols...Application Layer...DDS

- Data Distribution service is a data-centric middleware standard for device-to-device or machine-to-machine communication.
- Publish subscribe model where publishers create topics to which subscribers can use.
- Provides Quality-of-service control and configurable reliability.



IoT Protocols...Application Layer...AMQP

- Advanced Messaging Queuing Protocol used for business messaging.
- Supports both point-to-point and publisher/subscriber models, routing and queuing
- Broker here receives messages from publishers and route them over connections to consumers through messaging queues.



Some questions and answers

What is the Internet of Things (IoT) and how does it differ from traditional internet-connected devices?

- IoT refers to a network of interconnected physical devices that communicate and share data. Unlike traditional internet-connected devices, IoT devices are often embedded in everyday objects and can collect and exchange data without human intervention.

Some questions and answers

What are the key components of an IoT ecosystem?

IoT ecosystems typically include devices (sensors, actuators), connectivity (networks), data processing (cloud or edge computing), and applications that leverage the generated data.

Some questions and answers

What are the security challenges associated with IoT devices and networks?

Security challenges include device vulnerabilities, data privacy concerns, lack of standardized security protocols, and the potential for unauthorized access or manipulation of IoT devices.

Some questions and answers

What are the communication protocols commonly used in IoT devices?

Common protocols include MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), and HTTP/HTTPS.

Some questions and answers

How does IoT contribute to improving efficiency in industrial processes (Industrial IoT or IIoT)?

IIoT enables real-time monitoring, predictive maintenance, and data-driven decision-making, leading to increased operational efficiency and reduced downtime in industrial settings.

- Q1: What is one key capability of IoT devices in terms of adapting to changing contexts?

Dynamic adaptation with changing contexts and the ability to take actions based on operating conditions.

- Q2: What does self-configuring capability refer to in the context of IoT devices?

The ability of IoT devices to configure themselves, enabling a large number of devices to work together to provide specific functionality.

- Q3: How do IoT devices facilitate communication with each other and the infrastructure?

By supporting interoperable communication protocols, allowing seamless communication between devices and the overall infrastructure.

- Q4: In what ways can IoT devices take actions based on their operating conditions?

By dynamically adapting to changing contexts, user's context, or the sensed environment.

- Q5: What is the significance of interoperable communication protocols for IoT devices?

It enables IoT devices to communicate not only with each other but also with the broader infrastructure, promoting seamless connectivity.

- Q6: What are some key capabilities contributing to the development of IoT?

Communication and cooperation, addressability, identification, sensing, actuation, embedded information processing, localization, and user interfaces.

- Q7: How does IoT bridge the gap between the virtual and physical world?

Through the integration of various capabilities such as communication, sensing, actuation, and more.

- Q8: What is the significance of addressability in the context of IoT?

Addressability is a crucial capability that allows IoT devices to be uniquely identified and accessed.

- Q9: How does embedded information processing contribute to the functionality of IoT?

Embedded information processing enables IoT devices to process data locally, enhancing their autonomy and efficiency.

OSI Model
Questions

- Q1: What does OSI stand for in the context of networking?

OSI stands for Open Systems Interconnection.

- Q2: How many layers are there in the OSI model, and what are they?

There are seven layers in the OSI model: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

- Q3: What is the primary purpose of the Physical layer in the OSI model?

The Physical layer deals with the physical connection between devices, including the transmission and reception of raw binary data over a physical medium.

- Q4: What is the function of the Transport layer in the OSI model?

The Transport layer ensures end-to-end communication, error recovery, and flow control between devices on different networks.

- Q5: What does the Data Link layer do in the OSI model?

The Data Link layer handles the framing, addressing, and error detection within the local network segment.

- Q6: Which layers of the OSI model are responsible for end-to-end communication and user interfaces?

The Transport, Session, Presentation, and Application layers are responsible for end-to-end communication and user interfaces.

- Q7: What is the main purpose of the Network layer in the OSI model?

The Network layer is responsible for logical addressing, routing, and forwarding of data packets between different networks.