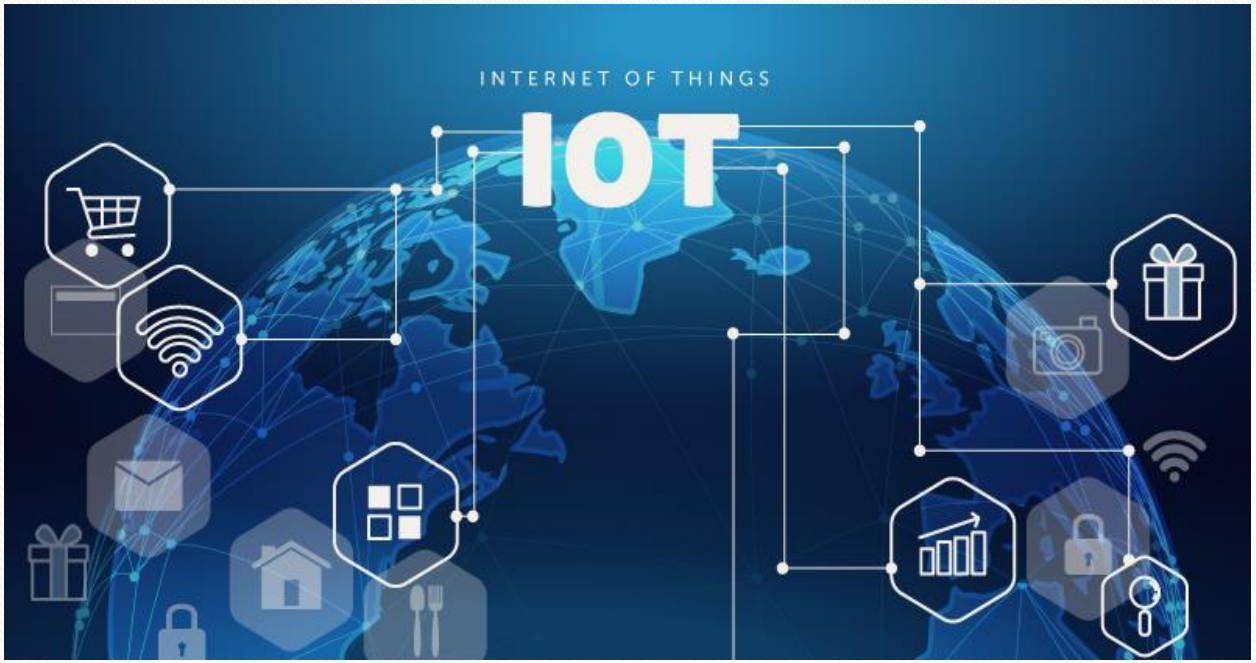
Internet of Things and Applications

Course Code: EE6434D

Module 1



Presented by

Dr. V. Karthikeyan

Assistant Professor

Department of Electrical Engineering

National Institute of Technology Calicut

Introduction

What is IoT Technology?

- ✓ Internet of Things technology can include any sensor, electronics or software that is connected to the internet and can be utilized remotely and exchange data. Often the technology works together for enhanced functionality.

What is a Platform for IoT??

- ✓ IoT applications typically incorporate a large amount of remotely accessed information made available through the internet. A platform for IoT simplifies the data access and aggregation of this data. While most software development platforms can facilitate or host IoT functionality, Mendix's low-code platform makes developing IoT enabled smart apps in-built and accessible with little technical knowledge.

Introduction

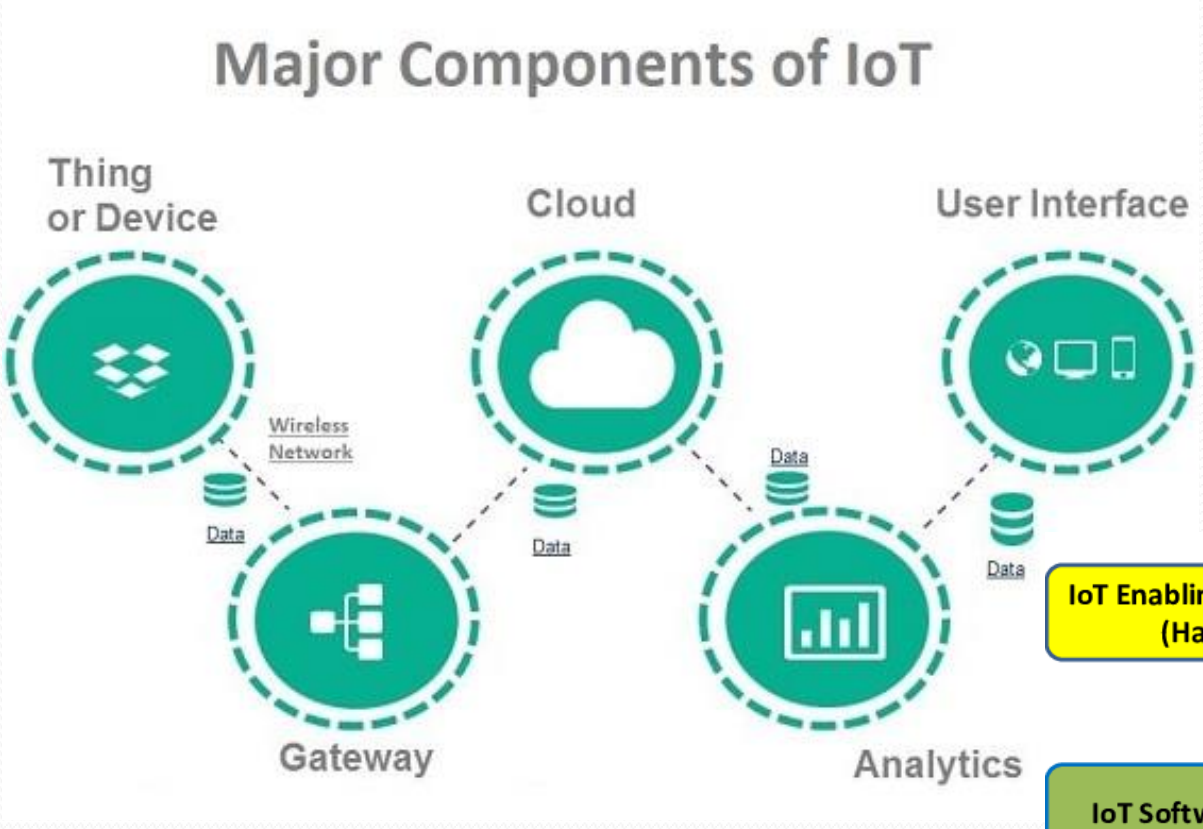
How Does the Internet of Things Work?

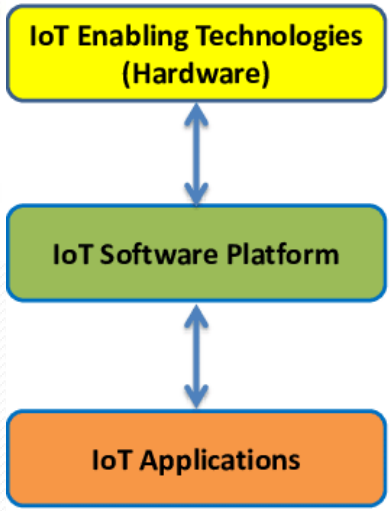
- ✓ The Internet of Things is an aggregation of internet enabled smart devices, sensors, databases and software that can be manipulated by scripts, applications and user interfaces across long distances. For example, a smart thermostat that is connected to the internet and can be controlled remotely by a phone application or an automated script.

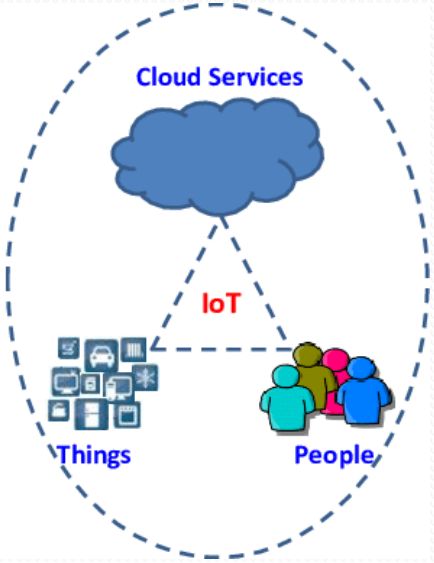
Who Came up With the Internet of Things?

- ✓ The concept of the Internet of Things is nearly as old as the internet itself with the first device coming online in 1982 at Carnegie Melon University. However, it was the co-founder of MIT's Auto-ID Lab, Kevin Ashton who coined the term in 1999.

Elements of an IoT ecosystem







Elements of an IoT ecosystem

1. Smart devices and sensors – Device connectivity

- ✓ Devices and sensors are the components of the device connectivity layer. These smart sensors are continuously collecting data from the environment and transmit the information to the next layer.
- ✓ Latest techniques in the semiconductor technology is capable of producing micro smart sensors for various applications.

Common sensors are:

- ✓ Temperature sensors and thermostats
- ✓ Pressure sensors
- ✓ Humidity / Moisture level
- ✓ Light intensity detectors
- ✓ Moisture sensors
- ✓ Proximity detection
- ✓ RFID tags

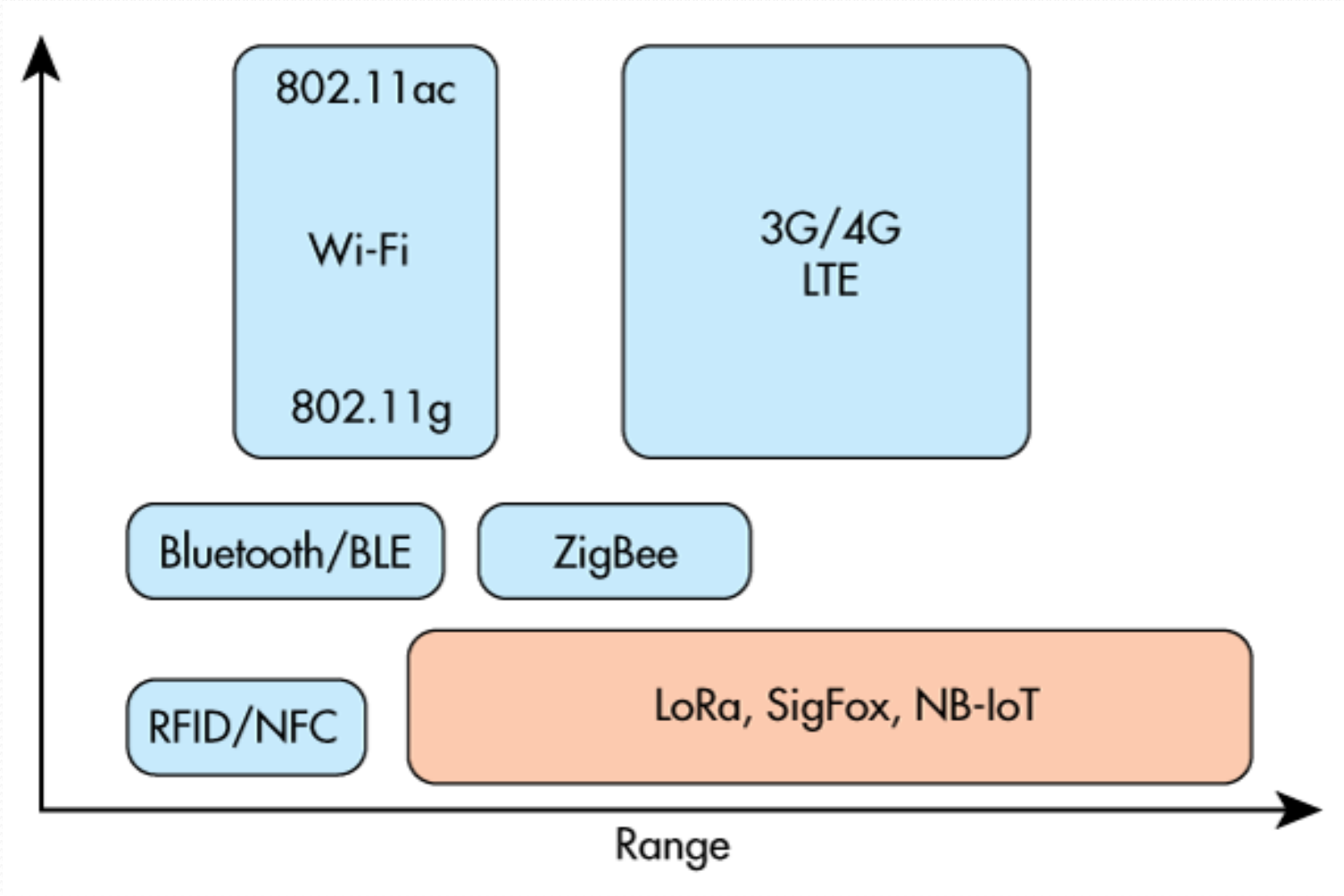
Elements of an IoT ecosystem

How the devices are connected?

- ✓ Most of the modern smart devices and sensors can be connected to low power wireless networks like Wi-Fi, ZigBee, Bluetooth, Z-wave, LoRAWAN etc…
- ✓ Each of these wireless technologies has its own pros and cons in terms of power, data transfer rate and overall efficiency.

- ✓ Developments in the low power, low cost wireless transmitting devices are promising in the area of IoT due to its long battery life and efficiency.
- ✓ Latest protocols like 6LoWPAN- IPv6 over Low Power Wireless Personal Area Networks have been adapted by many companies to implement energy efficient data transmission for IoT networks.
- ✓ 6LoWPAN uses reduced transmission time (typically short time pulses) and thus saves energy.

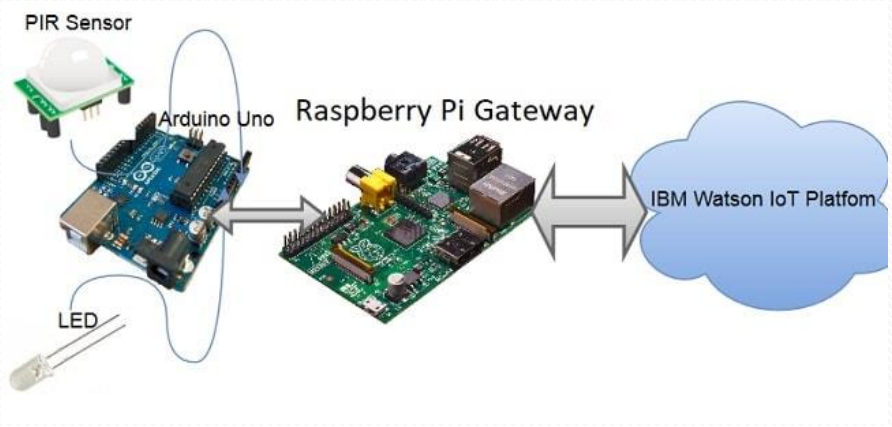
Elements of an IoT ecosystem



Elements of an IoT ecosystem

2. Gateway

- ✓ IoT Gateway manages the bidirectional data traffic between different networks and protocols.
- ✓ Another function of gateway is to translate different network protocols and make sure inter operation of the connected devices and sensors.



- ✓ Gateways can be configured to perform pre-processing of the collected data from thousands of sensors locally before transmitting it to the next stage. In some scenarios, it would be necessary due to compatibility of TCP/IP. (TC-Transmission control)
- ✓ IoT gateway offers certain level of security for the network and transmitted data with higher order encryption techniques. It acts as a middle layer between devices and cloud to protect the system from malicious attacks and unauthorized access.

Elements of an IoT ecosystem

3. Cloud

- ✓ Internet of things creates massive data from devices, applications and users which has to be managed in an efficient way.
- ✓ IoT cloud offers tools to collect, process, manage and store huge amount of data in real time. Industries and services can easily access these data remotely and make critical decisions when necessary.
- ✓ Basically, IoT cloud is a sophisticated high performance network of servers optimized to perform high speed data processing of billions of devices, traffic management and deliver accurate analytics. Distributed database management systems are one of the most important components of IoT cloud.
- ✓ Cloud system integrates billions of devices, sensors, gateways, protocols, data storage and provides predictive analytics. Companies use these analytics data for improvement of products and services, preventive measures for certain steps and build their new business model accurately.

Elements of an IoT ecosystem

4. Analytics

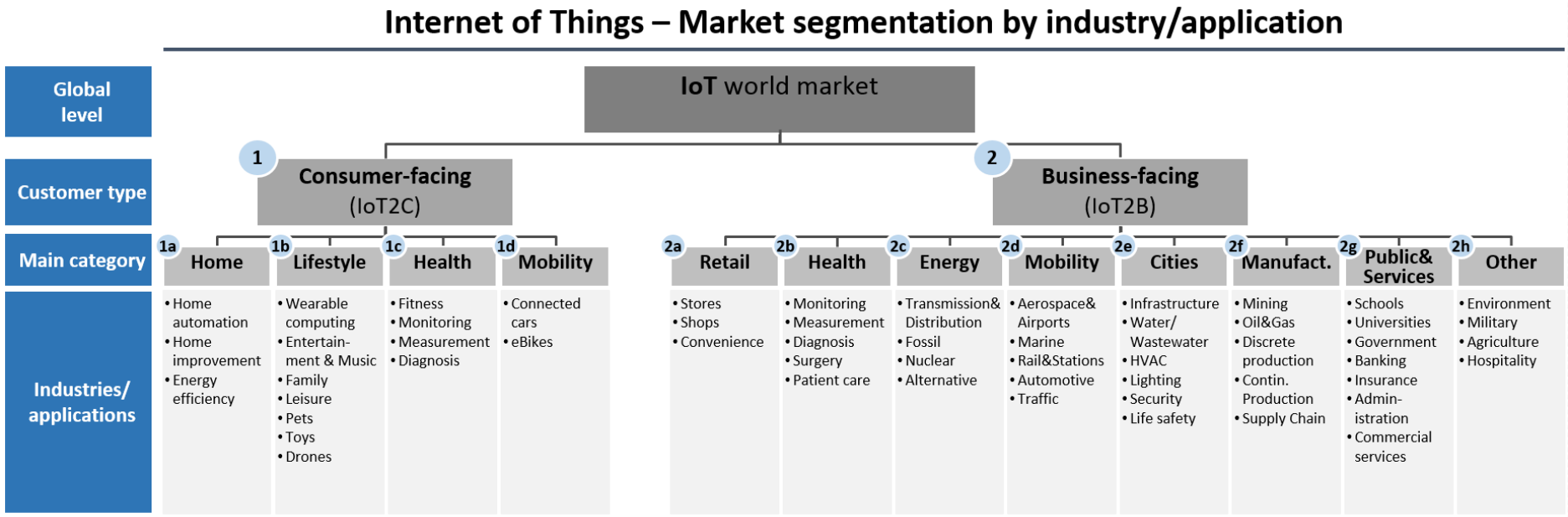
- ✓ Analytics is the process of converting analog data from billions of smart devices and sensors into useful insights which can be interpreted and used for detailed analysis.
- ✓ Smart analytics solutions are inevitable for IoT system for management and improvement of the entire system.
- ✓ One of the major advantages of an efficient IoT system is real time smart analytics which helps engineers to find out irregularities in the collected data and act fast to prevent an undesired scenario. Service providers can prepare for further steps if the information is collected accurately at the right time.
- ✓ Big enterprises use the massive data collected from IoT devices and utilize the insights for their future business opportunities. Careful analysis will help organizations to predict trends in the market and plan ahead for a successful implementation.
- ✓ Information is very significant in any business model and predictive analysis ensures success in concerned area of business line.

Elements of an IoT ecosystem

5. User interface

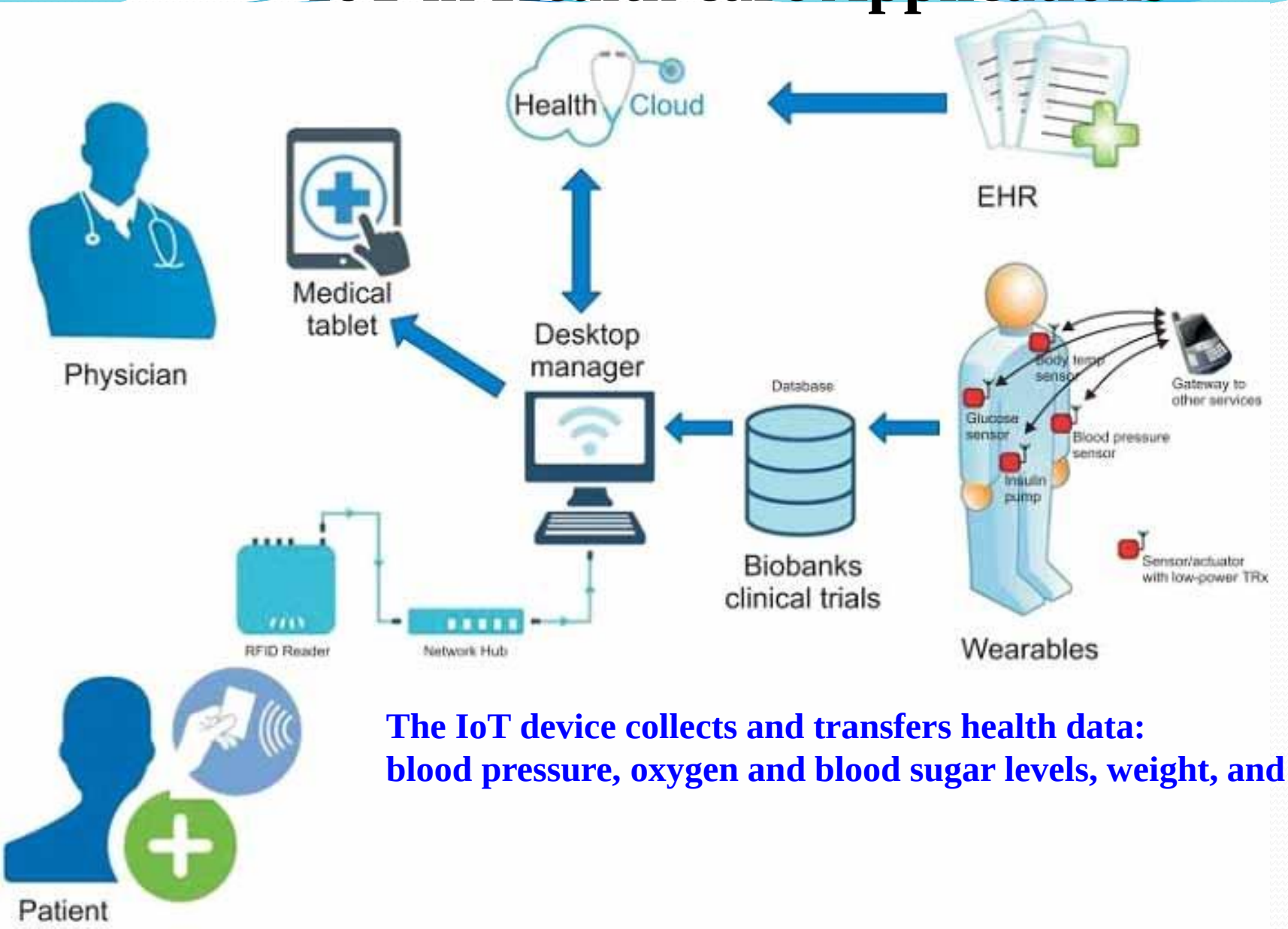
- ✓ User interfaces are the visible, tangible part of the IoT system which can be accessible by users. Designers will have to make sure a well designed user interface for minimum effort for users and encourage more interactions.
- ✓ Modern technology offers much interactive design to ease complex tasks into simple touch panels controls. Multicolours touch panels have replaced hard switches in our household appliances and the trend is increasing for almost every smart home devices.
- ✓ User interface design has higher significance in today's competitive market, it often determines the user whether to choose a particular device or appliance. Users will be interested to buy new devices or smart gadgets if it is very user friendly and compatible with common wireless standards.

IoT Business Drives



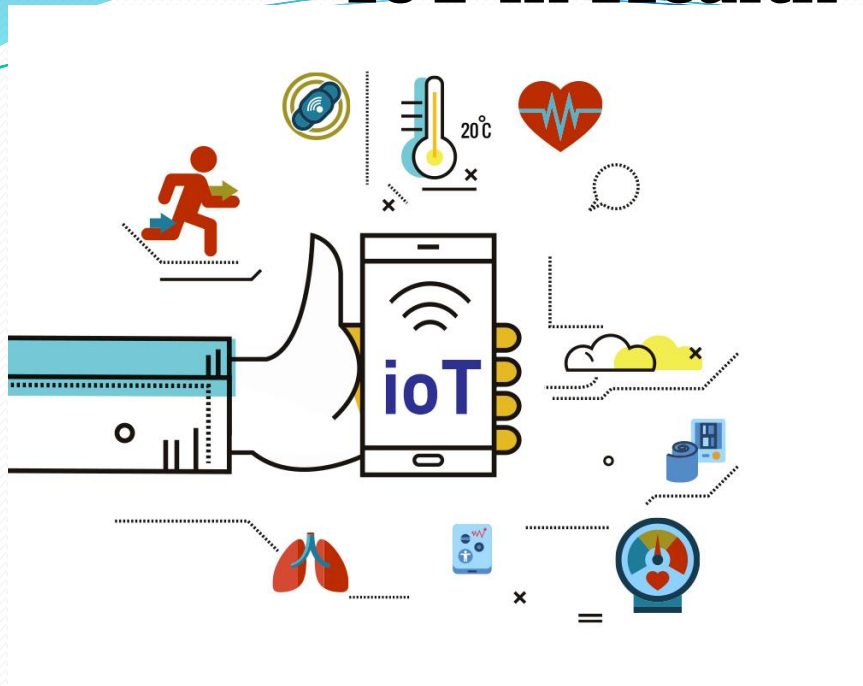
- ✓ It distinguishes consumer-facing IoT and business-facing IoT. Companies active in the IoT Consumer segment like the wearables manufacturers have very little overlap with industrial IoT companies like Cisco because their customers are different.
- ✓ It depicts main categories that play a major role in terms of importance and which are clearly different from each other.

IoT in Health care Applications



The IoT device collects and transfers health data:
blood pressure, oxygen and blood sugar levels, weight, and ECGs.

IoT in Health care Applications



These data are stored in the cloud and can be shared with an authorized person, who could be a physician, your insurance company, a participating health firm or an external consultant, to allow them to look at the collected data regardless of their place, time, or device.

Benefits in health care:

- ✓Simultaneous reporting and monitoring
- ✓Tracking patients, staff and alerts
- ✓Reducing emergency room wait time
- ✓Enhancing drug management
- ✓Ensuring availability of critical hardware

IoT in Health care Applications

Features of IoT in health care

Healthcare providers can broadly use the IoT data collected from the app for the following purposes:

Follow good clinical practices, varying from clinical record-keeping to sharing relevant information with the multidisciplinary team.

- ✓Pervasive monitoring: real-time, multi-stream integration
- ✓Enable chronic patients a platform to track, monitor, and quantify their health
- ✓Make available data for health risk assessment
- ✓Support continuity of care for chronic patients
- ✓Research Studies
  - ✓Determining clinical trial efficiency
  - ✓Performance monitoring
  - ✓Comparing treatment effects
  - ✓Evaluating novel therapeutics
  - ✓Measuring functional recovery in patients
- ✓Evaluate staffing patterns and determine the composition

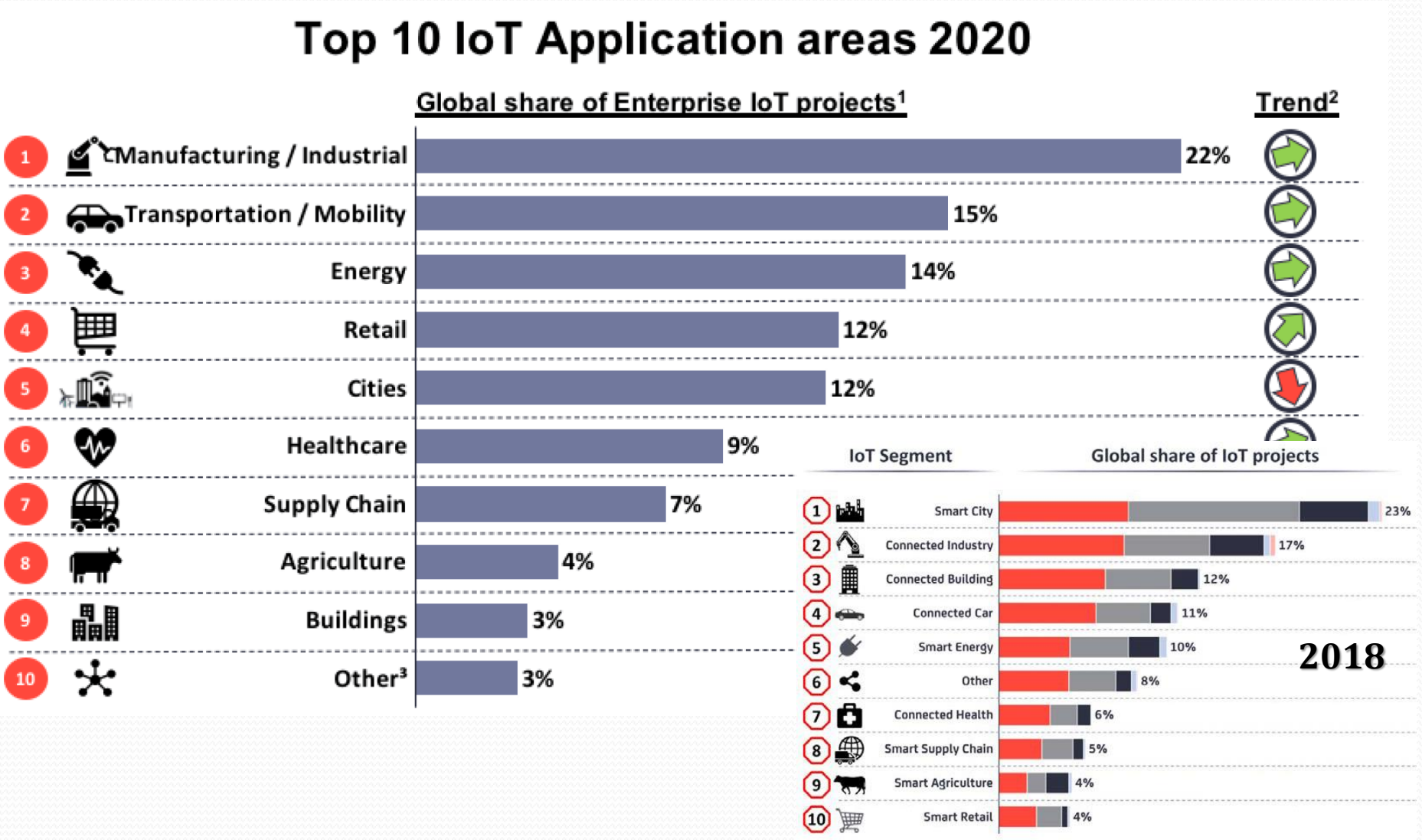
IoT in Health care Applications

Features of IoT in health care

- ✓Resource Utilization
  - ✓Determine service metrics
  - ✓Manage medication usage
  - ✓Evaluate diagnostic tests and procedure performed
- ✓Quality Assessments
  - ✓Patient outcome
  - ✓Patient readmission rate
  - ✓Patient satisfaction surveys
  - ✓Hospital quality measures

The Internet of Things in healthcare has brought significant developments in chronic patient care management and caregiver support that have ushered a new era of proactive healthcare delivery.

Typical IoT Applications



Typical IoT Applications

1. Smart home:

- ✓ Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels.
- ✓ More than 60,000 people currently search for the term “Smart Home” each month.
- ✓ The IoT Analytics company database for Smart Home includes 256 companies and start-ups. More companies are active in smart home than any other application in the field of IoT.
- ✓ This list includes prominent start-up names such as Nest or Alert Me as well as a number of multinational corporations like Philips, Haier, or Belkin.

2. Wearables

- ✓ Wearables remains a hot topic too. The Apple’s new smart watch has been released in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet.
- ✓ Of all the IoT startups, wearable's maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars!

Typical IoT Applications

3. Smart City

- ✓ Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring.
- ✓ Its popularity is fuelled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days.
- ✓ IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

4. Smart grids

- ✓ Smart grids is a special one. A future smart grid promises to use information about the behaviours of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity.

Indian Scenario in Forest Fires

✓***According to the India State of Forest Report 2019, over 30,000 incidents of forest fires were reported in India in 2019.***

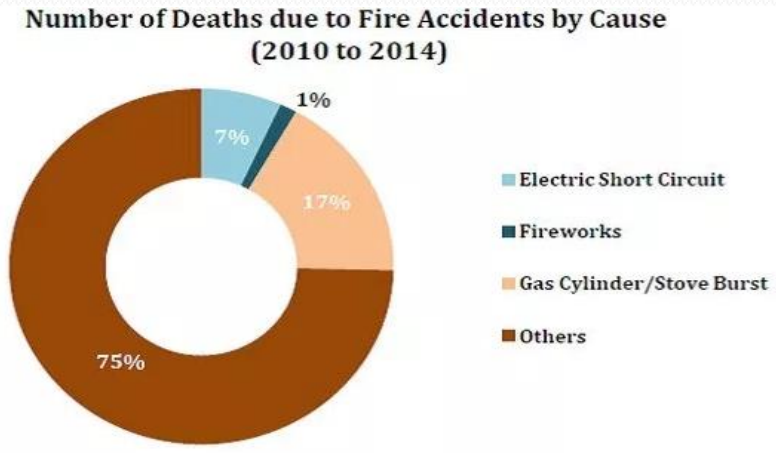
✓***Around 95 percent of the forest fires in India are on account of human activity.***

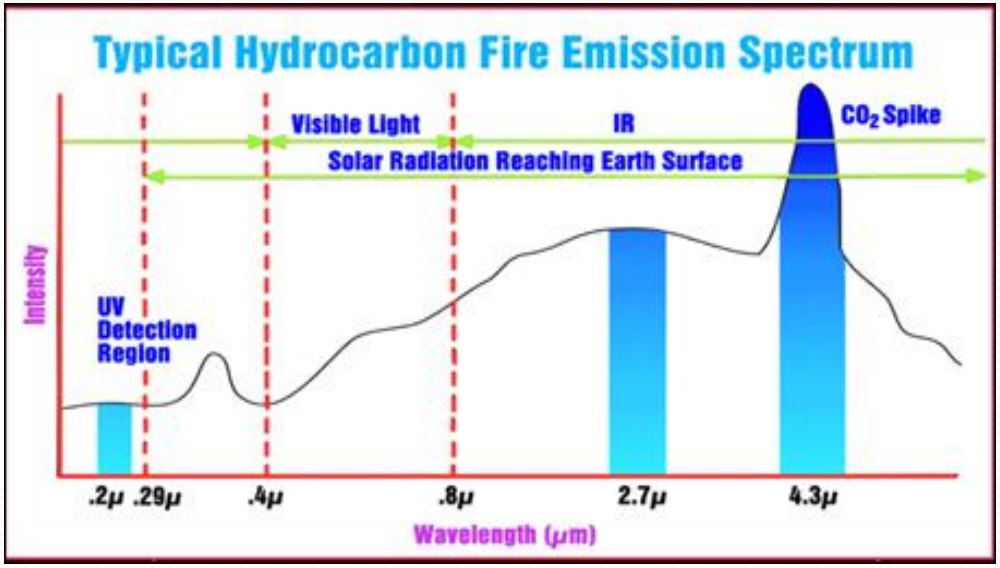
✓There are about 277,758 forest fire points – used to determine forest fire proneness – across India detected by FSI based on fire data over 13 years, from 2004/5 to 2017.

✓Of these Mizoram has the most forest fire points with over 32,600 fire points between 2005 and 2017.

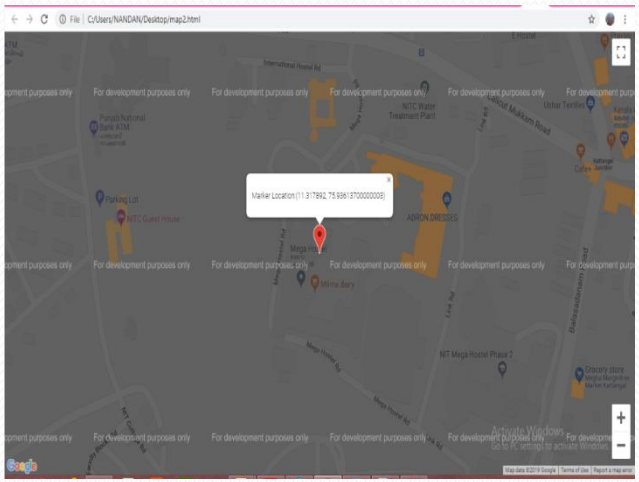
✓Chhattisgarh, Odisha, Madhya Pradesh, Assam and Maharashtra have between 20,000 to 26,000 forest fire points while moist forest clad Kerala has 1,700 points.

How IoT can help?





A fire emits radiation, which human eye experiences as the visible yellow red flames and h



- **Operating voltage: 3.3V-5.3V**
- **Detection angle : 0 degree-60 degree**
- **Operating temp: -25℃-85℃**

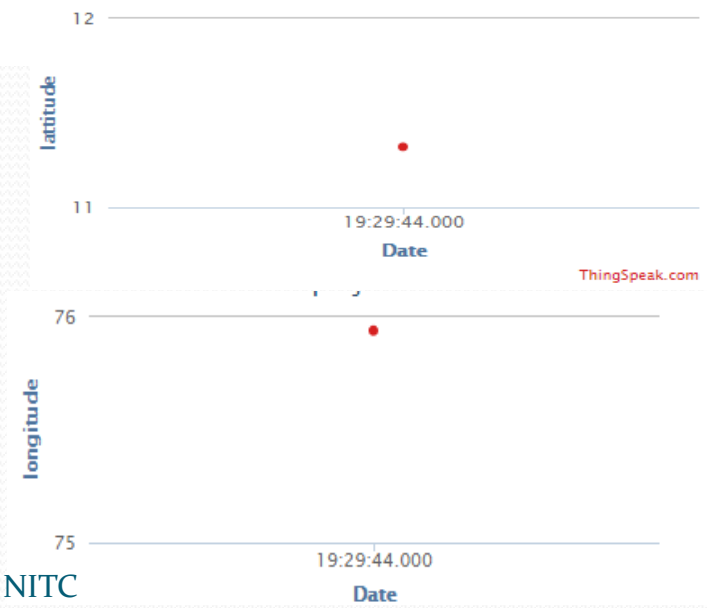
Code Explanation

```
#include <SoftwareSerial.h>
#include "ThingSpeak.h"
#include <ESP8266WiFi.h>
#include <TinyGPS++.h>
int LED = D7;
int flame_sensor = D6;
int flame_detected;
int flame=1;
static const int RXPin = 4, TXPin = 2;
static const uint32_t GPSBaud = 9600;
const char* ssid     = "nandhan";
const char* password = "explorer";

unsigned long myChannelNumber = 715910;
const char * myWriteAPIKey = "8P48KJX9RFW1L22D";

TinyGPSPlus gps;
WiFiClient  client;

SoftwareSerial ss(RXPin, TXPin);

void setup()
{
  pinMode(D5, OUTPUT);
  pinMode(LED, OUTPUT);
  pinMode(flame_sensor, INPUT);
  Serial.begin(115200);
  ss.begin(GPSBaud);
  Serial.println(F("DeviceExample.ino"));
  Serial.println();

  Serial.print("Connecting to ");
  Serial.println(ssid);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
   Serial.println("");
  Serial.println("WiFi connected");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());
  Serial.print("Netmask: ");
  Serial.println(WiFi.subnetMask());
  Serial.print("Gateway: ");
  Serial.println(WiFi.gatewayIP());
  ThingSpeak.begin(client);

}

void loop()
{
  flame_detected = digitalRead(flame_sensor);


  if (flame_detected == 1)
  {
```

Code Explanation

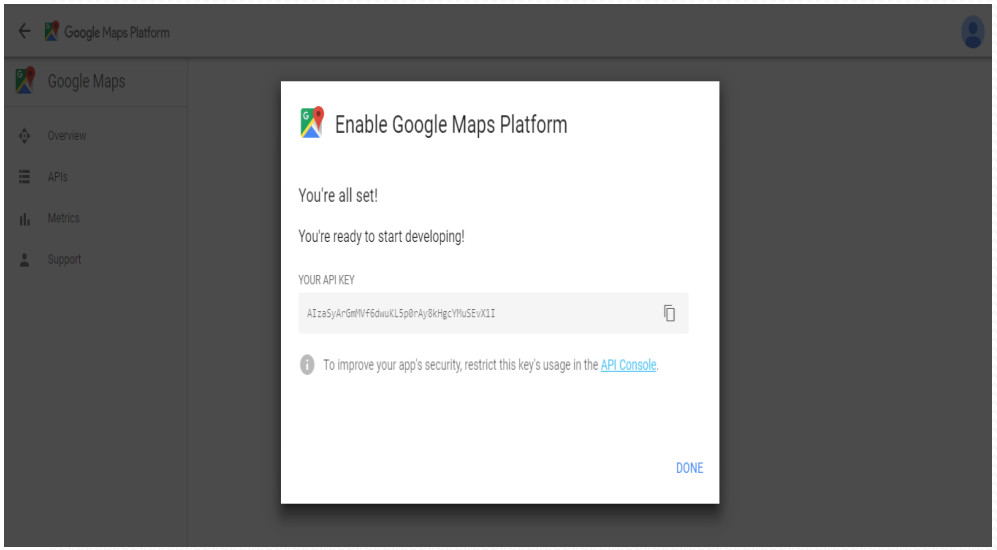
```
  Serial.println(flame);
  digitalWrite(D5, HIGH);
  digitalWrite(LED, HIGH);
  delay(200);
  digitalWrite(LED, LOW);

  while (ss.available() > 0)
  if (gps.encode(ss.read()))


if (millis() > 5000 && gps.charsProcessed() < 10)
{
  Serial.println(F("No GPS detected: check wiring."));
  while(true);
}

if (gps.location.isValid())
{
  String flame1;
  flame1=flame;
  double latitude = (gps.location.lat());
  double longitude = (gps.location.lng());

  String latbuf;
  latbuf += (String(latitude, 6));
  Serial.println(latbuf);

  String lonbuf;
  lonbuf += (String(longitude, 6));
```

```
  String lonbuf;
  lonbuf += (String(longitude, 6));
  Serial.println(lonbuf);

  ThingSpeak.setField(1, flame1);
  ThingSpeak.setField(2, latbuf);
  ThingSpeak.setField(3, lonbuf);
  ThingSpeak.writeFields(myChannelNumber, myWriteAPIKey);
  delay(20000);

}
else
{
  Serial.print(F("INVALID"));
}
```



Code Explanation

```
            initialize();
    });

        }
            window.setInterval(function(){
        loadmaps();
            }, 9000);
      function initialize() {
        //alert(y);
        var mapOptions = {
          zoom: 18,
          center: {lat: x, lng: y}
        };
        map = new google.maps.Map(document.getElementById('map'),
            mapOptions);

        var marker = new google.maps.Marker({
          position: {lat: x, lng: y},
          map: map
        });

        var infowindow = new google.maps.InfoWindow({
          content: '<p>Marker Location:' + marker.getPosition() + '</p>'
        });

        google.maps.event.addListener(marker, 'click', function() {
          infowindow.open(map, marker);
        });
      }

      google.maps.event.addDomListener(window, 'load', initialize);
    </script>
  </head>
  <body>
    <div id="map"></div>
  </body>
</html>
```



INTERFACING THING SPEAK WITH GOOGLE MAP

Indian Scenario in Pollution

According to the World Air Quality Report 2019 compiled by IQAir Air Visual, Ghaziabad is the most polluted city in the world

And what we get????

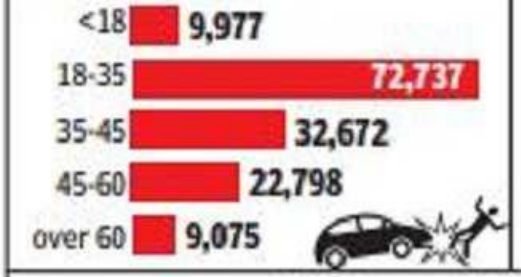
Indian Scenario in Accident

Over 1.51 lakh died in road accidents last year

Rising Road Fatalities

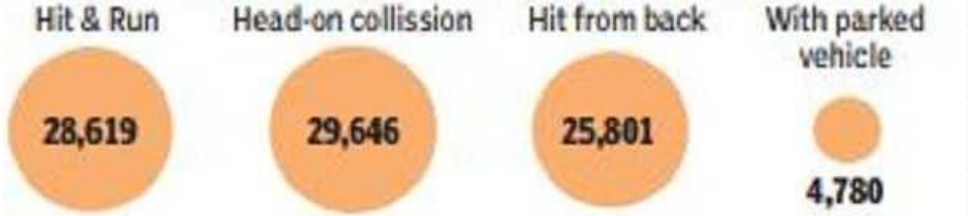
State	Deaths in 2018	Deaths in 2017	Deaths in 2016
Uttar Pradesh	22,256	20,124	19,320
Maharashtra	13,261	12,264	12,935
Tamil Nadu	12,216	16,157	17,218
Karnataka	10,990	10,609	11,133
Madhya Pradesh	10,706	10,177	9,646
All States/ Uts	**1,51,417**	**1,47,913**	**1,50,785**

Age-wise persons killed (2018)



Major users killed (2018)

Persons Killed in type of collission (Major reasons)



- As

Typical IoT Applications

5. Industrial internet

- ✓ The industrial internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial internet as the IoT concept with the highest overall potential, its popularity currently doesn't reach the masses like smart home or wearable do.
- ✓ The industrial internet however has a lot going for it. The industrial internet gets the biggest push compared to other non-consumer-oriented IoT concepts.

6. Connected car

- ✓ The connected car is coming up slowly in India. Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz around the connected car yet.
- ✓ But most large auto makers as well as some brave startups are working on connected car solutions.

Typical IoT Applications

7. Connected Health (Digital health/Telehealth/Telemedicine)

- ✓ Connected health remains the sleeping giant of the Internet of Things applications. The concept of a connected health care system and smart medical devices bears enormous potential not just for companies also for the well-being of people in general.
- ✓ Yet, Connected Health has not reached the masses yet. Prominent use cases and large-scale start-up successes are still to be seen.

8. Smart retail

- ✓ Proximity-based advertising as a subset of smart retail is starting to take off. But the popularity ranking shows that it is still a niche segment.

Typical IoT Applications

9. Smart supply chain

- ✓ Supply chains have been getting smarter for some years already. Solutions for tracking goods while they are on the road, or getting suppliers to exchange inventory information have been on the market for years.
- ✓ So while it is perfectly logic that the topic will get a new push with the Internet of Things, it seems that so far its popularity remains limited.

10. Smart farming

- ✓ Smart farming is an often overlooked business-case for the internet of Things because it does not really fit into the well-known categories such as health, mobility, or industrial.
- ✓ However, due to the remoteness of farming operations and the large number of livestock that could be monitored the Internet of Things could revolutionize the way farmers work. But this idea has not yet reached large-scale attention.
- ✓ Smart farming will become the important application field in the predominantly agricultural-product exporting countries.

Overview of IoT supported Hardware platforms

- ✓ This essentially refers to platforms that are used for the development of the “things” in the **internet of things.**
- ✓ It could refer to communication modules, Microcontrollers, and SoC modules with features that make them desirable for use in the development of IoT devices.
- ✓ The list below is in no particular order and by no means exhaustive as there are more development platforms than one could probably name, but it contains some of the **most comprehensive, and maker-friendly platforms**.

1. Particle.io:

Particle.io is one of the most comprehensive end to end IoT platforms. It is an all-in-one io platform that offers IoT hardware development platform, connectivity, device cloud and apps. Particle makes a long line of IoT hardware development products for both rapid prototypes and DFM level production.

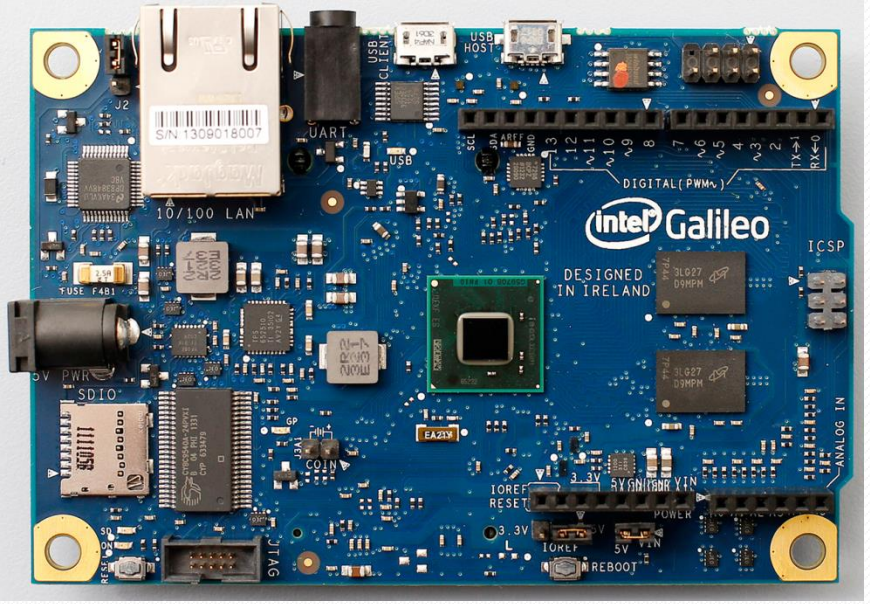
Overview of IoT supported Hardware platforms

- ✓ Building an IoT product starts with connecting the devices to the internet and all the Particle's microcontroller boards are enabled to communicate over either of Wi-Fi, cellular (2G/3G/LTE), or mesh. With some of their boards featuring multiple communication options on-board.
- ✓ Their microcontrollers are controlled by a special OS which enables developer to integrate the devices easily with particle's device cloud and apps.
- ✓ As a peck, their devices and communication modules come with CE and FCC certifications which reduce the cost of certificate, on when the product is ready to be scaled. Their boards are open source ensuring there is a lot of support for product development.

Overview of IoT supported Hardware platforms

2. Intel's Galileo IoT Development Boards

- ✓ While it's commonplace for IoT product companies to use prototyping boards to test out new ideas, these boards usually are not appropriate for deployment scale usage from a cost standpoint.
- ✓ When manufacturing a high-volume production run of a product, product engineers and designers will necessarily be concerned with the keeping the bill of materials (BoM) in check.
- ✓ To conserve costs, it's often necessary to alter the prototype design for a production build, tossing out the parts of the board that are not actually being used.



Overview of IoT supported Hardware platforms

- ✓ According to Intel's website, the **compute module was designed for experts, makers, entrepreneurs, and for use in industrial IoT applications**. The module provides ease-of-development for prototypes development and use in a range of commercial ventures when performance matters.
- ✓ The module uses a 22 nm Intel SoC that includes a dual core, dual threaded Intel Atom CPU at 500MHz and a 32-bit Intel® Quark microcontroller which runs at 100 MHz. The module and most of the other boards like the Intel Curie and the Intel Galileo has however been discontinued.
- ✓ **Currently most popular IoT hardware development platform from Intel is the *Up Squared groove IoT Development Kit*** which is a platform designed specifically to suit the rugged demands of industrial IoT applications.

Overview of IoT supported Hardware platforms

3. Arduino IoT Product Line

- ✓ It's impossible for the Arduino to be an unfamiliar name to anyone within the IoT space. Long before the IoT became mainstream, several of the Arduino boards were already being used to develop prototypes for connected devices.
- ✓ With the ease of programming and the plug and play nature of Arduino based system, it quickly became loved by many in the hardware space. The early Arduino boards, were mostly general purpose microcontrollers which were connected to the internet using GSM and WiFi modules, but as the IoT began to Open up, boards with special features that support the IoT were developed.
- ✓ Boards like the Arduino 101(developed with Intel), the MKR1000, Arduino WiFi Rev 2 and the MKR Vidor 4000 which is the first Arduino board based on FPGA Chip.

Overview of IoT supported Hardware platforms

- ✓ Each of these boards was made with the IoT in mind, and they all have different features that make them more suitable for specific IoT solution. The Arduino WiFi Rev 2 for instance comes with an IMU which makes it suitable for drone based applications.

Overview of IoT supported Hardware platforms

4. The Raspberry Pi

- ✓ While the Raspberry Pi is naturally a general purpose device, it will be injustice to ignore the contribution of the raspberry to the development of some of IoT products and projects currently in vogue.
- ✓ They are generally too robust and sophisticated to be used in the development of simple connected sensors or actuators, but they find application serving as data aggregators, hubs and device gateways in IoT projects.
- ✓ The latest of the raspberry pi boards; the Raspberry pi 3 model B+ features a 1.4GHz Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC, 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE, and a Gigabit Ethernet port over USB 2.0 (maximum throughput 300 Mbps).
- ✓ Asides several other features including 4 USB ports, Audio output, to mention a few, the board comes with a 1GB LPDDR2 SDRAM which makes it quite fast for IoT based tasks.

Overview of IoT supported Hardware platforms

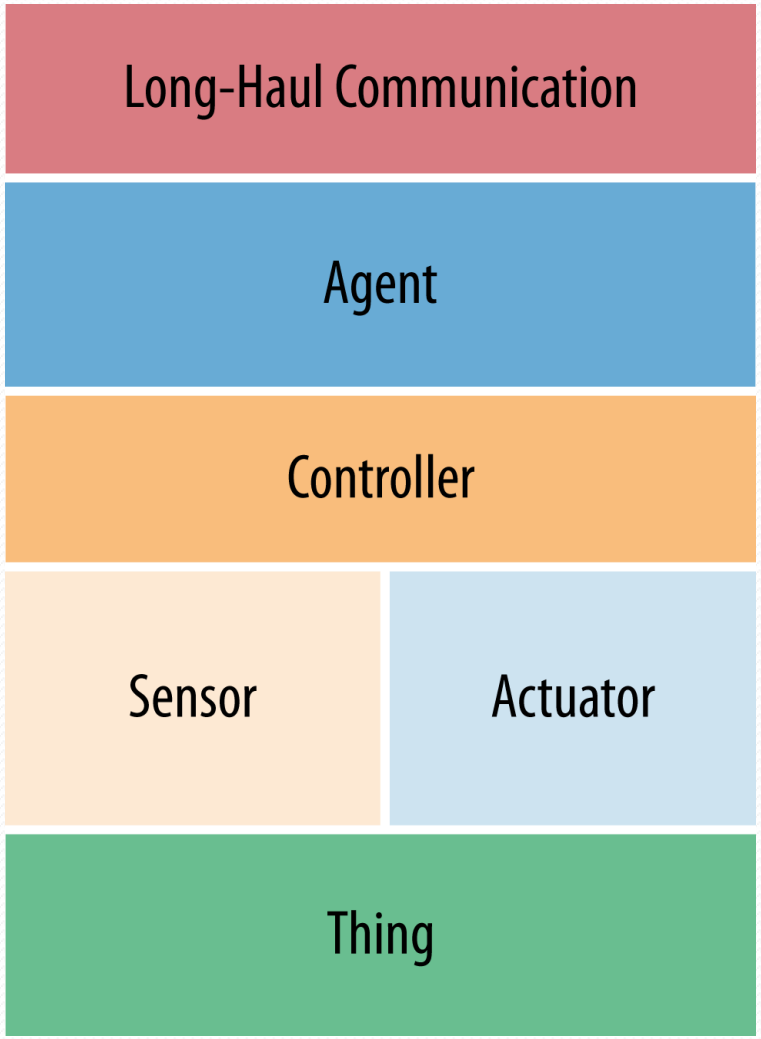
- ✓ The Raspberry pi compute module three (CM 3) is currently the latest and it contains the guts of a Raspberry Pi 3 (the BCM2837 processor and 1GB RAM) as well as a 4GB eMMC Flash device (which is the equivalent of the SD card in the Pi) running at a 1.2GHz processor speed all integrated on a small 67.6 mm x 31 mm board which fits into a standard DDR2 SODIMM connector (the same type of connector as used for laptop memory).

Sensors

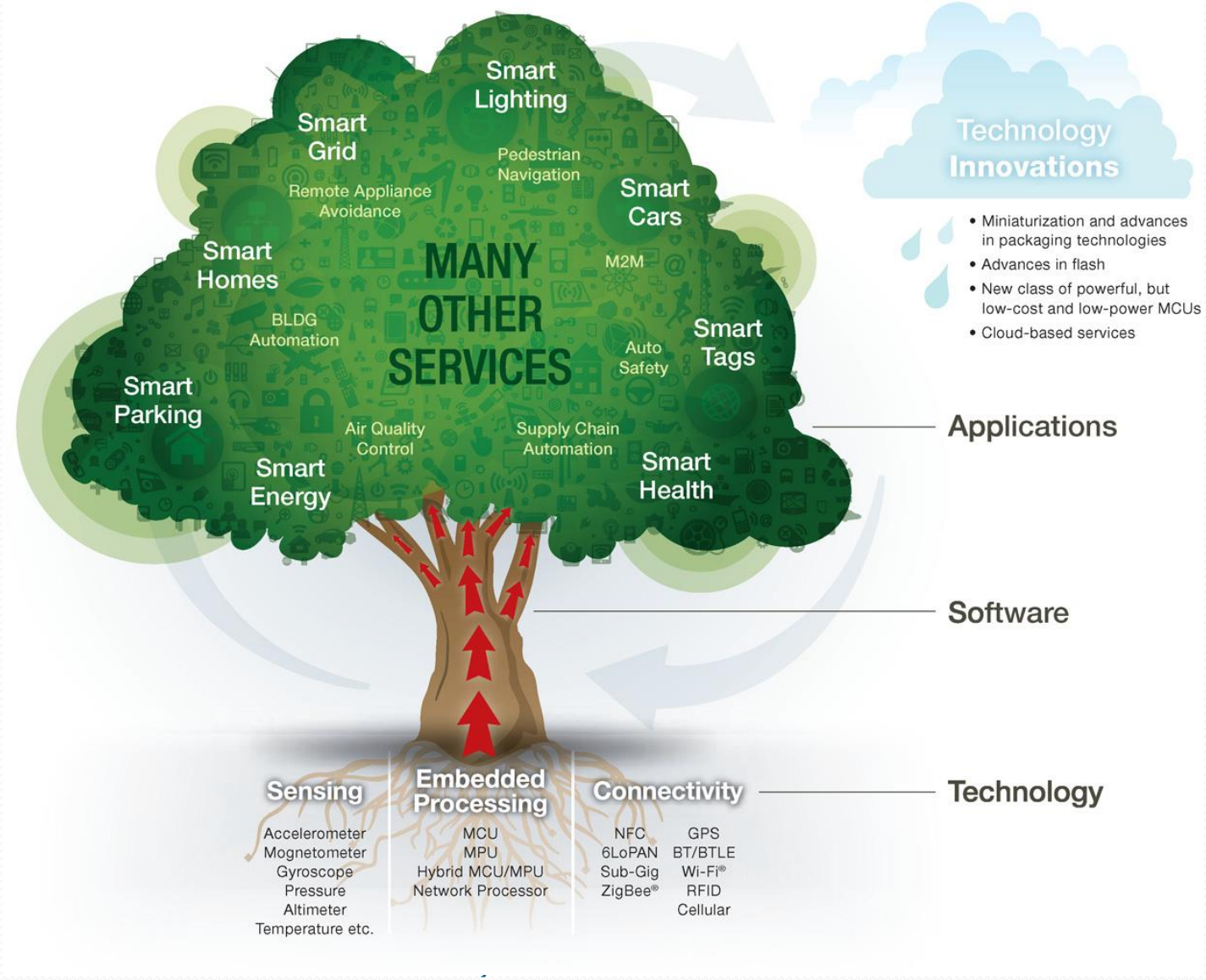
- ✓ Sensors may be physically hardwired, built into the product, or communicate via a short-haul communication protocol like Bluetooth
- ✓ Low Energy (LE) or ZigBee.

Examples of sensors include:

- ✓ Temperature sensors
- ✓ Light sensors
- ✓ Moisture sensors
- ✓ GPS receivers
- ✓ Vehicle on-board diagnostics
- ✓ Files and
- ✓ Product-specific data

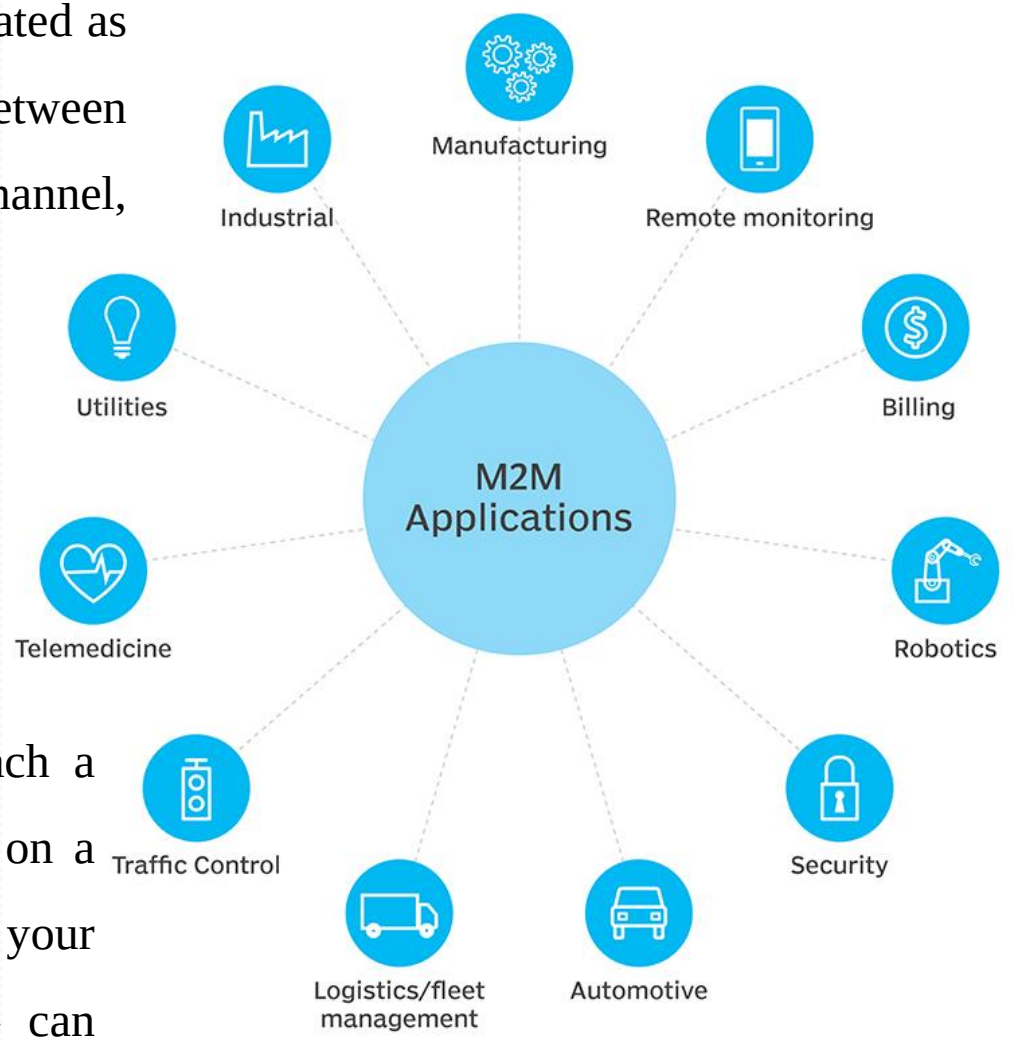


The IoT: Different Services and Technologies



M2M and Its Applications

- ✓ Machine to machine (commonly abbreviated as M2M) refers to direct communication between devices using any communications channel, including wired and wireless
- ✓ The "things" in the IoT, or the "machines" in M2M, are physical entities whose identity and state are being relayed to an internet-connected IT infrastructure.
- ✓ Almost anything to which you can attach a sensor — a cow in a field, a container on a cargo vessel, the air-conditioning unit in your office, or a lamppost in the street — can become a node in the Internet of Things.



M2M Applications

- ✓ Machine-to-machine communication is often used for remote monitoring. In product restocking, for example, a vending machine can message the distributor's network, or machine, when a particular item is running low to send a refill.
- ✓ An enabler of asset tracking and monitoring, M2M is vital in warehouse management and supply chain management.
- ✓ Utilities companies often rely on M2M devices and applications to not only harvest energy, such as oil and gas, but also to bill customers -- through the use of smart meters -- and to detect worksite factors, such as pressure, temperature, equipment status and more.
- ✓ In telemedicine, M2M devices can enable the real-time monitoring of patients' vital statistics, dispensing medicine when required, or tracking healthcare assets.
- ✓ M2M is also an important aspect of remote control, robotics, traffic control, security, logistics and fleet management, and automotive.

M2M Applications

a. **Security** : Surveillances, Alarm systems, Access control, Car/driver security

b. **Tracking & Tracing** : Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering

c. **Payment** : Point of sales, Vending machines, Gaming machines

d. **Health** : Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics

e. **Remote Maintenance/Control** : Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics

f. **Metering** : Power, Gas, Water, Heating, Grid control, Industrial metering

g. **Manufacturing** : Production chain monitoring and automation

h. **Facility Management** : Home / building / campus automation

M2M and IoT Diff?

M2M	IoT
Machines	Sensors
Hardware-based	Software-based
Vertical applications	Horizontal applications
Deployed in a closed system	Connects to a larger network
Machines communicating with machines	Machines communicating with machines, humans with machines, machines with humans
Uses non-IP protocol	Uses IP protocols
Can use the cloud, but not required to	Uses the cloud
Machines use point-to-point communication, usually embedded in hardware	Devices use IP networks to communicate
Often one-way communication	Back and forth communication
Main purpose is to monitor and control	Multiple applications; multilevel communications
Operates via triggered responses based on an action	Can, but does not have to, operate on triggered responses
Limited integration options, devices must have complementary communication standards	Unlimited integration options, but requires software that manages communications/protocols
Structured data	Structured and unstructured data

Data Collection and Analysis (DCA)

Data Collection and Analysis modules or capabilities are the essential components of any IoT platform or system, and they are constantly evolving in order to support more features and provide more capacity to external components (either higher layer applications leveraging on the data stored by the DCA module or other external systems exchanging information for analysis or processing).

The DCA module is part of the core layer of any IoT platform. Some of the main functions of a DCA module are:

User/customer data storing:

- ✓ Provides storage of the customer's information collected by sensors

User data & operation modelling:

- ✓ Allows the customer to create new sensor data models to accommodate collected information and the modelling of the supported operations

On demand data access:

- ✓ Provides application program interface (APIs) to access the collected data

Device event publish/subscribe/forwarding/notification:

- ✓ Provides APIs to access the collected data in real time conditions

Data Collection and Analysis (DCA)

Customer rules/filtering:

Allows the customer to establish its own filters and rules to correlate events

Customer task automation:

Provides the customer with the ability to manage his automatic processes. (e.g. scheduled platform originated data collection).

Customer workflows:

Allows the customer to create his own workflow to process the incoming events from a device

Multitenant structure:

Provides the structure to support multiple organizations and reseller schemes.

Data Collection and Analysis (DCA)

In the coming years, the main research efforts should be targeted to some features that should be included in any Data Collection and Analysis platform:

Multi-protocol

DCA platforms should be capable of handling or understanding different input (and output) protocols and formats.

De-centralisation

Sensors and measurements/observations captured by them should be stored in systems that can be de-centralised from a single platform. It is essential that different components, geographically distributed in different locations may cooperate and exchange data. Related with this concept, federation among different systems will make possible the global integration of IoT architectures.

Security

DCA platforms should increase the level of data protection and security, from the transmission of messages from devices (sensors, actuators, etc.) to the data stored in the platform.

Data mining

DCA systems should integrate capacities for the processing of the stored info, making it easier to extract useful data from the huge amount of contents that may be recorded.

Big Data

Big data is about the processing and analysis of large data repositories, so disproportionately large that it is impossible to treat them with the conventional tools of analytical databases.

- Web logs;
- RFID;
- Sensor networks;
- Social networks;
- Social data (due to the Social data revolution);
- Internet text and documents;
- Internet search indexing;
- Call detail records;
- Astronomy, atmospheric science, genomics, biogeochemical, biological, and other complex and/or interdisciplinary scientific research;
- Military surveillance;
- Medical records;
- Photography archives;
- Video archives;
- Large scale e-commerce.

Big Data

- ✓ Big data requires exceptional technologies to efficiently process large quantities of data within a tolerable amount of time.
- ✓ Technologies being applied to big data include massively parallel processing (MPP) databases, data-mining grids, distributed file systems, distributed databases, cloud computing platforms, the Internet, and scalable storage systems.
- ✓ These technologies are linked with many aspects derived from the analysis of natural phenomena such as climate and seismic data to environments such as health, safety or, of course, the business environment.
- ✓ Big data deals with unconventional, unstructured databases, which can reach petabytes, exabytes or zettabytes, and require specific treatments for their needs, either in terms of storage or processing/display.

Big Data

In future, it is expected a huge increase in adoption, and many, many questions that must be addressed. Among the imminent research targets in this field are:

- ✓ Privacy. Big data systems must avoid any suggestion that users and citizens in general perceive that their privacy is being invaded.
- ✓ Integration of both relational and NoSQL (Structured Query Language) systems.
- ✓ More efficient indexing, search and processing algorithms, allowing the extraction of results in reduced time and, ideally, near to “real time” scenarios.
- ✓ Optimised storage of data. Given the amount of information that the new IoT world may generate, it is essential to avoid that the storage requirements and costs increase exponentially.

Security for IoT

- ✓ As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important.
- ✓ IoT applications use sensors and actuators embedded in the environment and they collect large volumes of data on room temperatures, humidity, and lighting to optimize energy consumption and avoid operational failures that have a real impact on the environment.
- ✓ In the retail industry, a refrigerator failing to maintain proper cooling temperatures could place high value medical or food inventory at risk. Having all of these devices connected, it is as well needed have the right data model.
- ✓ The data model has to accommodate high data rate sensor data and to assimilate and analyze the information. In this context database read/write performance is critical, particularly with high data rate sensor data.
- ✓ The database must support high-speed read and writes, be continuously available (100% of the time) to gather this data at uniform intervals and be scalable in order to maintain a cost-effective horizontal data store over time.

Security for IoT

Advances are required in several areas to make the IoT secure from those with malicious intent, including

- ✓ DoS/DDOS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted.
- ✓ General attack detection and recovery/resilience to cope with IoT-specific threats, such as compromised nodes, malicious code hacking attacks.
- ✓ Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle of the system and assist operators to take the most appropriate protective action during attacks.
- ✓ The IoT requires a variety of access control and associated accounting schemes to support the various authorisation and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.
- ✓ The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches e.g. from machine learning, are required to lead to a self-managed IoT.

Representational State Transfer (REST)

- ✓ REST is a language and operating system independent architecture for designing network applications using simple HTTP to connect between machines. It was designed as a lightweight point-to-point, stateless client/server, cacheable protocol for simple client/server (request/reply) communications from devices to the cloud over TCP/IP.
- ✓ Use of stateless model supported by HTTP and can simplify server design and can easily be used in the presence of firewalls, but may result in the need for additional information exchange. It does not support Cookies or asynchronous, loosely coupled publish-and-subscribe message exchanges.
- ✓ Support for systems with more than a thousand nodes may result in poor performance and complexity.

Web of Things (WoT)

Definition:

The Web of Things (WoT) is a computing concept that describes a future where everyday objects are fully integrated with the Web. The prerequisite for WoT is for the "things" to have embedded computer systems that enable communication with the Web. Such smart devices would then be able to communicate with each other using existing Web standards.

Considered a subset of the Internet of Things (IoT), WoT focuses on software standards and frameworks such as REST, HTTP and URIs to create applications and services that combine and interact with a variety of network devices.

The key point is that this doesn't involve the reinvention of the means of communication because existing standards are used.

Internet of Things is more often used in the context of radiofrequency identification (RFID) and how physical objects are tied to the Internet and can communicate with each other. Both terms are difficult to define precisely, although they are related in their general theme.

Six major problems for enterprises connecting to the IoT

Walled off Internet

According to the World Economic Forum, the growing number of cross border attacks will start pushing national governments towards breaking up the internet in national, or even regional “walled gardens.” There are other pressures too that will push them to do this, including economic protectionism, regulatory divergence and the loss of government power relative to global online companies.

This will create major problems for the concept — and practice of a global IoT — leading to the erection of barriers to the flow of content and transactions. “Some might welcome a move towards a less hyper-globalized online world, but many would not, resistance would be likely, as would the rapid growth of illegal workarounds.

Cloud Attacks

Given that a large amount of the data that will run the IoT will be stored in the cloud it is likely that cloud providers will be one of the principle targets in this kind of war. While there is growing awareness of this problem, cybersecurity is still under-resourced in comparison to the potential scale of the threat. To get some kind of idea of the problem, the World Economic Forum report cites analysis that suggests that the takedown of a single cloud provider could cause $50 billion to $120 billion of economic damage

Six major problems for enterprises connecting to the IoT

AI-Built Security Issues

Although the threat magnitude of ransomware has already grown 35 times over the last year with ransomworms and other types of attacks, there is more to come.

The next big target for ransomware is likely to be cloud service providers and other commercial services with a goal of creating revenue streams.

The complex, hyperconnected networks cloud providers have developed one can produce a single point of failure for hundreds of businesses, government entities, critical infrastructures, and healthcare organizations.

The malware completely created by machines based on automated vulnerability detection and complex data analysis.

Polymorphic malware is not new, but it is about to take on a new face by leveraging AI to create sophisticated new code that can learn to evade detection through machine written routines.

Six major problems for enterprises connecting to the IoT

Botnet Problems

Millions of new connected consumer devices make a wide attack surface for hackers, who will continue to probe the connections between low-power, somewhat dumb devices and critical infrastructure.

The biggest security challenge is the creation of Distributed Destruction of Service (DDoS) attacks that employ swarms of poorly-protected consumer devices to attack public infrastructure through massively coordinated misuse of communication channels.

IoT botnets can direct enormous swarms of connected sensors like thermostats or sprinkler controllers to cause damaging and unpredictable spikes in infrastructure use, leading to things like power surges, destructive water hammer attacks, or reduced availability of critical infrastructure on a city or state-wide level.

Solutions for these attacks do exist, from smarter control software that can tell the difference between emergency and erroneous sensor data, and standards that put bounds on what data devices are allowed to send, or how often they're allowed to send it. But the challenge of securing consumer-grade sensors and devices remains, especially as they connect, in droves, to our shared infrastructure.

Six major problems for enterprises connecting to the IoT

Lack of Confidence

Amsterdam, Netherlands-based Gemalto is a cybersecurity firm that has researched the impact of security on the development of the IoT. It found that that 90 percent of consumers lack confidence in the security of Internet of Things devices.

This comes as more than two-thirds of consumers and almost 80% of organizations support governments getting involved in setting IoT security. In fact its recent State of IoT Security research report, released at the end of October showed the following data.

- ✓ 96 percent of businesses and 90 percent of consumers believe there should be IoT security regulations
- ✓ 54 percent of consumers own an average of four IoT devices, but only 14 percent believe that they are knowledgeable on IoT device security
- ✓ 65 percent of consumers are concerned about a hacker controlling their IoT device, while 60 percent are concerned about data being leaked

"It's clear that both consumers and businesses have serious concerns around IoT security and little confidence that IoT service providers and device manufacturers will be able to protect IoT devices and more importantly the integrity of the data created, stored and transmitted by these devices,“.

"Until there is confidence in IoT amongst businesses and consumers, it won't see mainstream adoption,”.

Six major problems for enterprises connecting to the IoT

Understanding IoT

In 2018, the real issue is how to increase the ability for people to understand the changes and their implications more clearly, and to take concrete actions to take advantage of the potential upside. "The pace of change has exceeded the rate of human capability to absorb — the cup is already full,“.

Internet of Things is moving into it’s adolescence as connected devices become smarter and more immersive, and expectations to convert IoT data to insights and financial value increase. Also, algorithms and data visualization templates have evolved so that new use cases can take advantage of earlier ones. The exponential adoption of IoT will drive down sensor and acquisition costs, enabling more and more viable business cases that have previously been too expensive.

Important Questions

Q #1) What is a simple definition of IoT?

Answer: IoT or Internet of Things is a network of connected devices that interact and exchange information with each other. The technology allows connection of two or more devices that connect with each other and sending and receiving information through the internet.

Q #2) What are some of the applications of IoT technology?

Answer: IoT based technologies have a lot of different applications. The technologies are used in process automation, home automation, smart cars, decision analytics, and smart grids. The list of IoT applications will grow as the technology evolves in the years ahead.

Q #3) How do IoT devices communicate with each other?

Answer: An IoT device is connected through an IP network to the internet. The devices connect to the net either through Ethernet — wired or wireless — or Bluetooth.

Q #4) Is there any difference between IoT and machine to machine (M2M)?

Answer: M2M entails the transfer of information from one device to another. The term basically refers to point-to-point communication between the two devices.

In contrast, IoT is a broader term that refers to a network of connected devices supporting data integration with a specific application. It involves multi-level communication and flexible responses.

Q #5) What is the Future of IoT Technology?

Answer: The applications of IoT looks promising in the years ahead. IoT technologies will likely be used with other technological trends like artificial intelligence (AI) and automated things to deliver integrated smart solutions. The integration of technologies will create disruptions in different industries driving new opportunities.