# Saving Sensor Data Into a Text File

CSE315

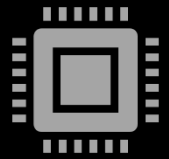
Peripheral And Interfacing

Created By:

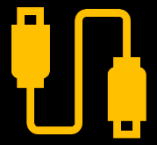
Alma Tanjin-18101088

Sk. Yeasin Kabir Joy-18101020

What is SD?

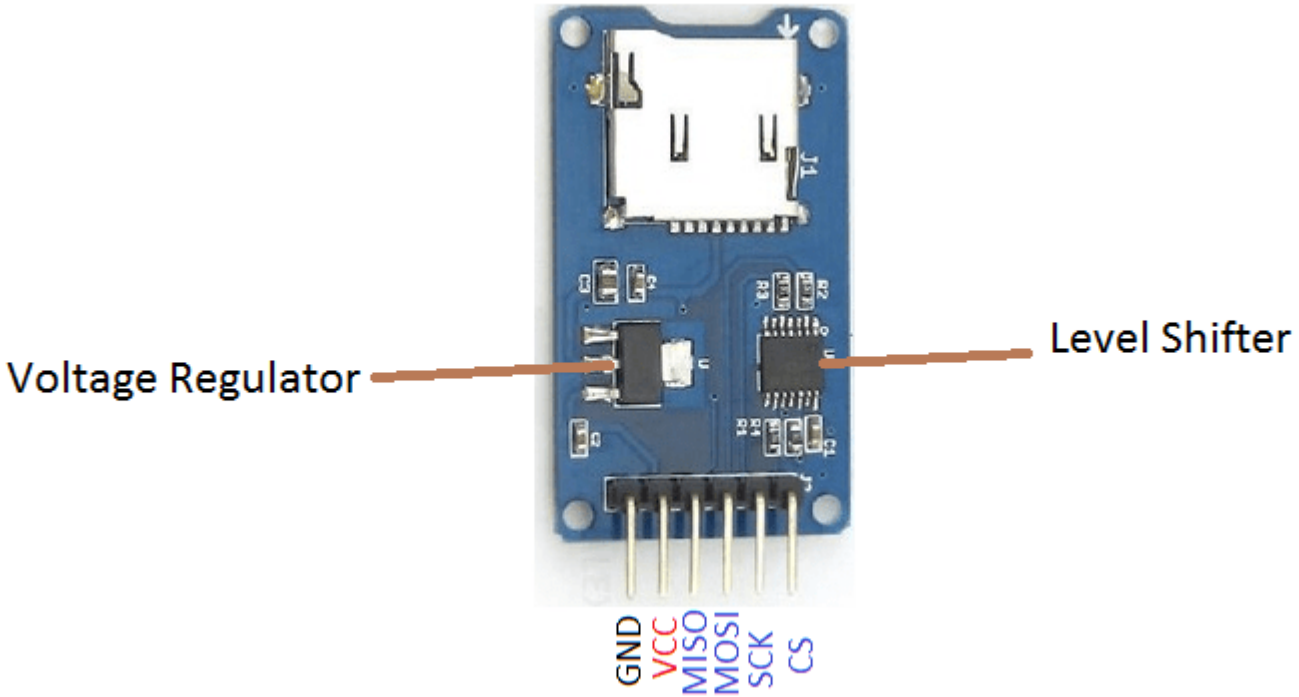


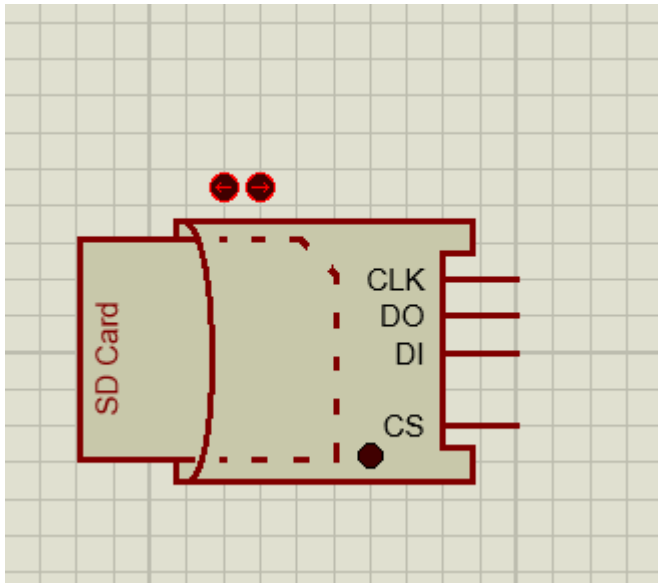
The **SD** modules allow you to communicate with the **memory card** and write or read the information on them.



The communication between the Arduino and the SD card uses SPI which takes place on digital pins 11, 12, and 13, Additionally, another pin must be used to select the SD card. This can be the hardware SS pin – pin 10

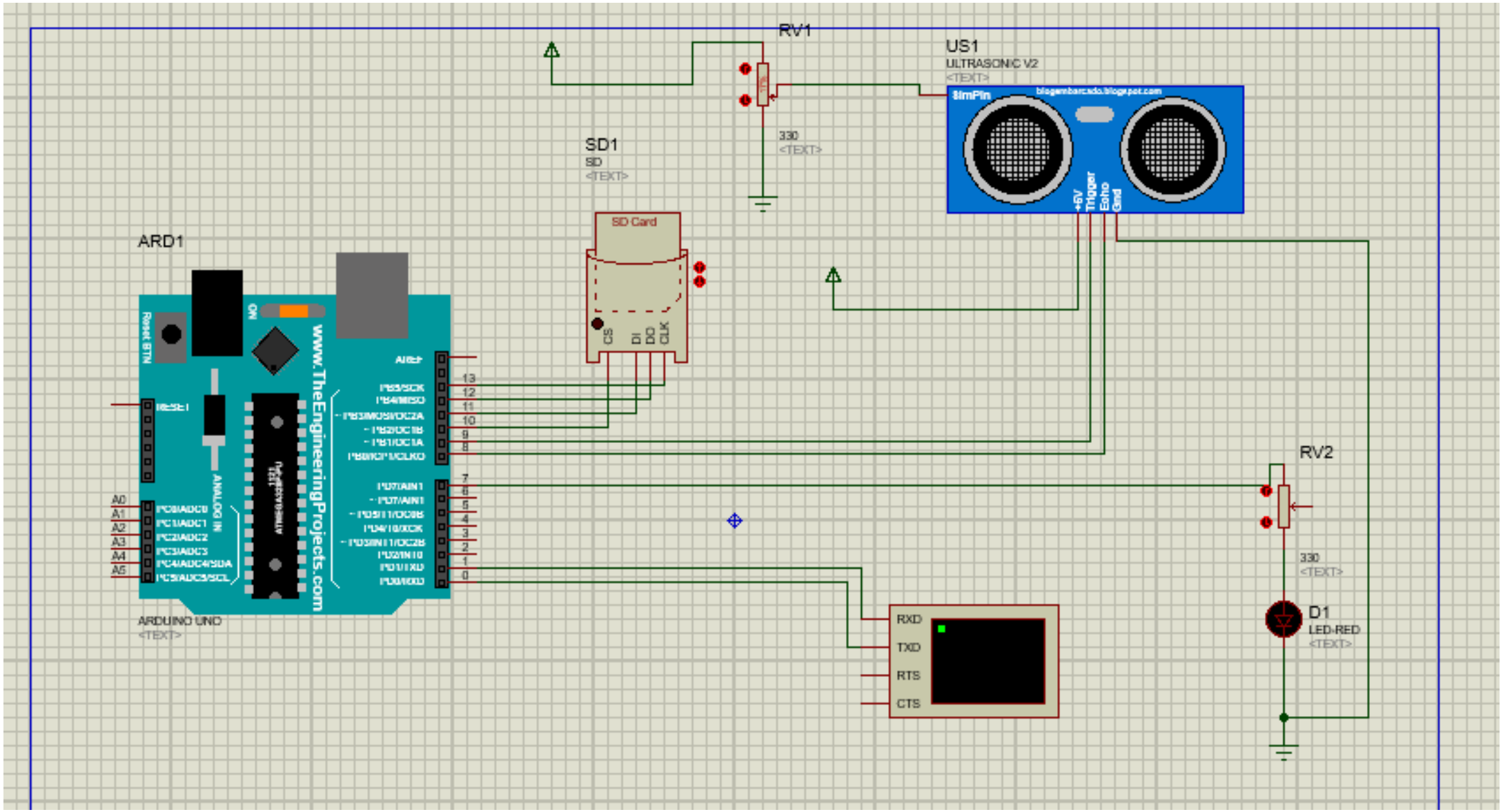
# Pin Configuration:



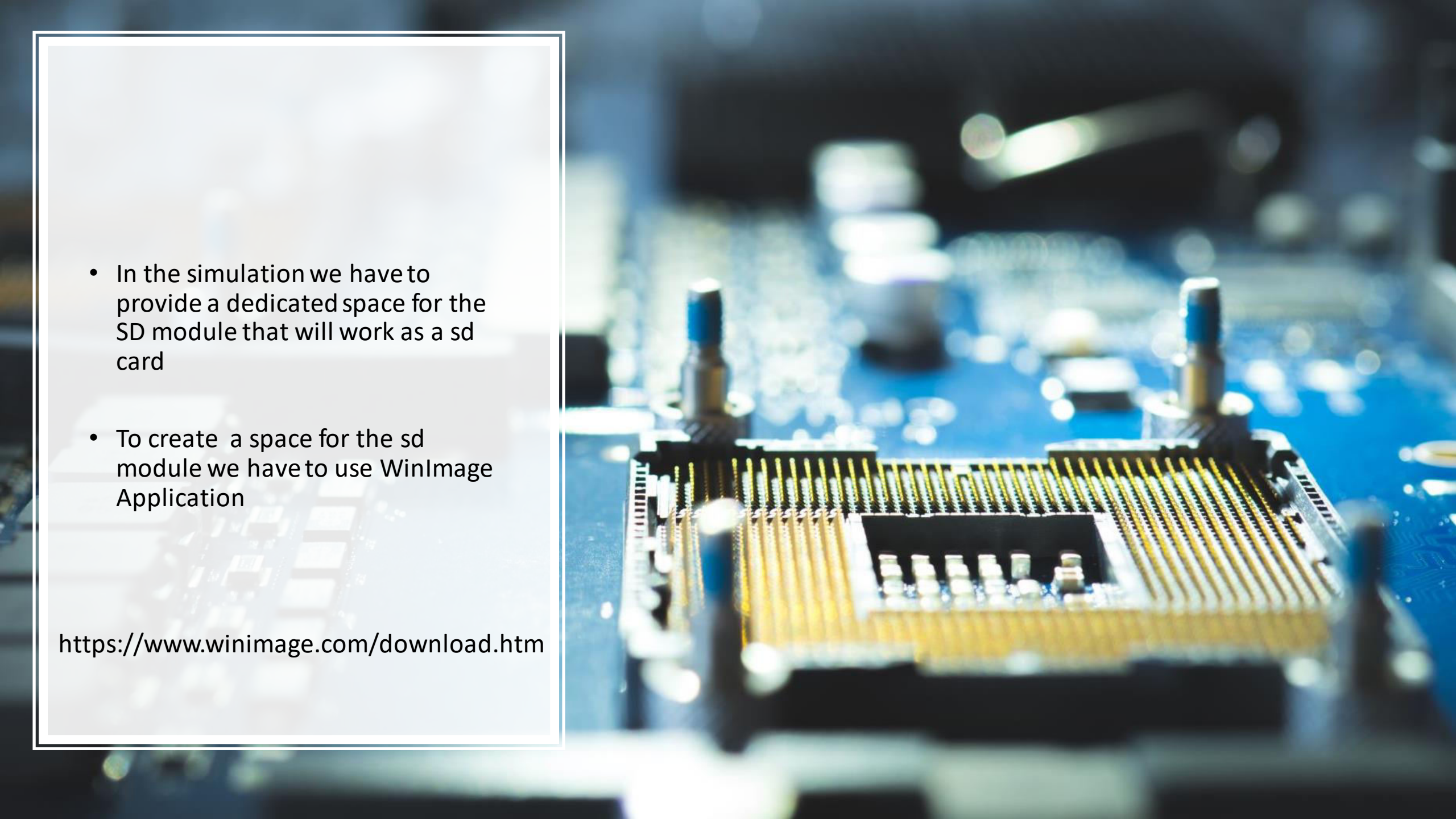



# Required Components:

- Arduino Uno
- Sonar Sensor
- SD Card Module
- LED
- POT
- POT HG
- Virtual Terminal


RV1
US1
ULTRASONIC V2
<TEXT>
SimPin
blogembarcado.blogspot.com
+5V
Trigger
Echo
Gnd
330
<TEXT>
SD1
SD
<TEXT>
SD Card
CS
DI
DO
CLK
ARD1
Reset BTN
ON
ANALOG IN
www.TheEngineeringProjects.com
A0
A1
A2
A3
A4
A5
13
12
11
10
9
8
7
6
5
4
3
2
1
0
RXD
TXD
RTS
CTS
RV2
330
<TEXT>
D1
LED-RED
<TEXT>
ARDUINO UNO
<TEXT>

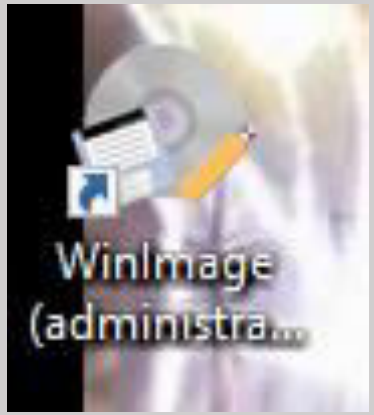
```
#include<SPI.h>
#include <SD.h>

const int trigPin = 9;
const int echoPin  = 8;
const int led = 7;
void setup(){
Serial.begin (9600);
pinMode(trigPin, OUTPUT);
pinMode(echoPin, INPUT);
pinMode(led, OUTPUT);
if (!SD.begin(10)) {
    Serial.println("initialization failed!");
    while (1);
  }
  Serial.println("initialization done.");
  delay(2000);
}
File myFile;
uint16_t line = 1;

void loop()
{

long duration, distance;
digitalWrite(trigPin, LOW);
delayMicroseconds(2);
digitalWrite(trigPin, HIGH);
delayMicroseconds(10);
digitalWrite(trigPin, LOW);
duration = pulseIn(echoPin, HIGH);
distance = (duration/2) * 0.034;

myFile = SD.open("test.txt", FILE_WRITE);

if (myFile) {
    Serial.print(line);
    Serial.print(":    Distance = ");
    Serial.println(distance);
    // Write data to SD card file (sensorData.txt)
    myFile.print(line++);
    myFile.print(":    Distance = ");
    myFile.println(distance);
    myFile.close();
    delay(500);
  }
else{
  Serial.println("no");
  }

if (distance < 10)
{
digitalWrite(led,HIGH);
}
else {
digitalWrite(led,LOW);
}
}
```



- In the simulation we have to provide a dedicated space for the SD module that will work as a sd card

- To create  a space for the sd module we have to use WinImage Application

https://www.winimage.com/download.htm




WinImage (unregistered)

File Image Disk Options Upgrade Help

New... Ctrl+N
Open... Ctrl+O
Close image
Save Ctrl+S
Save As...
Save as Text/HTML...

Print...
Configure Printer...

Batch Assistant...
Batch Assistant wizard...
Create Self-Extracting file...

1 C:\Users\Yeasin Kabir Joy\Desktop\sd.IMA
2 C:\Users\Yeasin Kabir Joy\Desktop\sd - Copy.IMA
3 C:\Users\Yeasin Kabir Joy\Desktop\sd1.imz
4 C:\Users\Yeasin Kabir Joy\Desktop\arduinoSD.imz
5 C:\Users\Yeasin Kabir Joy\Desktop\fhgfhg.mmc

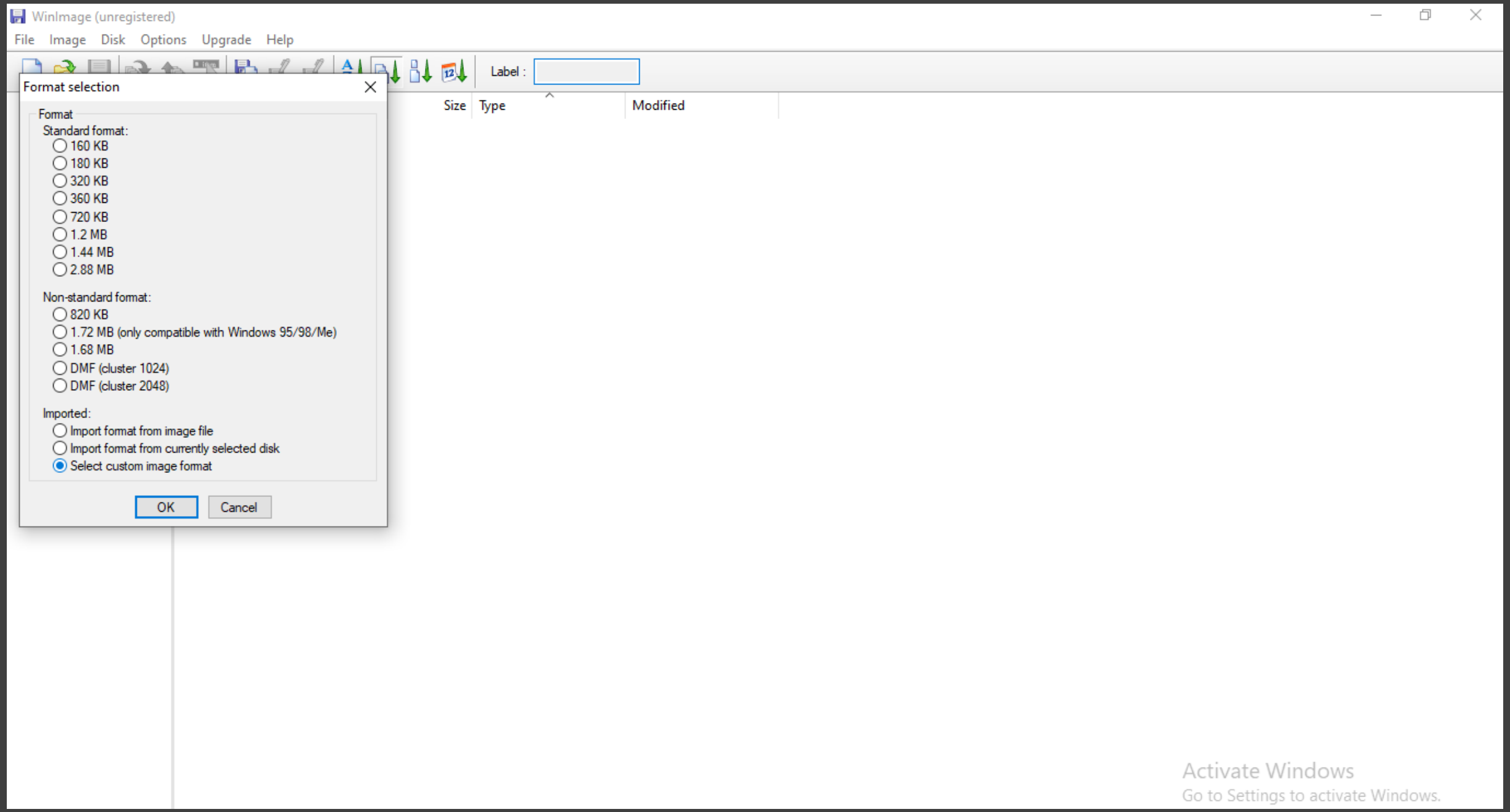
Exit Alt+F4

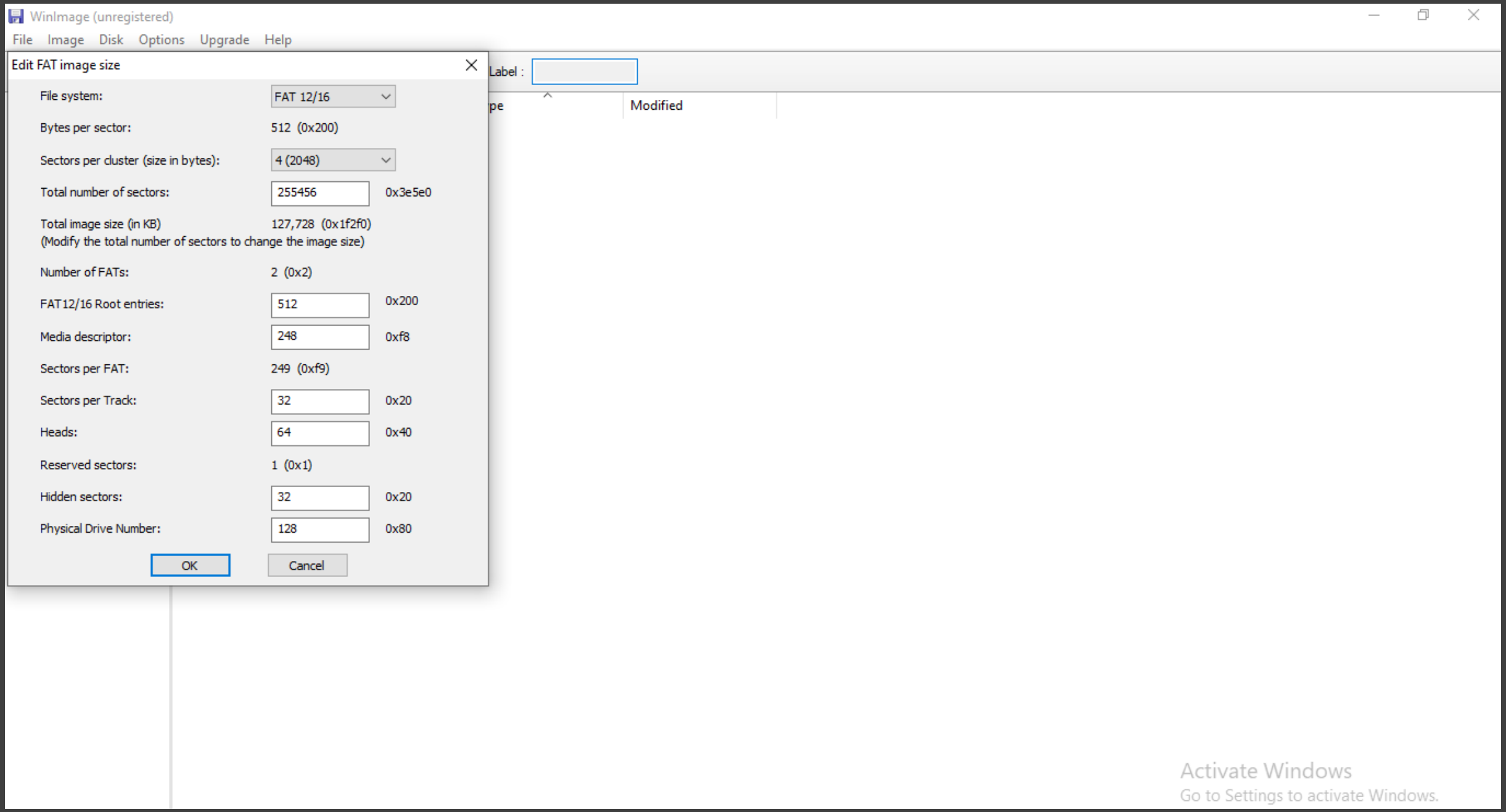
Label :

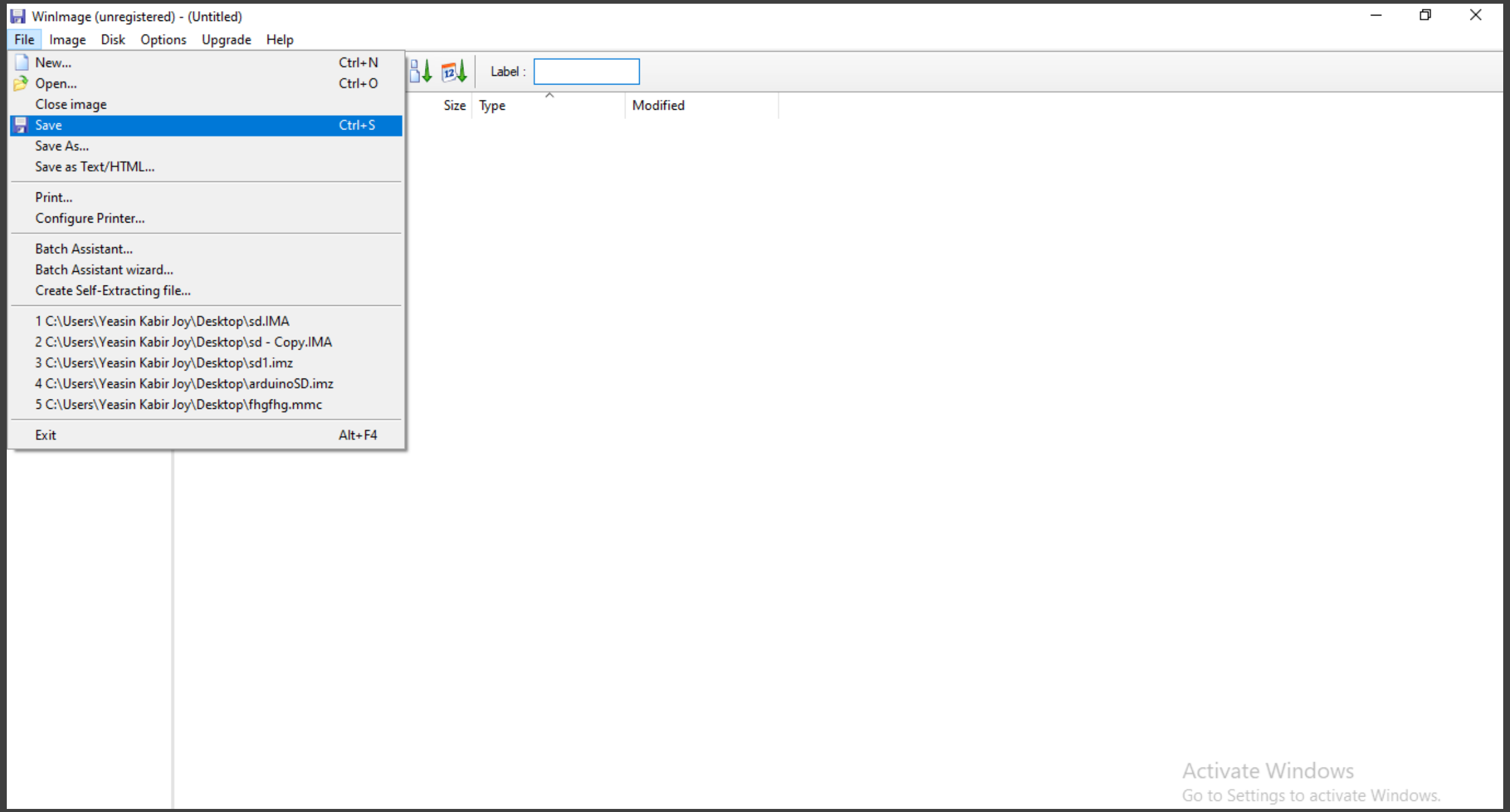
Size Type Modified

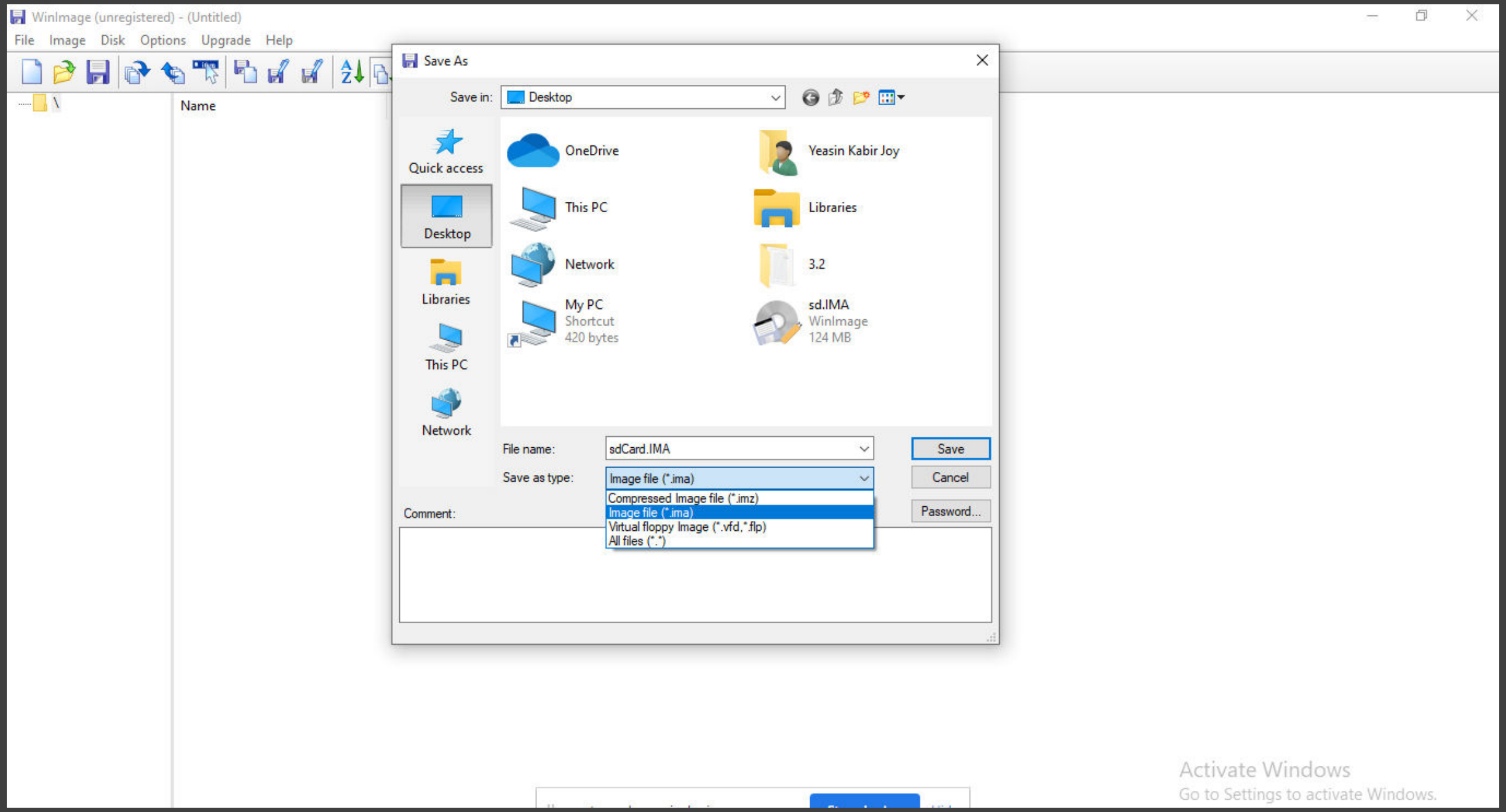
Activate Windows
Go to Settings to activate Windows.

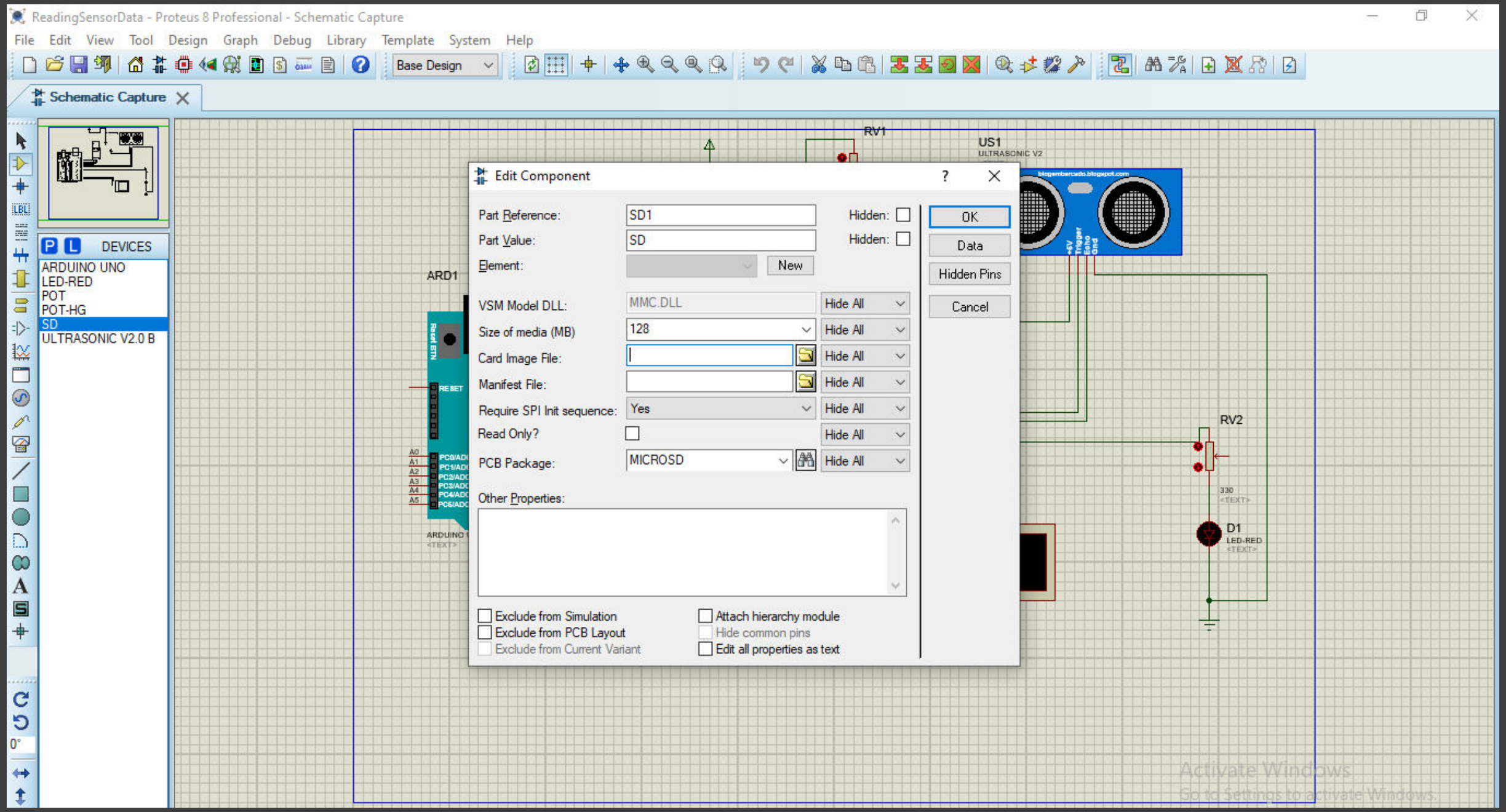
Create new image

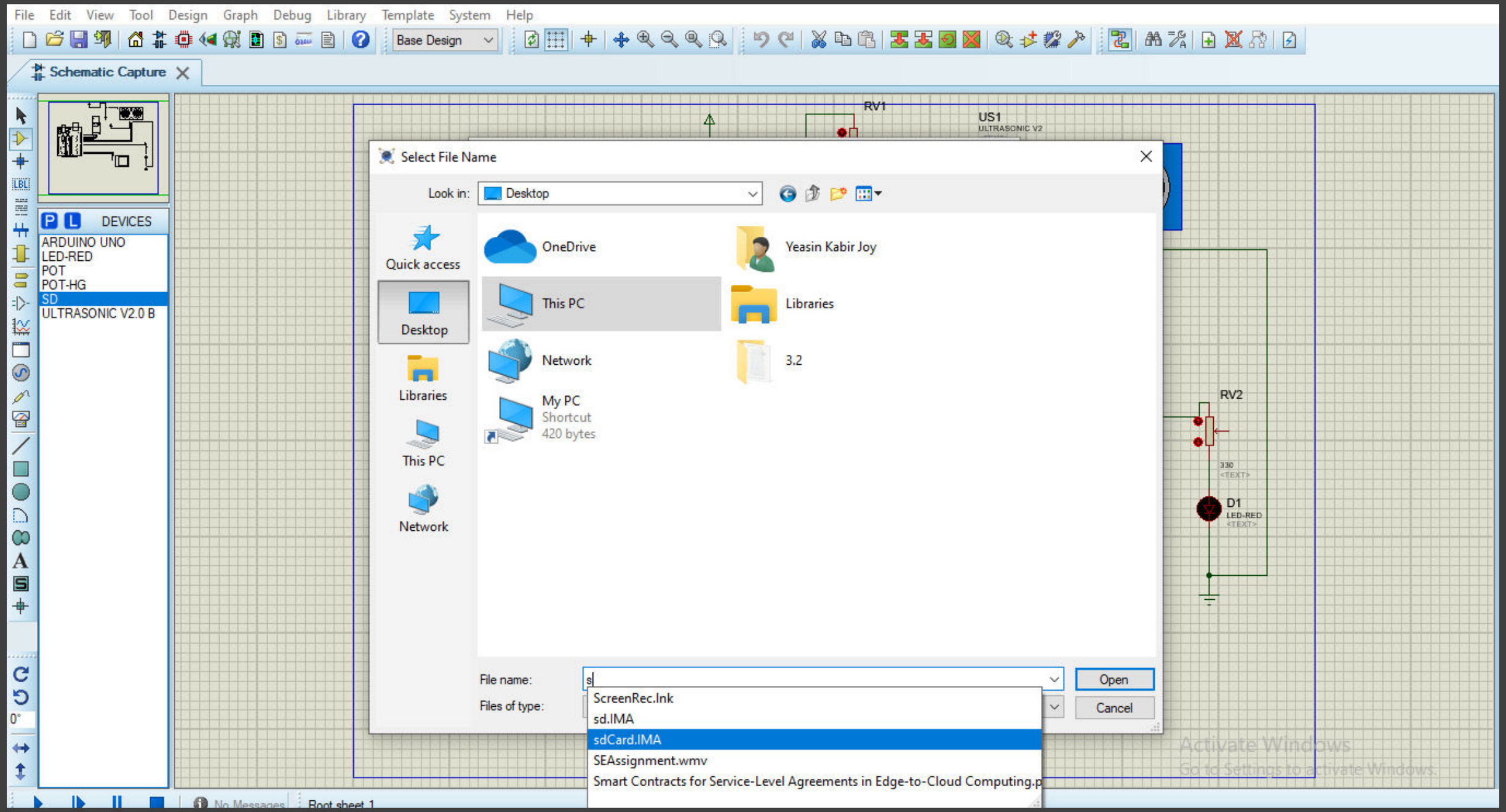

WinImage (unregistered)
File Image Disk Options Upgrade Help
Label :
Size Type Modified
Format selection
Format
Standard format:
160 KB
180 KB
320 KB
360 KB
720 KB
1.2 MB
1.44 MB
2.88 MB
Non-standard format:
820 KB
1.72 MB (only compatible with Windows 95/98/Me)
1.68 MB
DMF (cluster 1024)
DMF (cluster 2048)
Imported:
Import format from image file
Import format from currently selected disk
Select custom image format
OK
Cancel
Activate Windows
Go to Settings to activate Windows.

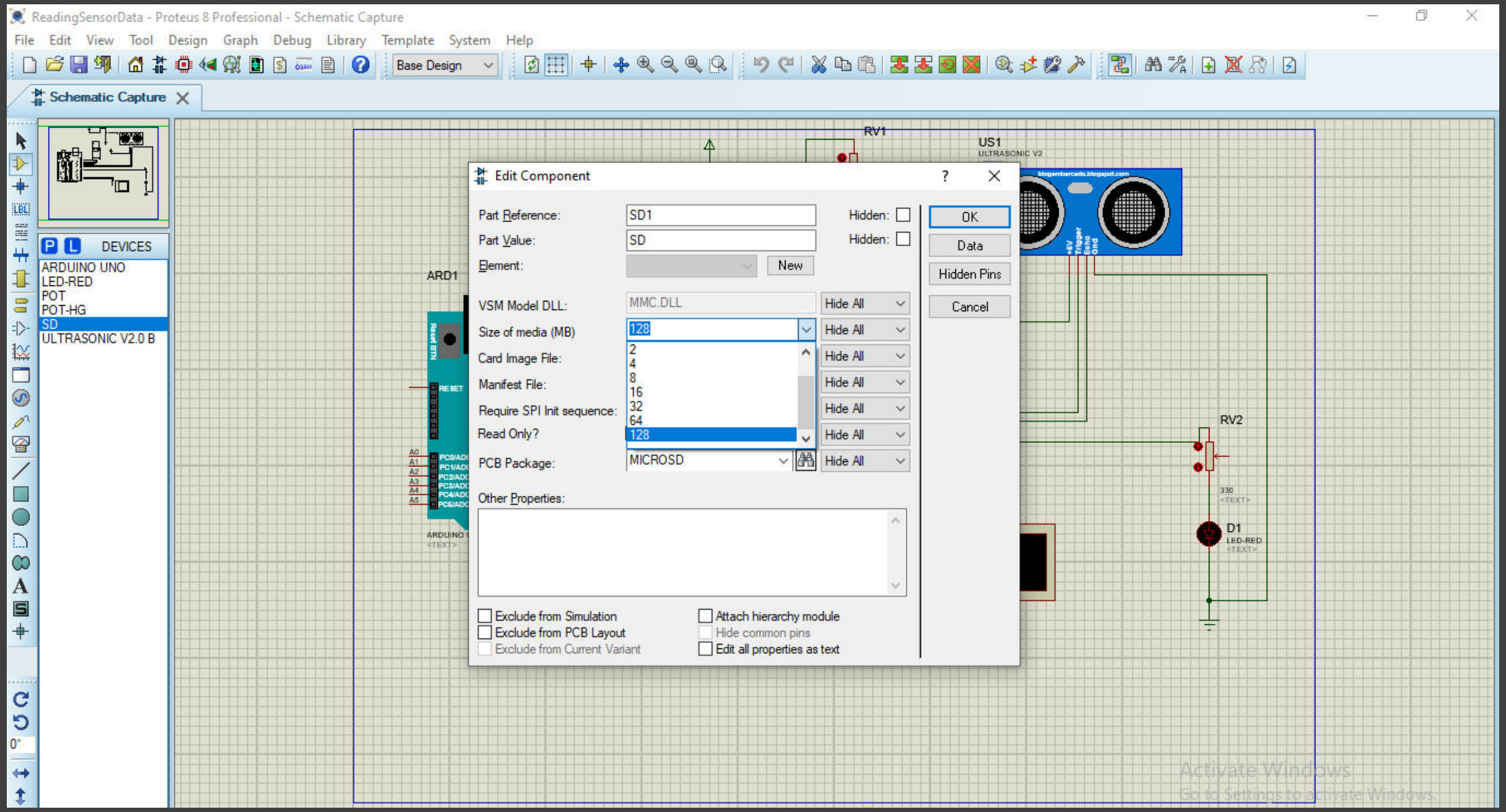

WinImage (unregistered)
File Image Disk Options Upgrade Help
Label :
pe
Modified
Edit FAT image size
File system:
FAT 12/16
Bytes per sector:
512 (0x200)
Sectors per cluster (size in bytes):
4 (2048)
Total number of sectors:
255456
0x3e5e0
Total image size (in KB)
127,728 (0x1f2f0)
(Modify the total number of sectors to change the image size)
Number of FATs:
2 (0x2)
FAT12/16 Root entries:
512
0x200
Media descriptor:
248
0xf8
Sectors per FAT:
249 (0xf9)
Sectors per Track:
32
0x20
Heads:
64
0x40
Reserved sectors:
1 (0x1)
Hidden sectors:
32
0x20
Physical Drive Number:
128
0x80
OK
Cancel
Activate Windows
Go to Settings to activate Windows.

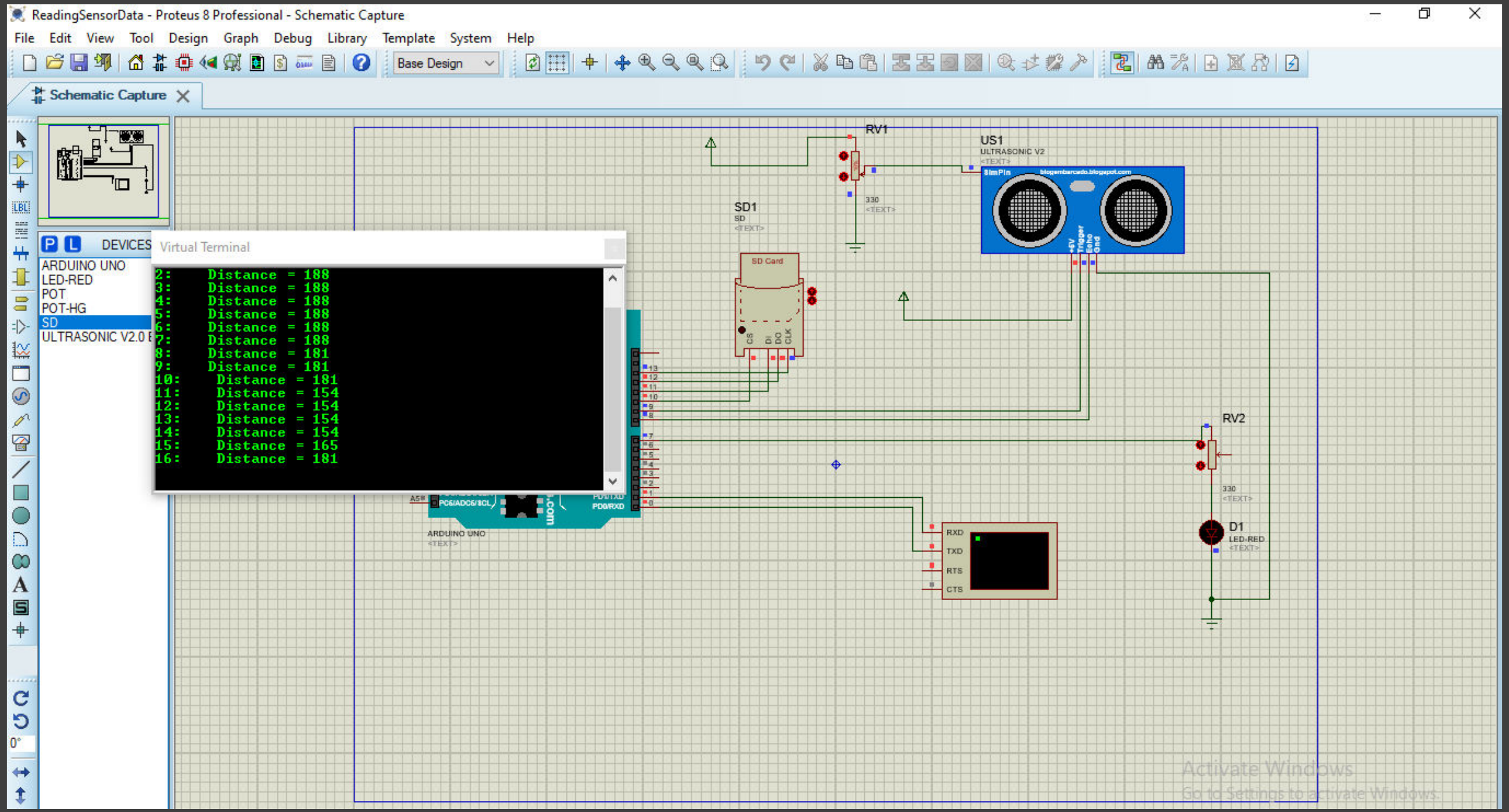

WinImage (unregistered) - (Untitled)
File
Image
Disk
Options
Upgrade
Help
New... Ctrl+N
Open... Ctrl+O
Close image
Save Ctrl+S
Save As...
Save as Text/HTML...
Print...
Configure Printer...
Batch Assistant...
Batch Assistant wizard...
Create Self-Extracting file...
1 C:\Users\Yeasin Kabir Joy\Desktop\sd.IMA
2 C:\Users\Yeasin Kabir Joy\Desktop\sd - Copy.IMA
3 C:\Users\Yeasin Kabir Joy\Desktop\sd1.imz
4 C:\Users\Yeasin Kabir Joy\Desktop\arduinoSD.imz
5 C:\Users\Yeasin Kabir Joy\Desktop\fhgfhg.mmc
Exit Alt+F4
Label :
Size
Type
Modified
Activate Windows
Go to Settings to activate Windows.

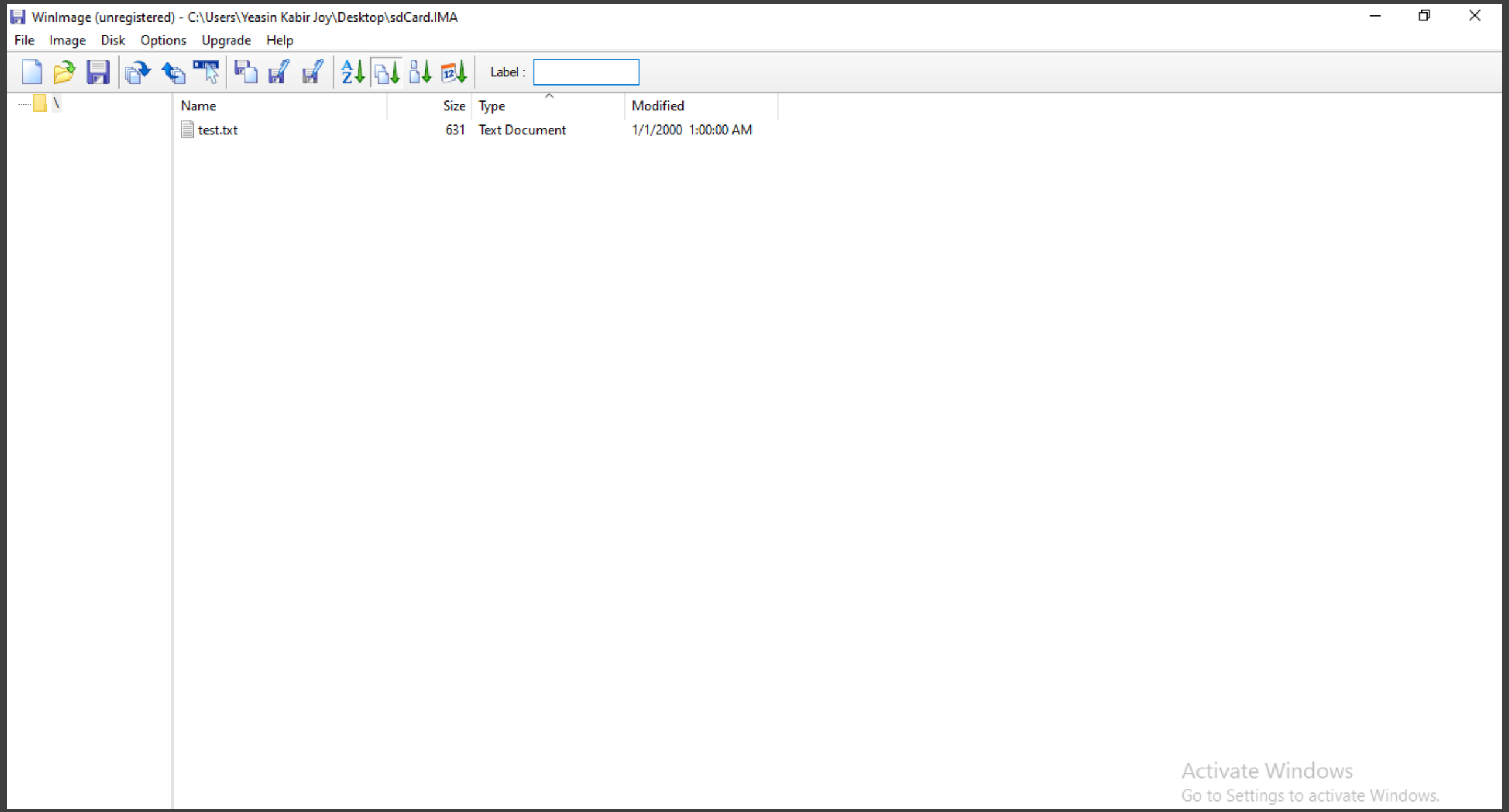

WinImage (unregistered) - (Untitled)
File Image Disk Options Upgrade Help
Name
Save As
Save in: Desktop
Quick access
Desktop
Libraries
This PC
Network
OneDrive
This PC
Network
My PC
Shortcut
420 bytes
Yeasin Kabir Joy
Libraries
3.2
sd.IMA
WinImage
124 MB
File name: sdCard.IMA
Save as type: Image file (*.ima)
Compressed Image file (*.imz)
Image file (*.ima)
Virtual floppy Image (*.vfd,*.flp)
All files (*.*)
Save
Cancel
Password...
Comment:
Activate Windows
Go to Settings to activate Windows.

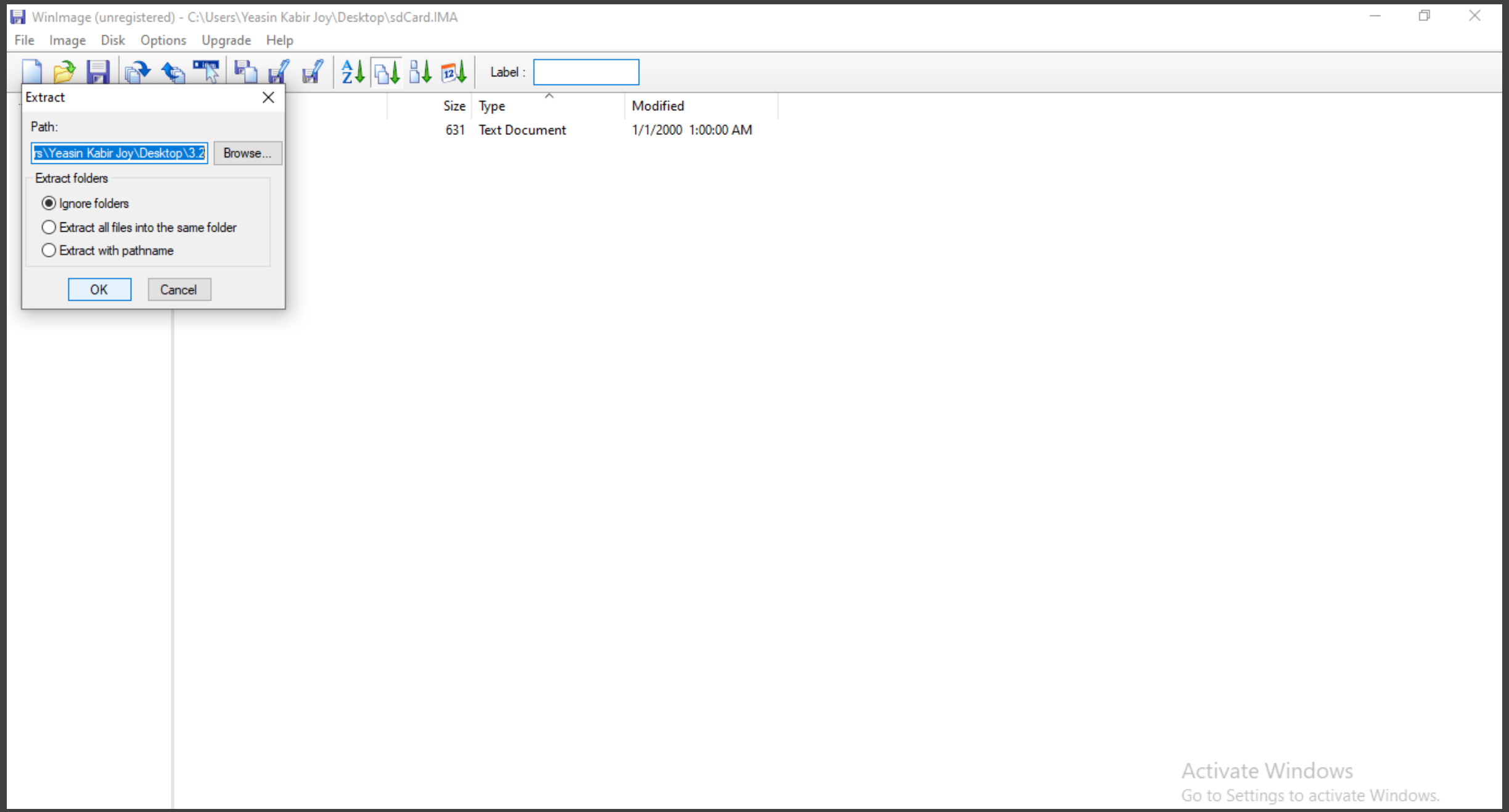

ReadingSensorData - Proteus 8 Professional - Schematic Capture
File Edit View Tool Design Graph Debug Library Template System Help
Base Design
Schematic Capture
DEVICES
ARDUINO UNO
LED-RED
POT
POT-HG
SD
ULTRASONIC V2.0 B
RV1
US1
ULTRASONIC V2
ARD1
RV2
330
D1
LED-RED
Edit Component
Part Reference:
SD1
Hidden:
Part Value:
SD
Hidden:
Element:
New
VSM Model DLL:
MMC.DLL
Hide All
Size of media (MB):
128
Hide All
Card Image File:
Hide All
Manifest File:
Hide All
Require SPI Init sequence:
Yes
Hide All
Read Only?
Hide All
PCB Package:
MICROSD
Hide All
Other Properties:
Exclude from Simulation
Exclude from PCB Layout
Exclude from Current Variant
Attach hierarchy module
Hide common pins
Edit all properties as text
OK
Data
Hidden Pins
Cancel
Activate Windows
Go to Settings to activate Windows.


File Edit View Tool Design Graph Debug Library Template System Help
Base Design
Schematic Capture
DEVICES
ARDUINO UNO
LED-RED
POT
POT-HG
SD
ULTRASONIC V2.0 B
RV1
US1
ULTRASONIC V2
RV2
330
D1
LED-RED
Select File Name
Look in:
Desktop
Quick access
Desktop
Libraries
This PC
Network
OneDrive
This PC
Network
My PC
Shortcut
420 bytes
Yeasin Kabir Joy
Libraries
3.2
File name:
s
Files of type:
Open
Cancel
ScreenRec.lnk
sd.IMA
sdCard.IMA
SEAssignment.wmv
Smart Contracts for Service-Level Agreements in Edge-to-Cloud Computing.p
Activate Windows
Go to Settings to activate Windows.
No Messages
Root sheet 1


ReadingSensorData - Proteus 8 Professional - Schematic Capture
File Edit View Tool Design Graph Debug Library Template System Help
Base Design
Schematic Capture
DEVICES
ARDUINO UNO
LED-RED
POT
POT-HG
SD
ULTRASONIC V2.0 B
RV1
US1
ULTRASONIC V2
ARD1
RV2
330
D1
LED-RED
Edit Component
Part Reference:
SD1
Hidden:
Part Value:
SD
Hidden:
Element:
New
VSM Model DLL:
MMC.DLL
Hide All
Size of media (MB)
128
Hide All
Card Image File:
Hide All
Manifest File:
Hide All
Require SPI Init sequence:
Hide All
Read Only?
Hide All
PCB Package:
MICROSD
Hide All
Other Properties:
OK
Data
Hidden Pins
Cancel
2
4
8
16
32
64
128
Exclude from Simulation
Exclude from PCB Layout
Exclude from Current Variant
Attach hierarchy module
Hide common pins
Edit all properties as text
Activate Windows
Go to Settings to activate Windows.


ReadingSensorData - Proteus 8 Professional - Schematic Capture
File Edit View Tool Design Graph Debug Library Template System Help
Base Design
Schematic Capture
DEVICES
ARDUINO UNO
LED-RED
POT
POT-HG
SD
ULTRASONIC V2.0
Virtual Terminal
2: Distance = 188
3: Distance = 188
4: Distance = 188
5: Distance = 188
6: Distance = 188
7: Distance = 188
8: Distance = 181
9: Distance = 181
10: Distance = 181
11: Distance = 154
12: Distance = 154
13: Distance = 154
14: Distance = 154
15: Distance = 165
16: Distance = 181
RV1
330
SD1
SD
SD Card
US1
ULTRASONIC V2
RV2
D1
LED-RED
ARDUINO UNO
RXD
TXD
RTS
CTS
Activate Windows
Go to Settings to activate Windows.


WinImage (unregistered) - C:\Users\Yeasin Kabir Joy\Desktop\sdCard.IMA
File Image Disk Options Upgrade Help
Label :
\
Name Size Type Modified
test.txt 631 Text Document 1/1/2000 1:00:00 AM
Activate Windows
Go to Settings to activate Windows.


WinImage (unregistered) - C:\Users\Yeasin Kabir Joy\Desktop\sdCard.IMA
File Image Disk Options Upgrade Help
Label :
Size Type Modified
631 Text Document 1/1/2000 1:00:00 AM
Extract
Path:
rs\Yeasin Kabir Joy\Desktop\3.2
Browse...
Extract folders
Ignore folders
Extract all files into the same folder
Extract with pathname
OK
Cancel
Activate Windows
Go to Settings to activate Windows.

WinImage (unregistered) - C:\Users\Yeasin Kabir Joy\Desktop\sdCard.IMA

File Image Disk Options Upgrade Help

\

Name

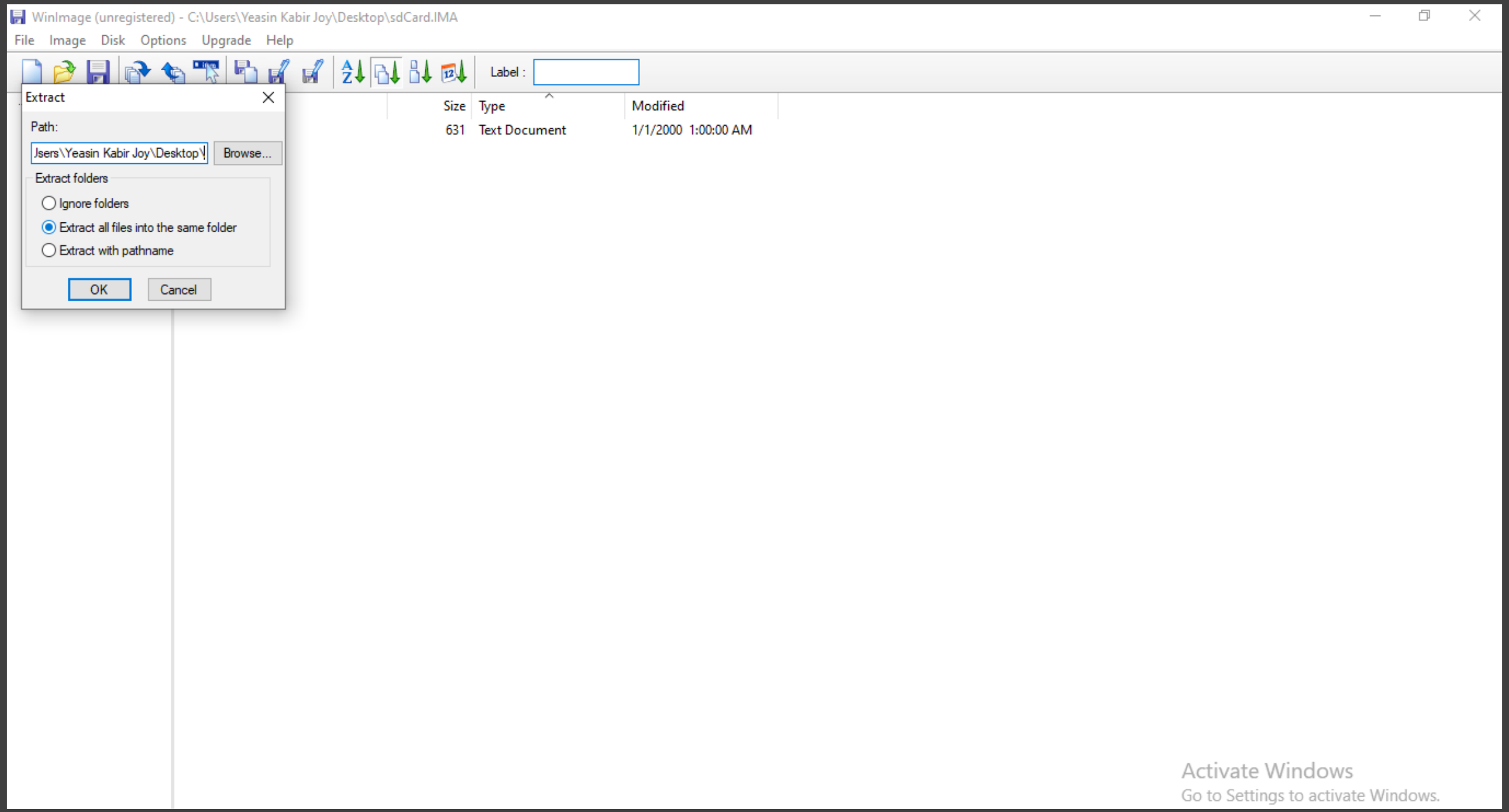
test.txt

test.txt - Notepad

File Edit Format View Help

```
8:     Distance = 181
9:     Distance = 181
10:     Distance = 181
11:     Distance = 154
12:     Distance = 154
13:     Distance = 154
14:     Distance = 154
15:     Distance = 165
16:     Distance = 181
17:     Distance = 181
18:     Distance = 188
19:     Distance = 188
20:     Distance = 188
21:     Distance = 188
22:     Distance = 165
23:     Distance = 133
24:     Distance = 103
25:     Distance = 65
26:     Distance = 65
27:     Distance = 65
28:     Distance = 65
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8


WinImage (unregistered) - C:\Users\Yeasin Kabir Joy\Desktop\sdCard.IMA
File Image Disk Options Upgrade Help
Label :
Size Type Modified
631 Text Document 1/1/2000 1:00:00 AM
Extract
Path:
Jsers\Yeasin Kabir Joy\Desktop\
Browse...
Extract folders
Ignore folders
Extract all files into the same folder
Extract with pathname
OK
Cancel
Activate Windows
Go to Settings to activate Windows.

Thank You!!

# Wifi Module
# ESP-8266

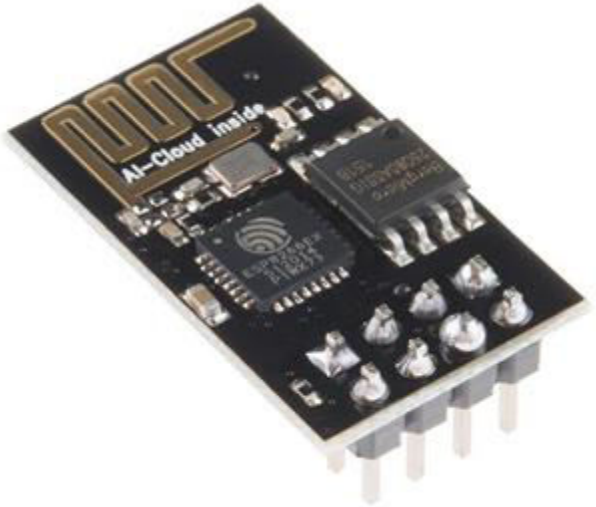
# What and Why Esp_8266

## WHAT is ESp8266

- The ESP8266 is a low-cost WiFi microchip, with a full TCP/IP stack and microcontroller capability.
- It has 32 bit microcontroller.
- 32 kib instruction RAM.
- Voltage range is 3.3V-3.6V
- Wi-Fi version is 802.11b/g/n

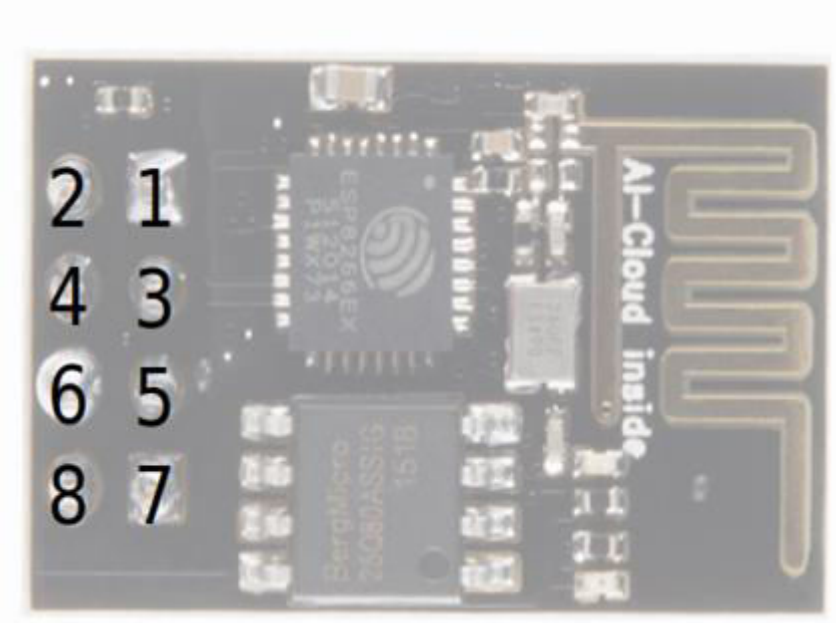
## Why Esp8266

- We can use Ethernet shield but it needs a RJ45 connection to be connected to a router via CAT cables.
- Esp8266 is cheaper than Ethernet shield.


AI-Cloud inside


AH1441
25Q41BT
E5N257

# Pin Config of Esp_8266




1-GND

2-TX

3.GPIO2

4-CHPD

5-GPIO0

6-RESET

7-RX

8-VCC

# AT commands

AT-Attention

AT+RST-Reset the board

AT+GMR-Firmware version

AT+CWMODE-Operating Mode

1.Client

2.Access point

3.Client and Access Point

AT+CWJAP=<wifi name><password> - Join network

AT+CWLAP- View available network

AT+CWQAP - Disconnect from network

AT+CWLIF - Show assigned IP address as access point

AT+CIFSR- Show assigned IP address when connected to network

AT+CIPCLOSE - Close socket connection

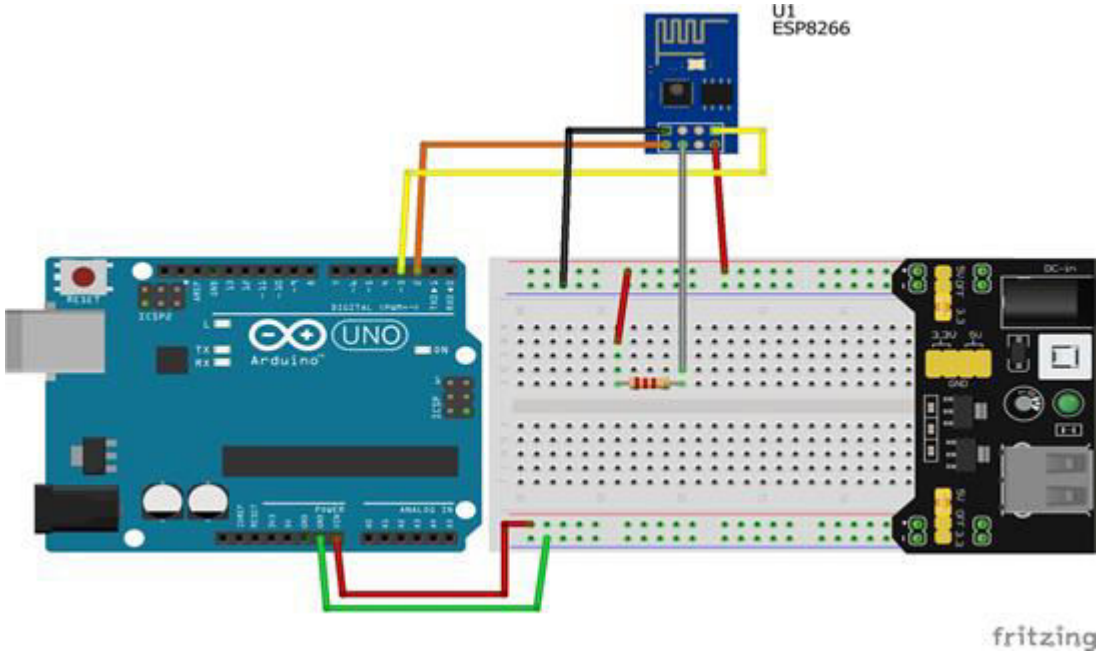
AT+CIPSTATUS - Show current status as socket client or server

# Components

1. Arduino Uno
2. ESP8266 ESP-01
3. Breadboard
4. SparkFun Breadboard Power Supply Stick - 5V/3.3V
5. Male/Female jumper wire
6. Resistor 1k ohm

# Connecting Esp_8266 to the internet using Arduino Uno

Step 1: Connection establishment between Esp and Arduino



# Connecting Esp_8266 to the internet using Arduino Uno

Step 2 : Uploading the code into  Arduino

```
#include <SoftwareSerial.h>
SoftwareSerial ESPserial(2,3); // RX | TX

void setup()
{
    Serial.begin(115200);     // communication with the host computer
    //while (!Serial)   { ; }

    // Start the software serial for communication with the ESP8266
    ESPserial.begin(115200);

    Serial.println("");
    Serial.println("Remember to to set Both NL & CR in the serial monitor.");
    Serial.println("Ready");
    Serial.println("");
}

void loop()
{
    // listen for communication from the ESP8266 and then write it to the serial monitor
    if ( ESPserial.available() )   {  Serial.write( ESPserial.read() );  }

    // listen for user input and send it to the ESP8266
    if ( Serial.available() )       {  ESPserial.write( Serial.read() );  }
}
```

# Connecting Esp_8266 to the internet using Arduino Uno

Step 3: AT commands

Command =AT

# Connecting Esp_8266 to the internet using Arduino Uno

Command= AT+UART_DEF=9600,8,1,0,0

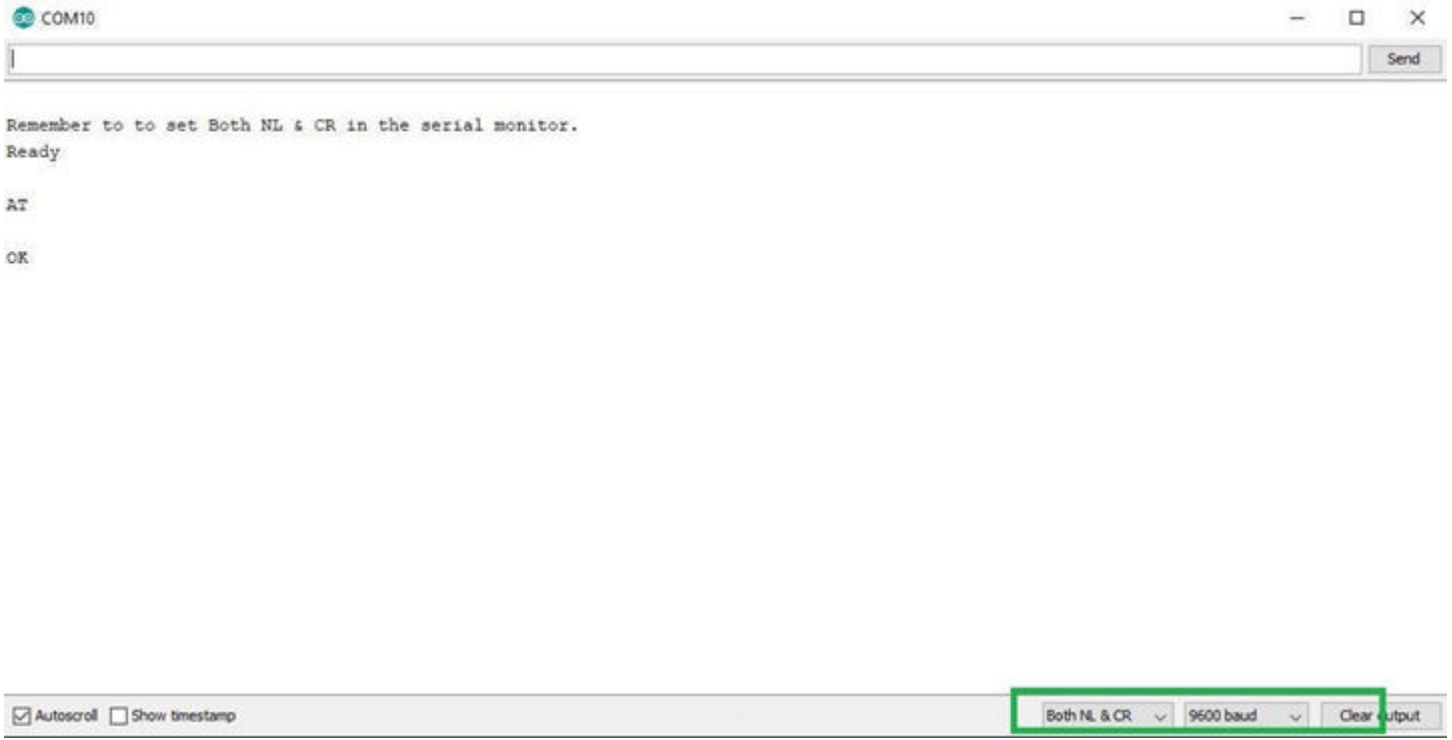
# Connecting Esp_8266 to the internet using Arduino Uno

Change bouth rate to 9600 in Code and upload it again

```
void setup()
{
    Serial.begin(115200);     // communication with the host computer
    //while (!Serial)   { ; }

    // Start the software serial for communication with the ESP8266
    ESPserial.begin(115200);

    Serial.println("");
    Serial.println("Remember to to set Both NL & CR in the serial monitor.");
```

# Connecting Esp_8266 to the internet using Arduino Uno

Close and serial monitor and give Command =AT



# Connecting Esp_8266 to the internet using Arduino Uno

Command: AT+CWMODE=1

# Connecting Esp_8266 to the internet using Arduino Uno

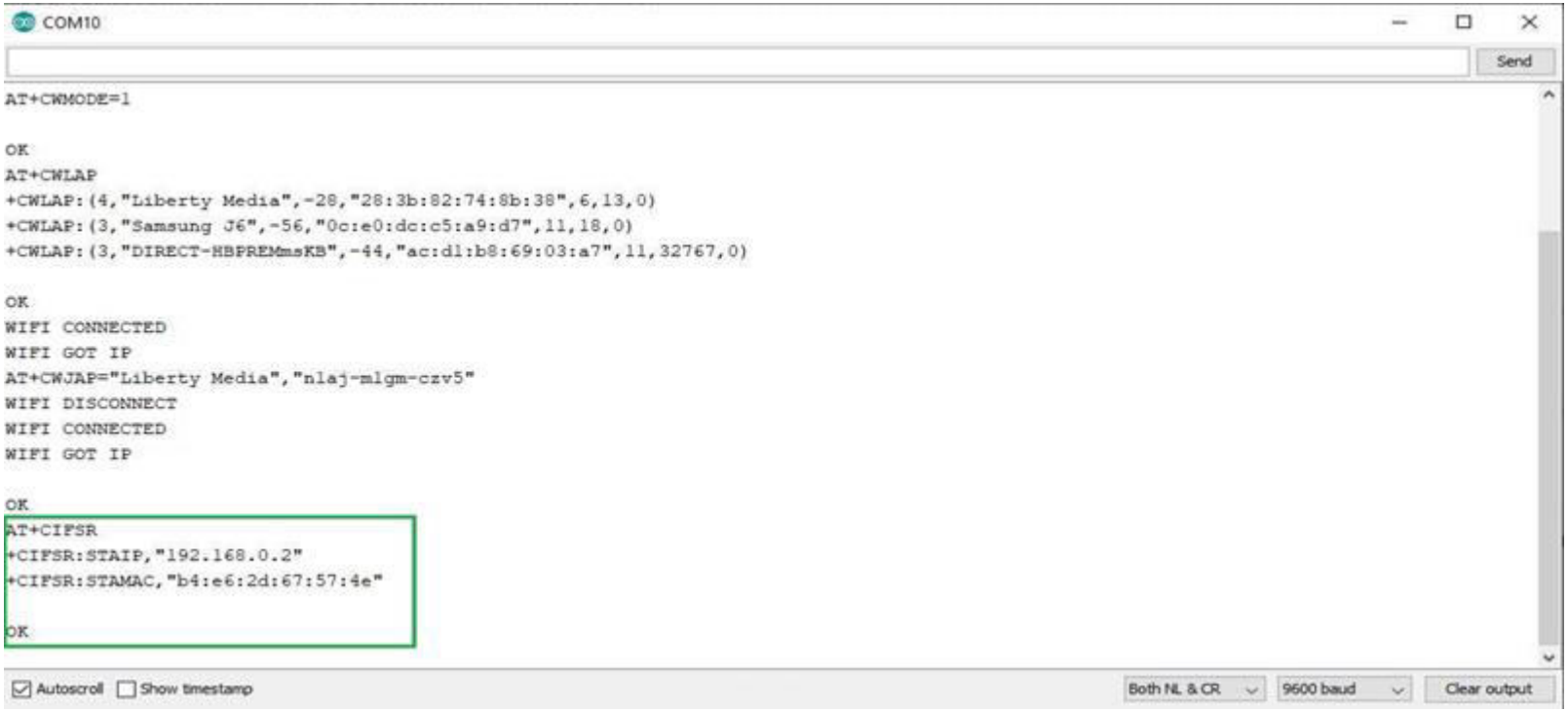
Command: AT+CWLAP

# Connecting Esp_8266 to the internet using Arduino Uno

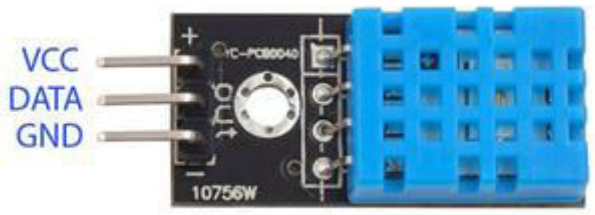
Command: AT+CWJAP="Liberty Media", "nlj-hyiyk187"

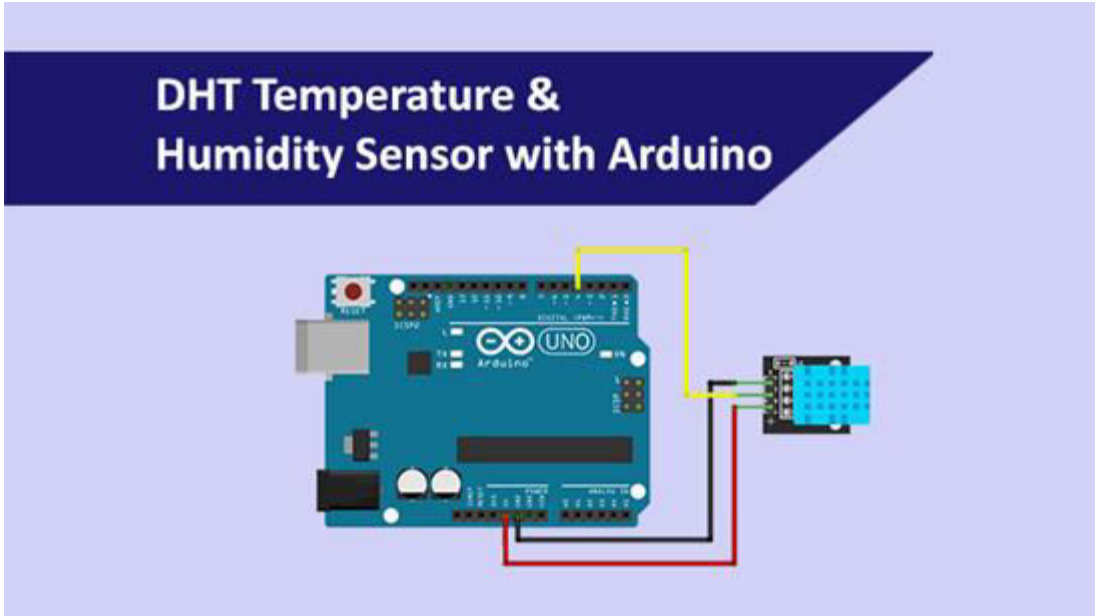
# Connecting Esp_8266 to the internet using Arduino Uno

Command: AT+CIFSR

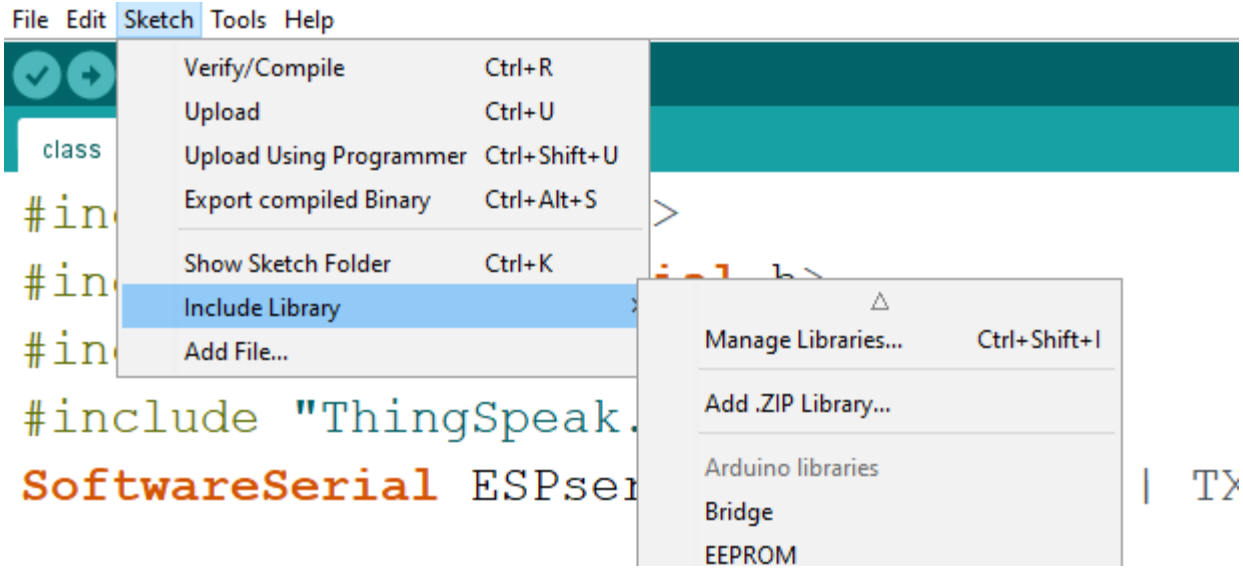


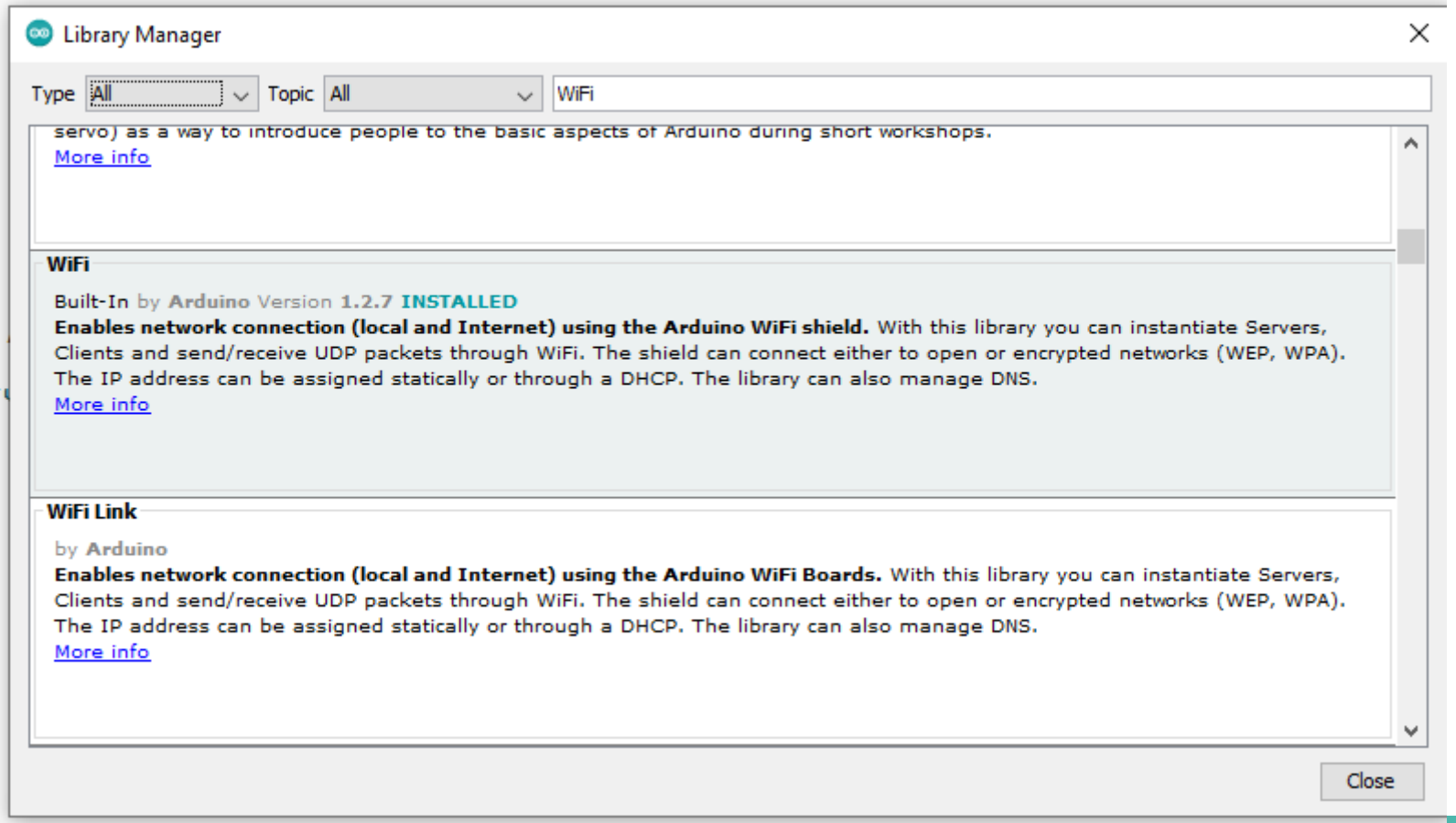
# Sending Temperature and Humidity To ThingSpeak.com

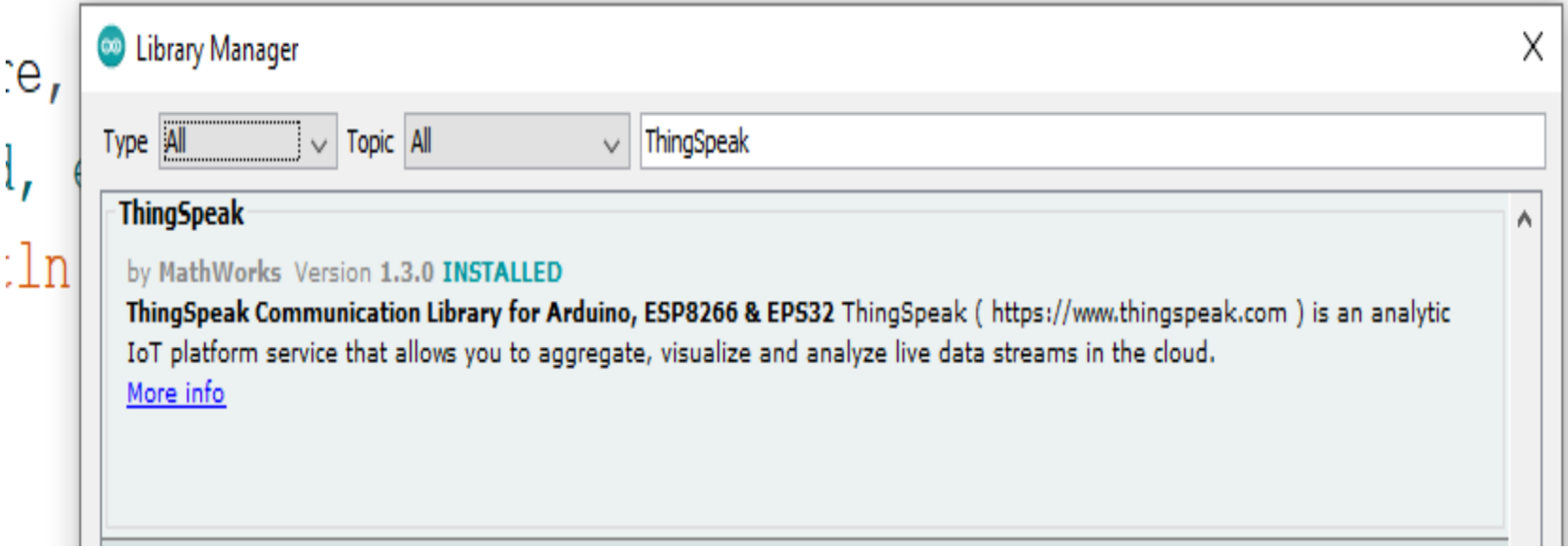


# Steps to connect the required library




Library Manager
Type All
Topic All
WiFi
servo) as a way to introduce people to the basic aspects of Arduino during short workshops.
More info
WiFi
Built-In by Arduino Version 1.2.7 INSTALLED
Enables network connection (local and Internet) using the Arduino WiFi shield. With this library you can instantiate Servers, Clients and send/receive UDP packets through WiFi. The shield can connect either to open or encrypted networks (WEP, WPA). The IP address can be assigned statically or through a DHCP. The library can also manage DNS.
More info
WiFi Link
by Arduino
Enables network connection (local and Internet) using the Arduino WiFi Boards. With this library you can instantiate Servers, Clients and send/receive UDP packets through WiFi. The shield can connect either to open or encrypted networks (WEP, WPA). The IP address can be assigned statically or through a DHCP. The library can also manage DNS.
More info
Close


Library Manager
Type All
Topic All
ThingSpeak
ThingSpeak
by MathWorks Version 1.3.0 INSTALLED
ThingSpeak Communication Library for Arduino, ESP8266 & EPS32 ThingSpeak ( https://www.thingspeak.com ) is an analytic IoT platform service that allows you to aggregate, visualize and analyze live data streams in the cloud.
More info

# Code:

```
#include <SimpleDHT.h>
#include <SoftwareSerial.h>
#include<WiFi.h>
#include "ThingSpeak.h"

// for DHT11,
//      DATA: 4
int pinDHT11 = 4;
SimpleDHT11 dht11(pinDHT11);
unsigned long myChannelNumber=1334605;
const char myWriteAPIKey = "2OFRMD7XGJO22Q97";
WiFiClient client;
void setup() {
  Serial.begin(9600);
  WiFi.begin(username,pass);
  ThingSpeak.begin(client);}
```

```
void loop() {
  byte temperature = 0;
  byte humidity = 0;
  int err = SimpleDHTErrSuccess;
  if ((err = dht11.read(&temperature, &humidity, NULL)) != SimpleDHTErrSuccess) {
    Serial.print("Read DHT11 failed, err="); Serial.print(SimpleDHTErrCode(err));
    Serial.print(","); Serial.println(SimpleDHTErrDuration(err)); delay(1000);
    return;
  }

  Serial.print("Temperature: ");
  float t=((float)temperature);
  float h=((float)humidity);
  Serial.print((float)temperature); Serial.print(" *C, ");
  Serial.print("Humidity: ");
  Serial.print((float)humidity); Serial.println(" H");
  delay(1000);
  ThingSpeak.setField(1,t);
  ThingSpeak.setField(2,h);
  ThingSpeak.writeFields(myChannelNumber,myWriteAPIKey);
  delay(2000);
}
```

# We cannot simulate  Esp8266 in Proteus .

# But we can simulate  DHT11 in Proteus .

# Code

```
#include <SimpleDHT.h>
int pinDHT11 = 4;
SimpleDHT11 dht11(pinDHT11);

void setup(){
  Serial.begin(9600);
}

void loop()
{
  byte temperature = 0;
  byte humidity = 0;
  int err = SimpleDHTErrSuccess;
  if ((err = dht11.read(&temperature, &humidity, NULL)) != SimpleDHTErrSuccess) {
    Serial.print("Read DHT11 failed, err="); Serial.print(SimpleDHTErrCode(err));
    Serial.print(","); Serial.println(SimpleDHTErrDuration(err)); delay(1000);
    return;
  }

  Serial.print("Temperature: ");
  Serial.print((float)temperature); Serial.print(" *C, ");
  Serial.print("Humidity: ");
  Serial.print((float)humidity); Serial.println(" H");
  delay(1000);
}
```

# Internet of Things (IoT)

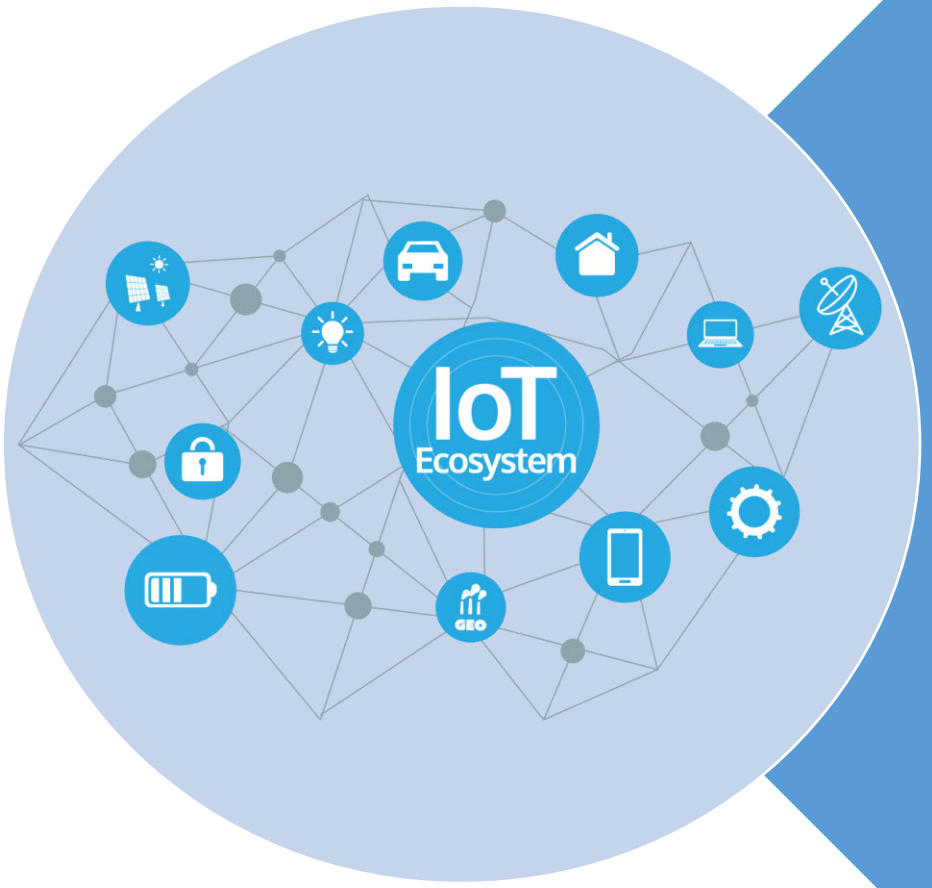
CSE 315

Peripherals & Interfacing

Abdullah Al Omar

Lecturer, CSE, UAP

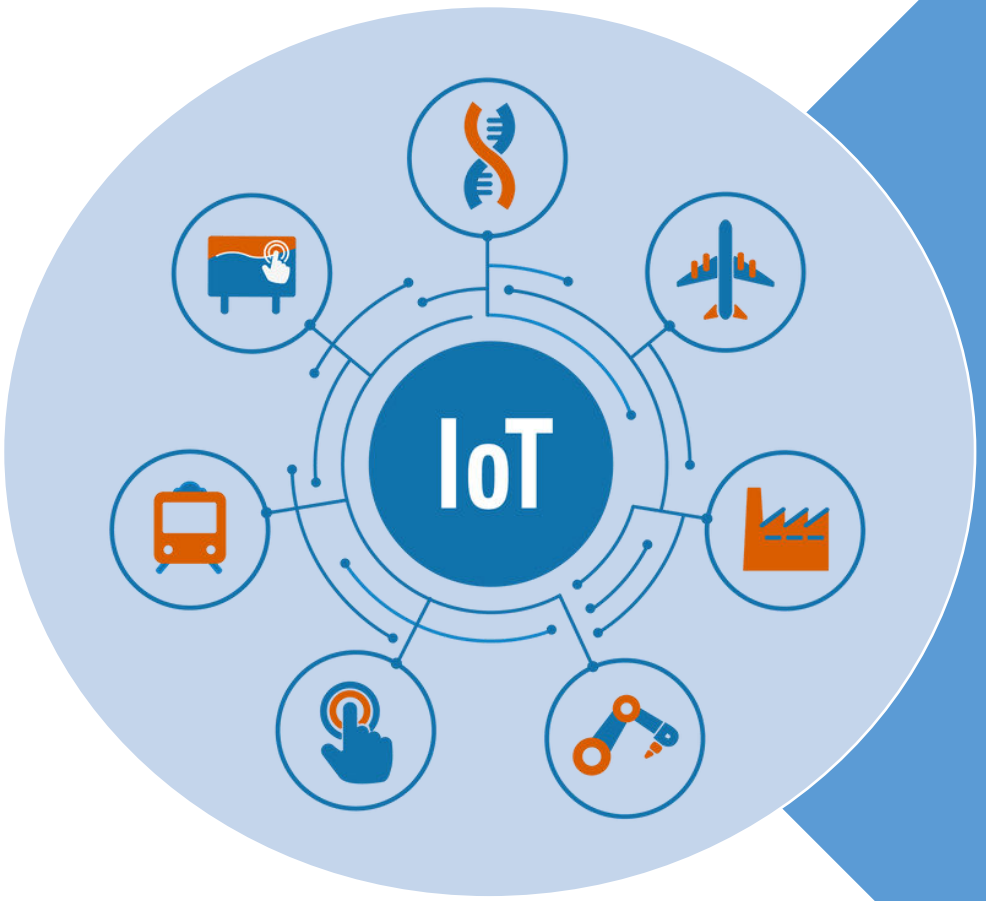
# What is Internet of Things?




The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UID) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

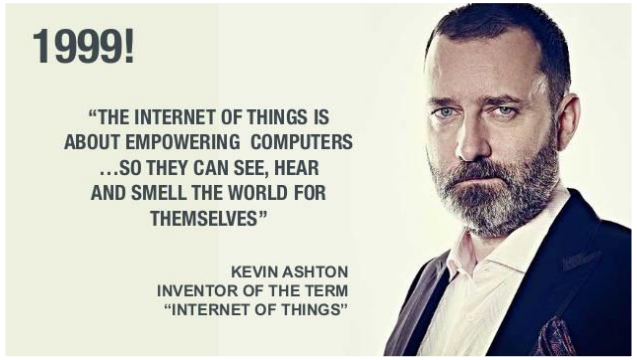
It is also referred as Machine to Machine (M2M), Skynet, Internet of Everything.

# What is Things?



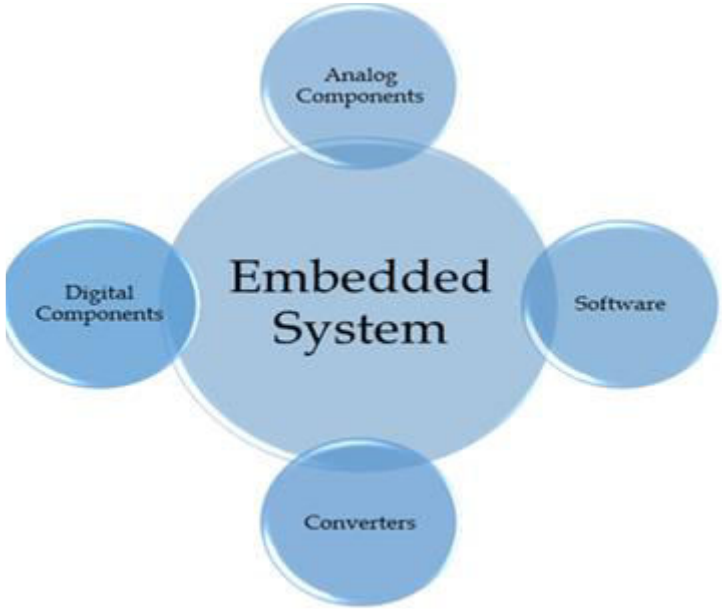

A **thing** in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network.

# Inventor of the term Internet of Things:

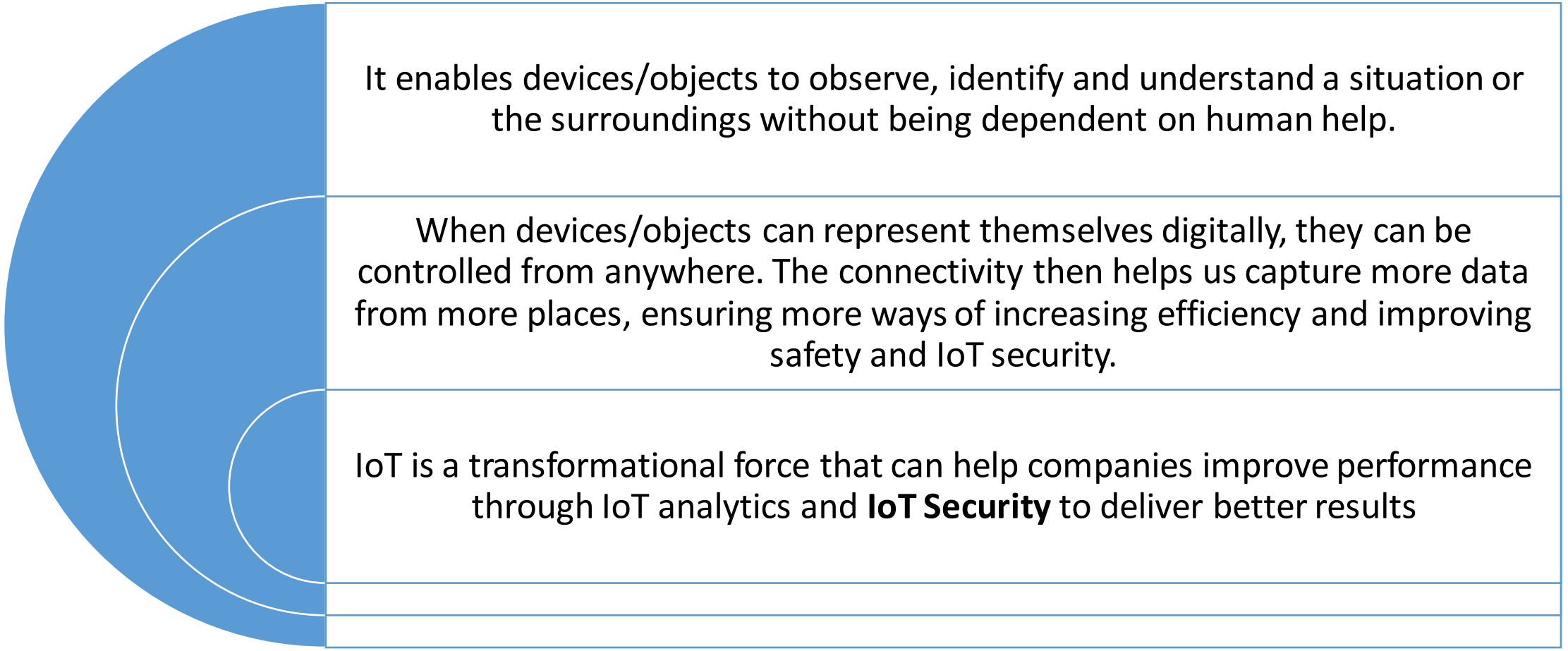



Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999.

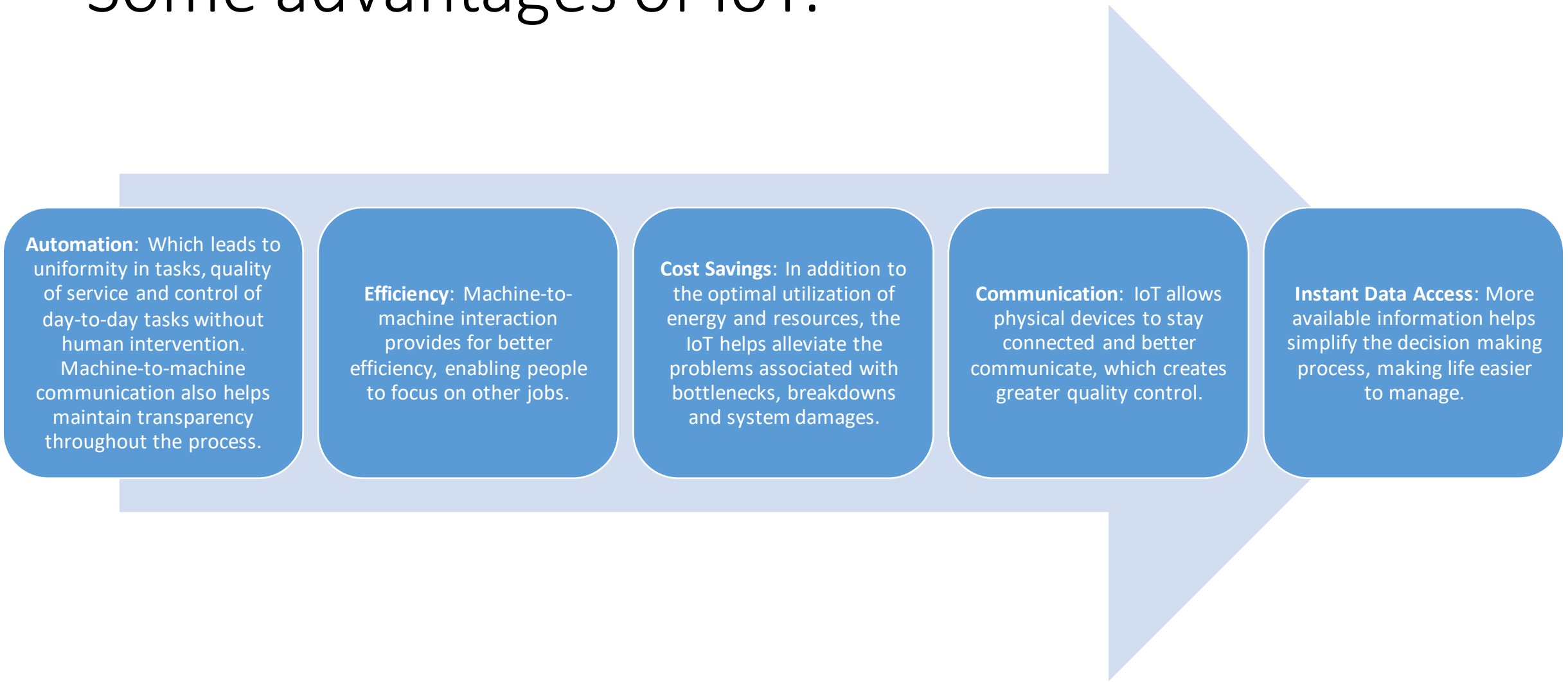
Although Ashton's was the first mention of the internet of things, the idea of connected devices has been around since the 1970s, under the monikers *embedded internet* and *pervasive computing*.



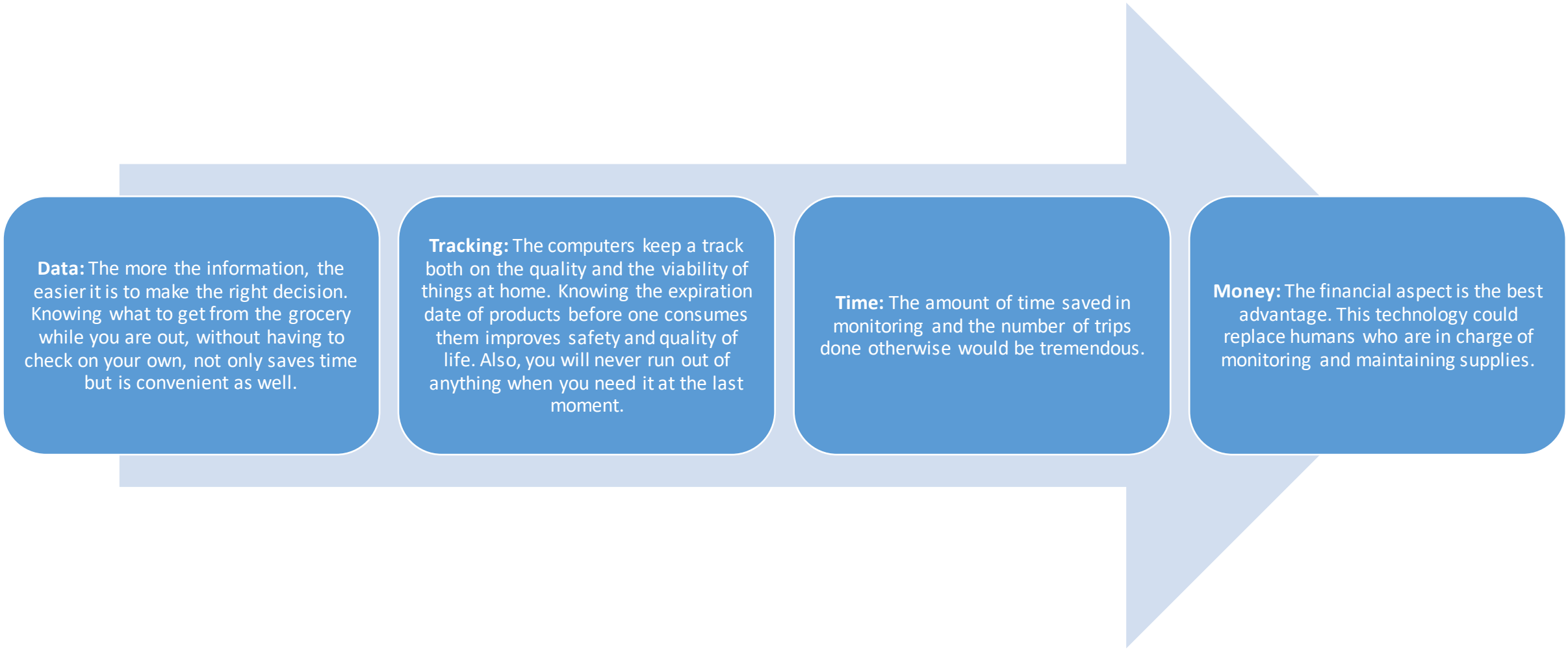
# Why IoT?


It enables devices/objects to observe, identify and understand a situation or the surroundings without being dependent on human help.
When devices/objects can represent themselves digitally, they can be controlled from anywhere. The connectivity then helps us capture more data from more places, ensuring more ways of increasing efficiency and improving safety and IoT security.
IoT is a transformational force that can help companies improve performance through IoT analytics and **IoT Security** to deliver better results

# Some advantages of IoT:



# Some advantages of IoT: (Contd.)



# How IoT works?

- There are two major subsystems involved in the IoT network viz. front end part and back end part. Front end is mainly consists of IoT sensors which are MEMS based. It includes optical sensors, light sensors, gesture and proximity sensors, touch and fingerprint sensors, pressure sensors and more.
- Back end consists of cellular, wireless and wired networks which are interfaced with IoT devices. The devices will report to the central servers and also interact with databases in the backbone network. Routers and gateways are part of the wireless backbone networks.

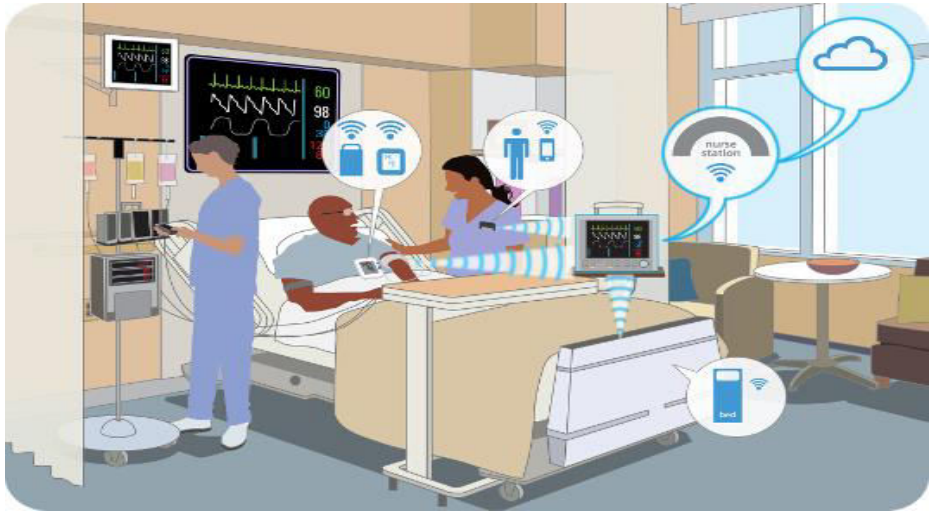
# IoT projects (basic):

- **IoT Based Humidity and Temperature Monitoring Using Arduino Uno**
- **IoT Connected Healthcare Applications**
- **IoT Based Intelligent Traffic Management System**
- **IoT Based Smart Parking System Using RFID**
- **IoT Based Smart Waste Management System for Smart City**
- **IoT Smart Home automation using Node Mcu**

# IoT Implementation:

Wearable Tech

Smart Appliances

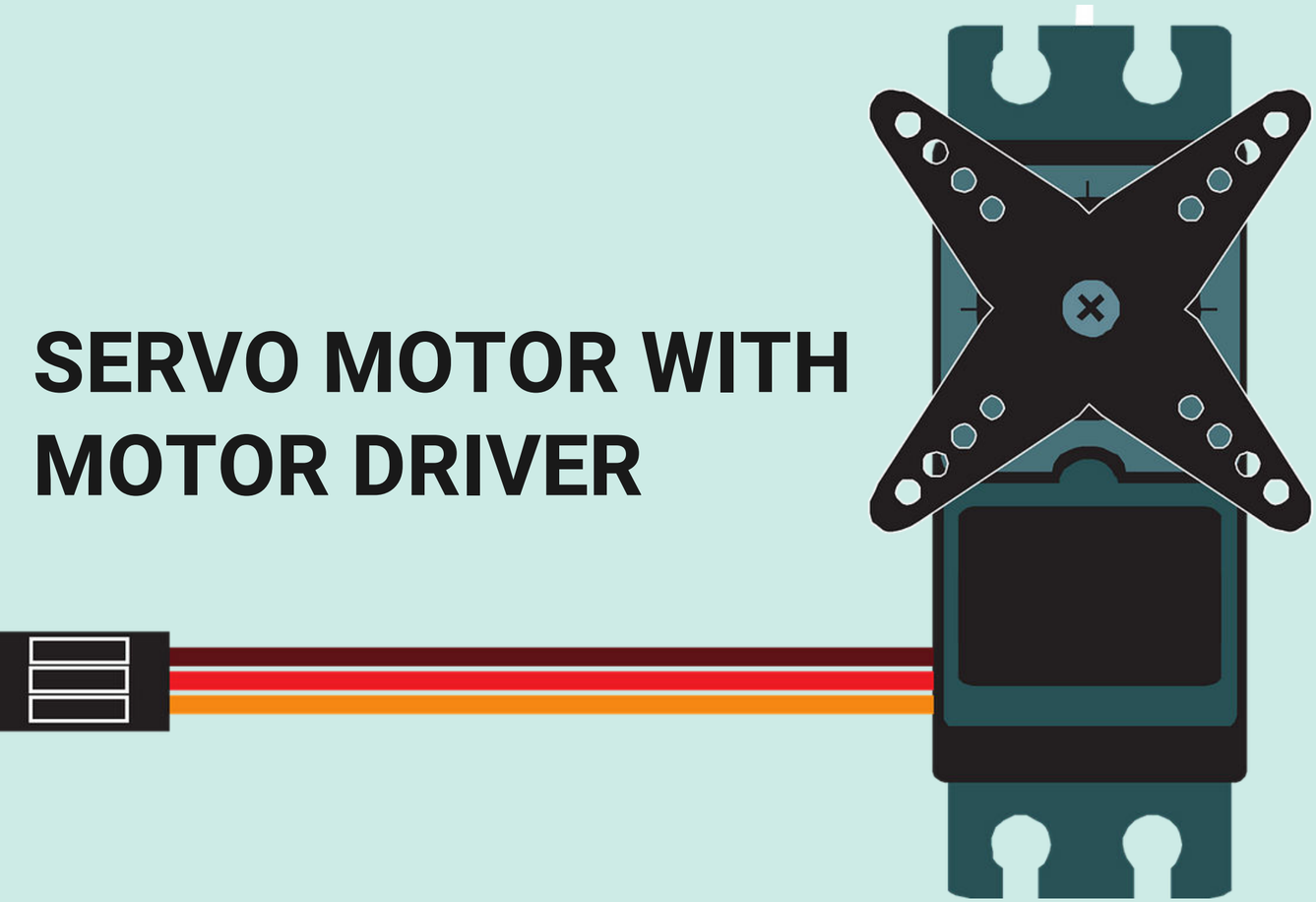




Healthcare

Thank you

01

# SERVO MOTOR WITH MOTOR DRIVER

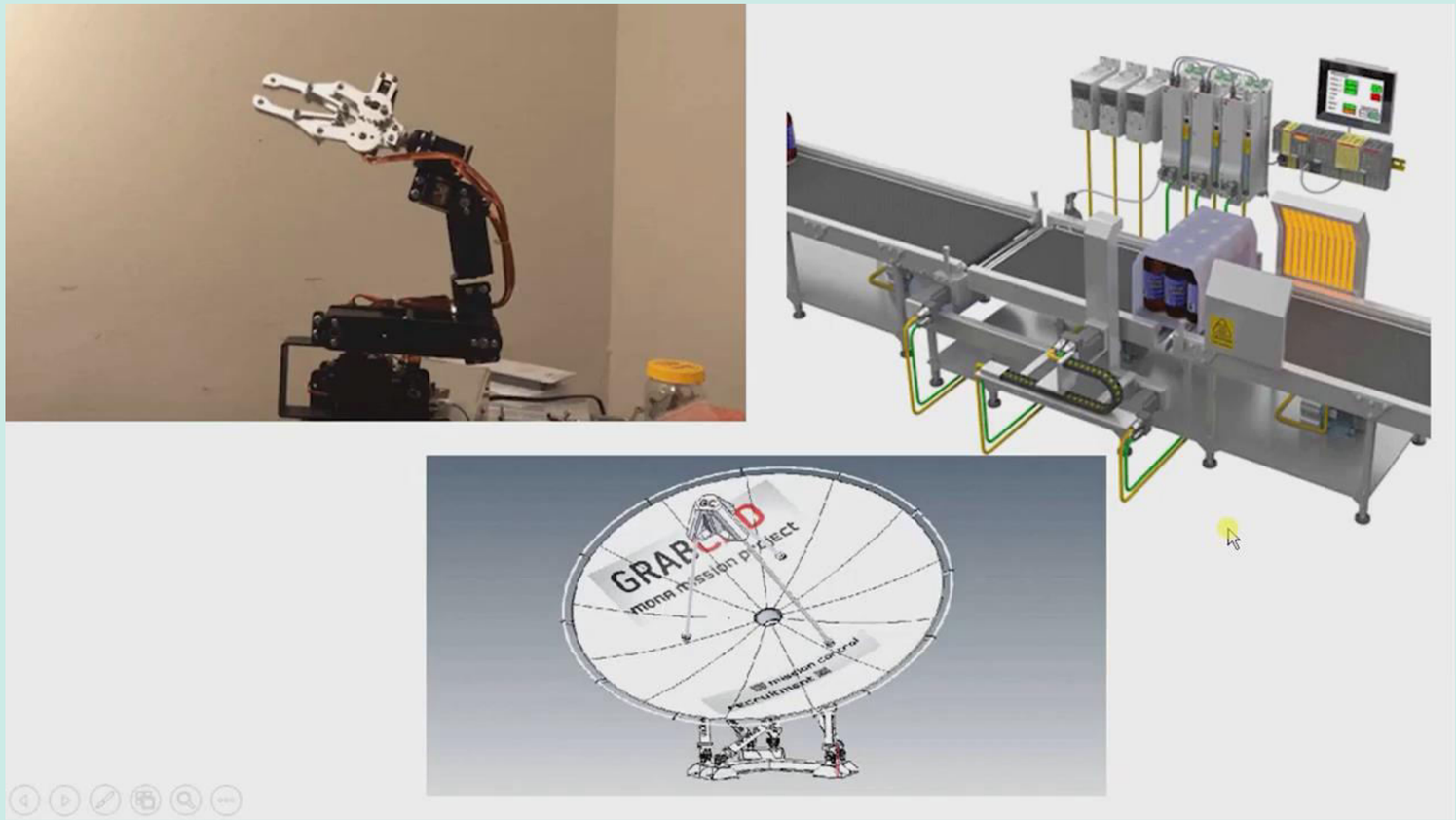


## CSE 315

Peripherals & Interfacing

# Have you ever wondered?

02




Servo motor with motor driver

03

# Agenda

- Servo Motor Basics
- Servo Motor Basics(Visuals)
- How does it work?
- Types
- Types Explanation
- Working Principles of a DC Servo Motor
- Working Principles of an AC Servo Motor
- Driving Servo Motors with L293D Shield
- Driving Servo Motors with L293D (Video)
- Code
- Code Explanation
- Servo Motor Applications

# Servo Motor Basics

04

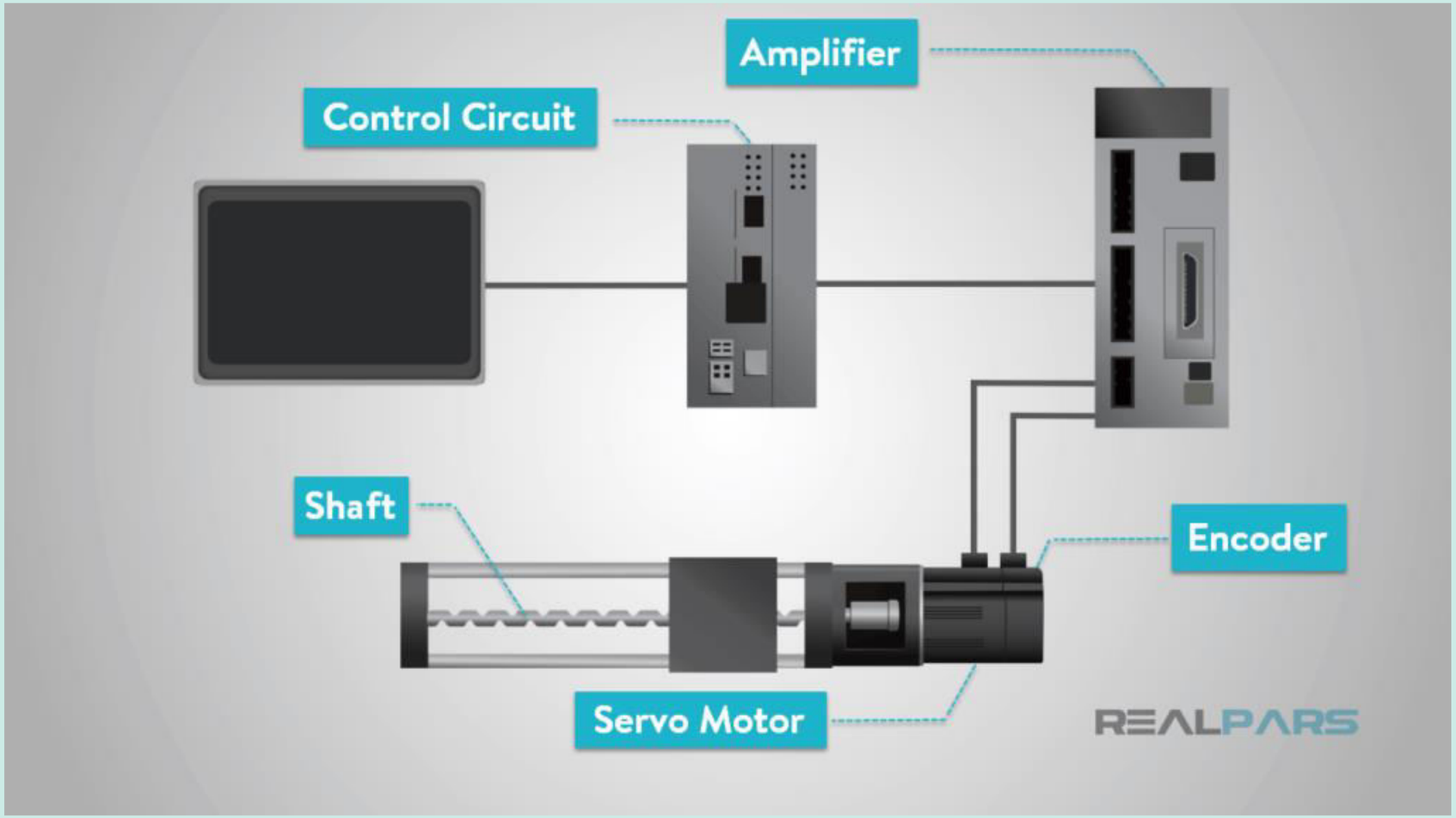
Servo motors are part of a closed-loop system and are comprised of several parts namely :

- Control circuit
- Servo motor
- Shaft
- Amplifier
- Encoder or resolver.

Servo motor with motor driver

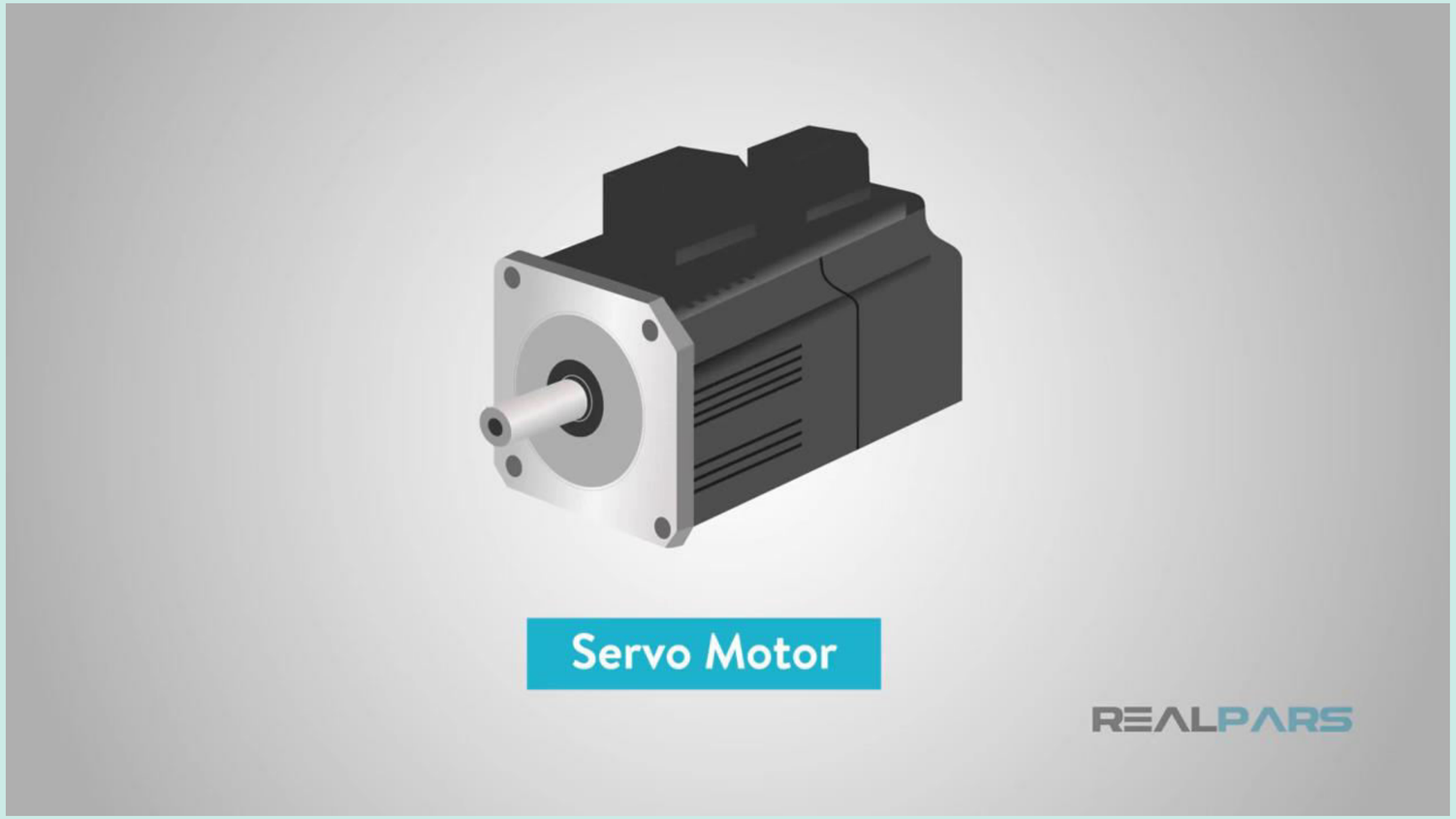
# Servo Motor Basics(Visuals)

05



# How Does it work?(Video)

06




Servo motor with motor driver

SOURCE

# Types(3 x 2)



- AC or DC
- Brush or Brushless(DC)
- Synchronous or Asynchronous(AC)

# AC or DC



| Point | AC | DC |
| --- | --- | --- |
| • Performance | speed is determined by the frequency of the applied voltage and the number of magnetic poles. | speed is directly proportional to the supply voltage with a constant load. |
| • Usablity | AC motors will withstand higher current and are more commonly used where high repetitions and high precision are required. | DC motors are also used in servo systems but recommended when there's no demand of high precision. |

# Brushed or Brushless(DC)



| Point | Brushed | Brushless |
| --- | --- | --- |
| • Cost & Usability | Brushed motors are generally less expensive and simpler to operate | Brushless motors are comparatively more expensive and harder to operate |
| • Performance | more reliable<br>have higher efficiency<br>and are less noisy. | Less reliable,<br>have lower efficiency,<br>and are more noisy. |

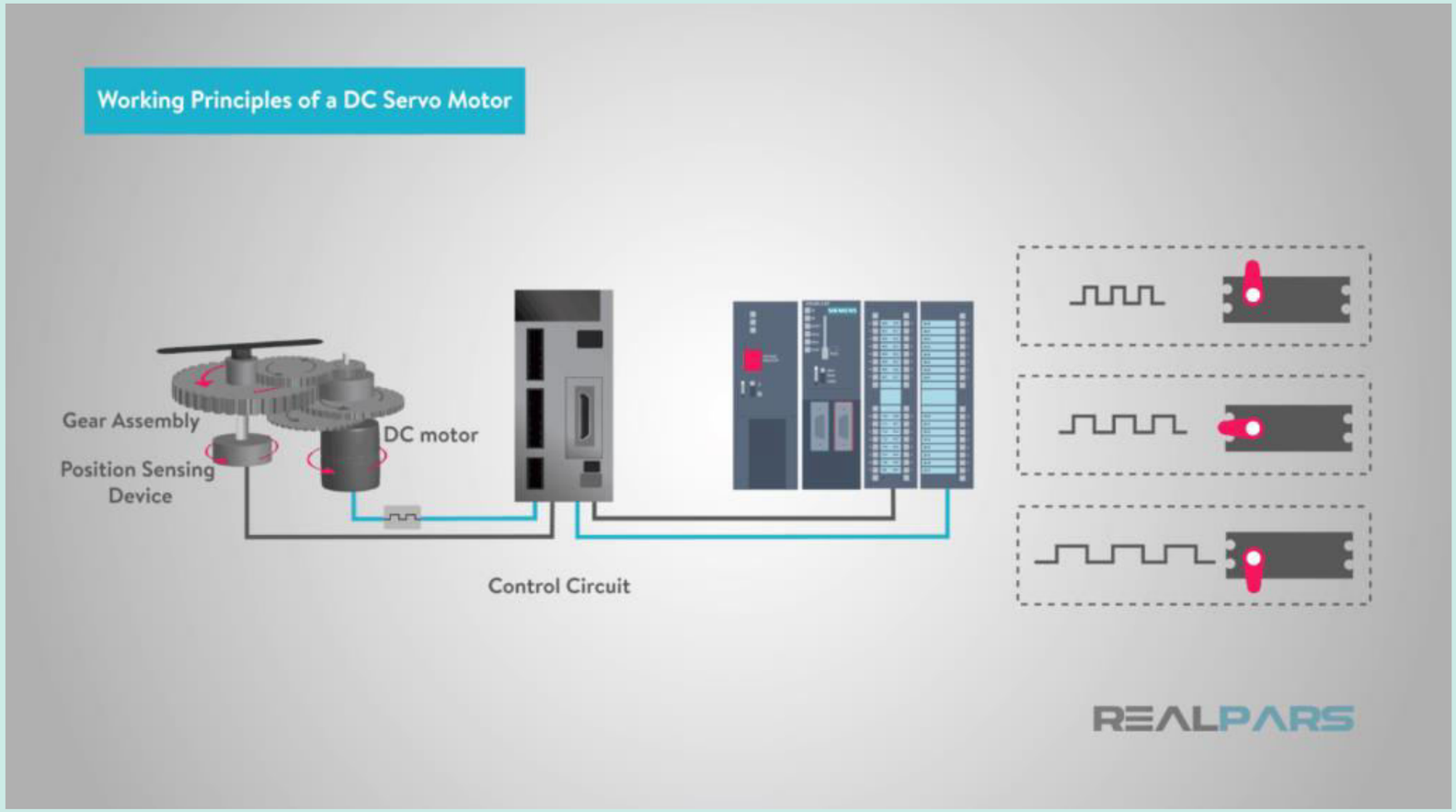
# Synchronous or Asynchronous(AC)



| Point | Synchronous | Asynchronous |
| --- | --- | --- |
| • Cost | Synchronous motor is costlier compared to asynchronous motors. | Asynchronous motor is cheaper compared to synchronous motors. |
| • Speed | Stator speed is equal to the speed of totor | Stator speed is not equal to the speed of rotor. Rotor is slower than stator. |

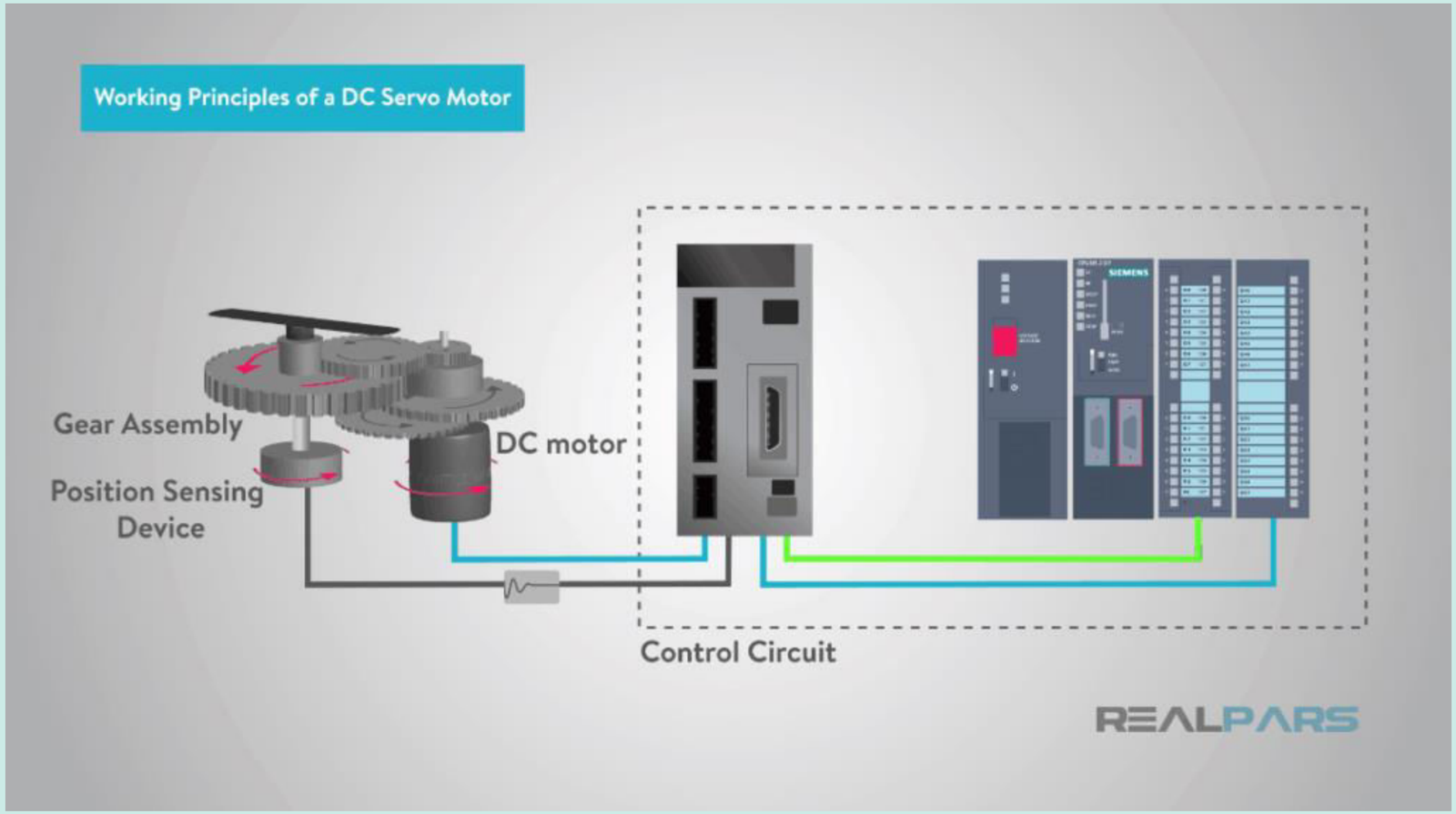
# Working Principles of a DC Servo Motor(1)





# Working Principles of a DC Servo Motor(2)






Servo motor with motor driver

SOURCE

# Working Principles of a DC Servo Motor(Video)

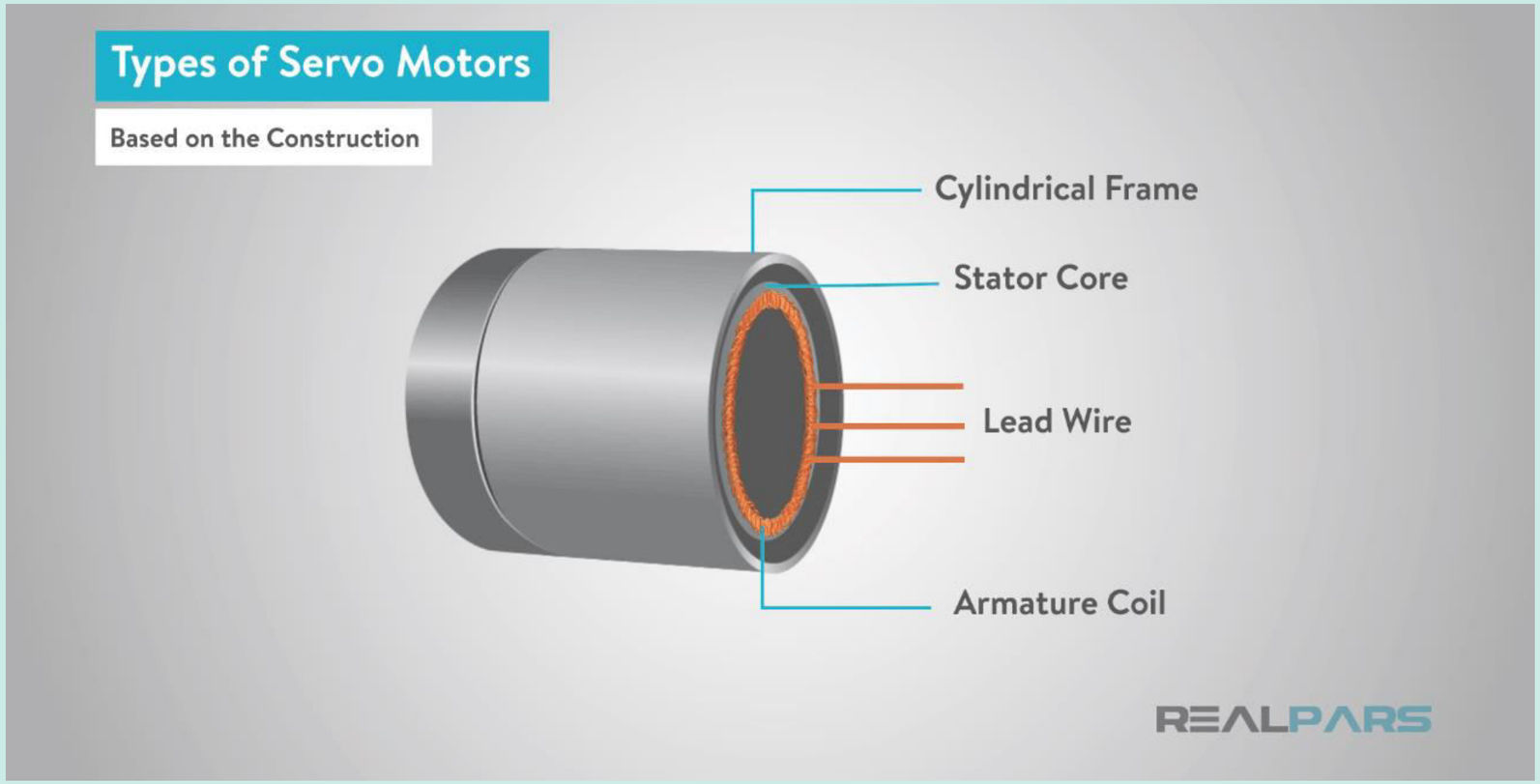



Servo motor with motor driver

SOURCE

# Working Principles of a AC Servo Motor(1)



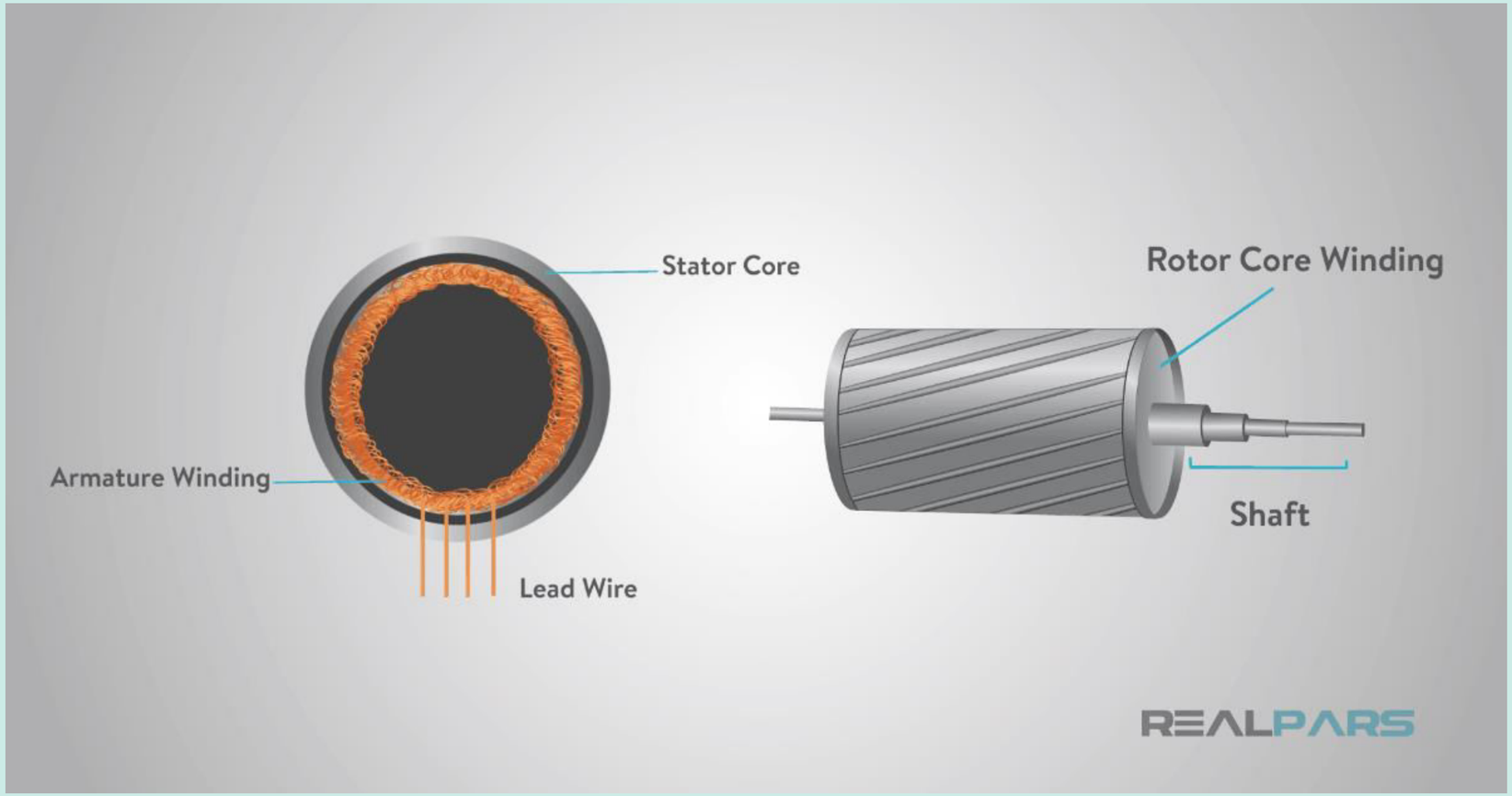



Servo motor with motor driver

SOURCE

# Working Principles of a AC Servo Motor(2)



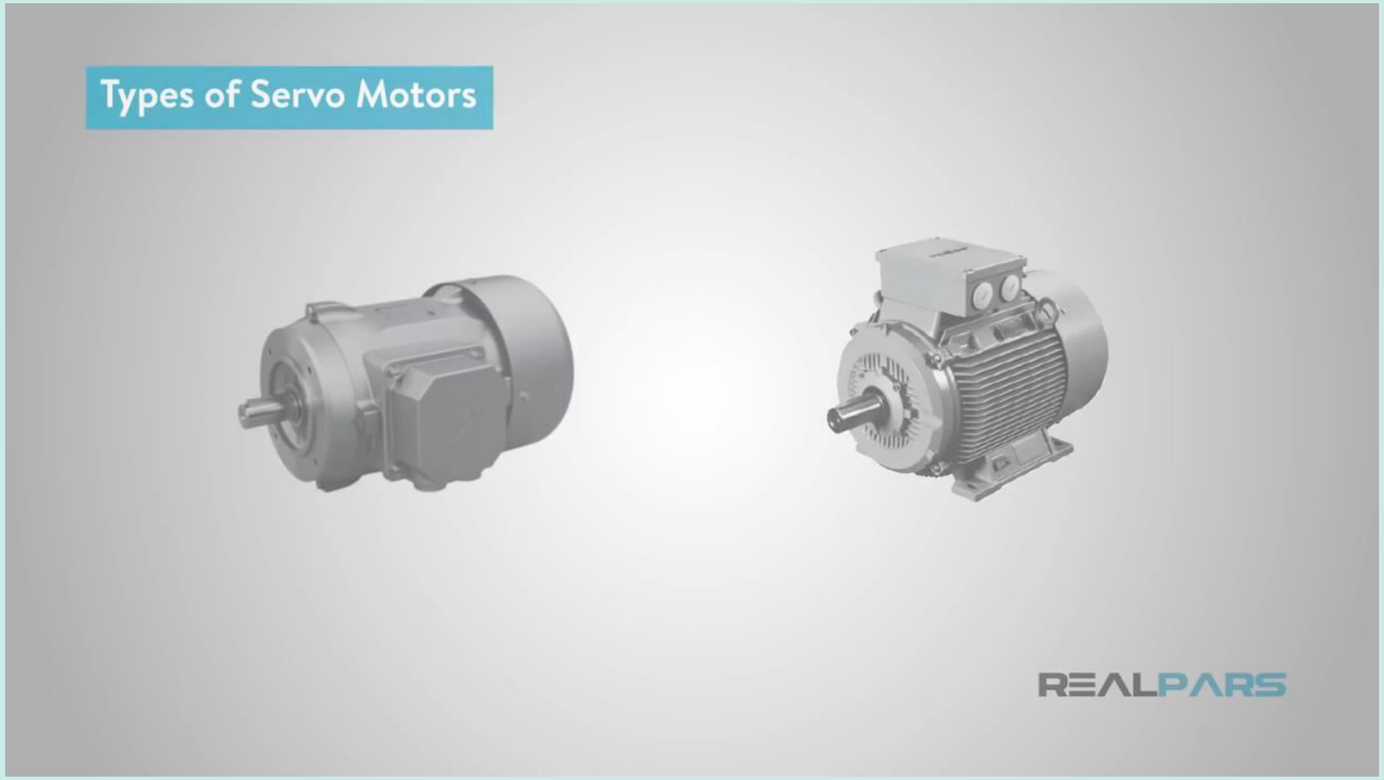



Servo motor with motor driver

SOURCE

# Working Principles of a AC Servo Motor(Video)- Synchronous



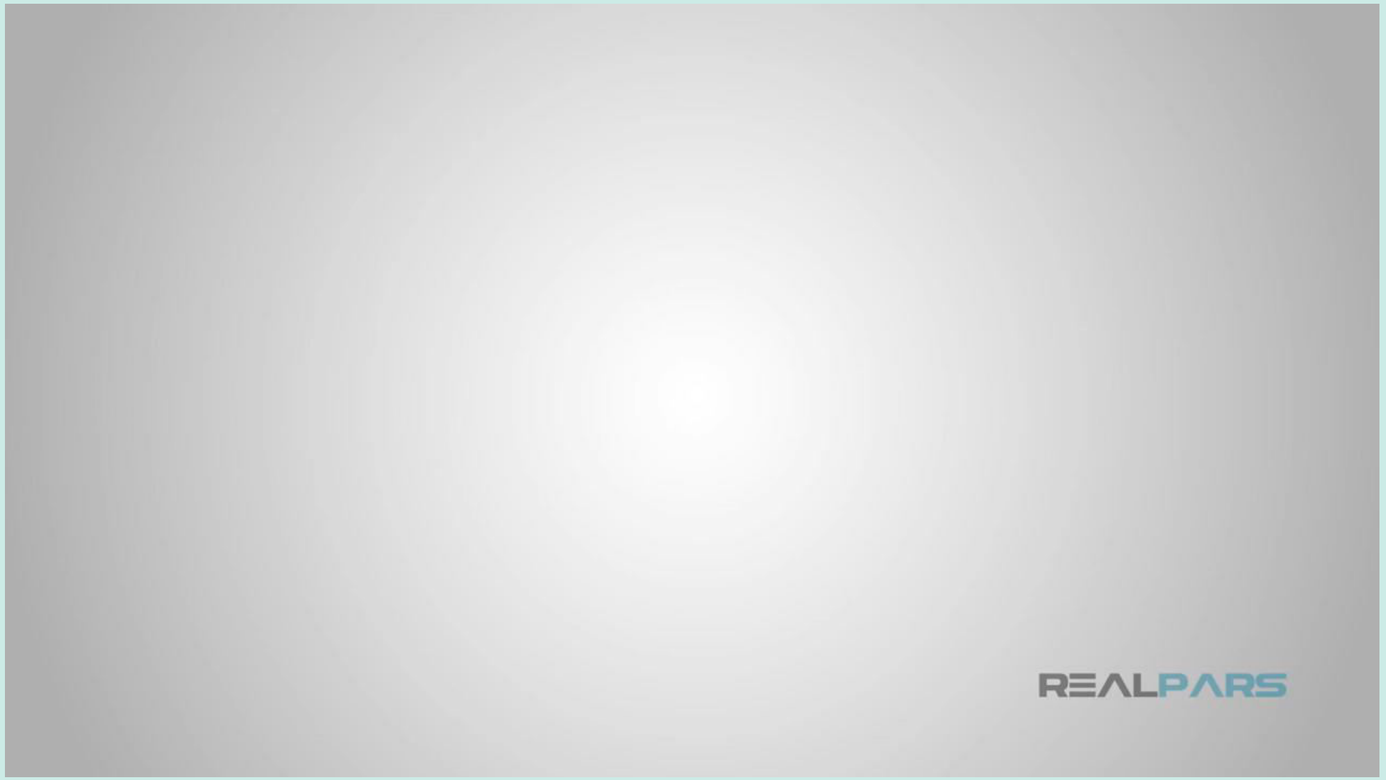



SOURCE

Servo motor with motor driver

# Working Principles of a AC Servo Motor(Video)-Asynchronous





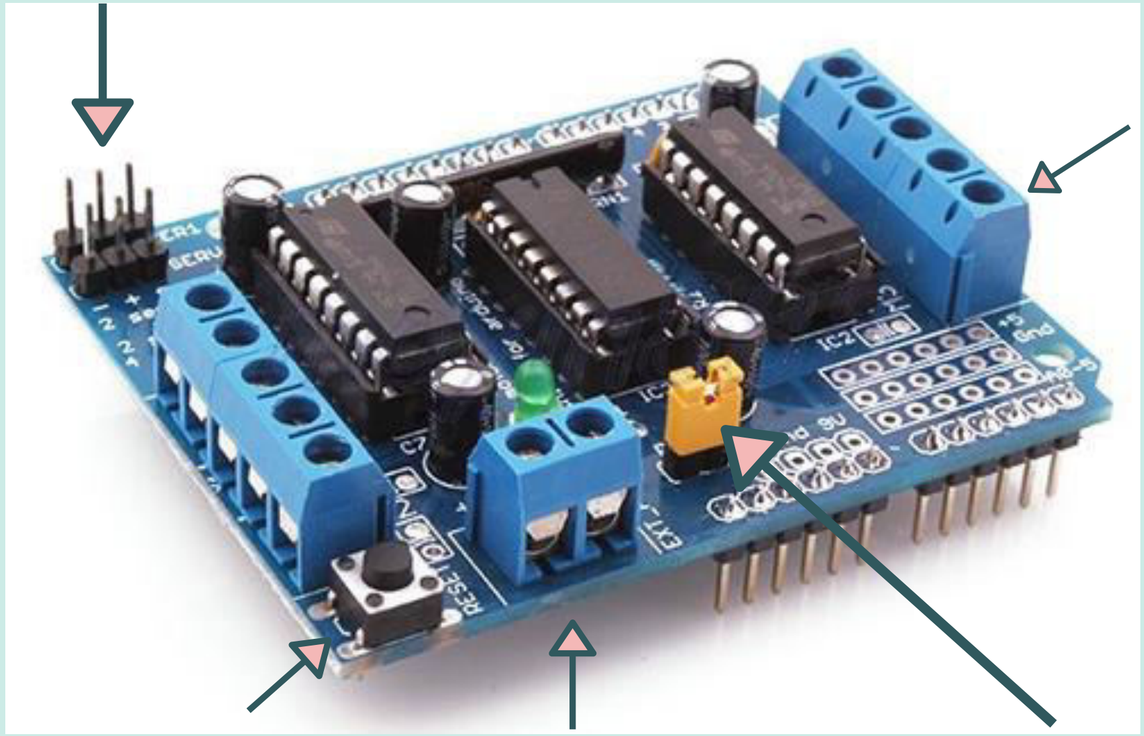

SOURCE

Servo motor with motor driver

# L293D Motor Driver



Servo Terminal



Stepper
#2

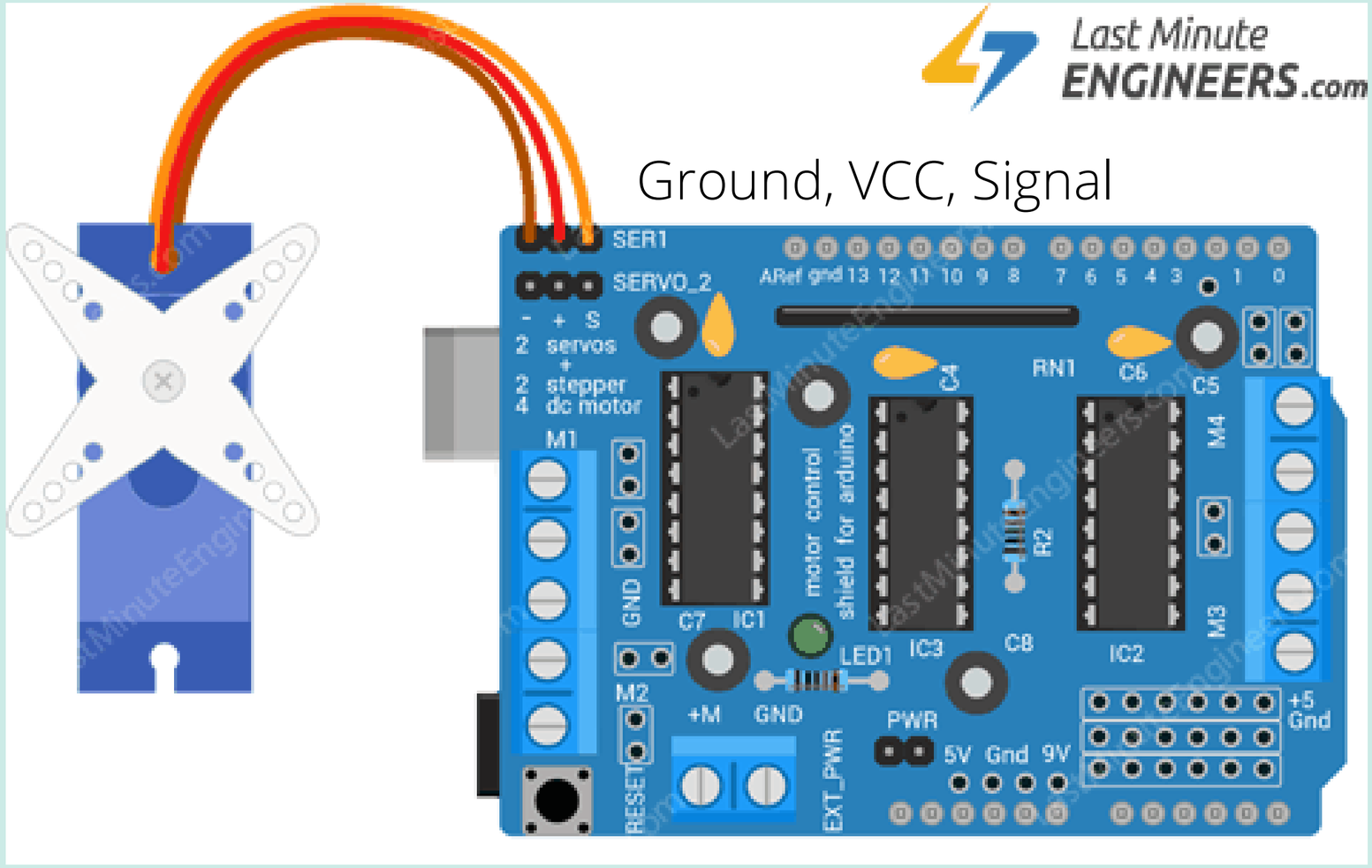
Reset

External Power
Supply Terminal

Power
Supply Terminal

# Driving Servo Motors with L293D Shield





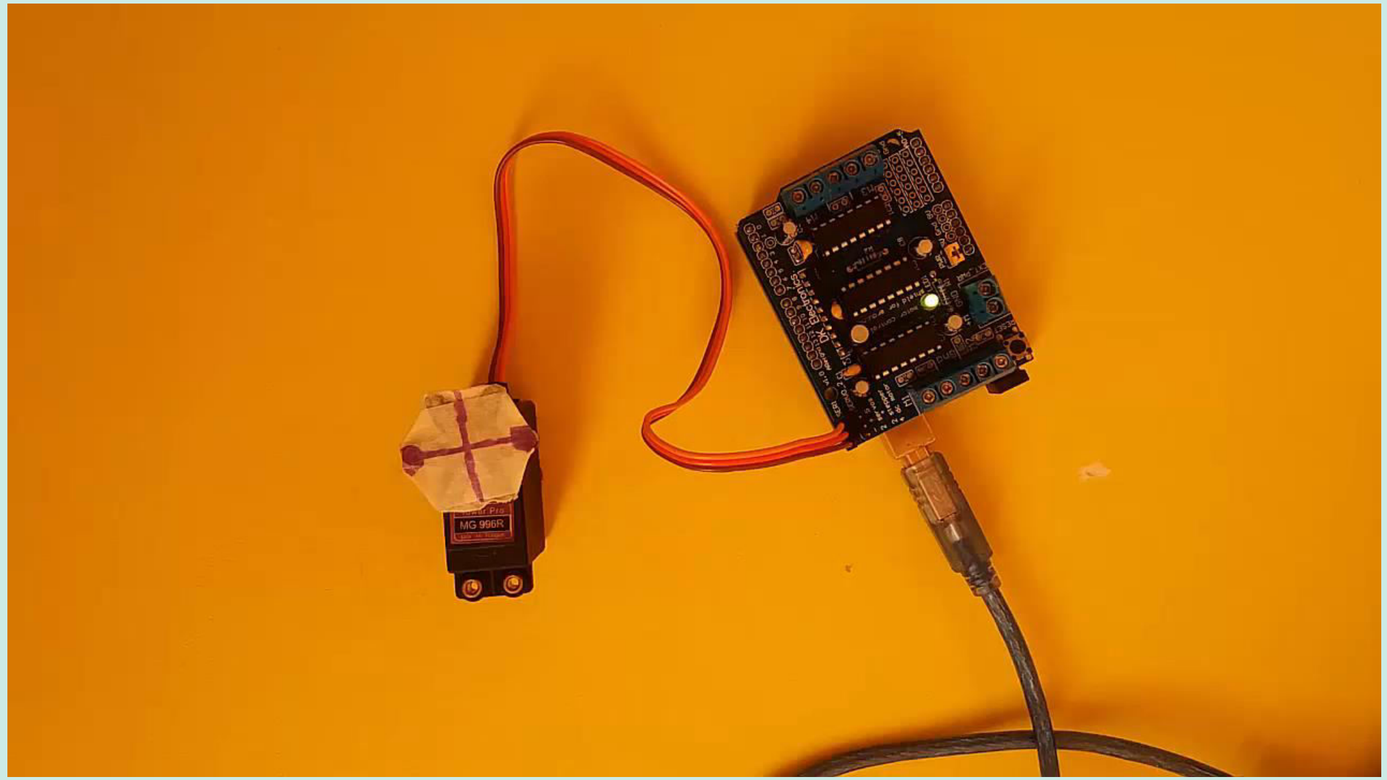

Orange: Signal

Red: VCC

Last: Ground

# Driving Servo Motors with L293D (Video)






See Codes

PLAY THIS ON YouTube

# Code + Explanation



**When the program starts running, the servo motor will rotate slowly from 0 degrees to 180 degrees, one degree at a time. When the motor has rotated 180 degrees, it will begin to rotate in the other direction until it returns to the home position.**

```
#include <Servo.h>          //Servo library

Servo servo_test;                 //initialize a servo object for the connected servo

int angle = 0;

void setup()
{
  servo_test.attach(9);           // attach the signal pin of servo to pin9 of
arduino
}
```

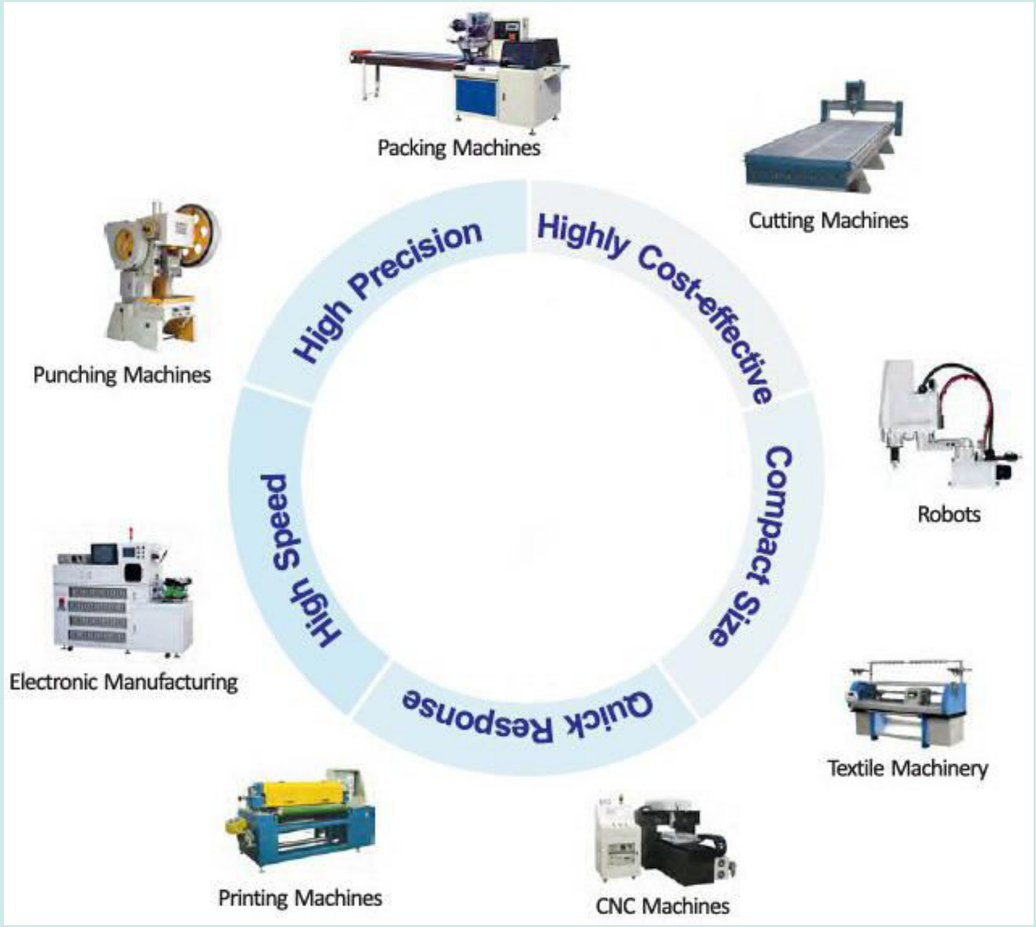
# Code + Explanation



```
void loop()
{
for(angle = 0; angle < 180; angle += 1)       // command to move from 0 degrees to 180 degrees
{
servo_test.write(angle);                  //command to rotate the servo to the specified angle
delay(15);
}

delay(1000);

for(angle = 180; angle>=1; angle-=5)    // command to move from 180 degrees to 0 degrees
{
servo_test.write(angle);              //command to rotate the servo to the specified angle
delay(5);
}
delay(1000);
}
```

# Servo Motor Applications





# Thank you!

**LET US KNOW IF YOU HAVE QUESTIONS OR CLARIFICATIONS.**

# Reference




- slide 3-17 (Servo Motor Basics, Type, Working Principles): https://realpars.com/servo-motor/
- Slide 18-19 (L293D Motor Driver): https://lastminuteengineers.com/l293d-motor-driver-shield-arduino-tutorial/
- Slide 20 (Connect with Arduino): https://youtu.be/zZ1sYtoo5gw
- Slide 21-22 (Code): https://www.allaboutcircuits.com/projects/servo-motor-control-with-an-arduino/

1. **What is Edge Computing? Discuss the benefits of Edge Computing.**

Answer: Edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network, on downstream data on behalf of cloud services and upstream data on behalf of IoT services. Here we define "edge" as any computing and network resources along the path between data sources and cloud data centers. For example, a smart phone is the edge between body things and cloud, a gateway in a smart home is the edge between home things and cloud, a micro data center and a cloudlet [14] is the edge between a mobile device and cloud.

**Benefits of Edge Computing:** Edge Computing have several benefits compared to traditional cloud-based computing

- Edge computing things not only are data consumers, but also play as data producers.
- At the edge, the things can not only request service and content from the cloud but also perform the computing tasks from the cloud.
- Edge can perform computing offloading, data storage, caching and processing, as well as distribute request and delivery service from cloud to user
- Edge provides the requirement efficiently in service such as reliability, security, and privacy protection.
- The energy consumption could also be reduced by 30%–40% by cloudlet offloading

2.**Why we need Edge Computing?** OR **Why Edge Computing is more efficient than Cloud Computing?**

**Answer:** 1) Push From Cloud Services:

- Putting all the computing tasks on the cloud has been proved to be an efficient way for data processing since the computing power on the cloud outclasses the capability of the things at the edge.
- If more data needs to be sent to the cloud for processing, the response time would be too long. In this case, the data needs to be processed at the edge for shorter response time, more efficient processing and smaller network pressure.

2) Pull From IoT:

- Almost all kinds of electrical devices will become part of IoT, and they will play the role of data producers as well as consumers, such as air quality sensors, LED bars, streetlights
- raw data produced by them will be enormous, making conventional cloud computing not efficient enough to handle all these data.
- This means most of the data produced by IoT will never be transmitted to the cloud, instead it will be consumed at the edge of the network.

3) Change From Data Consumer to Producer:

People are producing data nowadays from their mobile devices. The change from data consumer to data producer/consumer requires more function placement at the edge.

For example, it is very normal that people today take photos or do video recording then share the data through a cloud service such as YouTube, Facebook, Twitter, or Instagram. However, the image

or video clip could be fairly large and it would occupy a lot of bandwidth for uploading. In this case, the video clip should be demised and adjusted to suitable resolution at the edge before uploading to cloud. Another example would be wearable health devices. Since the physical data collected by the things at the edge of the network is usually private, processing the data at the edge could protect user privacy better than uploading raw data to cloud.

**2. Differentiate between Cloud Computing and Edge Computing through diagram.**

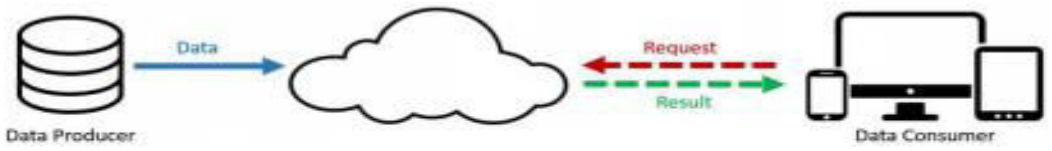



Fig. 1. Cloud computing paradigm.

Fig. 1 shows the conventional cloud computing structure. Data producers generate raw data and transfer it to cloud, and data consumers send request for consuming data to cloud, as noted by the blue solid line. The red dotted line indicates the request for consuming data being sent from data consumers to cloud, and the result from cloud is represented by the green dotted line. However, this structure is not sufficient for IoT. First, data quantity at the edge is too large, which will lead to huge unnecessary bandwidth and computing resource usage. Second, the privacy protection requirement will pose an obstacle for cloud computing in IoT.

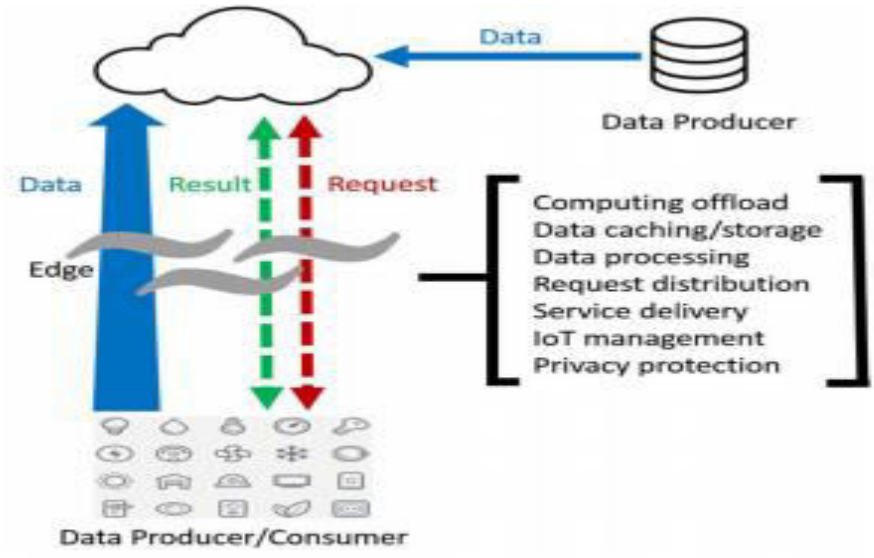



Fig. 2. Edge computing paradigm.

Fig. 2 illustrates the two-way computing streams in edge computing. In the edge computing paradigm, the things not only are data consumers, but also play as data producers. At the edge, the things can not only request service and content from the cloud but also perform the computing tasks from the cloud. Edge can perform computing offloading, data storage, caching and proce ssing, as well as distribute request and delivery service from cloud to user.

**4.Discuss about Cloud Offloading where edge computing could shine to further illustrate our vision of edge computing?**

Answer:

Numbers of researches have addressed the cloud offloading in terms of energy-performance tradeoff in a mobile-cloud environment .In edge computing, the edge has certain computation resources, and this provides a chance to offload part of the workload from cloud.

In the traditional content delivery network, only the data is cached at the edge servers. This is based on the fact that the content provider provides the data on the Internet. In the IoT, the data is produced and consumed at the edge. Thus, in the edge computing not only data but also operation s applied on the data should be cached at the edge.

Shopping with mobile devices is becoming more and more popular, it is important to improve the user experience, especially latency related. In such a scenario, if the shopping cart updating is offloaded from cloud servers to edge nodes, the latency will be dramatically reduced. As we mentioned, the users' shopping cart data and related operations both can be cached at the edge node.

**5. How can improve the interactive services quality by reducing the latency?**

Answer:

By leveraging edge computing, the latency and consequently the user experience for time -sensitive application could be improved significantly. r. One simple solution is to cache the data to all edges the user may reach. Then the synchronization issue between edge nodes rises up. All these issues could become challenges for future investigation. At the bottom line, we can improve the interactive services quality by reducing the latency. Similar applications also include the following.

- Navigation applications can move the navigating or searching services to the edge for a local area, in which case only a few map blocks are involved.
- Content filtering/aggregating could be done at the edge nodes to reduce the data volume to be transferred.
- Real-time applications such as vision-aid entertainment games, augmented reality, and connected health, could make fast responses by using edge nodes.

**6. how Edge Computing illustrate our vision of edge computing in Smart City and Smart Home?**

**Answer: Smart Home:** IoT would benefit the home environment a lot. Some products have been developed and are available on the market such as smart light, smart TV, and robot vacuum. However, just adding a Wi-Fi module to the current electrical device and connecting it to the cl oud is not enough for a smart home.

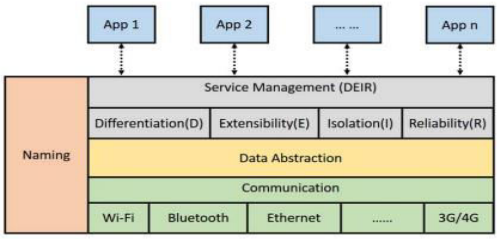



Fig. 3. Structure of edgeOS in the smart home environment.

Fig.3 shows the structure of a variant of edgeOS in the smart home environment. EdgeOS needs to collect data from mobile devices and all kinds of things through multiple communication methods such as Wi-Fi, BlueTooth, ZigBee, or a cellular network.

**Smart City:** The edge computing paradigm can be flexibly expanded from a single home to community, or even city scale. Edge computing claims that computing should happen as close as possible to the data source. Edge computing could be an ideal platform for smart city considering the following characteristics.

- Large Data Quantity: A city populated by 1 million people will produce 180 PB data per day by 2019 , contributed by public safety, health, utility, and transports, etc. Building centralized cloud data centers to handle all of the data is unrealistic because the traffic workload would be too heavy. In this case, edge computing could be an efficient solution by processing the data at the edge of the network.
- Low Latency: For applications that require predictable and low latency such as health emergency or public safety, edge computing is also an appropriate since it could save the data transmission time
- Location Awareness: For geographic-based applications such as transportation and utility management, edge computing exceed cloud computing due to the location awareness

**7. What are the potential benefits of collaborative edge?**

**Answer:** To show the potential benefits of collaborative edge, we use connected healthcare as a case study.

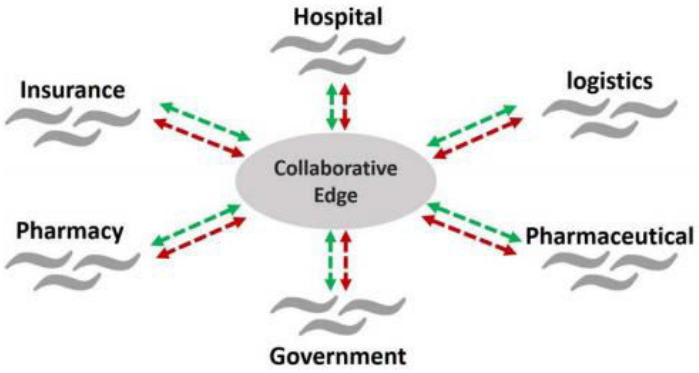
A patient theoretically will follow the prescription to get the pills from a pharmacy. One possibility is that a patient did not follow the therapy. Then the hospital has to take the responsibility for hospitalization since it cannot get the proof that the patient did not take the pills. Now, via collaborative edge, the pharmacy can provide the purchasing record of a patient to the hospital, which significantly facilitates healthcare accountability.

At the same time, the pharmacies retrieve the population of the flu outbreak using the collaborative edge services provided by hospitals. An apparent benefit is that the pharmacies have enough inventory to obtain much more profits.

Behind the drug purchasing, the pharmacy can leverage data provided by pharmaceutical companies and retrieve the locations, prices and inventories of all drug warehouses. It also sends a transport price query request to the logistics companies. Then the pharmacy can make an order plan by solving the total cost optimization problem according to retrieved information.

The centers for disease control and prevention, as our government representative in our case, is monitoring the flu population increasing at wide range areas, can consequently raise a flu alert to the people in the involved areas. Besides, further actions can be taken to prevent the spread of flu outbreak. After the flu outbreak, the insurance companies have to pay the bill for the patients based on the policy. The insurance companies can analyze the proportion of pe ople who has the flu during the outbreak.

Thus most of the participants can benefit from collaborative edge in terms of reducing operational cost and improving profitability.




.

Future Generation Computer Systems 29 (2013) 1645–1660

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# Internet of Things (IoT): A vision, architectural elements, and future directions

Jayavardhana Gubbi [a], Rajkumar Buyya [b,*], Slaven Marusic [a], Marimuthu Palaniswami [a]

[a] Department of Electrical and Electronic Engineering, The University of Melbourne, Vic - 3010, Australia

[b] Department of Computing and Information Systems, The University of Melbourne, Vic - 3010, Australia

## HIGHLIGHTS

- Presents vision and motivations for Internet of Things (IoT).
- Application domains in the IoT with a new approach in defining them.
- Cloud-centric IoT realization and challenges.
- Open challenges and future trends in Cloud Centric Internet of Things.

## ARTICLE INFO

*Article history:*
Received 8 July 2012
Received in revised form
22 December 2012
Accepted 30 January 2013
Available online 24 February 2013

*Keywords:*
Internet of Things
Ubiquitous sensing
Cloud computing
Wireless sensor networks
RFID
Smart environments

## ABSTRACT

Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly. This paper presents a Cloud centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A Cloud implementation using *Aneka*, which is based on interaction of private and public Clouds is presented. We conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.



## 1. Introduction

The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency IDentification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities. Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that Cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere.

Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IoT. With the growing presence of WiFi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident. However, for the Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment. For technology to *disappear* from the consciousness of the user, the Internet of Things demands: (1) a shared understanding of the situation of its users and their appliances,

* Corresponding author. Tel.: +61 3 83441344; fax: +61 3 93481184.
*E-mail addresses:* rbuyya@unimelb.edu.au, raj@cs.mu.oz.au (R. Buyya).
*URL:* http://www.buyya.com (R. Buyya).

0167-739X/$ – see front matter 
http://dx.doi.org/10.1016/j.future.2013.01.010

(2) software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant, and (3) the analytics tools in the Internet of Things that aim for autonomous and smart behavior. With these three fundamental grounds in place, smart connectivity and context-aware computation can be accomplished.

The term Internet of Things was first coined by Kevin Ashton in 1999 in the context of supply chain management [1]. However, in the past decade, the definition has been more inclusive covering wide range of applications like healthcare, utilities, transport, etc. [2]. Although the definition of 'Things' has changed as technology evolved, the main goal of making a computer sense information without the aid of human intervention remains the same. A radical evolution of the current Internet into a Network of interconnected *objects* that not only harvests information from the environment (sensing) and interacts with the physical world (actuation/command/control), but also uses existing Internet standards to provide services for information transfer, analytics, applications, and communications. Fueled by the prevalence of devices enabled by open wireless technology such as Bluetooth, radio frequency identification (RFID), Wi-Fi, and telephonic data services as well as embedded sensor and actuator nodes, IoT has stepped out of its infancy and is on the verge of transforming the current static Internet into a fully integrated Future Internet [3]. The Internet revolution led to the interconnection between people at an unprecedented scale and pace. The next revolution will be the interconnection between objects to create a smart environment. Only in 2011 did the number of interconnected devices on the planet overtake the actual number of people. Currently there are 9 billion interconnected devices and it is expected to reach 24 billion devices by 2020. According to the GSMA, this amounts to $1.3 trillion revenue opportunities for mobile network operators alone spanning vertical segments such as health, automotive, utilities and consumer electronics. A schematic of the interconnection of objects is depicted in Fig. 1, where the application domains are chosen based on the scale of the impact of the data generated. The users span from individual to national level organizations addressing wide ranging issues.

This paper presents the current trends in IoT research propelled by applications and the need for convergence in several interdisciplinary technologies. Specifically, in Section 2, we present the overall IoT vision and the technologies that will achieve it followed by some common definitions in the area along with some trends and taxonomy of IoT in Section 3. We discuss several application domains in IoT with a new approach in defining them in Section 4 and Section 5 provides our Cloud centric IoT vision. A case study of data analytics on the Aneka/Azure cloud platform is given in Section 6 and we conclude with discussions on open challenges and future trends in Section 7.

## 2. Ubiquitous computing in the next decade

The effort by researchers to create a human-to-human interface through technology in the late 1980s resulted in the creation of the ubiquitous computing discipline, whose objective is to embed technology into the background of everyday life. Currently, we are in the post-PC era where smart phones and other handheld devices are changing our environment by making it more interactive as well as informative. Mark Weiser, the forefather of Ubiquitous Computing (ubicomp), defined a smart environment [4] as "the physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network".

The creation of the Internet has marked a foremost milestone towards achieving ubicomp's vision which enables individual devices to communicate with any other device in the world. The inter-networking reveals the potential of a seemingly endless amount of distributed computing resources and storage owned by various owners.

In contrast to Weiser's Calm computing approach, Rogers proposes a human centric ubicomp which makes use of human creativity in exploiting the environment and extending their capabilities [5]. He proposes a domain specific ubicomp solution when he says—"In terms of who should benefit, it is useful to think of how ubicomp technologies can be developed not for the Sal's of the world, but for particular domains that can be set up and customized by an individual firm or organization, such as for agricultural production, environmental restoration or retailing".

Caceres and Friday [6] discuss the progress, opportunities and challenges during the 20 year anniversary of ubicomp. They discuss the building blocks of ubicomp and the characteristics of the system to adapt to the changing world. More importantly, they identify two critical technologies for growing the ubicomp infrastructure—*Cloud Computing* and the *Internet of Things*.

The advancements and convergence of micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics has resulted in the development of miniature devices having the ability to sense, compute, and communicate wirelessly in short distances. These miniature devices called nodes interconnect to form a wireless sensor networks (WSN) and find wide ranging applications in environmental monitoring, infrastructure monitoring, traffic monitoring, retail, etc. [7]. This has the ability to provide a ubiquitous sensing capability which is critical in realizing the overall vision of ubicomp as outlined by Weiser [4]. For the realization of a complete IoT vision, efficient, secure, scalable and market oriented computing and storage resourcing is essential. Cloud computing [6] is the most recent paradigm to emerge which promises reliable services delivered through next generation data centers that are based on virtualized storage technologies. This platform acts as a receiver of data from the ubiquitous sensors; as a computer to analyze and interpret the data; as well as providing the user with easy to understand web based visualization. The ubiquitous sensing and processing works in the background, *hidden* from the user.

This novel integrated Sensor–Actuator–Internet framework shall form the core technology around which a smart environment will be shaped: information generated will be shared across diverse platforms and applications, to develop a common operating picture (COP) of an environment, where control of certain unrestricted 'Things' is made possible. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases. To take full advantage of the available Internet technology, there is a need to deploy large-scale, platform-independent, wireless sensor network infrastructure that includes data management and processing, actuation and analytics. Cloud computing promises high reliability, scalability and autonomy to provide ubiquitous access, dynamic resource discovery and composability required for the next generation Internet of Things applications. Consumers will be able to choose the service level by changing the Quality of Service parameters.

## 3. Definitions, trends and elements

### 3.1. Definitions

As identified by Atzori et al. [8], Internet of Things can be realized in three paradigms—internet-oriented (middleware), things oriented (sensors) and semantic-oriented (knowledge). Although this type of delineation is required due to the interdisciplinary nature of the subject, the usefulness of IoT can be unleashed only in an application domain where the three paradigms intersect.
The RFID group defines the Internet of Things as –

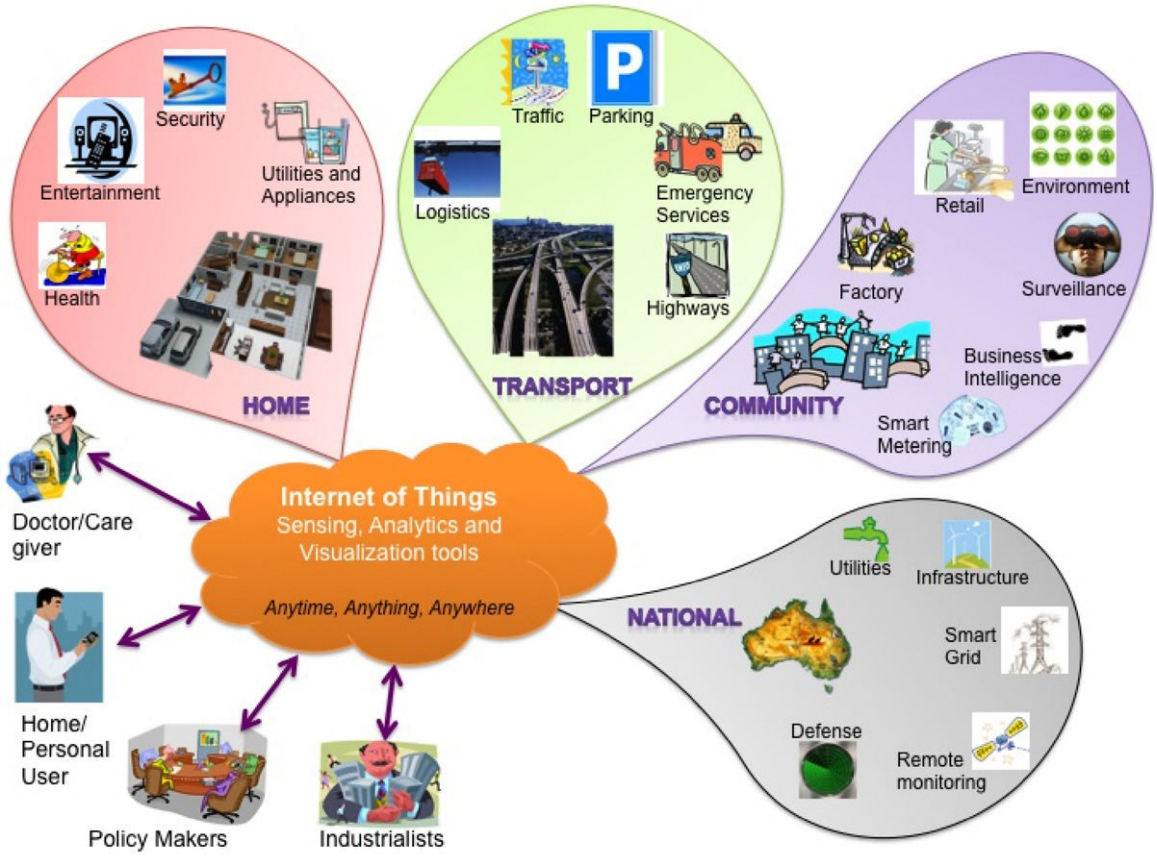



**Fig. 1.** Internet of Things schematic showing the end users and application areas based on data.

- The worldwide network of interconnected objects uniquely addressable based on standard communication protocols.

According to Cluster of European research projects on the Internet of Things [2] –

- 'Things' are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention.

According to Forrester [9], a smart environment –

- Uses information and communications technologies to make the critical infrastructure components and services of a city's administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient.

In our definition, we make the definition more user centric and do not restrict it to any standard communication protocol. This will allow long-lasting applications to be developed and deployed using the available state-of-the-art protocols at any given point in time. Our definition of the Internet of Things for smart environments is –

- Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with Cloud computing as the unifying framework.

### 3.2. Trends

Internet of Things has been identified as one of the emerging technologies in IT as noted in Gartner's IT Hype Cycle (see Fig. 2). A Hype Cycle [10] is a way to represent the emergence, adoption, maturity, and impact on applications of specific technologies. It has been forecasted that IoT will take 5–10 years for market adoption.

The popularity of different paradigms varies with time. The web search popularity, as measured by the Google search trends during the last 10 years for the terms Internet of Things, Wireless Sensor Networks and Ubiquitous Computing are shown in Fig. 3 [11]. As it can be seen, since IoT has come into existence, search volume is consistently increasing with the falling trend for Wireless Sensor Networks. As per Google's search forecast (dotted line in Fig. 3), this trend is likely to continue as other enabling technologies converge to form a genuine Internet of Things.

### 3.3. IoT elements

We present a taxonomy that will aid in defining the components required for the Internet of Things from a high level perspective. Specific taxonomies of each component can be found elsewhere [12–14]. There are three IoT components which enables seamless ubicomp: (a) Hardware—made up of sensors, actuators and embedded communication hardware (b) Middleware—on demand storage and computing tools for data analytics and (c) Presentation—novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications. In this section, we discuss a few enabling technologies in these categories which will make up the three components stated above.

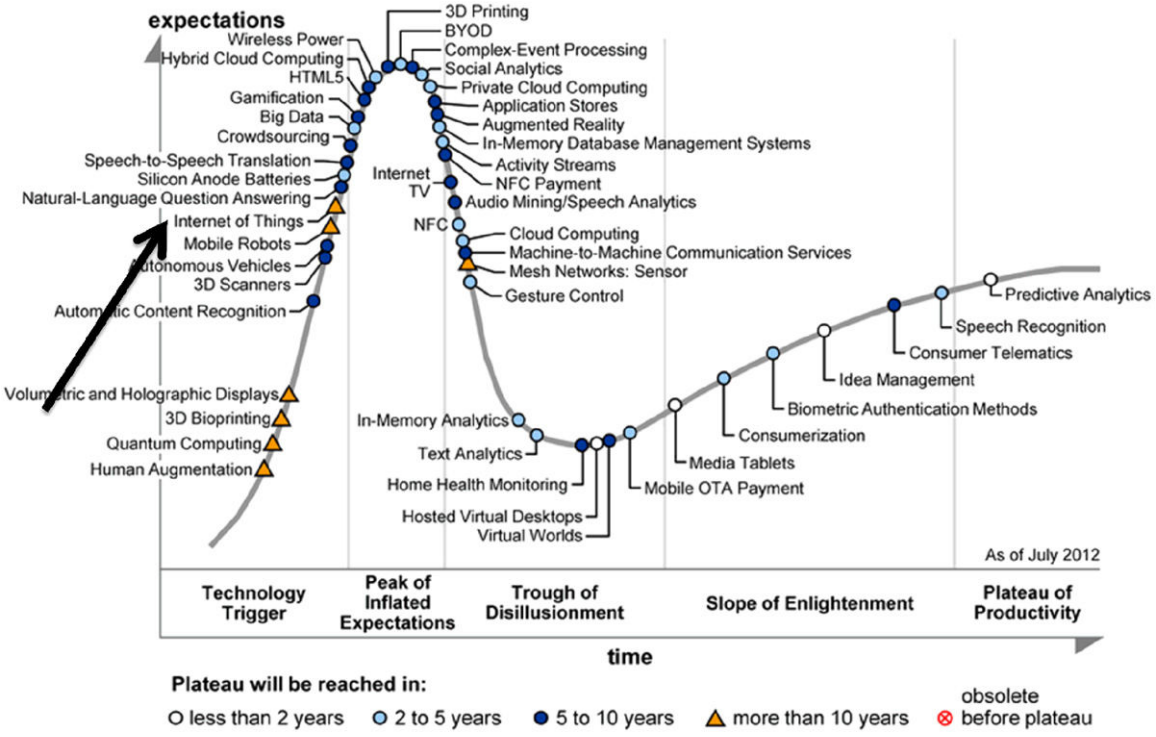



**Fig. 2.** Gartner 2012 Hype Cycle of emerging technologies.
*Source:* Gartner Inc. [10].

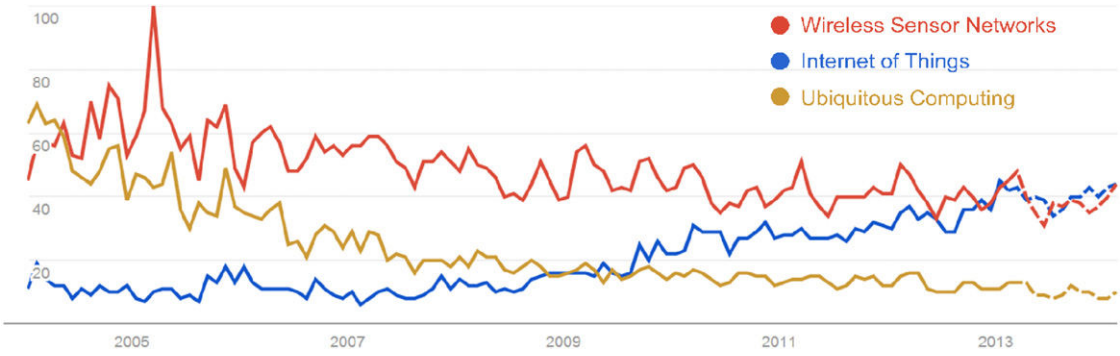



**Fig. 3.** Google search trends since 2004 for terms Internet of Things, Wireless Sensor Networks, Ubiquitous Computing.

### 3.3.1. Radio Frequency Identification (RFID)

RFID technology is a major breakthrough in the embedded communication paradigm which enables design of microchips for wireless data communication. They help in the automatic identification of anything they are attached to acting as an electronic barcode [15,16]. The passive RFID tags are not battery powered and they use the power of the reader's interrogation signal to communicate the ID to the RFID reader. This has resulted in many applications particularly in retail and supply chain management. The applications can be found in transportation (replacement of tickets, registration stickers) and access control applications as well. The passive tags are currently being used in many bank cards and road toll tags which are among the first global deployments. Active RFID readers have their own battery supply and can instantiate the communication. Of the several applications, the main application of active RFID tags is in port containers [16] for monitoring cargo.

### 3.3.2. Wireless Sensor Networks (WSN)

Recent technological advances in low power integrated circuits and wireless communications have made available efficient, low cost, low power miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing, analysis and dissemination of valuable information, gathered in a variety of environments [7]. Active RFID is nearly the same as the lower end WSN nodes with limited processing capability and storage. The scientific challenges that must be overcome in order to realize the enormous potential of WSNs are substantial and multidisciplinary in nature [7]. Sensor data are shared among sensor nodes and sent to a distributed or centralized system for analytics. The components that make up the WSN monitoring network include:

(a) WSN hardware—Typically a node (WSN core hardware) contains sensor interfaces, processing units, transceiver units and power supply. Almost always, they comprise of multiple A/D converters for sensor interfacing and more modern sensor nodes have the ability to communicate using one frequency band making them more versatile [7].
(b) WSN communication stack—The nodes are expected to be deployed in an ad-hoc manner for most applications. Designing

an appropriate topology, routing and MAC layer is critical for the scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base station. Node drop outs, and consequent degraded network lifetimes, are frequent. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet [17].

(c) WSN Middleware—A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner [17]. This is based on the idea of isolating resources that can be used by several applications. A platform-independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture (OSWA) [18]. OSWA is built upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method (SWE) by the Open Geospatial Consortium (OGC).

(d) Secure Data aggregation—An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors [18]. Node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important.

#### 3.3.3. Addressing schemes

The ability to uniquely identify 'Things' is critical for the success of IoT. This will not only allow us to uniquely identify billions of devices but also to control remote devices through the Internet. The few most critical features of creating a unique address are: uniqueness, reliability, persistence and scalability.

Every element that is already connected and those that are going to be connected, must be identified by their unique identification, location and functionalities. The current IPv4 may support to an extent where a group of cohabiting sensor devices can be identified geographically, but not individually. The Internet Mobility attributes in the IPV6 may alleviate some of the device identification problems; however, the heterogeneous nature of wireless nodes, variable data types, concurrent operations and confluence of data from devices exacerbates the problem further [19].

Persistent network functioning to channel the data traffic ubiquitously and relentlessly is another aspect of IoT. Although, the TCP/IP takes care of this mechanism by routing in a more reliable and efficient way, from source to destination, the IoT faces a bottleneck at the interface between the gateway and wireless sensor devices. Furthermore, the scalability of the device address of the existing network must be sustainable. The addition of networks and devices must not hamper the performance of the network, the functioning of the devices, the reliability of the data over the network or the effective use of the devices from the user interface.

To address these issues, the Uniform Resource Name (URN) system is considered fundamental for the development of IoT. URN creates replicas of the resources that can be accessed through the URL. With large amounts of spatial data being gathered, it is often quite important to take advantage of the benefits of metadata for transferring the information from a database to the user via the Internet [20]. IPv6 also gives a very good option to access the resources uniquely and remotely. Another critical development in addressing is the development of a lightweight IPv6 that will enable addressing home appliances uniquely.

Wireless sensor networks (considering them as building blocks of IoT), which run on a different stack compared to the Internet, cannot possess IPv6 stack to address individually and hence a subnet with a gateway having a URN will be required. With this in mind, we then need a layer for addressing sensor devices by the relevant gateway. At the subnet level, the URN for the sensor devices could be the unique IDs rather than human-friendly names as in the www, and a lookup table at the gateway to address this device. Further, at the node level each sensor will have a URN (as numbers) for sensors to be addressed by the gateway. The entire network now forms a web of connectivity from users (high-level) to sensors (low-level) that is addressable (through URN), accessible (through URL) and controllable (through URC).

#### 3.3.4. Data storage and analytics

One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data. Storage, ownership and expiry of the data become critical issues. The internet consumes up to 5% of the total energy generated today and with these types of demands, it is sure to go up even further. Hence, data centers that run on harvested energy and are centralized will ensure energy efficiency as well as reliability. The data have to be stored and used intelligently for smart monitoring and actuation. It is important to develop artificial intelligence algorithms which could be centralized or distributed based on the need. Novel fusion algorithms need to be developed to make sense of the data collected. State-of-the-art non-linear, temporal machine learning methods based on evolutionary algorithms, genetic algorithms, neural networks, and other artificial intelligence techniques are necessary to achieve automated decision making. These systems show characteristics such as interoperability, integration and adaptive communications. They also have a modular architecture both in terms of hardware system design as well as software development and are usually very well-suited for IoT applications. More importantly, a centralized infrastructure to support storage and analytics is required. This forms the IoT middleware layer and there are numerous challenges involved which are discussed in future sections. As of 2012, Cloud based storage solutions are becoming increasingly popular and in the years ahead, Cloud based analytics and visualization platforms are foreseen.

#### 3.3.5. Visualization

Visualization is critical for an IoT application as this allows the interaction of the user with the environment. With recent advances in touch screen technologies, use of smart tablets and phones has become very intuitive. For a lay person to fully benefit from the IoT revolution, attractive and easy to understand visualization has to be created. As we move from 2D to 3D screens, more information can be provided in meaningful ways for consumers. This will also enable policy makers to convert data into knowledge, which is critical in fast decision making. Extraction of meaningful information from raw data is non-trivial. This encompasses both event detection and visualization of the associated raw and modeled data, with information represented according to the needs of the end-user.

## 4. Applications

There are several application domains which will be impacted by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact [21]. We categorize the applications into four application domains: (1) Personal and Home; (2) Enterprize; (3) Utilities; and (4) Mobile. This is depicted in Fig. 1, which represents Personal and Home IoT at the scale of an individual or home, Enterprize IoT at the scale of a community, Utility IoT at a national or regional scale and Mobile IoT which is usually spread across other domains mainly due to the nature of connectivity and scale. There is a huge crossover

in applications and the use of data between domains. For instance, the Personal and Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company which can in turn optimize the supply and demand in the Utility IoT. The internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities. A few typical applications in each domain are given.

### 4.1. Personal and home

The sensor information collected is used only by the individuals who directly own the network. Usually WiFi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound).

Ubiquitous healthcare [8] has been envisioned for the past two decades. IoT gives a perfect platform to realize this vision using body area sensors and IoT back end to upload the data to servers. For instance, a Smartphone can be used for communication along with several interfaces like Bluetooth for interfacing sensors measuring physiological parameters. So far, there are several applications available for Apple iOS, Google Android and Windows Phone operating systems that measure various parameters. However, it is yet to be centralized in the cloud for general physicians to access the same.

An extension of the personal body area network is creating a home monitoring system for elderly care, which allows the doctor to monitor patients and the elderly in their homes thereby reducing hospitalization costs through early intervention and treatment [22,23].

Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. This will see consumers become involved in the IoT revolution in the same manner as the Internet revolution itself [24,25]. Social networking is set to undergo another transformation with billions of interconnected objects [26,27]. An interesting development will be using a Twitter like concept where individual 'Things' in the house can periodically tweet the readings which can be easily followed from anywhere creating a *TweetOT*. Although this provides a common framework using cloud for information access, a new security paradigm will be required for this to be fully realized [28].

### 4.2. Enterprize

We refer to the 'Network of Things' within a work environment as an enterprize based application. Information collected from such networks are used only by the owners and the data may be released selectively. Environmental monitoring is the first common application which is implemented to keep track of the number of occupants and manage the utilities within the building (e.g., HVAC, lighting).

Sensors have always been an integral part of the factory setup for security, automation, climate control, etc. This will eventually be replaced by a wireless system giving the flexibility to make changes to the setup whenever required. This is nothing but an IoT subnet dedicated to factory maintenance.

One of the major IoT application areas that is already drawing attention is Smart Environment IoT [21,28]. There are several testbeds being implemented and many more planned in the coming years. Smart environment includes subsystems as shown in Table 1 and the characteristics from a technological perspective are listed briefly. It should be noted that each of the sub domains cover many focus groups and the data will be shared. The applications or use-cases within the urban environment that can benefit from the realization of a smart city WSN capability are shown in Table 2. These applications are grouped according to their impact areas. This includes the effect on citizens considering health and well being issues; transport in light of its impact on mobility, productivity, pollution; and services in terms of critical community services managed and provided by local government to city inhabitants.

### 4.3. Utilities

The information from the networks in this application domain is usually for service optimization rather than consumer consumption. It is already being used by utility companies (smart meter by electricity supply companies) for resource management in order to optimize cost *vs.* profit. These are made up of very extensive networks (usually laid out by large organization on a regional and national scale) for monitoring critical utilities and efficient resource management. The backbone network used can vary between cellular, WiFi and satellite communication.

Smart grid and smart metering is another potential IoT application which is being implemented around the world [38]. Efficient energy consumption can be achieved by continuously monitoring every electricity point within a house and using this information to modify the way electricity is consumed. This information at the city scale is used for maintaining the load balance within the grid ensuring high quality of service.

Video based IoT [39], which integrates image processing, computer vision and networking frameworks, will help develop a new challenging scientific research area at the intersection of video, infrared, microphone and network technologies. Surveillance, the most widely used camera network applications, helps track targets, identify suspicious activities, detect left luggage and monitor unauthorized access. Automatic behavior analysis and event detection (as part of sophisticated video analytics) is in its infancy and breakthroughs are expected in the next decade as pointed out in the 2012 Gartner Chart (refer Fig. 2).

Water network monitoring and quality assurance of drinking water is another critical application that is being addressed using IoT. Sensors measuring critical water parameters are installed at important locations in order to ensure high supply quality. This avoids accidental contamination among storm water drains, drinking water and sewage disposal. The same network can be extended to monitor irrigation in agricultural land. The network is also extended for monitoring soil parameters which allows informed decision making concerning agriculture [40].

### 4.4. Mobile

Smart transportation and smart logistics are placed in a separate domain due to the nature of data sharing and backbone implementation required. Urban traffic is the main contributor to traffic noise pollution and a major contributor to urban air quality degradation and greenhouse gas emissions. Traffic congestion directly imposes significant costs on economic and social activities in most cities. Supply chain efficiencies and productivity, including just-in-time operations, are severely impacted by this congestion causing freight delays and delivery schedule failures. Dynamic traffic information will affect freight movement, allow better planning and improved scheduling. The transport IoT will enable the use of large scale WSNs for online monitoring of travel times, origin–destination (O–D) route choice behavior, queue lengths and air pollutant and noise emissions. The IoT is likely to replace the traffic information provided by the existing sensor networks of inductive loop vehicle detectors employed at the intersections of existing traffic control systems. They will also underpin the development of scenario-based models for the planning and design of mitigation and alleviation plans, as well as improved algorithms for urban traffic control, including multi-objective control systems. Combined with information gathered from the urban traffic control

**Table 1**
Smart environment application domains.

| | Smart home/office | Smart retail | Smart city | Smart agriculture/forest | Smart water | Smart transportation |
|---|---|---|---|---|---|---|
| Network size | Small | Small | Medium | Medium/large | Large | Large |
| Users | Very few, family members | Few, community level | Many, policy makers, general public | Few, landowners, policy makers | Few, government | Large, general public |
| Energy | Rechargeable battery | Rechargeable battery | Rechargeable battery, energy harvesting | Energy harvesting | Energy harvesting | Rechargeable battery, Energy harvesting |
| Internet connectivity | Wifi, 3G, 4G LTE backbone | Wifi, 3G, 4G LTE backbone | Wifi, 3G, 4G LTE backbone | Wifi, satellite communication | Satellite communication, microwave links | Wifi, satellite communication |
| Data management | Local server | Local server | Shared server | Local server, shared server | Shared server | Shared server |
| IoT devices | RFID, WSN | RFID, WSN | RFID, WSN | WSN | Single sensors | RFID, WSN, single sensors |
| Bandwidth requirement | Small | Small | Large | Medium | Medium | Medium/large |
| Example testbeds | Aware home [29] | SAP future retail center [30] | Smart Santander [31], citySense [32] | SiSViA [33] | GBROOS [34], SEMAT [35] | A few trial implementations [36,37] |

**Table 2**
Potential IoT applications identified by different focus groups of the city of Melbourne.

| | |
|---|---|
| Citizens | |
| Healthcare | Triage, patient monitoring, personnel monitoring, disease spread modeling and containment—real-time health status and predictive information to assist practitioners in the field, or policy decisions in pandemic scenarios |
| Emergency services, defense | Remote personnel monitoring (health, location); resource management and distribution, response planning; sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios |
| Crowd monitoring | Crowd flow monitoring for emergency management; efficient use of public and retail spaces; workflow in commercial environments |
| Transport | |
| Traffic management | Intelligent transportation through real-time traffic information and path optimization |
| Infrastructure monitoring | Sensors built into infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination |
| Services | |
| Water | Water quality, leakage, usage, distribution, waste management |
| Building management | Temperature, humidity control, activity monitoring for energy usage management, *D* heating, Ventilation and Air Conditioning (HVAC) |
| Environment | Air pollution, noise monitoring, waterways, industry monitoring |

system, valid and relevant information on traffic conditions can be presented to travelers [41].

The prevalence of Bluetooth technology (BT) devices reflects the current IoT penetration in a number of digital products such as mobile phones, car hands-free sets, navigation systems, etc. BT devices emit signals with a unique Media Access Identification (MAC-ID) number that can be read by BT sensors within the coverage area. Readers placed at different locations can be used to identify the movement of the devices. Complemented by other data sources such as traffic signals, or bus GPS, research problems that can be addressed include vehicle travel time on motorways and arterial streets, dynamic (time dependent) O–D matrices on the network, identification of critical intersections, and accurate and reliable real time transport network state information [37]. There are many privacy concerns by such usages and digital forgetting is an emerging domain of research in IoT where privacy is a concern [42].

Another important application in mobile IoT domain is efficient logistics management [37]. This includes monitoring the items being transported as well as efficient transportation planning. The monitoring of items is carried out more locally, say, within a truck replicating enterprize domain but transport planning is carried out using a large scale IoT network.

## 5. Cloud centric Internet of Things

The vision of IoT can be seen from two perspectives—'Internet' centric and 'Thing' centric. The Internet centric architecture will involve internet services being the main focus while data is contributed by the objects. In the object centric architecture [43], the smart objects take the center stage. In our work, we develop an Internet centric approach. A conceptual framework integrating the ubiquitous sensing devices and the applications is shown in Fig. 4. In order to realize the full potential of cloud computing as well as ubiquitous sensing, a combined framework with a cloud at the center seems to be most viable. This not only gives the flexibility of dividing associated costs in the most logical manner but is also highly scalable. Sensing service providers can join the network and offer their data using a storage cloud; analytic tool developers can provide their software tools; artificial intelligence experts can provide their data mining and machine learning tools useful in converting information to knowledge and finally computer graphics designers can offer a variety of visualization tools. Cloud computing can offer these services as Infrastructures, Platforms or Software where the full potential of human creativity can be tapped using them as services. This in some sense agrees with the ubicomp vision of Weiser as well as Rogers' human centric approach. The data generated, tools used and the visualization created *disappears* into the background, tapping the full potential of the Internet of Things in various application domains. As can be seen from Fig. 4, the Cloud integrates all ends of ubicomp by providing scalable storage, computation time and other tools to build new businesses. In this section, we describe the cloud platform using Manjrasoft Aneka and Microsoft Azure platforms to demonstrate how cloud integrates storage, computation and visualization paradigms. Furthermore, we introduce an important realm of interaction between clouds which is useful for combining public and private clouds using Aneka. This interaction is critical for application developers in order to bring sensed information, analytics algorithms and visualization under one single seamless framework.

However, developing IoT applications using low-level Cloud programming models and interfaces such as Thread and MapRe-

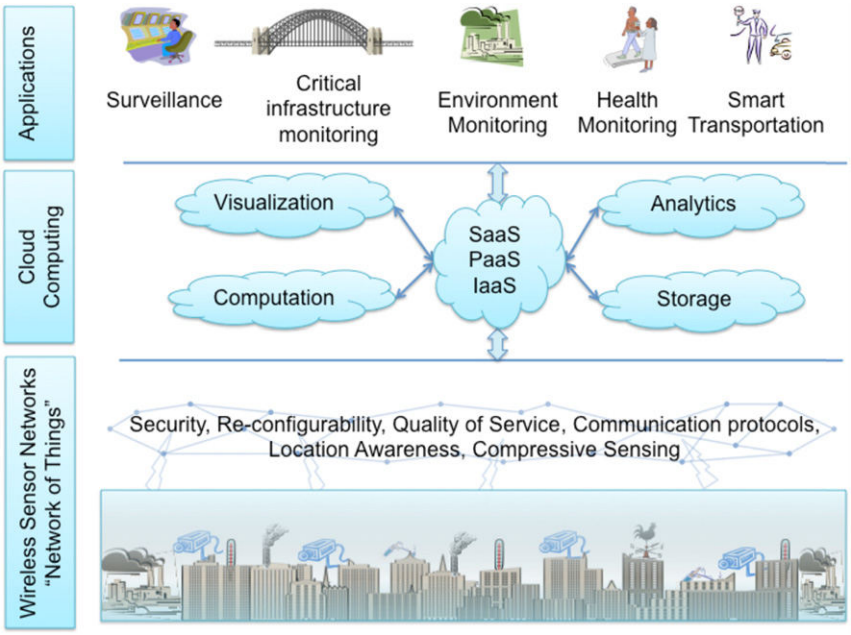



**Fig. 4.** Conceptual IoT framework with Cloud Computing at the center.

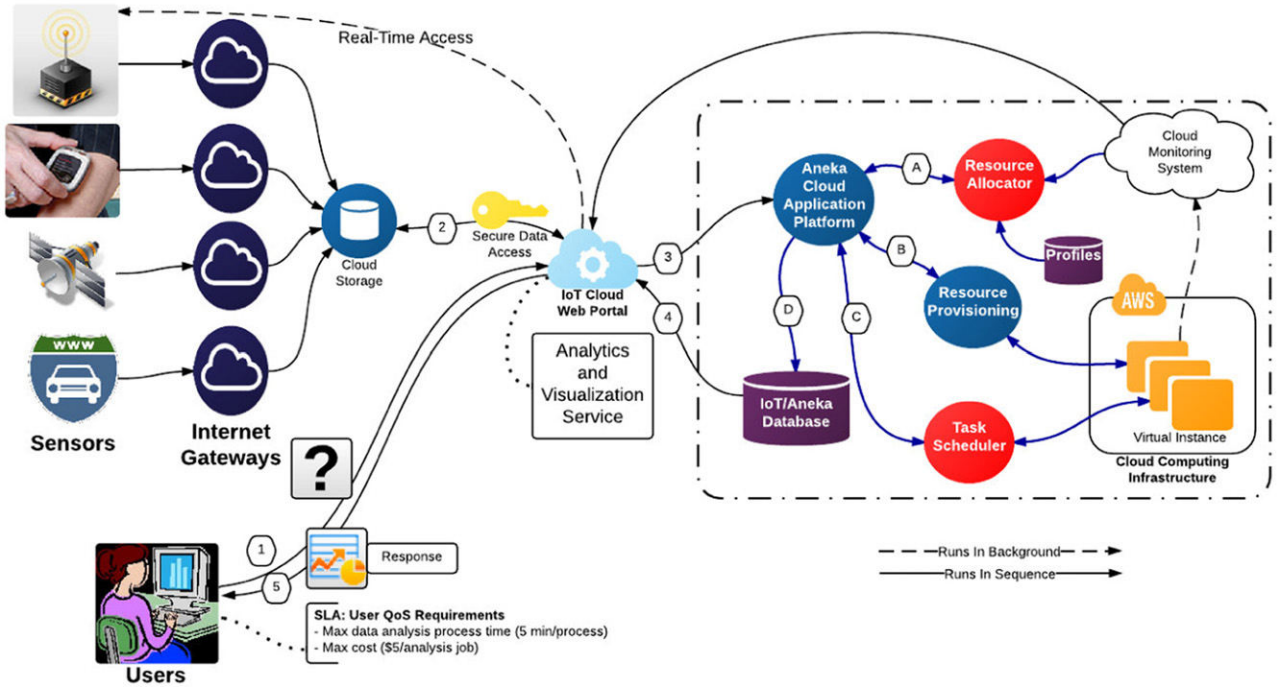



**Fig. 5.** A model of end-to-end interaction between various stakeholders in Cloud centric IoT framework.

duce models is complex. To overcome this, we need a IoT application specific framework for rapid creation of applications and their deployment on Cloud infrastructures. This is achieved by mapping the proposed framework to Cloud APIs offered by platforms such as Aneka. Therefore, the new IoT application specific framework should be able to provide support for (1) reading data streams either from senors directly or fetch the data from databases, (2) easy expression of data analysis logic as functions/operators that process data streams in a transparent and scalable manner on Cloud infrastructures, and (3) if any events of interest are detected, outcomes should be passed to output streams, which are connected to a visualization program. Using such a framework, the developer of IoT applications will able to harness the power of Cloud computing without knowing low-level details of creating reliable and scale applications. A model for the realization of such an environment for IoT applications is shown in Fig. 5, thus reducing the time and cost involved in engineering IoT applications.

### 5.1. Aneka cloud computing platform

Aneka is a .NET-based application development Platform-as-a-Service (PaaS), which can utilize storage and compute resources of both public and private clouds [44]. It offers a runtime environment and a set of APIs that enable developers to build cus-

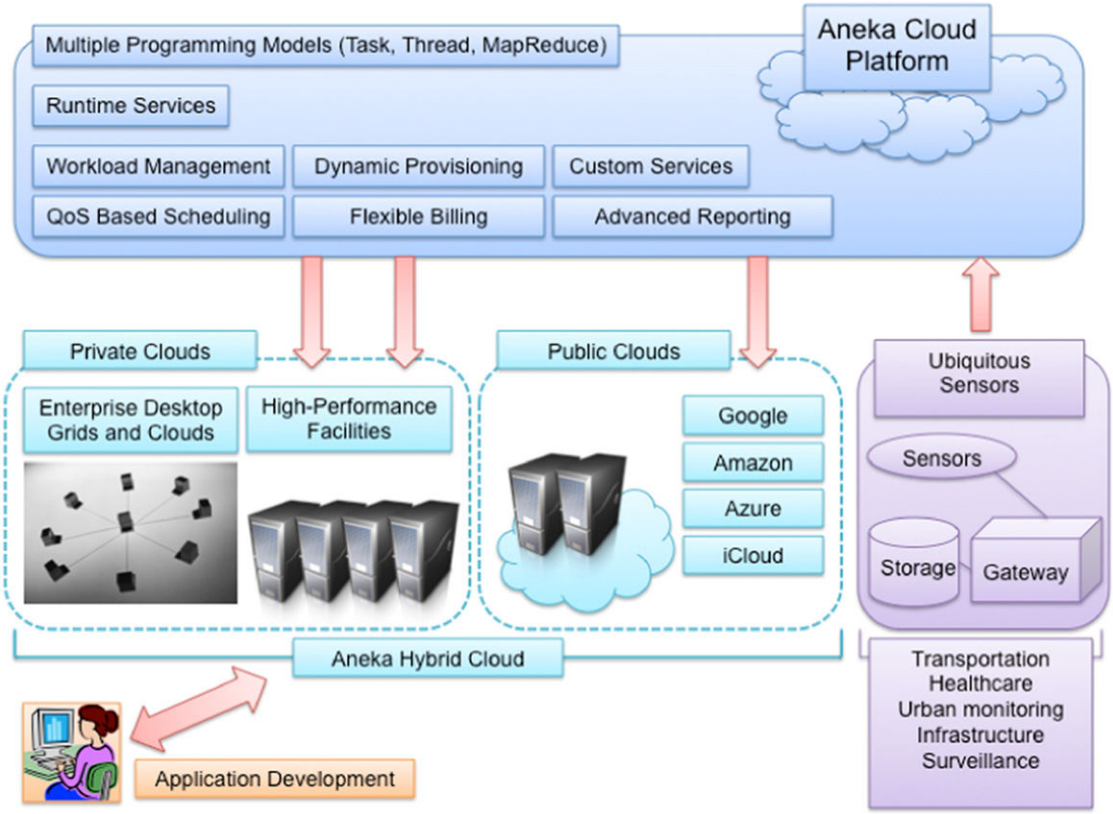



**Fig. 6.** Overview of Aneka within Internet of Things architecture.

tomized applications by using multiple programming models such as Task Programming, Thread Programming and MapReduce Programming. Aneka provides a number of services that allow users to control, auto-scale, reserve, monitor and bill users for the resources used by their applications. In the context of Smart Environment application, Aneka PaaS has another important characteristic of supporting the provisioning of resources on public clouds such as Microsoft Azure, Amazon EC2, and GoGrid, while also harnessing private cloud resources ranging from desktops and clusters, to virtual data centers. An overview of Aneka PaaS is shown in Fig. 6 [45]. For the application developer, the cloud service as well as ubiquitous sensor data is hidden and they are provided as services at a cost by the Aneka provisioning tool. Automatic management of clouds for hosting and delivering IoT services as SaaS (Software-as-a-Service) applications will be the integrating platform of the Future Internet. There is a need to create data and service sharing infrastructure which can be used for addressing several application scenarios. For example, anomaly detection in sensed data carried out at the Application layer is a service which can be shared between several applications. Existing/new applications deployed as a hosted service and accessed over the Internet are referred to as SaaS. To manage SaaS applications on a large scale, the Platform as a Service (PaaS) layer needs to coordinate the cloud (resource provisioning and application scheduling) without impacting the Quality of Service (QoS) requirements of any application. The autonomic management components are to be put in place to schedule and provision resources with a higher level of accuracy to support IoT applications. This coordination requires the PaaS layer to support autonomic management capabilities required to handle the scheduling of applications and resource provisioning such that the user QoS requirements are satisfied. The autonomic management components are thus put in place to schedule and provision resources with a higher level of accuracy to support IoT applications. The autonomic management system will tightly integrate the following services with the Aneka framework: Accounting, Monitoring and Profiling, Scheduling, and Dynamic Provisioning. Accounting, Monitoring, and Profiling will feed the sensors of the autonomic manager, while the managers' effectors will control Scheduling and Dynamic Provisioning. From a logical point of view the two components that will mostly take advantage of the introduction of autonomic features in Aneka are the application scheduler and the Dynamic Resource Provisioning.

### *5.2. Application scheduler and Dynamic Resource Provisioning in Aneka for IoT applications*

The Aneka scheduler is responsible for assigning each resource to a task in an application for execution based on user QoS parameters and the overall cost for the service provider. Depending on the computation and data requirements of each Sensor Application, it directs the dynamic resource provisioning component to instantiate or terminate a specified number of computing, storage, and network resources while maintaining a queue of tasks to be scheduled. This logic is embedded as multi-objective application scheduling algorithms. The scheduler is able to mange resource failures by re-allocating those tasks to other suitable Cloud resources.

The Dynamic Resource Provisioning component implements the logic for provisioning and managing virtualized resources in the private and public cloud computing environments based on the resource requirements as directed by the application scheduler. This is achieved by dynamically negotiating with the Cloud Infrastructure as a Service (IaaS) providers for the right kind of resource for a certain time and cost by taking into account the past execution history of applications and budget availability. This decision is made at runtime, when SaaS applications continuously send requests to the Aneka cloud platform [46].

**Table 3**
Microsoft Azure components.

| Microsoft Azure | On demand compute services, storage services |
|---|---|
| SQL Azure | Supports Transact-SQL and support for the synchronization of relational data across SQL Azure and on-premises SQL server |
| AppFabric | Interconnecting cloud and on-premise applications; Accessed through the HTTP REST API |
| Azure Marketplace | Online service for making transactions on apps and data |

## 6. IoT Sensor data analytics SaaS using Aneka and Microsoft Azure

Microsoft Azure is a cloud platform, offered by Microsoft, includes four components as summarized in Table 3 [44]. There are several advantages for integrating Azure and Aneka. Aneka can launch any number of instances on the Azure cloud to run their applications. Essentially, it provides the provisioning infrastructure. Similarly, Aneka provides advanced PaaS features as shown in Fig. 6. It provides multiple programming models (Task, Thread, MapReduce), runtime execution services, workload management services, dynamic provisioning, QoS based scheduling and flexible billing.

As discussed earlier, to realize the ubicomp vision, tools and data need to be shared between application developers to create new apps. There are two major hurdles in such an implementation. Firstly, interaction between clouds becomes critical which is addressed by Aneka in the InterCloud model. Aneka support for the InterCloud model enables the creation of a hybrid Cloud computing environment that combines the resources of private and public Clouds. That is, whenever a private Cloud is unable to meet application QoS requirements, Aneka leases extra capability from a public Cloud to ensure that the application is able to execute within a specified deadline in a seamless manner [45]. Secondly, data analytics and artificial intelligence tools are computationally demanding, which requires huge resources. For data analytics and artificial intelligence tools, the Aneka task programming model provides the ability of expressing applications as a collection of independent tasks. Each task can perform different operations, or the same operation on different data, and can be executed in any order by the runtime environment. In order to demonstrate this, we have used a scenario where there are multiple analytics algorithms and multiple data sources. A schematic of the interaction between Aneka and Azure is given in Fig. 7, where Aneka Worker Containers are deployed as instances of Azure Worker Role [44]. The Aneka Master Container will be deployed in the on-premises private cloud, while Aneka Worker Containers will be run as instances of Microsoft Azure Worker Role. As shown in Fig. 7, there are two types of Microsoft Azure Worker Roles used. These are the Aneka Worker Role and Message Proxy Role. In this case, one instance of the Message Proxy Role and at least one instance of the Aneka Worker Role are deployed. The maximum number of instances of the Aneka Worker Role that can be launched is limited by the subscription offer of Microsoft Azure Service that a user selects. In this deployment scenario, when a user submits an application to the Aneka Master, the job units will be scheduled by the Aneka Master by leveraging on-premises Aneka Workers, if they exist, and Aneka Worker instances on Microsoft Azure simultaneously. When Aneka Workers finish the execution of Aneka work units, they will send the results back to Aneka Master, and then Aneka Master will send the result back to the user application.

There are many interoperability issues when scaling across multiple Clouds. Aneka overcomes this problem by providing a framework, which enables the creation of adaptors for different Cloud infrastructures, as there is currently no ''interoperability'' standard. These standards are currently under development by many forums and when such standards become real, a new adaptor for Aneka will be developed. This will ensure that the IoT applications making use of Aneka can seamlessly benefit from either private, public or hybrid Clouds.

Another important feature required for a seamless independent IoT working architecture is SaaS to be updated by the developers dynamically. In this example, analytics tools (usually in the form of DLLs) have to be updated and used by several clients. Due to administrative privileges provided by Azure, this becomes a non-trivial task. Management Extensibility Framework (MEF) provides a simple solution to the problem. The MEF is a composition layer for .NET that improves the flexibility, maintainability and testability of large applications. MEF can be used for third-party plugins, or it can bring the benefits of a loosely-coupled plugin-like architecture for regular applications. It is a library for creating lightweight, extensible applications. It allows application developers to discover and use extensions with no configuration required. It also lets extension developers easily encapsulate code and avoid fragile hard dependencies. MEF not only allows extensions to be reused within applications, but across applications as well. MEF provides a standard way for the host application to expose itself and consume external extensions. Extensions, by their nature, can be reused amongst different applications. However, an extension could still be implemented in a way that is application specific. The extensions themselves can depend on one another and MEF will make sure they are wired together in the correct order. One of the key design goals of an IoT web application is that it would be extensible and MEF provides this solution. With MEF we can use different algorithms (as and when it becomes available) for IoT data analytics: e.g. drop an analytics assembly into a folder and it instantly becomes available to the application. The system context diagram of the developed data analytics is given in Fig. 8 [47].

## 7. Open challenges and future directions

The proposed Cloud centric vision comprises a flexible and open architecture that is user centric and enables different players to interact in the IoT framework. It allows interaction in a manner suitable for their own requirements, rather than the IoT being thrust upon them. In this way, the framework includes provisions to meet different requirements for data ownership, security, privacy, and sharing of information.

Some open challenges are discussed based on the IoT elements presented earlier. The challenges include IoT specific challenges such as privacy, participatory sensing, data analytics, GIS based visualization and Cloud computing apart from the standard WSN challenges including architecture, energy efficiency, security, protocols, and Quality of Service. The end goal is to have Plug n' Play smart objects which can be deployed in any environment with an interoperable backbone allowing them to blend with other smart objects around them. Standardization of frequency bands and protocols plays a pivotal role in accomplishing this goal. A roadmap of key developments in IoT research in the context of pervasive applications is shown in Fig. 9, which includes the technology drivers and key application outcomes expected in the next decade [8]. The section ends with a few international initiatives in the domain which could play a vital role in the success of this rapidly emerging technology.

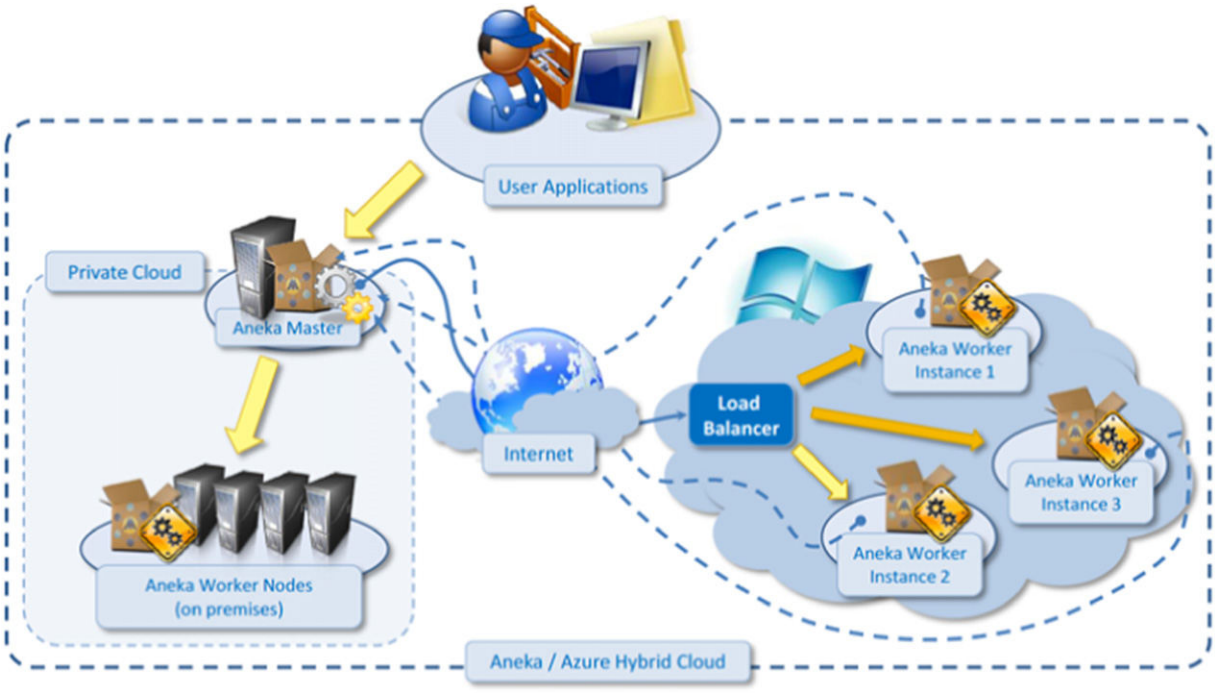



**Fig. 7.** Schematic of Aneka/Azure Interaction for data analytics application.

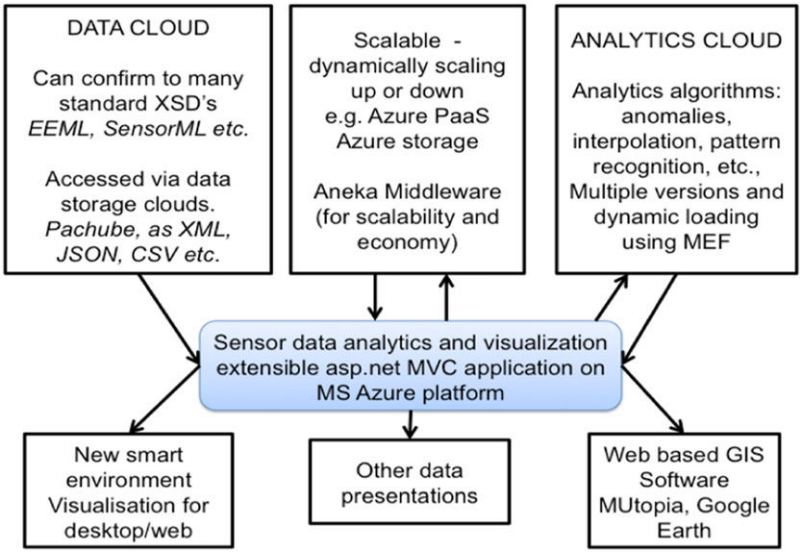



**Fig. 8.** System context diagram.

### 7.1. Architecture

Overall architecture followed at the initial stages of IoT research will have a severe bearing on the field itself and needs to be investigated. Most of the works relating to IoT architecture have been from the wireless sensor networks perspective [46]. European Union projects of SENSEI [48] and Internet of Things-Architecture (IoT-A) [49] have been addressing the challenges particularly from the WSN perspective and have been very successful in defining the architecture for different applications. We are referring architecture to overall IoT where the user is at the center and will enable the use of data and infrastructure to develop new applications. An architecture based on cloud computing at the center has been proposed in this paper. However, this may not be the best option for every application domain particularly for defense where human intelligence is relied upon. Although we see cloud centric architecture to be the best where cost based services are required, other architectures should be investigated for different application domains.

### 7.2. Energy efficient sensing

Efficient heterogeneous sensing of the urban environment needs to simultaneously meet competing demands of multiple sensing modalities. This has implications on network traffic, data storage, and energy utilization. Importantly, this encompasses both fixed and mobile sensing infrastructure [50] as well as continuous and random sampling. A generalized framework is required for data collection and modeling that effectively exploits spatial and temporal characteristics of the data, both in the sensing domain as well as the associated transform domains. For example, urban noise mapping needs an uninterrupted collection of noise

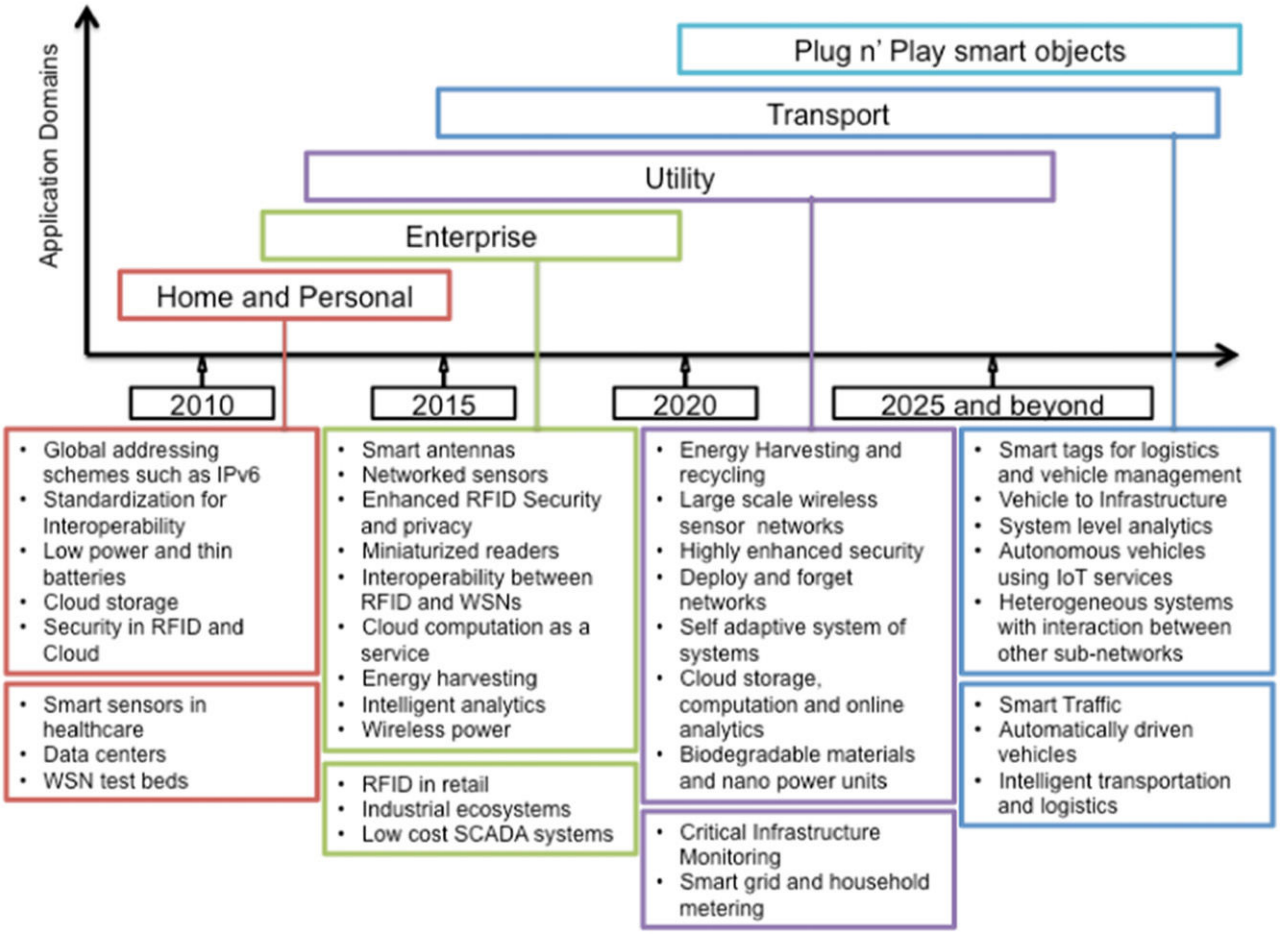



**Fig. 9.** Roadmap of key technological developments in the context of IoT application domains envisioned.

levels using battery powered nodes using fixed infrastructure and participatory sensing [50] as a key component for health and quality of life services for its inhabitants.

Compressive sensing enables reduced signal measurements without impacting accurate reconstruction of the signal. A signal sparse in one basis may be recovered from a small number of projections onto a second basis that is incoherent with the first [51]. The problem reduces to finding sparse solutions through smallest $l1$-norm coefficient vector that agrees with the measurements. In the ubiquitous sensing context, this has implications for data compression, network traffic and the distribution of sensors. Compressive wireless sensing (CWS) utilizes synchronous communication to reduce the transmission power of each sensor [52]; transmitting noisy projections of data samples to a central location for aggregation.

### 7.3. Secure reprogrammable networks and privacy

Security will be a major concern wherever networks are deployed at large scale. There can be many ways the system could be attacked—disabling the network availability; pushing erroneous data into the network; accessing personal information; etc. The three physical components of IoT—RFID, WSN and cloud are vulnerable to such attacks. Security is critical to any network [53,54] and the first line of defense against data corruption is cryptography.

Of the three, RFID (particularly passive) seems to be the most vulnerable as it allows person tracking as well as the objects and no high level intelligence can be enabled on these devices [16]. These complex problems however have solutions that can be provided using cryptographic methods and deserve more research before they are widely accepted.

Against outsider attackers, encryption ensures data confidentiality, whereas message authentication codes ensure data integrity and authenticity [55]. Encryption, however, does not protect against insider malicious attacks, to address which non-cryptographic means are needed, particularly in WSNs. Also, periodically, new sensor applications need to be installed, or existing ones need to be updated. This is done by remote wireless reprogramming of all nodes in the network. Traditional network reprogramming consists solely of a data dissemination protocol that distributes code to all the nodes in the network without authentication, which is a security threat. A secure reprogramming protocol allows the nodes to authenticate every code update and prevent malicious installation. Most such protocols (e.g., [53]) are based on the benchmark protocol Deluge [54]. We need cryptographic add-ons to Deluge, which lays the foundation for more sophisticated algorithms to be developed.

Security in the cloud is another important area of research which will need more attention. Along with the presence of the data and tools, cloud also handles economics of IoT which will make it a bigger threat from attackers. Security and identity protection becomes critical in hybrid clouds where private as well as public clouds will be used by businesses [56].

Remembering forever in the context of IoT raises many privacy issues as the data collected can be used in positive (for advertisement services) and negative ways (for defamation). Digital forgetting could emerge as one of the key areas of research to address the concerns and the development of an appropriate framework to protect personal data [42].

### 7.4. Quality of service

Heterogeneous networks are (by default) multi-service; providing more than one distinct application or service. This implies not only multiple traffic types within the network, but also the ability of a single network to support all applications without QoS compromise [57]. There are two application classes: throughput and delay tolerant elastic traffic of (e.g. monitoring weather parameters at low sampling rates), and the bandwidth and delay sensitive inelastic (real-time) traffic (e.g. noise or traffic monitoring), which can be further discriminated by data-related applications (e.g. high-vs.-low resolution videos) with different QoS requirements. Therefore, a controlled, optimal approach to serve different network traffics, each with its own application QoS needs is required [58]. It is not easy to provide QoS guarantees in wireless networks, as segments often constitute 'gaps' in resource guarantee due to resource allocation and management ability constraints in shared wireless media. Quality of Service in Cloud computing is another major research area which will require more and more attention as the data and tools become available on clouds. Dynamic scheduling and resource allocation algorithms based on particle swarm optimization are being developed. For high capacity applications and as IoT grows, this could become a bottleneck.

### 7.5. New protocols

The protocols at the sensing end of IoT will play a key role in complete realization. They form the backbone for the data tunnel between sensors and the outer world. For the system to work efficiently, an energy efficient MAC protocol and appropriate routing protocol are critical. Several MAC protocols have been proposed for various domains with TDMA (collision free), CSMA (low traffic efficiency) and FDMA (collision free but requires additional circuitry in nodes) schemes available to the user [59]. None of them are accepted as a standard and with more 'things' available this scenario is going to get more cluttered, which requires further research.

An individual sensor can drop out for a number of reasons, so the network must be self-adapting and allow for multi-path routing. Multi-hop routing protocols are used in mobile ad hoc networks and terrestrial WSNs [60]. They are mainly divided into three categories—data centric, location based and hierarchical, again based on different application domains. Energy is the main consideration for the existing routing protocols. In the case of IoT, it should be noted that a backbone will be available and the number of hops in the multi-hop scenario will be limited. In such a scenario, the existing routing protocols should suffice in practical implementation with minor modifications.

### 7.6. Participatory sensing

A number of projects have begun to address the development of people centric (or participatory) sensing platforms [50,61–63]. As noted earlier, people centric sensing offers the possibility of low cost sensing of the environment localized to the user. It can therefore give the closest indication of environmental parameters experienced by the user. It has been noted that environmental data collected by the user forms a social currency [64]. This results in more timely data being generated compared to the data available through a fixed infrastructure sensor network. Most importantly, it is the opportunity for the user to provide feedback on their experience of a given environmental parameter that offers valuable information in the form of context associated with a given event.

The limitations of people centric sensing place a new significance on the reference data role provided by a fixed infrastructure IoT as a backbone. The problem of missing samples is a fundamental limitation of people centric sensing. Relying on users volunteering data and on the inconsistent gathering of samples obtained across varying times and varying locations (based on a user's desired participation and given location or travel path), limits the ability to produce meaningful data for any applications and policy decisions. Only in addressing issues and implications of data ownership, privacy and appropriate participation incentives, can such a platform achieve genuine end-user engagement. Further sensing modalities can be obtained through the addition of sensor modules attached to the phone for application specific sensing, such as air quality sensors [65] or biometric sensors. In such scenarios, smart phones become critical IoT nodes which are connected to the cloud on one end and several sensors at the other end.

### 7.7. Data mining

Extracting useful information from a complex sensing environment at different spatial and temporal resolutions is a challenging research problem in artificial intelligence. Current state-of-the-art methods use shallow learning methods where pre-defined events and data anomalies are extracted using supervised and unsupervised learning [66]. The next level of learning involves inferring local activities by using temporal information of events extracted from shallow learning. The ultimate vision will be to detect complex events based on larger spatial and longer temporal scales based on the two levels before. The fundamental research problem that arises in complex sensing environments of this nature is how to simultaneously learn representations of events and activities at multiple levels of complexity (i.e., events, local activities and complex activities). An emerging focus in machine learning research has been the field of deep learning [67], which aims to learn multiple layers of abstraction that can be used to interpret given data. Furthermore, the resource constraints in sensor networks create novel challenges for deep learning in terms of the need for adaptive, distributed and incremental learning techniques.

### 7.8. GIS based visualization

As new display technologies emerge, creative visualization will be enabled. The evolution from CRT to Plasma, LCD, LED, and AMOLED displays has given rise to highly efficient data representation (using touch interface) with the user being able to navigate the data better than ever before. With emerging 3D displays, this area is certain to have more research and development opportunities. However, the data that comes out of ubiquitous computing is not always ready for direct consumption using visualization platforms and requires further processing. The scenario becomes very complex for heterogeneous spatio-temporal data [68]. New visualization schemes for the representation of heterogeneous sensors in a 3D landscape that varies temporally have to be developed [69]. Another challenge of visualizing data collected within IoT is that they are geo-related and are sparsely distributed. To cope with such a challenge, a framework based on Internet GIS is required.

### 7.9. Cloud computing

Integrated IoT and Cloud computing applications enabling the creation of smart environments such as Smart Cities need to be able to (a) combine services offered by multiple stakeholders and (b) scale to support a large number of users in a reliable and decentralized manner. They need to be able operate in both wired and wireless network environments and deal with constraints such as access devices or data sources with limited power and unreliable connectivity. The Cloud application platforms need to be enhanced to support (a) the rapid creation of applications by providing domain specific programming tools and environments and (b) seamless execution of applications harnessing capabilities

of multiple dynamic and heterogeneous resources to meet quality of service requirements of diverse users.

The Cloud resource management and scheduling system should be able to dynamically prioritize requests and provision resources such that critical requests are served in real time. To deliver results in a reliable manner, the scheduler needs to be augmented with task duplication algorithms for failure management. Specifically, the Cloud application scheduling algorithms need to exhibit the following capability:

1. Multi-objective optimization: The scheduling algorithms should be able to deal with QoS parameters such as response time, cost of service usage, maximum number of resources available per unit price, and penalties for service degradation.
2. Task duplication based fault tolerance: Critical tasks of an application will be transparently replicated and executed on different resources so that if one resource fails to complete the task, the replicated version can be used. This logic is crucial in real-time tasks that need to be processed to deliver services in a timely manner.

### *7.10. International activities*

Internet of Things activities are gathering momentum around the world, with numerous initiatives underway across industry, academia and various levels of government, as key stakeholders seek to map a way forward for the coordinated realization of this technological evolution. In Europe, substantial effort is underway to consolidate the cross-domain activities of research groups and organizations, spanning M2M, WSN and RFID into a unified IoT framework. Supported by the European Commission 7th Framework program (EU-FP7), this includes the Internet of Things European Research Cluster (IERC). Encompassing a number of EU FP7 projects, its objectives are: to establish a cooperation platform and research vision for IoT activities in Europe and become a contact point for IoT research around the world. It includes projects such as CASAGRAS2, a consortium of international partners from Europe, the USA, China, Japan and Korea exploring issues surrounding RFID and its role in realizing the Internet of Things. Also, IERC includes the Internet of Things Architecture (IoT-A) project established to determine an architectural reference model for the interoperability of Internet-of-Things systems and key building blocks to achieve this. At the same time, the IoT Initiative (IoT-i) is a coordinated action established to support the development of the European IoT community. The IoT-i project brings together a consortium of partners to create a joint strategic and technical vision for the IoT in Europe that encompasses the currently fragmented sectors of the IoT domain holistically. Simultaneously, the Smart Santander project is developing a city scale IoT testbed for research and service provision deployed across the city of Santander, Spain, as well as sites located in the UK, Germany, Serbia and Australia.

At the same time large scale initiatives are underway in Japan, Korea, the USA and Australia, where industry, associated organizations and government departments are collaborating on various programs, advancing related capabilities towards an IoT. This includes smart city initiatives, smart grid programs incorporating smart metering technologies and roll-out of high speed broadband infrastructure. A continuing development of RFID related technologies by industry and consortiums such as the Auto-ID lab (founded at MIT and now with satellite labs at leading universities in South Korea, China, Japan, United Kingdom, Australia and Switzerland) dedicated to creating the Internet of Things using RFID and Wireless Sensor Networks are being pursued. Significantly, the need for consensus around IoT technical issues has seen the establishment of the Internet Protocol for Smart Objects (IPSO) Alliance, now with more than 60 member companies from leading technology, communications and energy companies, working with standards bodies, such as IETF, IEEE and ITU to specify new IP-based technologies and promote industry consensus for assembling the parts for the Internet of Things. Substantial IoT development activity is also underway in China, with its 12th Five Year Plan (2011–2015), specifying IoT investment and development to be focused on: smart grid; intelligent transportation; smart logistics; smart home; environment and safety testing; industrial control and automation; health care; fine agriculture; finance and service; military defense. This is being aided by the establishment of an Internet of Things center in Shanghai (with a total investment over US $100 million) to study technologies and industrial standards. An industry fund for the Internet of Things, and an Internet of Things Union 'Sensing China' has been founded in Wuxi, initiated by more than 60 telecom operators, institutes and companies who are the primary drivers of the industry.

## 8. Summary and conclusions

The proliferation of devices with communicating–actuating capabilities is bringing closer the vision of an Internet of Things, where the sensing and actuation functions seamlessly blend into the background and new capabilities are made possible through access of rich new information sources. The evolution of the next generation mobile system will depend on the creativity of the users in designing new applications. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary apps.

Presented here is a user-centric cloud based model for approaching this goal through the interaction of private and public clouds. In this manner, the needs of the end-user are brought to the fore. Allowing for the necessary flexibility to meet the diverse and sometimes competing needs of different sectors, we propose a framework enabled by a scalable cloud to provide the capacity to utilize the IoT. The framework allows networking, computation, storage and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment. The standardization which is underway in each of these themes will not be adversely affected with Cloud at its center. In proposing the new framework associated challenges have been highlighted ranging from appropriate interpretation and visualization of the vast amounts of data, through to the privacy, security and data management issues that must underpin such a platform in order for it to be genuinely viable. The consolidation of international initiatives is quite clearly accelerating progress towards an IoT, providing an overarching view for the integration and functional elements that can deliver an operational IoT.

## Acknowledgments

There have been many contributors for this to take shape and the authors are thankful to each of them. We specifically would like to thank Mr. Kumaraswamy Krishnakumar, Mr. Mohammed Alrokayan, Dr. Jiong Jin, Dr. Yee Wei Law, Prof. Mike Taylor, Prof. D. Nandagopal, Mr. Aravinda Rao and Prof. Chris Leckie. The work is partially supported by Australian Research Council's LIEF (LE120100129), Linkage grants (LP120100529) and Research Network on Intelligent Sensors, Sensor networks and Information Processing (ISSNIP). The authors are participants in European 7th Framework projects on Smart Santander and the Internet of Things-Initiative and are thankful for their support.

## References


[1] K. Ashton, That "Internet of Things" thing, RFiD Journal (2009).
[2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.
[3] J. Buckley (Ed.), The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.
[4] M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC in the late 1980s, IBM Systems Journal (1999).
[5] Y. Rogers, Moving on from Weiser's vision of calm computing: engaging ubicomp experiences, in: UbiComp 2006: Ubiquitous Computing, 2006.
[6] R. Caceres, A. Friday, Ubicomp systems at 20: progress, opportunities, and challenges, IEEE Pervasive Computing 11 (2012) 14–21.
[7] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422.
[8] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805.
[9] J. Belissent, Getting clever about smart cities: new opportunities require new business models, Forrester Research, 2010.
[10] Gartner's hype cycle special report for 2011, Gartner Inc., 2012. http://www.gartner.com/technology/research/hype-cycles/.
[11] Google Trends, Google (n.d.). http://www.google.com/trends.
[12] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (2009) 599–616.
[13] S. Tilak, N. Abu-Ghazaleh, W. Heinzelman, A taxonomy of wireless micro-sensor network models, ACM Mobile Computing and Communications Review 6 (2002) 28–36.
[14] M. Tory, T. Moller, Rethinking visualization: a high-level taxonomy, in: IEEE Symposium on Information Visualization, 2004, INFOVIS 2004, 2004, pp. 151–158.
[15] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, et al., Building the Internet of Things using RFID The RFID ecosystem experience, IEEE Internet Computing 13 (2009) 48–55.
[16] A. Juels, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications 24 (2006) 381–394.
[17] A. Ghosh, S.K. Das, Coverage and connectivity issues in wireless sensor networks: a survey, Pervasive and Mobile Computing 4 (2008) 303–334.
[18] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, N. Xiong, Secure Data Aggregation in Wireless Sensor Networks: A Survey, 2006, pp. 315–320.
[19] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From today's Intranet of Things to a future Internet of Things: a wireless- and mobility-related view, IEEE Wireless Communications 17 (2010) 43–51.
[20] N. Honle, U.P. Kappeler, D. Nicklas, T. Schwarz, M. Grossmann, Benefits of integrating meta data into a context model, 2005, pp. 25–29.
[21] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, A survey on facilities for experimental Internet of Things research, IEEE Communications Magazine 49 (2011) 58–67.
[22] L. Haiyan, C. Song, W. Dalei, N. Stergiou, S. Ka-Chun, A remote markerless human gait tracking for e-healthcare based on content-aware wireless multimedia communications, IEEE Wireless Communications 17 (2010) 44–50.
[23] G. Nussbaum, People with disabilities: assistive homes and environments, in: Computers Helping People with Special Needs, 2006.
[24] A. Alkar, U. Buhur, An Internet based wireless home automation system for multifunctional devices, IEEE Transactions on Consumer Electronics 51 (2005) 1169–1174.
[25] M. Darianian, M.P. Michael, Smart home mobile RFID-based Internet-of-Things systems and services, in: 2008 International Conference on Advanced Computer Theory and Engineering, 2008, pp. 116–120.
[26] H.S. Ning, Z.O. Wang, Future Internet of Things architecture: like mankind neural system or social organization framework? IEEE Communications Letters 15 (2011) 461–463.
[27] L. Atzori, A. Iera, G. Morabito, SIoT: giving a social structure to the Internet of Things, IEEE Communications Letters 15 (2011) 1193–1195.
[28] X. Li, R.X. Lu, X.H. Liang, X.M. Shen, J.M. Chen, X.D. Lin, Smart community: an Internet of Things application, IEEE Communications Magazine 49 (2011) 68–75.
[29] C. Kidd, R. Orr, G. Abowd, C. Atkeson, I. Essa, B. MacIntyre, et al., The Aware Home: a living laboratory for ubiquitous computing research, in: Lecture Notes in Computer Science, 1999, pp. 191–198.
[30] S.R.L. Labs, Future Retail Center, SAP Research Living Labs (n.d.). http://www.sap.com/corporate-en/our-company/innovation/research/livinglabs/futureretail/index.epx.
[31] J. Hernández-Muñoz, J. Vercher, L. Muñoz, J. Galache, M. Presser, L. Gómez, J. Pettersson, Smart cities at the forefront of the future Internet, in: J. Domingue, A. Galis, A. Gavras, T. Zahariadis, D. Lambert (Eds.), The Future Internet, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 447–462.
[32] R.N. Murty, G. Mainland, I. Rose, A.R. Chowdhury, A. Gosain, J. Bers, et al., CitySense: an urban-scale wireless sensor network and testbed, 2008, pp. 583–588.
[33] System of monitoring and environmental surveillance, 2011. http://www.dimap.es/enviromental-agriculture-services.html.
[34] S. Bainbridge, C. Steinberg, M. Furnas, GBROOS—an ocean observing system for the Great Barrier Reef, in: International Coral Reef Symposium, 2010, pp. 529–533.
[35] R. Johnstone, D. Caputo, U. Cella, A. Gandelli, C. Alippi, F. Grimaccia, et al., Smart environmental measurement & analysis technologies (SEMAT): wireless sensor networks in the marine environment, Stockholm, 2008.
[36] M. Zhang, T. Yu, G.F. Zhai, Smart transport system based on "The Internet of Things", Applied Mechanics and Materials 48–49 (2011) 1073–1076.
[37] H. Lin, R. Zito, M. Taylor, A review of travel-time prediction in transport and logistics, Proceedings of the Eastern Asia Society for Transportation Studies 5 (2005) 1433–1448.
[38] M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, in: Advances in Energy Engineering, ICAEE, 2010, pp. 69–72.
[39] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks 51 (2007) 921–960.
[40] H. Jun-Wei, Y. Shouyi, L. Leibo, Z. Zhen, W. Shaojun, A crop monitoring system based on wireless sensor network, Procedia Environmental Sciences 11 (2011) 558–565.
[41] P. Kumar, S. Ranganath, W. Huang, K. Sengupta, Framework for real-time behavior interpretation from traffic video, IEEE Transactions on Intelligent Transportation Systems 6 (2005) 43–53.
[42] V. Mayer-Schönberger, Failing to forget the "Drunken Pirate", in: Delete: the Virtue of Forgetting in the Digital Age (New in Paper), first ed., Princeton University Press, 2011, pp. 3–15.
[43] T.S. Lopez, D.C. Ranasinghe, M. Harrison, D. McFarlane, Adding sense to the Internet of Things an architecture framework for smart objective systems, Pervasive Ubiquitous Computing 16 (2012) 291–308.
[44] Y. Wei, K. Sukumar, C. Vecchiola, D. Karunamoorthy, R. Buyya, Aneka cloud application platform and its integration with windows Azure, in: R. Ranjan, J. Chen, B. Benatallah, L. Wang (Eds.), Cloud Computing: Methodology, Systems, and Applications, first ed., CRC Press, Boca Raton, 2011, p. 30.
[45] C. Vecchiola, R.N. Calheiros, D. Karunamoorthy, R. Buyya, Deadline-driven provisioning of resources for scientific applications in hybrid clouds with Aneka, Future Generation Computer Systems (2012) 58–65.
[46] A.P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, Architecture and protocols for the Internet of Things: a case study, 2010, pp. 678–683.
[47] J. Gubbi, K. Krishnakumar, R. Buyya, M. Palaniswami, A cloud computing framework for data analytics in smart city applications, Technical Report No. CLOUDS-TR-2012-2A, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, 2012.
[48] SENSEI, Integrated EU project—7th framework (n.d.). http://www.ict-sensei.org/index.php.
[49] European lighthouse integrated project—7th framework, Internet of Things—Architecture, 2012. http://www.iot-a.eu/.
[50] R.K. Rana, C.T. Chou, S.S. Kanhere, N. Bulusu, W. Hu, Ear-phone: an end-to-end participatory urban noise mapping system, in: ACM Request Permissions, 2010.
[51] D. Donoho, Compressed sensing, IEEE Transactions on Information Theory 52 (2006) 1289–1306.
[52] W. Bajwa, J. Haupt, A. Sayeed, R. Nowak, Compressive wireless sensing, in: ACM, 2006.
[53] M. Navajo, I. Ballesteros, S. D'Elia, A. Sassen, M. Goyet, J. Santaella, et al., Draft report of the task force on interdisciplinary research activities applicable to the Future Internet, European Union Task Force Report, 2010.
[54] D. Tang, Event detection in sensor networks, School of Engineering and Applied Sciences, The George Washington University, 2009.
[55] D.B. Neill, Fast Bayesian scan statistics for multivariate event detection and visualization, Statistics in Medicine 30 (2011) 455–469.
[56] L.M. Kaufman, Data security in the world of cloud computing, IEEE Security and Privacy Magazine 7 (2009) 61–64.
[57] E. Vera, L. Mancera, S.D. Babacan, R. Molina, A.K. Katsaggelos, Bayesian compressive sensing of wavelet coefficients using multiscale Laplacian priors, in: Statistical Signal Processing, 2009, SSP'09, IEEE/SP 15th Workshop on., 2009, pp. 229–232.
[58] H. El-Sayed, A. Mellouk, L. George, S. Zeadally, Quality of service models for heterogeneous networks: overview and challenges, Annals of Telecommunications 63 (2008) 639–668.
[59] I. Demirkol, C. Ersoy, F. Alagoz, MAC protocols for wireless sensor networks: a survey, IEEE Communications Magazine 44 (2006) 115–121.
[60] J. Al-Karaki, A. Kamal, Routing techniques in wireless sensor networks: a survey, IEEE Wireless Communications 11 (2004) 6–28.
[61] A.T. Campbell, S.B. Eisenman, N.D. Lane, E. Miluzzo, R.A. Peterson, People-centric urban sensing, ACM, 2006.
[62] E. Kanjo, NoiseSPY: a real-time mobile phone platform for urban noise monitoring and mapping, Mobile Networks and Applications 15 (2009) 562–574.
[63] S. Santini, B. Ostermaier, A. Vitaletti, First experiences using wireless sensor networks for noise pollution monitoring, ACM, Glasgow, Scotland, 2008.
[64] S. Kuznetsov, E. Paulos, Participatory sensing in public spaces: activating urban surfaces with sensor probes, in: ACM Request Permissions, 2010.
[65] R. Honicky, E.A. Brewer, E. Paulos, R. White, *N*-smarts: networked suite of mobile atmospheric real-time sensors, ACM, 2008, pp. 25–29.
[66] R.V. Kulkarni, A. Förster, G.K. Venayagamoorthy, Computational intelligence in wireless sensor networks: a survey, IEEE Communications Surveys & Tutorials 13 (2011) 68–96.
[67] Y. Bengio, Learning Deep Architectures for AI, first ed., Now Publishers Inc., 2009.
[68] G.P. Bonneau, G.M. Nielson, F. Post (Eds.), Data Visualization: The State of the Art, Kluwer Academic, London, 2003.
[69] L. Ren, F. Tian, X. Zhang, L. Zhang, DaisyViz: a model-based user interface toolkit for interactive information visualization systems, Journal of Visual Languages and Computing 21 (2010) 209–229.

**Jayavardhana Gubbi** received the Bachelor of Engineering degree from Bangalore University, Bengaluru, India, in 2000, the Ph.D. degree from the University of Melbourne, Melbourne, Vic., Australia, in 2007. For three years, he was a Research Assistant at the Indian Institute of Science, where he was engaged in speech technology for Indian languages. Dr. Gubbi is a Research Fellow in the Department of Electrical and Electronic Engineering at the University of Melbourne. Currently, from 2010 to 2014, he is an ARC Australian Postdoctoral Fellow - Industry (APDI) working on an industry linkage grant in video processing. His current research interests include Video Processing, Internet of Things and ubiquitous healthcare devices. He has coauthored more than 40 papers in peer reviewed journals, conferences, and book chapters over the last ten years. Dr. Gubbi has served as Conference Secretary and Publications Chair in several international conferences in the area of wireless sensor networks, signal processing and pattern recognition.

**Rajkumar Buyya** is Professor of Computer Science and Software Engineering; and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at the University of Melbourne, Australia. He is the founding CEO of Manjrasoft, a spin-off company of the university, commercializing its innovations in Cloud Computing. He has authored over 430 publications and four textbooks. He also edited several books including "Cloud Computing: Principles and Paradigms" (Wiley Press, USA, Feb 2011). He is one of the highly cited authors in computer science and software engineering worldwide (h-index = 66 and 21300+ citations).

Software technologies for Grid and Cloud computing developed under Dr. Buyya's leadership have gained rapid acceptance and are in use at several academic institutions and commercial enterprizes in 40 countries around the world. Dr. Buyya has led the establishment and development of key community activities, including serving as foundation Chair of the IEEE Technical Committee on Scalable Computing and five IEEE/ACM conferences. These contributions and the international research leadership of Dr. Buyya are recognized through the award of the "2009 IEEE Medal for Excellence in Scalable Computing". Manjrasoft's Aneka Cloud technology developed under his leadership has received the "2010 Asia Pacific Frost & Sullivan New Product Innovation Award" and "2011 Telstra Innovation Challenge, People's Choice Award". He is currently serving as the first Editor-in-Chief (EiC) of IEEE Transactions on Cloud Computing. For further information on Dr. Buyya, please visit his cyberhome: www.buyya.com.

**Slaven Marusic** is a Senior Research Fellow in Sensor Networks at the Department of Electrical and Electronic Engineering, at the University of Melbourne. Completing his Ph.D. at La Trobe University specializing in signal and image processing, before taking a Senior Lecturer role at the University of New South Wales, Dr Marusic returned to Melbourne also taking up the Role of Program Manager for the ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). In this capacity he has facilitated numerous international research collaborations across academia and industry. He was the General Co-Chair of the 6th International Conference on ISSNIP, Brisbane 2010, and has served on numerous organizing and technical program committees. His research work has encompassed multidisciplinary contributions in the areas of image and video processing, sensor networks and biomedical signal processing, applied variously to environmental monitoring, healthcare, smart grids and more recently, urban living.

**M. Palaniswami** received his B.E. (Hons) from the University of Madras, M.E. from the Indian Institute of Science, India, and Ph.D. from the University of Newcastle, Australia before joining the University of Melbourne, where he is a Professor of Electrical Engineering and Director/Convener of a large ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) with about 200 researchers and interdisciplinary themes as the focus for the center. Previously, he was a Co-Director of the Center of Expertise on Networked Decision & Sensor Systems. He served on various international boards and advisory committees including being a panel member for the National Science Foundation (NSF). He has published more than 340 refereed journal and conference papers, including a number of books, edited volumes and book chapters. He was given a Foreign Specialist Award by the Ministry of Education, Japan in recognition of his contributions to the field of Machine Learning. He received the University of Melbourne Knowledge Transfer Excellence Award and Commendation Awards. He served as an Associate Editor for journals/transactions including IEEE Transactions on Neural Networks and Computational Intelligence for Finance. He is the Subject Editor for the International Journal on Distributed Sensor Networks. Through his research, he supported various local and international companies. As an international investigator, he is involved in FP6 and FP7 initiatives in the areas of Smart City and Internet of Things (IoT). In order to develop a new research capacity, he founded the international conference series on sensors, sensor networks and information processing. His research interests include smart sensors and sensor networks, machine learning, neural networks, support vector machines, signal processing, biomedical engineering and control. He is a Fellow of the IEEE.

Computer Networks 54 (2010) 2787–2805

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# The Internet of Things: A survey

Luigi Atzori [a], Antonio Iera [b], Giacomo Morabito [c,*]

[a] DIEE, University of Cagliari, Italy
[b] University "Mediterranea" of Reggio Calabria, Italy
[c] University of Catania, Italy

ARTICLE INFO

*Article history:*
Received 10 December 2009
Received in revised form 27 April 2010
Accepted 14 May 2010
Available online 1 June 2010
Responsible Editor: E. Ekici

*Keywords:*
Internet of Things
Pervasive computing
RFID systems

ABSTRACT

This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.



## 1. Introduction

The *Internet of Things* (*IoT*) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of *things* or *objects* – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals [1].

Unquestionably, the main strength of the IoT idea is the high impact it will have on several aspects of everyday-life and behavior of potential users. From the point of view of a private user, the most obvious effects of the IoT introduction will be visible in both working and domestic fields. In this context, domotics, assisted living, e-health, enhanced learning are only a few examples of possible application scenarios in which the new paradigm will play a leading role in the near future. Similarly, from the perspective of business users, the most apparent consequences will be equally visible in fields such as, automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods.

By starting from the considerations above, it should not be surprising that IoT is included by the US National Intelligence Council in the list of six "Disruptive Civil Technologies" with potential impacts on US national power [2]. NIC foresees that "by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more". It highlights future opportunities that will arise, starting from the idea that "popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development". The possible threats deriving from a widespread adoption of such a technology are also stressed. Indeed, it is emphasized that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date".

* Corresponding author. Tel.: +39 095 7382355; fax: +39 095 7382397.
*E-mail addresses:* l.atzori@diee.unica.it (L. Atzori), antonio.iera@unirc.it (A. Iera), giacomo.morabito@diit.unict.it (G. Morabito).

1389-1286/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2010.05.010

Actually, many challenging issues still need to be addressed and both technological as well as social knots have to be untied before the IoT idea being widely accepted. Central issues are making a full interoperability of interconnected devices possible, providing them with an always higher *degree of smartness* by enabling their adaptation and autonomous behavior, while guaranteeing trust, privacy, and security. Also, the IoT idea poses several new problems concerning the networking aspects. In fact, the *things* composing the IoT will be characterized by low resources in terms of both computation and energy capacity. Accordingly, the proposed solutions need to pay special attention to resource efficiency besides the obvious scalability problems.

Several industrial, standardization and research bodies are currently involved in the activity of development of solutions to fulfill the highlighted technological requirements. This survey gives a picture of the current state of the art on the IoT. More specifically, it:

- provides the readers with a description of the different visions of the Internet of Things paradigm coming from different scientific communities;
- reviews the enabling technologies and illustrates which are the major benefits of spread of this paradigm in everyday-life;
- offers an analysis of the major research issues the scientific community still has to face.

The main objective is to give the reader the opportunity of understanding what has been done (protocols, algorithms, proposed solutions) and what still remains to be addressed, as well as which are the enabling factors of this evolutionary process and what are its weaknesses and risk factors.

The remainder of the paper is organized as follows. In Section 2, we introduce and compare the different visions of the IoT paradigm, which are available from the literature. The IoT main enabling technologies are the subject of Section 3, while the description of the principal applications, which in the future will benefit from the full deployment of the IoT idea, are addressed in Section 4. Section 5 gives a glance at the open issues on which research should focus more, by stressing topics such as addressing, networking, security, privacy, and standardization efforts. Conclusions and future research hints are given in Section 6.

## 2. One paradigm, many visions

Manifold definitions of *Internet of Things* traceable within the research community testify to the strong interest in the IoT issue and to the vivacity of the debates on it. By browsing the literature, an interested reader might experience a real difficulty in understanding what IoT really means, which basic ideas stand behind this concept, and which social, economical and technical implications the full deployment of IoT will have.

The reason of today apparent fuzziness around this term is a consequence of the name "Internet of Things" itself, which syntactically is composed of two terms. The first one pushes towards a network oriented vision of IoT, while the second one moves the focus on generic "objects" to be integrated into a common framework.

Differences, sometimes substantial, in the IoT visions raise from the fact that stakeholders, business alliances, research and standardization bodies start approaching the issue from either an "*Internet* oriented" or a "*Things* oriented" perspective, depending on their specific interests, finalities and backgrounds.

It shall not be forgotten, anyway, that the words "Internet" and "Things", when put together, assume a meaning which introduces a disruptive level of innovation into today ICT world. In fact, "Internet of Things" semantically means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [3]. This implies a huge number of (heterogeneous) objects involved in the process.

The object unique addressing and the representation and storing of the exchanged information become the most challenging issues, bringing directly to a third, "*Semantic* oriented", perspective of IoT.

In Fig. 1, the main concepts, technologies and standards are highlighted and classified with reference to the IoT vision/s they contribute to characterize best. From such an illustration, it clearly appears that the IoT paradigm shall be the result of the convergence of the three main visions addressed above.

The very first definition of IoT derives from a "Things oriented" perspective; the considered things were very simple items: Radio-Frequency IDentification (RFID) tags. The terms "Internet of Things" is, in fact, attributed to The Auto-ID Labs [4], a world-wide network of academic research laboratories in the field of networked RFID and emerging sensing technologies. These institutions, since their establishment, have been targeted to architect the IoT, together with EPCglobal [5]. Their focus has primarily been on the development of the Electronic Product Code™ (EPC) to support the spread use of RFID in world-wide modern trading networks, and to create the industry-driven global standards for the EPCglobal Network™. These standards are mainly designed to improve object visibility (i.e. the traceability of an object and the awareness of its status, current location, etc.). This is undoubtedly a key component of the path to the full deployment of the IoT vision; but it is not the only one.

In a broader sense, IoT cannot be just a global EPC system in which the only objects are RFIDs; they are just a part of the full story! And the same holds for the alternative Unique/Universal/Ubiquitous IDentifier (uID) architecture [6], whose main idea is still the development of (middleware based) solutions for a global visibility of objects in an IoT vision. It is the authors' opinion that, starting from RFID centric solutions may be positive as the main aspects stressed by RFID technology, namely item traceability and addressability, shall definitely be addressed also by the IoT. Notwithstanding, alternative, and somehow more complete, IoT visions recognize that the term IoT implies a much wider vision than the idea of a mere objects identification.

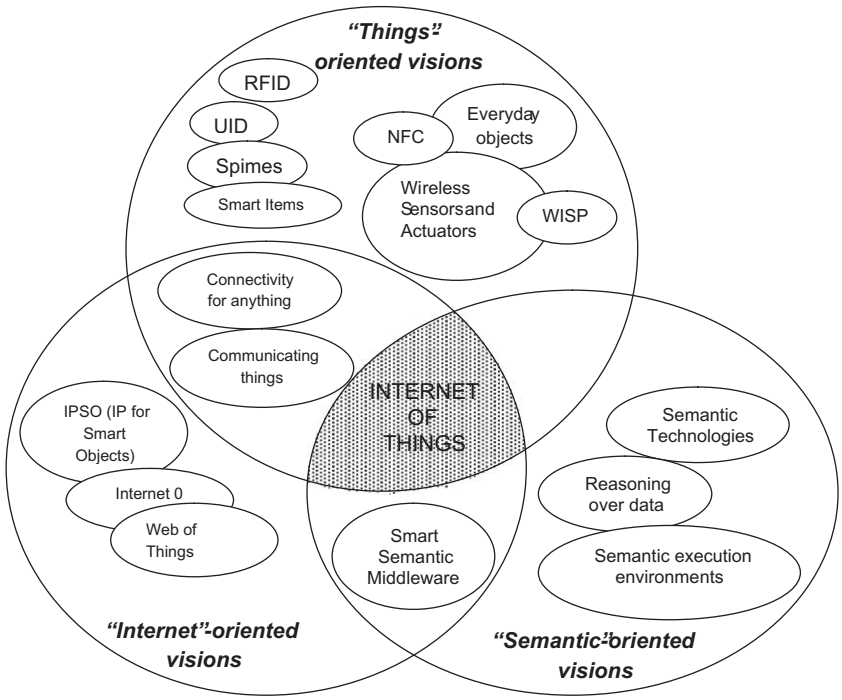



**Fig. 1.** "Internet of Things" paradigm as a result of the convergence of different visions.

According to the authors of [7], RFID still stands at the forefront of the technologies driving the vision. This a consequence of the RFID maturity, low cost, and strong support from the business community. However, they state that a wide portfolio of device, network, and service technologies will eventually build up the IoT. Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID are recognized as "the atomic components that will link the real world with the digital world". It is also worth recalling that major projects are being carried out with the aim of developing relevant platforms, such as the WISP (Wireless Identification and Sensing Platforms) project.

The one in [7] is not the only "Things oriented" vision clearly speaking of something going beyond RFID. Another one has been proposed by the United Nations, which, during the 2005 Tunis meeting, predicted the advent of IoT. A UN Report states that a new era of ubiquity is coming where humans may become the minority as generators and receivers of traffic and changes brought about by the Internet will be dwarfed by those prompted by the networking of everyday objects [8].

Similarly, other relevant institutions have stressed the concept that IoT has primarily to be focused on the "Things" and that the road to its full deployment has to start from the augmentation in the Things' intelligence. This is why a concept that emerged aside IoT is the *spime*, defined as an object that can be tracked through space and time throughout its lifetime and that will be sustainable, enhanceable, and uniquely identifiable [9]. Although quite *theoretical*, the *spime* definition finds some real-world implementations in so called *Smart Items*. These are a sort of sensors not only equipped with usual wireless communication, memory, and elaboration capabilities, but also with new potentials. Autonomous and proactive behavior, context awareness, collaborative communications and elaboration are just some required capabilities.

The definitions above paved the way to the ITU vision of the IoT, according to which: "from anytime, anyplace connectivity for anyone, we will now have connectivity for *anything*" [10]. A similar vision is available from documents and communications of the European Commission, in which the most recurrent definition of IoT involves "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts" [3].

An IoT vision statement, which goes well beyond a mere "RFID centric" approach, is also proposed by the consortium CASAGRAS [11]. Its members focus on "a world where things can automatically communicate to computers and each other providing services to the benefit of the human kind". CASAGRAS consortium (i) proposes a vision of IoT as a global infrastructure which connects both virtual and physical generic objects and (ii) highlights the importance of including existing and evolving Internet and network developments in this vision. In this sense, IoT becomes the natural enabling architecture for the deployment of independent federated services and applications, characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

This definition plays the role of *trait d'union* between what we referred to as a "Things oriented" vision and an "Internet oriented" vision.

Within the latter category falls the IoT vision of the IPSO (IP for Smart Objects) Alliance [11], a forum formed in September 2008 by 25 founding companies to promote the Internet Protocol as the network technology for connecting Smart Objects around the world. According to the IPSO vision, the IP stack is a light protocol that already connects a huge amount of communicating devices and runs on tiny and battery operated embedded devices. This guarantees that IP has all the qualities to make IoT a reality. By reading IPSO whitepapers, it seems that through a wise IP adaptation and by incorporating IEEE 802.15.4 into the IP architecture, in the view of 6LoWPAN [12], the full deployment of the IoT paradigm will be automatically enabled.

Internet Ø [13] follows a similar approach of reducing the complexity of the IP stack to achieve a protocol designed to route "IP over anything". In some forums this is looked at as the wisest way to move from the Internet of Devices to the Internet of Things. According to both the IPSO and Internet Ø approaches, the IoT will be deployed by means of a sort of *simplification* of the current IP to adapt it to any object and make those objects addressable and reachable from any location.

As said before, it is worth noticing that "Semantic oriented" IoT visions are available in the literature [14–17]. The idea behind them is that the number of items involved in the Future Internet is destined to become extremely high. Therefore, issues related to how to represent, store, interconnect, search, and organize information generated by the IoT will become very challenging. In this context, semantic technologies could play a key role. In fact, these can exploit appropriate modeling solutions for things description, reasoning over data generated by IoT, semantic execution environments and architectures that accommodate IoT requirements and scalable storing and communication infrastructure [14].

A further vision correlated with the IoT is the so called "Web of Things" [18], according to which Web standards are re-used to connect and integrate into the Web everyday-life objects that contain an embedded device or computer.

## 3. Enabling technologies

Actualization of the IoT concept into the real world is possible through the integration of several enabling technologies. In this section we discuss the most relevant ones. Note that it is not our purpose to provide a comprehensive survey of each technology. Our major aim is to provide a picture of the role they will likely play in the IoT. Interested readers will find references to technical publications for each specific technology.

### 3.1. Identification, sensing and communication technologies

"Anytime, anywhere, anymedia" has been for a long time the vision pushing forward the advances in communication technologies. In this context, wireless technologies have played a key role and today the ratio between radios and humans is nearing the 1 to 1 value [19].

However, the reduction in terms of size, weight, energy consumption, and cost of the radio can take us to a new era where the above ratio increases of orders of magnitude. This will allow us to integrate radios in almost all objects and thus, to add the world "anything" to the above vision, which leads to the IoT concept.

In this context, key components of the IoT will be RFID systems [20], which are composed of one or more reader(s) and several RFID tags. Tags are characterized by a unique identifier and are applied to objects (even persons or animals). Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs. Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the *real world* into the *virtual world*. Therefore, they can be used in an incredibly wide range of application scenarios, spanning from logistics to e-health and security.

From a physical point of view a RFID tag is a small microchip[1] attached to an antenna (that is used for both receiving the reader signal and transmitting the tag ID) in a package which usually is similar to an adhesive sticker [21]. Dimensions can be very low: Hitachi has developed a tag with dimensions 0.4 mm $\times$ 0.4 mm $\times$ 0.15 mm.

Usually, RFID tags are *passive*, i.e., they do not have onboard power supplies and harvest the energy required for transmitting their ID from the query signal transmitted by a RFID reader in the proximity. In fact, this signal generates a current into the tag antenna by induction and such a current is utilized to supply the microchip which will transmit the tag ID. Usually, the gain (power of the signal received by the reader divided by the power of the signal transmitted by the same reader) characterizing such systems is very low. However, thanks to the highly directive antennas utilized by the readers, tags ID can be correctly received within a radio range that can be as long as a few meters. Transmission may occur in several frequency bands spanning from low frequencies (LF) at 124–135 kHz up to ultra high frequencies (UHF) at 860–960 MHz that have the longest range.

Nevertheless, there are also RFID tags getting power supply by batteries. In this case we can distinguish *semi-passive* from *active* RFID tags. In *semi-passive* RFIDs batteries power the microchip while receiving the signal from the reader (the radio is powered with the energy harvested by the reader signal). Differently, in *active* RFIDs the battery powers the transmission of the signal as well. Obviously the radio coverage is the highest for active tags even if this is achieved at the expenses of higher production costs.

Sensor networks will also play a crucial role in the IoT. In fact, they can cooperate with RFID systems to better track the status of things, i.e., their location, temperature, movements, etc. As such, they can augment the awareness of a certain environment and, thus, act as a further bridge between physical and digital world. Usage of sensor net-

[1] New RFID tags, named *chipless tags*, are under study which do not use microchips so as to decrease production cost [96].

works has been proposed in several application scenarios, such as environmental monitoring, e-health, intelligent transportation systems, military, and industrial plant monitoring.

Sensor networks consist of a certain number (which can be very high) of sensing nodes communicating in a wireless multi-hop fashion. Usually nodes report the results of their sensing to a small number (in most cases, only one) of special nodes called *sinks*. A large scientific literature has been produced on sensor networks in the recent past, addressing several problems at all layers of the protocol stack [22]. Design objectives of the proposed solutions are energy efficiency (which is the scarcest resource in most of the scenarios involving sensor networks), scalability (the number of nodes can be very high), reliability (the network may be used to report urgent alarm events), and robustness (sensor nodes are likely to be subject to failures for several reasons).

Today, most of commercial wireless sensor network solutions are based on the IEEE 802.15.4 standard, which defines the physical and MAC layers for low-power, low bit rate communications in wireless personal area networks (WPAN) [23]. IEEE 802.15.4 does not include specifications on the higher layers of the protocol stack, which is necessary for the seamless integration of sensor nodes into the Internet. This is a difficult task for several reasons, the most important are given below:

- Sensor networks may consist of a very large number of nodes. This would result in obvious problems as today there is a scarce availability of IP addresses.
- The largest physical layer packet in IEEE 802.15.4 has 127 bytes; the resulting maximum frame size at the media access control layer is 102 octets, which may further decrease based on the link layer security algorithm utilized. Such sizes are too small when compared to typical IP packet sizes.
- In many scenarios sensor nodes spend a large part of their time in a *sleep* mode to save energy and cannot communicate during these periods. This is absolutely anomalous for IP networks.

Integration of sensing technologies into passive RFID tags would enable a lot of completely new applications into the IoT context, especially into the e-health area [24]. Recently, several solutions have been proposed in this direction. As an example, the WISP project is being carried out at Intel Labs to develop *wireless identification and sensing platforms* (WISP) [25]. WISPs are powered and read by standard RFID readers, harvesting the power from the reader's querying signal. WISPs have been used to measure quantities in a certain environment, such as light, temperature, acceleration, strain, and liquid level.

Sensing RFID systems will allow to build RFID sensor networks [26], which consist of small, RFID-based sensing and computing devices, and RFID readers, which are the sinks of the data generated by the sensing RFID tags and provide the power for the network operation.

Table 1 compares the characteristics of RFID systems (RFID), wireless sensor networks (WSN), and RFID sensor networks (RSN) [26]. Observe that the major advantages of:

- RFID systems are the very small size and the very low cost. Furthermore, their lifetime is not limited by the battery duration;
- wireless sensor networks are the high radio coverage and the communication paradigm, which does not require the presence of a reader (communication is peer-to-peer whereas, it is asymmetric for the other types of systems);
- RFID sensor network are the possibility of supporting sensing, computing, and communication capabilities in a passive system.

### 3.2. Middleware

The middleware is a software layer or a set of sub-layers interposed between the technological and the application levels. Its feature of hiding the details of different technologies is fundamental to exempt the programmer from issues that are not directly pertinent to her/his focus, which is the development of the specific application enabled by the IoT infrastructures. The middleware is gaining more and more importance in the last years due to its major role in simplifying the development of new services and the integration of legacy technologies into new ones. This excepts the programmer from the exact knowledge of the variegate set of technologies adopted by the lower layers.

As it is happening in other contexts, the middleware architectures proposed in the last years for the IoT often follow the *Service Oriented Architecture* (SOA) approach. The adoption of the SOA principles allows for decomposing complex and monolithic systems into applications consisting of an ecosystem of simpler and well-defined components. The use of common interfaces and standard protocols gives a horizontal view of an enterprise system. Thus, the development of business processes enabled by the SOA is the result of the process of designing workflows of coordinated services, which eventually are associated with objects actions. This facilitates the interaction among the parts of an enterprise and allows for reducing the time necessary to adapt itself to the changes imposed by the market evolution [27]. A SOA approach also allows for software and hardware reusing, be-

**Table 1**
Comparison between RFID systems, wireless sensor networks, and RFID sensor networks.

| | Processing | Sensing | Communication | Range (m) | Power | Lifetime | Size | Standard |
|---|---|---|---|---|---|---|---|---|
| RFID | No | No | Asymmetric | 10 | Harvested | Indefinite | Very small | ISO18000 |
| WSN | Yes | Yes | Peer-to-peer | 100 | Battery | <3 years | Small | IEEE 802.15.4 |
| RSN | Yes | Yes | Asymmetric | 3 | Harvested | Indefinite | Small | None |

cause it does not impose a specific technology for the service implementation [28].

Advantages of the SOA approach are recognized in most studies on middleware solutions for IoT. While a commonly accepted layered architecture is missing, the proposed solutions face essentially the same problems of abstracting the devices functionalities and communications capabilities, providing a common set of services and an environment for service composition. These common objectives lead to the definition of the middleware sketch shown in Fig. 2. It tries to encompass all the functionalities addressed in past works dealing with IoT middleware issues. It is quite similar to the scheme proposed in [29], which addresses the middleware issues with a complete and integrated architectural approach. It relies on the layers explained in Sections 3.2.1–3.2.5.

*3.2.1. Applications*

Applications are on the top of the architecture, exporting all the system's functionalities to the final user. Indeed, this layer is not considered to be part of the middleware but exploits all the functionalities of the middleware layer. Through the use of standard web service protocols and service composition technologies, applications can realize a perfect integration between distributed systems and applications.

*3.2.2. Service composition*

This is a common layer on top of a SOA-based middleware architecture. It provides the functionalities for the composition of single services offered by networked objects to build specific applications. On this layer there is no notion of devices and the only visible assets are services. An important insight into the service landscape is to have a repository of all currently connected service instances, which are executed in run-time to build composed services. The logic behind the creation and the management of complex services, can be expressed in terms of workflows of business processes, using workflow languages. In this context, a frequent choice is to adopt standard languages such as the Business Process Execution Language (BPEL) and Jolie [29,30]. Workflow languages define business processes that interact with external entities through Web Service operations, defined by using the Web Service Definition Language (WSDL) [31]. Workflows can be nested, so it is possible to call a workflow from inside another one. The creation of complex processes can be represented as a sequence of coordinated actions performed by single components.

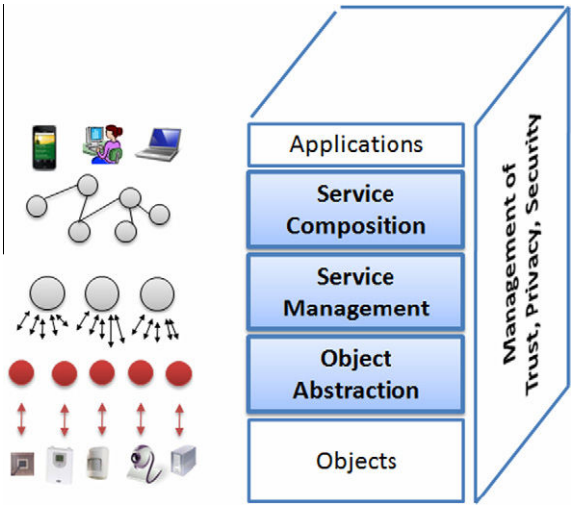



**Fig. 2.** SOA-based architecture for the IoT middleware.

*3.2.3. Service management*

This layer provides the main functions that are expected to be available for each object and that allow for their management in the IoT scenario. A basic set of services encompasses: object dynamic discovery, status monitoring, and service configuration. At this layer, some middleware proposals include an expanded set of functionalities related to the QoS management and lock management, as well as some semantic functions (e.g., police and context management) [32]. This layer might enable the remote deployment of new services during run-time, in order to satisfy application needs. A service repository is built at this layer so as to know which is the catalogue of services that are associated to each object in the network. The upper layer can then compose complex services by joining services provided at this layer.

*3.2.4. Object abstraction*

The IoT relies on a vast and heterogeneous set of objects, each one providing specific functions accessible through its own dialect. There is thus the need for an abstraction layer capable of harmonizing the access to the different devices with a common language and procedure. Accordingly, unless a device offers discoverable web services on an IP network, there is the need to introduce a wrapping layer, consisting of two main sub-layers: the interface and the communication sub-layers. The first one provides a web interface exposing the methods available through a standard web service interface and is responsible for the management of all the incoming/outcoming messaging operations involved in the communication with the external world. The second sub-layer implements the logic behind the web service methods and translates these methods into a set of device-specific commands to communicate with the real-world objects.

Some works proposed the embedding of TCP/IP stacks in the devices, such as the TinyTCP, the mIP and the IwIP (see [33] and references herein), which provide a socket like interface for embedded applications. Embedded web servers can then be integrated in the objects, performing the function of this object abstraction layer. However, more often this wrapping function is provided through a proxy, which is then responsible to open a communication socket with the device's console and send all the commands to it by using different communication languages. It is then responsible to make the conversion into a standard web service language and, sometimes, elaborate the request to reduce the complexity of the operations required by the end-device [30].

*3.2.5. Trust, privacy and security management*

The deployment of automatic communication of objects in our lives represents a danger for our future. Indeed, unseen by users, embedded RFID tags in our personal devices, clothes, and groceries can unknowingly be triggered to reply with their ID and other information. This potentially enables a surveillance mechanism that would pervade large parts of our lives. The middleware must then include functions related to the management of the trust, privacy and security of all the exchanged data. The related functions may be either built on one specific layer of the previous ones or (it happens more often) distributed through the entire stack, from the object abstraction to the service composition, in a manner that does not affect system performance or introduce excessive overheads.

While most of the proposed middleware solutions make use of the SOA approach, some others have followed a different way, especially if developed for a specific scenario (target application, specific set of objects or limited geographical scenario). One remarkable project is the Fosstrak one, which is specifically focused on the management of RFID related applications [34]. It is an open source RFID infrastructure that implements the interfaces defined in the EPC Network specifications. It provides the following services related to RFID management: data dissemination, data aggregation, data filtering, writing to a tag, trigger RFID reader from external sensors, fault and configuration management, data interpretation, sharing of RFID triggered business events, lookup and directory service, tag identifier management, and privacy [35]. All these functions are made available to the application layer to ease the deployment of RFID-related services. In [36], the authors present another RFID-related middleware which relies on three functionalities: the tag, the place, and the scenic managers. The first allows the user to associate each tag to an object; the second supports creating and editing location information associated to RFID antennas; the third one is used to combine the events collected by the antennas and the developed related applications.

Another architecture that does not follow the SOA approach is proposed in the e-SENSE project, which focuses on issues related to capturing ambient intelligence through wireless sensor networks. The proposed architecture is divided into four logical subsystems, namely the application, management, middleware, and connectivity subsystems. Each subsystem comprises various protocol and control entities, which offer a wide range of services and functions at service access points to other subsystems [37]. This entire stack is implemented in a full function sensor node and in a gateway node; while a reduced-function sensor node has fewer functions. In the e-SENSE vision the middleware subsystem has the only purpose to develop and handle an infrastructure where information sensed by nodes is processed in a distributed fashion and, if necessary, the result is transmitted to an actuating node and/or to the fixed infrastructure by means of a gateway. The other functions that we have assigned to the middleware shown in Fig. 2 are attributed to other components and layers. The project UbiSec&Sens was also aimed at defining a comprehensive architecture for medium and large scale wireless sensor networks, with a particular attention to the security issues so as to provide a trusted and secure environment for all applications [38]. The middleware layer in this architecture mostly focuses on: (i) the secure long-term logging of the collected environmental data over time and over some regions (TinyPEDS), (ii) functions that provides the nodes in the network with the abstraction of shared memory (TinyDSM), (iii) the implementation of distributed information storage and collection (DISC) protocol for wireless sensor networks.

## 4. Applications

Potentialities offered by the IoT make possible the development of a huge number of applications, of which only a very small part is currently available to our society. Many are the domains and the environments in which new applications would likely improve the quality of our lives: at home, while travelling, when sick, at work, when jogging and at the gym, just to cite a few. These environments are now equipped with objects with only primitive intelligence, most of times without any communication capabilities. Giving these objects the possibility to communicate with each other and to elaborate the information perceived from the surroundings imply having different environments where a very wide range of applications can be deployed. These can be grouped into the following domains:

- Transportation and logistics domain.
- Healthcare domain.
- Smart environment (home, office, plant) domain.
- Personal and social domain.

Among the possible applications, we may distinguish between those either directly applicable or closer to our current living habitudes and those futuristic, which we can only fancy of at the moment, since the technologies and/or our societies are not ready for their deployment (see Fig. 3). In the following subsections we provide a review of the short-medium term applications for each of these categories and a range of futuristic applications.

### *4.1. Transportation and logistics domain*

Advanced cars, trains, buses as well as bicycles along with roads and/or rails are becoming more instrumented with sensors, actuators, and processing power. Roads themselves and transported goods are also equipped with tags and sensors that send important information to traffic control sites and transportation vehicles to better route the traffic, help in the management of the depots, provide the tourist with appropriate transportation information, and monitor the status of the transported goods. Below, the main applications in the transportation and logistics domain are described.

#### *4.1.1. Logistics*

Real-time information processing technology based on RFID and NFC can realize real-time monitoring of almost every link of the supply chain, ranging from commodity design, raw material purchasing, production, transportation,

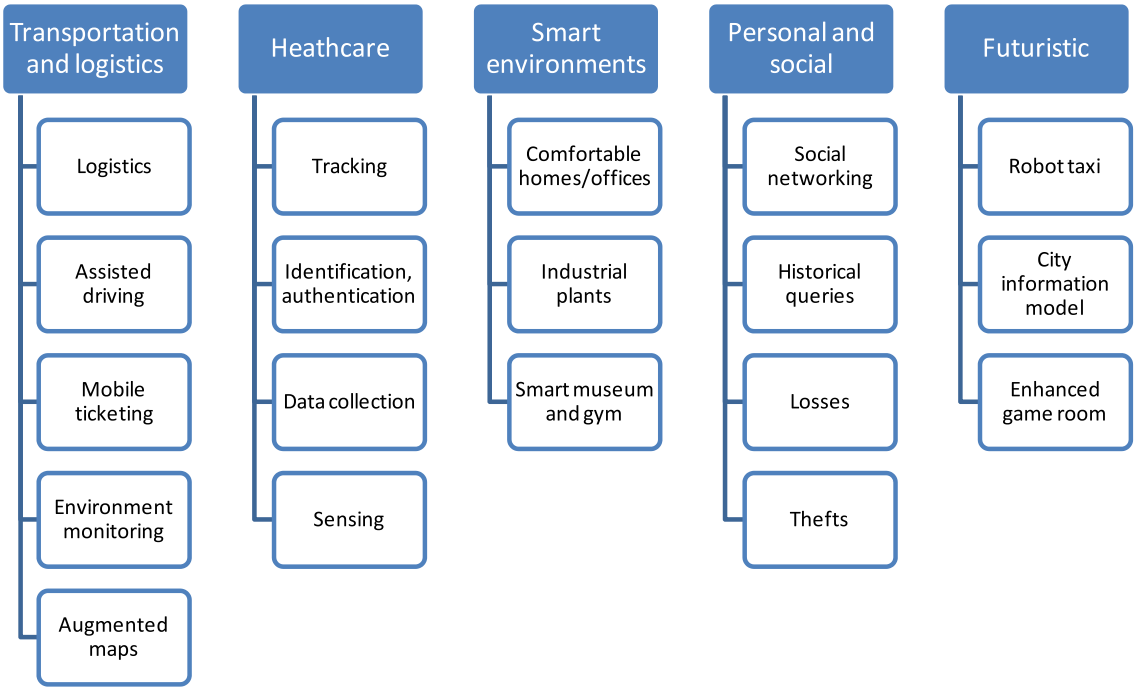



**Fig. 3.** Applications domains and relevant major scenarios.

storage, distribution and sale of semi-products and products, returns' processing and after-sales service. It is also possible to obtain products related information, promptly, timely, and accurately so that enterprises or even the whole supply chain can respond to intricate and changeable markets in the shortest time. The application result is that the reaction time of traditional enterprises is 120 days from requirements of customers to the supply of commodity while advanced companies that make use of these technologies (such as Wal-mart and Metro) only needs few days and can basically work with zero safety stock [39,40]. Additionally, real-time access to the ERP program helps the shop assistants to better inform customers about availability of products and give them more product information in general [41].

*4.1.2. Assisted driving*

Cars, trains, and buses along with the roads and the rails equipped with sensors, actuators and processing power may provide important information to the driver and/or passengers of a car to allow better navigation and safety. Collision avoidance systems and monitoring of transportation of hazardous materials are two typical example functions. Governmental authorities would also benefit from more accurate information about road traffic patterns for planning purposes. Whereas the private transportation traffic could better find the right path with appropriate information about the jam and incidents. Enterprises, such as freight companies, would be able to perform more effective route optimization which allows energy savings. Information about the movement of the vehicles transporting goods together with information about the type and status of the goods can be integrated to provide important information about the delivery time, delivery delays, and faults. This information can be also combined with the status of the warehouses in order to automate the refilling of the magazines.

*4.1.3. Mobile ticketing*

Posters or panels providing information (description, costs, schedule) about transportation services can be equipped with an NFC tag, a visual marker, and a numeric identifier. The user can then get information about several categories of options from the web by either hovering his mobile phone over the NFC tag, or pointing the mobile phone to the visual markers. The mobile phone automatically gets information from the associated web services (stations, numbers of passengers, costs, available seats and type of services) and allows the user to buy the related tickets [42].

*4.1.4. Monitoring environmental parameters*

Perishable goods such as fruits, fresh-cut produce, meat, and dairy products are vital parts of our nutrition. From the production to the consumption sites thousands of kilometers or even more are covered and during the transportation the conservation status (temperature, humidity, shock) need to be monitored to avoid uncertainty in quality levels for distribution decisions. Pervasive computing and sensor technologies offer great potential for improving the efficiency of the food supply chain [43,44].

#### 4.1.5. Augmented maps

Touristic maps can be equipped with tags that allow NFC-equipped phones to browse it and automatically call web services providing information about hotels, restaurants, monuments and events related to the area of interest for the user [45]. There is a collection of Physical Mobile Interaction (PMI) techniques that can be employed to augment the information of the map:

- hovering within read range of a tag so that additional information regarding the marker is displayed on the phone screen;
- single selection/de-selection of tags by pressing a specific key when the tag is hovered;
- multi-selection/de-selection of different tags;
- polygon drawing by selecting the tags in a polygon that delimits an area of interest;
- picking-and-dropping, so that selected markers that have been 'picked up' using the phone can be dropped in the itinerary of interest;
- context menu displaying when a marker is hovered [46].

### 4.2. Healthcare domain

Many are the benefits provided by the IoT technologies to the healthcare domain and the resulting applications can be grouped mostly into: tracking of objects and people (staff and patients), identification and authentication of people, automatic data collection and sensing [47].

#### 4.2.1. Tracking

Tracking is the function aimed at the identification of a person or object in motion. This includes both real-time position tracking, such as the case of patient-flow monitoring to improve workflow in hospitals, and tracking of motion through choke points, such as access to designated areas. In relation to assets, tracking is most frequently applied to continuous inventory location tracking (for example for maintenance, availability when needed and monitoring of use), and materials tracking to prevent left-ins during surgery, such as specimen and blood products.

#### 4.2.2. Identification and authentication

It includes patient identification to reduce incidents harmful to patients (such as wrong drug/dose/time/procedure), comprehensive and current electronic medical record maintenance (both in the in- and out-patient settings), and infant identification in hospitals to prevent mismatching. In relation to staff, identification and authentication is most frequently used to grant access and to improve employee morale by addressing patient safety issues. In relation to assets, identification and authentication is predominantly used to meet the requirements of security procedures, to avoid thefts or losses of important instruments and products.

#### 4.2.3. Data collection

Automatic data collection and transfer is mostly aimed at reducing form processing time, process automation (including data entry and collection errors), automated care and procedure auditing, and medical inventory management. This function also relates to integrating RFID technology with other health information and clinical application technologies within a facility and with potential expansions of such networks across providers and locations.

#### 4.2.4. Sensing

Sensor devices enable function centered on patients, and in particular on diagnosing patient conditions, providing real-time information on patient health indicators. Application domains include different telemedicine solutions, monitoring patient compliance with medication regiment prescriptions, and alerting for patient well-being. In this capacity, sensors can be applied both in in-patient and out-patient care. Heterogeneous wireless access-based remote patient monitoring systems can be deployed to reach the patient everywhere, with multiple wireless technologies integrated to support continuous bio-signal monitoring in presence of patient mobility [48].

### 4.3. Smart environments domain

A smart environment is that making its "employment" easy and comfortable thanks to the intelligence of contained objects, be it an office, a home, an industrial plant, or a leisure environment.

#### 4.3.1. Comfortable homes and offices

Sensors and actuators distributed in houses and offices can make our life more comfortable in several aspects: rooms heating can be adapted to our preferences and to the weather; the room lighting can change according to the time of the day; domestic incidents can be avoided with appropriate monitoring and alarm systems; and energy can be saved by automatically switching off the electrical equipments when not needed. For instance, we may think of energy providers that use dynamically changing energy prices to influence the overall energy consumption in a way that smoothes load peaks. An automation logic may optimize the power consumption costs throughout the day by observing when the prices, which are provided by an external web service and are set according to the current energy production and consumption, are cheap and by considering the specific requirements of each appliances at home (battery charger, refrigerator, ovens) [30].

#### 4.3.2. Industrial plants

Smart environments also help in improving the automation in industrial plants with a massive deployment of RFID tags associated to the production parts. In a generic scenario, as production parts reach the processing point, the tag is read by the RFID reader. An event is generated by the reader with all the necessary data, such as the RFID number, and stored on the network. The machine/robot gets notified by this event (as it has subscribed to the service) and picks up the production part. By matching data from the enterprise system and the RFID tag, it knows how to further process the part. In parallel, a wireless sensor mounted on the machine monitors the vibration and if

it exceeds a specific threshold an event is raised to immediately stop the process (quality control). Once such an emergency event is propagated, devices that consume it react accordingly. The robot receives the emergency shutdown event and immediately stops its operation. The plant manager also immediately sees the status of the so called Enterprise Resource Planning (ERP) orders, the production progress, the device status, as well as a global view on all the elements and the possible side effects of a production line delay due to shop-floor device malfunctions [29].

#### 4.3.3. Smart museum and gym

As to smart leisure environments, the museum and the gym are two representative examples where the IoT technologies can help in exploiting their facilities at the best. In the museum, for instance, expositions in the building may evoke various historical periods (Egyptian period or ice age) with widely diverging climate conditions. The building adjusts locally to these conditions while also taking into account outdoor conditions. In the gym, the personal trainer can upload the exercise profile into the training machine for each trainee, who is then automatically recognized by the machine through the RFID tag. Health parameters are monitored during the whole training session and the reported values are checked to see if the trainee is overtraining or if she/he is too relaxed when doing the exercises.

### 4.4. Personal and social domain

The applications falling in this domain are those that enable the user to interact with other people to maintain and build social relationships. Indeed, things may automatically trigger the transmission of messages to friends to allow them to know what we are doing or what we have done in the past, such as moving from/to our house/office, travelling, meeting some common mates or playing soccer [36]. The following are the major applications.

#### 4.4.1. Social networking

This application is related to the automatic update of information about our social activities in social networking web portals, such as Twitter and Plazes. We may think of RFIDs that generate events about people and places to give users real-time updates in their social networks, which are then gathered and uploaded in social networking websites. Application user interfaces display a feed of events that their friends have preliminarily defined and the users can control their friend lists as well as what events are disclosed to which friends.

#### 4.4.2. Historical queries

Historical queries about objects and events data let users study trends in their activities over time. This can be extremely useful for applications that support long-term activities such as business projects and collaborations. A digital diary application can be built that records and displays events for example in a Google Calendar for later perusal. This way, users can look back over their diaries to see how and with whom they've spent their time. Historical trends plots can also be automatically generated using the Google Charts API to display where, how, and with whom or what they have spent their time over some arbitrary period.

#### 4.4.3. Losses

A search engine for things is a tool that helps in finding objects that we don't remember where have been left. The simplest web-based RFID application is a search engine for things that lets users view the last recorded location for their tagged objects or search for a particular object's location. A more proactive extension of this application leverages user-defined events to notify users when the last recorded object location matches some conditions.

#### 4.4.4. Thefts

An application similar to the previous one may allow the user to know if some objects are moved from a restricted area (the owner house or office), which would indicate that the object is being stolen. In this case, the event has to be notified immediately to the owner and/or to the security guards. For example, the application can send an SMS to the users when the stolen objects leave the building without any authorization (such as a laptop, a wallet or an ornament).

### 4.5. Futuristic applications domain

The applications described in the previous sections are realistic as they either have been already deployed or can be implemented in a short/medium period since the required technologies are already available. Apart from these, we may envision many other applications, which we herein define *futuristic* since these rely on some (communications, sensing, material and/or industrial processes) technologies that either are still to come or whose implementation is still too complex. These applications are even more interesting in terms of required research and potential impact. An interesting analysis of this kind of applications is provided by SENSEI FP7 Project [49] from which we have taken the three most appealing applications.

#### 4.5.1. Robot taxi

In future cities, robot taxis swarm together, moving in flocks, providing service where it is needed in a timely and efficient manner. The robot taxis respond to real-time traffic movements of the city, and are calibrated to reduce congestion at bottlenecks in the city and to service pick-up areas that are most frequently used. With or without a human driver, they weave in and out of traffic at optimum speeds, avoiding accidents through proximity sensors, which repel them magnetically from other objects on the road. They can be hailed from the side of the street by pointing a mobile phone at them or by using hand gestures. The user's location is automatically tracked via GPS and enables users to request a taxi to be at a certain location at a particular time by just pointing it out on a detailed map. On the rare occasions they are not in use, the taxis head for 'pit-stops' where they automatically stack themselves into tight bays which are instrumented with sensors where actuators set off recharging batteries, perform simple maintenance tasks and clean the cars. The pit-stops

communicate with each other to ensure no over or under-utilization [49].

#### 4.5.2. City information model

The idea of a City Information Model (CIM) is based on the concept that the status and performance of each buildings and urban fabrics – such as pedestrian walkways, cycle paths and heavier infrastructure like sewers, rail lines, and bus corridors – are continuously monitored by the city government operates and made available to third parties via a series of APIs, even though some information is confidential. Accordingly, nothing can be built legally unless it is compatible with CIM. The facilities management services communicate with each other and the CIM, sharing energy in the most cost-effective and resource-efficient fashion. They automatically trade surplus energy with each other and prices are calculated to match supply and demand. In this sense, planning and design is an ongoing social process, in which the performance of each item is being reported in real-time and compared with others. Population changes can be inferred, as can movement patterns, environmental performance, as well as the overall efficiency of products and buildings.

#### 4.5.3. Enhanced game room

The enhanced game room as well as the players are equipped with a variety of devices to sense location, movement, acceleration, humidity, temperature, noise, voice, visual information, heart rate and blood pressure. The room uses this information to measure excitement and energy levels so that to control the game activity according to status of the player. Various objects are also placed throughout the room and the point of the game is to crawl and jump from one to the other without touching the floor. Points are awarded for long jumps and difficult places to reach. The game also puts a target on the wall-mounted screen. Whoever reaches that target first, wins. As the players work their way around the room, the game keeps track of their achievements. Their controller recognizes RFID tags on objects in the room. To score, they have to touch the object with it. As the game progresses, the system gradually makes it more difficult. At first the objects they have to reach are nearby and easy to reach. At some point it gets too difficult and both players must touch the floor with their feet. Then the game makes a loud noise to indicate that this was wrong. The room now notices that one player is a bit taller and faster than the other so it starts putting the objects a bit closer to him, so that he can keep up. The game then adapts the difficulty level and the target according to the achievements of the players so that to keep high the excitement level perceived by the console through the sensing devices.

## 5. Open issues

Although the enabling technologies described in Section 3 make the IoT concept feasible, a large research effort is still required. In this section, we firstly review the standardization activities that are being carried out on different IoT-related technologies (Section 5.1). Secondly, we show the most important research issues that need to be addressed to meet the requirements characterizing IoT scenarios. More specifically, in Section 5.2 we focus on addressing and networking issues, whereas in Section 5.3 we describe the problems related to security and privacy.

In Table 2 we summarize the open research issues, the causes for which they are specifically crucial for IoT scenarios and the sections when such issues will be discussed in detail.

### 5.1. Standardization activity

Several contributions to the full deployment and standardization of the IoT paradigm are coming from the scientific community. Among them, the most relevant are

**Table 2**
Open research issues.

| Open issue | Brief description of the cause | Details in |
|---|---|---|
| Standards | There are several standardization efforts but they are not integrated in a comprehensive framework | Section 5.1 |
| Mobility support | There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems | Section 5.2 |
| Naming | Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and *vice versa* | Section 5.2 |
| Transport protocol | Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in *objects* | Section 5.2 |
| Traffic characterization and QoS support | The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes | Section 5.2 |
| Authentication | Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem | Section 5.3 |
| Data integrity | This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection | Section 5.3 |
| Privacy | A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques | Section 5.3 |
| Digital forgetting | All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years | Section 5.3 |

provided by the different sections of the Auto-ID Lab scattered all over the world [50,51,34], by the European Commission [52] and European Standards Organisations (ETSI, CEN, CENELEC, etc.), by their international counterparts (ISO, ITU), and by other standards bodies and consortia (IETF, EPCglobal, etc.). Inputs are particularly expected from the Machine-to-Machine Workgroup of the European Telecommunications Standards Institute (ETSI) and from some Internet Engineering Task Force (IETF) Working Groups. 6LoWPAN [53], aiming at making the IPv6 protocol compatible with low capacity devices, and ROLL [54], more interested in the routing issue for Internet of the Future scenarios, are the best candidates.

In Table 3 we summarize the fundamental characteristics of the main standards of interest in terms of objectives of the standard, status of the standardization process, communication range, data rate, and cost of devices. In the table we highlight the standards that are discussed in detail in this section.

With regards to the RFID technology, it is currently slowed down by fragmented efforts towards standardization, which is focusing on a couple of principal areas: RFID frequency and readers-tags (tags-reader) communication protocols, data formats placed on tags and labels. The major standardization bodies dealing with RFID systems are EPCglobal, ETSI, and ISO.

More specifically, EPCglobal is a subsidiary of the global not-for-profit standards organization GS1. It mainly aims at supporting the global adoption of a unique identifier for each tag, which is called Electronic Product Code (EPC), and related industry-driven standards. The production of a recommendation for the "EPCglobal Architecture Framework" is a EPCglobal objective, shared with a community of experts and several organizations, including Auto-ID Labs, GS1 Global Office, GS1 Member Organizations, government agencies, and non-governmental organizations (NGOs). Interesting results are already available [5].

As for the European Commission efforts, the event that might have the strongest influence on the future RFID standardization process is undoubtedly the official constitution of the so called "Informal working group on the implementation of the RFID". This is composed of stakeholders (industry, operators, European standard organisations, civil society organisations, data protection authorities, etc.) required "to be familiar with RFID in general, the Data Protection Directive and the RFID Recommendation".

One of these stakeholders, CEN (European Committee for Standardization) [55], although does not conduct any activity specifically related to the IoT, is interested in RFID evolution towards IoT. Among its Working Groups (WGs), the most relevant to the IoT are WG 1-4 BARCODES, WG 5 RFID, and the Global RFID Interoperability Forum for Standards (GRIFS). This latter is a two-year-project coordinated by GS1, ETSI, and CEN and aimed at defining standards related to physical objects (readers, tags, sensors), communications infrastructures, spectrum for RFID use, privacy and security issues affecting RFID [56].

Differently from these projects, ISO [57] focuses on technical issues such as the frequencies utilized, the modulation schemes, and the anti-collision protocol.

With regards to the IoT paradigm at large, a very interesting standardization effort is now starting in ETSI [58] (the European Telecommunications Standards Institute, which produces globally-applicable ICT related standards). Within ETSI, in fact, the Machine-to-Machine (M2M) Technical Committee was launched, to the purpose of conducting standardization activities relevant to M2M systems and sensor networks (in the view of the IoT). M2M is a real leading paradigm towards IoT, but there is very little standardization for it, while the multiplicity of the solutions on the market use standard Internet, Cellular, and Web technologies. Therefore, the goals of the ETSI M2M committee include: the development and the maintenance of an end-to-end architecture for M2M (with end-to-end IP philosophy behind it), strengthening the standardization efforts on M2M, including sensor network integration, naming, addressing, location, QoS, security, charging, management, application, and hardware interfaces [59].

As for the Internet Engineering Task Force (IETF) activities related to the IoT, we can say that recently the *IPv6*

**Table 3**
Characteristics of the most relevant standardization activities.

| Standard | Objective | Status | Comm. range (m) | Data rate (kbps) | Unitary cost ($) |
|---|---|---|---|---|---|
| *Standardization activities discussed in this section* | | | | | |
| EPCglobal | Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products | Advanced | ~1 | ~$10^2$ | ~0.01 |
| GRIFS | European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the *Internet of Things* | Ongoing | ~1 | ~$10^2$ | ~0.01 |
| M2M | Definition of cost-effective solutions for machine-to-machine (M2M) communications, which should allow the related market to take off | Ongoing | N.S. | N.S. | N.S. |
| 6LoWPAN | Integration of low-power IEEE 802.15.4 devices into IPv6 networks | Ongoing | 10–100 | ~$10^2$ | ~1 |
| ROLL | Definition of routing protocols for heterogeneous low-power and lossy networks | Ongoing | N.S. | N.S. | N.S. |
| *Other relevant standardization activities* | | | | | |
| NFC | Definition of a set of protocols for low range and bidirectional communications | Advanced | ~$10^{-2}$ | Up to 424 | ~0.1 |
| Wireless Hart | Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices | Advanced | 10–100 | ~$10^2$ | ~1 |
| ZigBee | Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products | Advanced | 10–100 | ~$10^2$ | ~1 |

*over Low-Power Wireless Personal Area Networks* (6LoWPAN) IETF group was born [53]. 6LoWPAN is defining a set of protocols that can be used to integrate sensor nodes into IPv6 networks. Core protocols composing the 6LoWPAN architecture have been already specified and some commercial products have been already released that implement this protocol suite. The 6LoWPAN working group is currently moving four Internet-Drafts towards last call in the standards track (Improved Header Compression, 6LoWPAN Neighbour Discovery) and informational track (Use Cases, Routing Requirements) [60].

A further relevant IETF Working Group is named *Routing Over Low power and Lossy networks* (ROLL). It has recently produced the RPL (pronounced "ripple") routing protocol draft. This will be the basis for routing over low-power and lossy networks including 6LoWPAN, which still needs lots of contributions to reach a full solution.

We clearly understand, from what is described above, that an emerging idea is to consider the IoT standardisation as an integral part of the Future Internet definition and standardisation process. This assertion was recently made by the cluster of European R&D projects on the IoT (CERP-IoT). According to it, the integration of different *things* into wider networks, either mobile or fixed, will allow their interconnection with the Future Internet [61].

What is worth pointing out in the cited standardization areas is the tight collaboration between standardization Institutions and other world-wide Interest Groups and Alliances. It seems that the whole industry is willing to cooperate on achieving the IoT. IPSO, but also the ZigBee Alliance, the IETF and the IEEE work in the same direction of IP standards integration [61].

### 5.2. Addressing and networking issues

The IoT will include an incredibly high number of nodes, each of which will produce content that should be retrievable by any authorized user regardless of her/his position. This requires effective addressing policies. Currently, the IPv4 protocol identifies each node through a 4-byte address. It is well known that the number of available IPv4 addresses is decreasing rapidly and will soon reach zero. Therefore, it is clear that other addressing policies should be used other than that utilized by IPv4.

In this context, as we already said in Section 5.1, IPv6 addressing has been proposed for low-power wireless communication nodes within the 6LoWPAN context. IPv6 addresses are expressed by means of 128 bits and therefore, it is possible to define $10^{38}$ addresses, which should be enough to identify any object which is worth to be addressed. Accordingly, we may think to assign an IPv6 address to all the *things* included in the network. However, since RFID tags use 64–96 bit identifiers, as standardized by EPCglobal, solutions are required for enabling the addressing of RFID tags into IPv6 networks. Recently, integration of RFID tags into IPv6 networks has been investigated [62] and methodologies to integrate RFID identifiers and IPv6 addresses have been proposed. For example, in [63] authors propose to use the 64 bits of the interface identifier of the IPv6 address to report the RFID tag identifier, whereas the other 64 bits of the network prefix are used to address the gateway between the RFID system and the Internet.

Accordingly, the gateway will handle messages generated by RFID tags that must leave the RFID system and enter the Internet as follows. A new IPv6 packet will be created. Its payload will contain the message generated by the tag, whereas its source address will be created by concatenating the gateway ID (which is copied into the network prefix part of the IPv6 address) and the RFID tag identifier (which is copied into the interface identifier part of the IPv6 address). Analogously, the gateway will handle IPv6 packets coming from the Internet and directed towards a certain RFID tag as follows. The specific RFID tag, which represents the destination of the message, will be easily recognized as its identifier is reported into the interface identifier part of the IPv6 address; the specific message (which in most cases represents the request of a certain operation) will be, instead, notified to the relevant RFID reader(s).

This approach, however, cannot be used if the RFID tag identifier is long 96 bits, as allowed by the EPCglobal standard. To solve this problem, in [64] a methodology is proposed that uses an appropriate network element, called *agent*, that maps the RFID identifier (regardless of its length) into a 64 bits field which will be used as the interface ID of the IPv6 address. Obviously, the agent must keep updated a mapping between the IPv6 addresses generated and the RFID tag identifier.

A complete different approach is illustrated in [65], where the RFID message and headers are included into the IPv6 packet payload as shown in Fig. 4.

It is important to note, however, that in all the above cases RFID mobility is not supported. In fact, the common basic assumption is that each RFID can be reached through a given gateway between the network and the RFID system.

It follows that appropriate mechanisms are required to support mobility in the IoT scenarios. In this contexts, the overall system will be composed of a large number of subsystems with extremely different characteristics. In the past, several solutions have been proposed for the mobility management [66]; however, their validity in the IoT scenarios should be proven as they may have problems in terms of scalability and adaptability to be applied in such a heterogeneous environment. To this purpose it is important to note that higher scalability can be achieved by solutions based on the utilization of a home agent (like Mobile IP [67]), rather than by solutions based on *home location registers* (HLR) and *visitor location registers* (VLR), which are widely used in cellular networks. In fact, Mobile IP-like protocols do not use central servers, which are critical from a scalability point of view.

Another issue regards the way in which addresses are obtained. In the traditional Internet any host address is identified by querying appropriate servers called *domain name servers* (DNS). Objective of DNSs is to provide the IP address of a host from a certain input name. In the IoT, communications are likely to occur between (or with) *objects* instead of hosts. Therefore, the concept of *Object Name Service* (ONS) must be introduced, which associates a reference to a description of the specific object and the related RFID tag identifier [68,5]. In fact, the

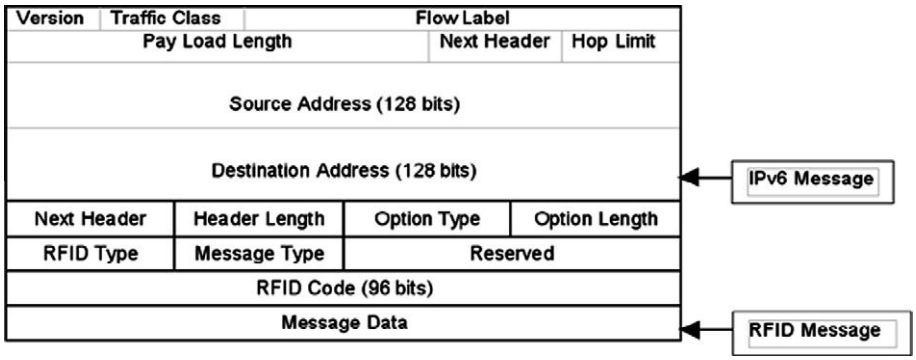



**Fig. 4.** Encapsulation of RFID message into an IPv6 packet.

tag identifier is mapped into a *Internet Uniform Reference Locator* (URL), which points to relevant information of the object. In the IoT, the ONS should operate in both directions, i.e., should be able to associate the description of the object specified to a given RFID tag identifier, and vice versa. Inverting the function is not easy and requires an appropriate service, which is called *Object Code Mapping Service* (OCMS). Desired characteristics for OCMSs are reported in [69], where a P2P approach is suggested in order to improve scalability. However, note that design and assessment of OCMS in complex operational environments, such as the IoT, are still open issues.

Also a new conception of the transport layer is required for the IoT. Major goals of the transport layer are to guarantee end-to-end reliability and to perform end-to-end congestion control. In the traditional Internet, the protocol utilized at the transport layer for reliable communications is the *Transmission Control Protocol* (TCP) [70]. It is obvious that TCP is inadequate for the IoT, due to the following reasons:

1. *Connection setup*: TCP is connection oriented and each session begins with a connection setup procedure (the so called *three ways handshake*). This is unnecessary, given that most of the communications within the IoT will involve the exchange of a small amount of data and, therefore, the setup phase would last for a considerable portion of the session time. Furthermore, the connection setup phase involves data to be processed and transmitted by end-terminals, which in most cases are limited in terms of both energy and communication resources, such as sensor nodes and RFID tags.
2. *Congestion control*: TCP is responsible of performing end-to-end congestion control. In the IoT this may cause performance problems as most of the communications will exploit the wireless medium, which is known to be a challenging environment for TCP [71]. Furthermore, if the amount of data to be exchanged in a single session is very small, TCP congestion control is useless, given that the whole TCP session will be concluded with the transmission of the first segment and the consequent reception of the corresponding acknowledgement.
3. *Data buffering:* TCP requires data to be stored in a memory buffer both at the source and at the destination. In fact, at the source data should be buffered so that it can be retransmitted in case it is lost. At the destination data should be buffered to provide ordered delivery of data to the application. Management of such buffers may be too costly in terms of required energy for battery-less devices.

As a consequence, TCP cannot be used efficiently for the end-to-end transmission control in the IoT. Up to date, no solutions have been proposed for the IoT and therefore, research contributions are required.

Furthermore, we do not know what will be the characteristics of the traffic exchanged by smart objects in the IoT. Whereas it is fundamental to investigate such characteristics as they should be the basis for the design of the network infrastructures and protocols.

Accordingly, another important research issue concerning the networking aspects is related to traffic characterization. It is well known that traffic characteristics in wireless sensor networks strongly depend on the application scenario (see [72], for example). This was not a problem as the interest was focused on the traffic flow inside the wireless sensor network itself. Complications arise when, according to the IoT paradigm, sensor nodes become part of the overall Internet. In fact, in this scenario, the Internet will be traversed by a large amount of data generated by sensor networks deployed for heterogeneous purposes and thus, with extremely different traffic characteristics. Furthermore, since the deployment of large scale and distributed RFID systems are still at the very beginning, the characteristics of the related traffic flows have not been studied so far, and therefore, the traffic which will traverse the IoT is completely unknown.

On the contrary characterization of the traffic is very important as it is necessary to network providers for planning the expansion of their infrastructures (if needed).

Finally, traffic characterization and modeling together with a list of traffic requirements is needed to devise appropriate solutions for supporting quality of service (QoS). In fact, if some work has been done for supporting QoS in wireless sensor networks [73], the problem is still completely unexplored in RFID systems. Accordingly, a large research effort is needed in the field of QoS support in the IoT. We believe that there will be several analogies with QoS for machine-to-machine communications. Since such types of communications have been already

addressed in recent years [74], we can apply to the IoT scenarios QoS management schemes proposed for M2M scenarios. Obviously, this should be just a starting point and specific solutions for the IoT should be introduced in the future.

### 5.3. Security and privacy

People will resist the IoT as long as there is no public confidence that it will not cause serious threats to privacy. All the talking and complains (see [75] for example) following the announcement by the Italian retailer Benetton on the plan to tag a complete line of clothes (around 15 million RFIDs) has been the first, clear confirmation of this mistrust towards the use that will be done of the data collected by the IoT technologies [76].

Public concerns are indeed likely to focus on a certain number of security and privacy issues [21,77].

#### 5.3.1. Security

The IoT is extremely vulnerable to attacks for several reasons. First, often its components spend most of the time unattended; and thus, it is easy to physically attack them. Second, most of the communications are wireless, which makes eavesdropping extremely simple. Finally, most of the IoT components are characterized by low capabilities in terms of both energy and computing resources (this is especially the case for passive components) and thus, they cannot implement complex schemes supporting security.

More specifically, the major problems related to security concern *authentication* and *data integrity*. Authentication is difficult as it usually requires appropriate authentication infrastructures and servers that achieve their goal through the exchange of appropriate messages with other nodes. In the IoT such approaches are not feasible given that passive RFID tags cannot exchange too many messages with the authentication servers. The same reasoning applies (in a less restrictive way) to the sensor nodes as well.

In this context, note that several solutions have been proposed for sensor networks in the recent past [78]. However, existing solutions can be applied when sensor nodes are considered as part of a sensor network connected to the rest of the Internet via some nodes playing the roles of gateways. In the IoT scenarios, instead, sensor nodes must be seen as nodes of the Internet, so that it becomes necessary to authenticate them even from nodes not belonging to the same sensor network.

In the last few years, some solutions have been proposed for RFID systems, however, they all have serious problems as described in [21].

Finally, none of the existing solutions can help in solving the *proxy attack* problem, also known as the *man-in-the-middle attack*. Consider the case in which a node is utilized to identify something or someone and, accordingly, provides access to a certain service or a certain area (consider an electronic passport for example, or some keys based on RFID). The attack depicted in Fig. 5 could be successfully performed.

Consider the case in which $A$ is the node that wants to authenticate other system elements through some RF mechanism and that an attacker wants to stole the identity of the element $B$ (please note that that $B$ can be any IoT element capable of computing and communicating). The attacker will position two transceivers. The first close to $A$, which we call $B'$ and the second close to $B$, which we call $A'$. The basic idea is to make $A$ believe that $B'$ is $B$, and make $B$ believe that $A'$ is $A$. To this purpose, node $B'$ will transmit the query signal received by the authenticating node $A$ to the transceiver $A'$. The transceiver $A'$ will transmit such signal so that $B$ can receive it. Observe, that the signal transmitted by $A'$ is an exact replica of the signal transmitted by $A$. Accordingly, it is impossible for node $B$ to understand that the signal was not transmitted by $A$ and therefore, it will reply with its identification. Node $A'$ receives such reply and transmits it to node $B'$, that will transmit it to node $A$. Node $A$ cannot distinguish that such reply was not transmitted by $B$, and therefore, will identify the transceiver $B'$ as the element $B$ and provide access accordingly. Observe that this can be done regardless of the fact that the signal is encrypted or not.

Data integrity solutions should guarantee that an adversary cannot modify data in the transaction without the system detecting the change. The problem of data integrity has been extensively studied in all traditional computing and communication systems and some preliminary results exist for sensor networks, e.g., [79]. However, new problems arise when RFID systems are integrated in the Internet as they spend most of the time unattended. Data can be modified by adversaries while it is stored in the node or when it traverses the network [80]. To protect data against the first type of attack, memory is protected in most tag technologies and solutions have been proposed for wireless sensor networks as well [81]. For example, both *EPCglobal Class-1 Generation-2* and *ISO/IEC 18000–3* tags protect both read and write operations on their memory with a password. In fact, *EPCglobal Class-1 Generation-2* tags have five areas of memory, each of which can be protected in read or write with a password independently of each others. Whereas, *ISO/18000–3* tags define a pointer to a memory address and protect with a password all memory areas with a lower memory address. To protect data against the second type of attack, messages may be protected according to the *Keyed-Hash Message Authentication Code* (HMAC) scheme [82]. This is based on a common

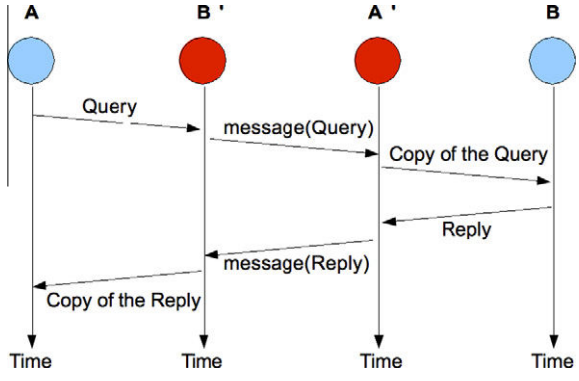



**Fig. 5.** Man in the middle attack.

secret key shared between the tag and the destination of the message, which is used in combination with a hash function to provide authentication.

Observe that the above solutions proposed to support data integrity when RFID systems are considered have serious problems. In fact, the password length supported by most tag technologies is too short to provide strong levels of protections. Moreover, even if longer passwords are supported, still their management remains a challenging task, especially when entities belonging to different organizations, as in the case of the IoT, are involved.

Finally, please note that that all the solutions proposed to support security use some cryptographic methodologies. Typical cryptographic algorithms spend large amount of resources in terms of energy and bandwidth both at the source and the destination. Such solutions cannot be applied to the IoT, given that they will include elements (like RFID tags and sensor nodes) that are seriously constrained in terms of energy, communications, and computation capabilities. It follows that new solutions are required able to provide a satisfactory level of security regardless of the scarcity of resources. In this context, a few solutions have been proposed for light symmetric key cryptographic schemes (see [83,84] for RFID scenarios and [78] for sensor network scenarios). However, as we already said, key management schemes are still at an early stage (especially in the case of RFID) and require large research efforts.

#### 5.3.2 Privacy

The concept of *privacy* is deeply rooted into our civilizations, is recognized in all legislations of civilized countries and, as we already said, concerns about its protection have proven to be a significant barrier against the diffusion of the technologies involved in the IoT [75]. People concerns about privacy are indeed well justified. In fact, the ways in which data collection, mining, and provisioning will be accomplished in the IoT are completely different from those that we now know and there will be an amazing number of occasions for personal data to be collected. Therefore, for human individuals it will be impossible to personally control the disclosure of their personal information.

Furthermore, the cost of information storage continues to decrease and is now approaching $10^{-9}$ euro per byte. Accordingly, once information is generated, will most probably be retained indefinitely, which involves denial of digital forgetting in people perspective.

It follows that the IoT really represents an environment in which privacy of individuals is seriously menaced in several ways. Furthermore, while in the traditional Internet problems of privacy arise mostly for Internet users (individuals playing an active role), in the IoT scenarios privacy problems arise even for people not using any IoT service.

Accordingly, privacy should be protected by ensuring that individuals can control which of their personal data is being collected, who is collecting such data, and when this is happening. Furthermore, the personal data collected should be used only in the aim of supporting authorized services by authorized service providers; and, finally, the above data should be stored only until it is strictly needed.

For example, consider the application scenario regarding *Comfortable homes and offices* described in Section 4.3, and focus on the case of a building where several offices are located. In this case, some sensing capabilities will be deployed in the environment to track position of people and control the lighting or heating accordingly. If the tracking system is deployed only for increasing comfort of the offices while reducing energy consumption, then, appropriate policies to protect privacy should be applied guaranteeing that:

- the tracking system does not collect information about the position and movements of individual users but only considers aggregate users (position and movements of people should not be linkable to their identities);
- people are informed of the scope and the way in which their movements are tracked by the system (taking people informed about possible leaks of their privacy is essential and required by most legislations);
- data collected by the tracking system should be processed for the purposes of controlling the lighting and heating and then deleted by the storage system.

To handle the data collection process appropriate solutions are needed in all the different subsystems interacting with human beings in the IoT. For example, in the context of traditional Internet services the W3C group has defined the *Platform for Privacy Preferences* (P3P) [85], which provides a language for the description of the privacy preferences and policies and therefore, allows automatic negotiation of the parameters concerning privacy based on the needs of personal information for running the service and the privacy requirements set by the user. Always in the context of traditional Internet services, through appropriate settings of the applications run on the user terminals, the time instants when personal information are being released can be easily detected and the entity collecting such data can be identified through well established authentication procedures.

The problem becomes impossible to be solved in the case of sensor networks. In fact, individuals entering in an area where a sensor network is deployed cannot control what information is being collected about themselves. For example, consider a sensor network composed of cameras deployed in a certain area. The only way an individual can avoid such cameras not to take her/his image is not to enter into the area. In this context, a possible solution that can reduce privacy problems might be to restrict the network's ability to gather data at a detail level that could compromise privacy [86]. For example, a sensor network might anonymize data by reporting only approximate locations of sensed individuals and tradeoff privacy requirements with the level of details required by the application. Another example regarding sensor networks composed of cameras deployed for video surveillance purposes. In this case, images of people can be blurred in order to protect their privacy [87]. If some event occurs, then the image of relevant people can be reconstructed by the law enforcement personnel.

In the case of RFID systems, the problem is twofold. In fact, on the one hand usually RFID tags are passive and reply to readers queries regardless of the desire of their proprietary. On the other hand an attacker can eavesdrop the reply from a tag to another authorized reader. Solutions to the first type of problems proposed so far are based on authentication of authorized readers (which have been discussed above). However, such solutions require tags that are able to perform authentication procedures. This involves higher costs and an authentication infrastructure, which, as we have already said, cannot be deployed in complex systems like those expected in IoT scenarios. Accordingly, solutions have been recently proposed (see [88] for example) that use a new system that, on the basis of preferences set by the user, negotiates privacy on her/his behalf. The privacy decisions taken by the above system can be enforced by creating collisions in the wireless channel with the replies transmitted by the RFID tags, which should not be read [89].

Avoiding eavesdropping by attacker in RFID systems can be accomplished through protecting the communication with encryption as explained above. However, these types of solutions still allow malicious readers to detect the presence of the RFID tags scanned by the authorized reader. To fix this problem, there is a new family of solutions in which the signal transmitted by the reader has the form of a pseudo-noise. Such noisy signal is modulated by the RFID tags and therefore, its transmission cannot be detected by malicious readers [90].

In order to ensure that the personal data collected is used only to support authorized services by authorized providers, solutions have been proposed that usually rely on a system called *privacy broker* [91]. The proxy interacts with the user on the one side and with the services on the other. Accordingly, it guarantees that the provider obtains only the information about the user which is strictly needed. The user can set the preferences of the proxy. When sensor networks and RFID systems are included in the network, then the proxy operates between them and the services. However, note that in this case the individual cannot set and control the policies utilized by the privacy brokers. Moreover, observe that such solutions based on privacy proxies suffer from scalability problems.

Finally, studies are still at the beginning regarding digital forgetting as this has been recognized as an important issue only recently [92]. In fact, as the cost of storage decreases, the amount of data that can be memorized increases dramatically. Accordingly, there is the need to create solutions that periodically delete information that is of no use for the purpose it was generated. Accordingly, the new software tools that will be developed in the future should support such forgetting functionalities. For example, a few experimental solutions have been developed and released for public use in the recent past that allow users to insert and share pictures and other types of files over the Internet with the assurance that such pictures will expire at a certain date and will be deleted afterwards (see drop.io and the Guest Pass features on Flickr for example [93]). Porting of such solutions to the IoT context is not straightforward and requires further research effort.

## 6. Conclusions

The Internet has changed drastically the way we live, moving interactions between people at a *virtual* level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus leading to the vision of "anytime, anywhere, anymedia, anything" communications.

To this purpose, we observe that the IoT should be considered as part of the overall Internet of the future, which is likely to be dramatically different from the Internet we use today. In fact, it is clear that the current Internet paradigm, which supports and has been built around host-to-host communications, is now a limiting factor for the current use of the Internet. It has become clear that Internet is mostly used for the publishing and retrieving of information (regardless of the host where such information is published or retrieved from) and therefore, information should be the focus of communication and networking solutions. This leads to the concept of data-centric networks, which has been investigated only recently [94]. According to such a concept, data and the related queries are self-addressable and self-routable.

In this perspective, the current trend, which we have highlighted in Section 5.2, of assigning an IPv6 address to each IoT element so as to make it possible to reach them from any other node of the network, looks more suitable for the traditional Internet paradigm. Therefore, it is possible that the Internet evolution will require a change in the above trend.

Another interesting paradigm which is emerging in the Internet of the Future context is the so called *Web Squared*, which is an evolution of the Web 2.0. It is aimed at integrating web and sensing technologies [95] together so as to enrich the content provided to users. This is obtained by taking into account the information about the user context collected by the sensors (microphone, cameras, GPS, etc.) deployed in the user terminals. In this perspective, observe that Web Squared can be considered as one of the applications running over the IoT, like the Web is today an (important) application running over the Internet.

In this paper, we have surveyed the most important aspects of the IoT with emphasis on what is being done and what are the issues that require further research. Indeed, current technologies make the IoT concept feasible but do not fit well with the scalability and efficiency requirements they will face. We believe that, given the interest shown by industries in the IoT applications, in the next years addressing such issues will be a powerful driving factor for networking and communication research in both industrial and academic laboratories.

## References

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.
[2] National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008-07, April 2008, <http://www.dni.gov/nic/NIC_home.html>.

[3] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008.
[4] Auto-Id Labs, <http://www.autoidlabs.org/>.
[5] The EPCglobal Architecture Framework, EPCglobal Final Version 1.3, Approved 19 March 2009, <www.epcglobalinc.org>.
[6] K. Sakamura, Challenges in the age of ubiquitous computing: a case study of T-engine – an open development platform for embedded systems, in: Proceedings of ICSE'06, Shanghai, China, May 2006.
[7] M. Presser, A. Gluhak, The Internet of Things: Connecting the Real World with the Digital World, EURESCOM mess@ge – The Magazine for Telecom Insiders, vol. 2, 2009, <http://www.eurescom.eu/message>.
[8] M. Botterman, for the European Commission Information Society and Media Directorate General, Networked Enterprise & RFID Unit – D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic, May 2009.
[9] B. Sterling, Shaping Things – Mediawork Pamphlets, The MIT Press, 2005.
[10] ITU Internet Reports, The Internet of Things, November 2005.
[11] A. Dunkels, J.P. Vasseur, IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #1, September 2008, <http://www.ipso-alliance.org>.
[12] J. Hui, D. Culler, S. Chakrabarti, 6LoWPAN: Incorporating IEEE 802.15.4 Into the IP Architecture – Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #3, January 2009, <http://www.ipso-alliance.org>.
[13] N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things, Scientific American 291 (4) (2004) 76–81.
[14] I. Toma, E. Simperl, Graham Hench, A joint roadmap for semantic technologies and the internet of things, in: Proceedings of the Third STI Roadmapping Workshop, Crete, Greece, June 2009.
[15] A. Katasonov, O. Kaykova, O. Khriyenko, S. Nikitin, V. Terziyan, Smart semantic middleware for the internet of things, in: Proceedings of the Fifth International Conference on Informatics in Control, Automation and Robotics, Funchal, Madeira, Portugal, May 2008.
[16] W. Wahlster, Web 3.0: Semantic Technologies for the Internet of Services and of Things, Lecture at the 2008 Dresden Future Forum, June 2008.
[17] I. Vázquez, Social Devices: Semantic Technology for the Internet of Things, Week@ESI, Zamudio, Spain, June 2009.
[18] D. Guinard, T. Vlad, Towards the web of things: web mashups for embedded devices, in: Proceedings of the International World Wide Web Conference 2009 (WWW 2009), Madrid, Spain, April 2009.
[19] L. Srivastava, Pervasive, ambient, ubiquitous: the magic of radio, in: European Commission Conference "From RFID to the Internet of Things", Bruxelles, Belgium, March 2006.
[20] K. Finkenzeller, RFID Handbook, Wiley, 2003.
[21] A. Jules, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications 24 (2) (2006) 381–394.
[22] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422.
[23] <http://ieee802.org/15>.
[24] G. Marrocco, C. Occhiuzzi, F. Amato, Sensor-oriented passive RFID, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[25] <http://seattle.intel-research.net/wisp/>.
[26] M. Buettner, B. Greenstein, A. Sample, J.R. Smith, D. Wetherall, Revisiting smart dust with RFID sensor networks, in: Proceedings of ACM HotNets 2008, Calgary, Canada, October 2008.
[27] S. De Deugd, R. Carroll, K. Kelly, B. Millett, J. Ricker, SODA: service oriented device architecture, IEEE Pervasive Computing 5 (3) (2006) 94–96.
[28] J. Pasley, How BPEL and SOA are changing web services development, IEEE Internet Computing 9 (3) (2005) 60–67.
[29] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza, V. Trifa, SOA-based integration of the internet of things in enterprise services, in: Proceedings of IEEE ICWS 2009, Los Angeles, Ca, USA, July 2009.
[30] C. Buckl, S. Sommer, A. Scholz, A. Knoll, A. Kemper, J. Heuer, A. Schmitt, Services to the field: an approach for resource constrained sensor/actor networks, in: Proceedings of WAINA'09, Bradford, United Kingdom, May 2009.
[31] OASIS, Web Services Business Process Execution Language Version 2.0, Working Draft, <http://docs.oasis-open.org/wsbpel/2.0/wsbpelspecificationdraft.pdf>.
[32] Hydra Middleware Project, FP6 European Project, <http://www.hydramiddleware.eu>.
[33] S. Duquennoy, G. Grimaud, J.-J. Vandewalle, The web of things: interconnecting devices with high usability and performance, in: Proceedings of ICESS '09, HangZhou, Zhejiang, China, May 2009.
[34] <http://www.fosstrak.org>.
[35] C. Floerkemeier, C. Roduner, M. Lampe, RFID application development with the Accada middleware platform, IEEE System Journal 1 (2) (2007) 82–94.
[36] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, G. Borriello, Building the internet of things using RFID: the RFID ecosystem experience, IEEE Internet Computing 13 (3) (2009) 48–55.
[37] <http://www.ist-e-sense.org>.
[38] <http://www.ist-ubisecsens.org>.
[39] R. Yuan, L. Shumin, Y. Baogang, Value Chain Oriented RFID System Framework and Enterprise Application, Science Press, Beijing, 2007.
[40] METRO Group Future Store Initiative, <http://www.futurestore.org/>.
[41] S. Karpischek, F. Michahelles, F. Resatsch, E. Fleisch, Mobile sales assistant – an NFC-based product information system for retailers, in: Proceedings of the First International Workshop on Near Field Communications 2009, Hagenberg, Austria, February 2009.
[42] G. Broll, E. Rukzio, M. Paolucci, M. Wagner, A. Schmidt, H. Hussmann, PERCI: pervasive service interaction with the internet of things, IEEE Internet Computing 13 (6) (2009) 74–81.
[43] A. Ilic, T. Staake, E. Fleisch, Using sensor information to reduce the carbon footprint of perishable goods, IEEE Pervasive Computing 8 (1) (2009) 22–29.
[44] A. Dada, F. Thiesse, Sensor applications in the supply chain: the example of quality-based issuing of perishables, in: Proceedings of Internet of Things 2008, Zurich, Switzerland, May 2008.
[45] D. Reilly, M. Welsman-Dinelle, C. Bate, K. Inkpen, Just point and click? Using handhelds to interact with paper maps, in: Proceedings of ACM MobileHCI'05, University of Salzburg, Austria, September 2005.
[46] R. Hardy, E. Rukzio, Touch & interact: touch-based interaction of mobile phones with displays, in: Proceedings of ACM MobileHCI '08, Amsterdam, The Netherlands, September 2008.
[47] A.M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De Vries, J. Krapelse, RFID Application in Healthcare – Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery, RAND Europe, February 2009.
[48] D. Niyato, E. Hossain, S. Camorlinga, Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization, IEEE Journal on Selected Areas in Communications 27 (4) (2009) 412–423.
[49] SENSEI FP7 Project, Scenario Portfolio, User and Context Requirements, Deliverable 1.1, <http://www.sensei-project.eu/>.
[50] C. Floerkemeier, R. Bhattacharyya, S. Sarma, Beyond RFID, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[51] J. Sung, T. Sanchez Lopez, D. Kim, The EPC sensor network for RFID and WSN integration infrastructure, in: Proceedings of IEEE PerComW'07, White Plains, NY, USA, March 2007.
[52] Commission of the European Communities, Early Challenges Regarding the "Internet of Things", 2008.
[53] N. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF RFC 4919, August 2007.
[54] M. Weiser, The computer for the 21st century, ACM Mobile Computing and Communications Review 3 (3) (1999) 3–11.
[55] <http://www.cen.eu>.
[56] A. Nilssen, Security and privacy standardization in internet of things, in: eMatch'09 – Future Internet Workshop, Oslo, Norway, September 2009.
[57] <http://www.iso.org>.
[58] <http://www.etsi.org>.
[59] Z. Shelby, ETSI M2M Standardization, March 16, 2009, <http://zachshelby.org>.
[60] Z. Shelby, News from the 75th IETF, August 3, 2009, <http://zachshelby.org>.
[61] G. Santucci, Internet of the future and internet of things: what is at stake and how are we getting prepared for them? in: eMatch'09 – Future Internet Workshop, Oslo, Norway, September 2009.
[62] Y.-W. Ma, C.-F. Lai, Y.-M. Huang, J.-L. Chen, Mobile RFID with IPv6 for phone services, in: Proceedings of IEEE ISCE 2009, Kyoto, Japan, May 2009.

[63] S.-D. Lee, M.-K. Shin, H.-J. Kim, EPC vs. IPv6 mapping mechanism, in: Proceedings of Ninth International Conference on Advanced Communication Technology, Phoenix Park, South Korea, February 2007.
[64] D.G. Yoo, D.H. Lee, C.H. Seo, S.G. Choi, RFID networking mechanism using address management agent, in: Proceedings of NCM 2008, Gyeongju, South Korea, September 2008.
[65] <http://ipv6.com/articles/applications/Using-RFID-and-IPv6.htm>.
[66] I.F. Akyildiz, J. Xie, S. Mohanty, A survey on mobility management in next generation All-IP based wireless systems, IEEE Wireless Communications Magazine 11 (4) (2004) 16–28.
[67] C. Perkins, IP Mobility Support for IPv4, IETF RFC 3344, August 2002.
[68] M. Mealling, Auto-ID Object Name Service (ONS) v1.0, Auto-ID Center Working Draft, August 2003.
[69] V. Krylov, A. Logvinov, D. Ponomarev, EPC Object Code Mapping Service Software Architecture: Web Approach, MERA Networks Publications, 2008.
[70] V. Cerf, Y. Dalal, C. Sunshine, Specification of Internet Transmission Control Program, IETF RFC 675, December 1974.
[71] T. V Lakshman, U. Madhow, The performance of TCP/IP for networks with high bandwidth-delay products and random loss, IEEE/ACM Transactions on Networking 5 (3) (1997) 336–350.
[72] I. Demirkol, F. Alagoz, H. Deliç, C. Ersoy, Wireless sensor networks for intrusion detection: packet traffic modeling, IEEE Communication Letters 10 (1) (2006) 22–24.
[73] D. Chen, P.K. Varshney, QoS support in wireless sensor networks: a survey, in: Proceedings of International Conference on Wireless Networks 2004, Las Vegas, NE, USA, June 2004.
[74] T. Van Landegem, H. Viswanathan, Anywhere, Anytime, Immersive Communications, Enriching Communications, vol. 2, No. 1, 2008, <http://www2.alcatel-lucent.com/enrich/en/previous-editions/>.
[75] <http://www.boycottbenetton.com/>.
[76] Benetton to tag 15 million items, RFID Journal (March) (2003), <http://www.rfidjournal.com/article/articleview/344/1/1/>.
[77] J. Bukley, From RFID to the internet of things: final report, in: European Commission Conference "From RFID to the Internet of Things", Brussels, Belgium, March 2006.
[78] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the Ninth ACM Conference on Computer and Communications Security, Washington, DC, USA, November 2002.
[79] R. Acharya, K. Asha, Data integrity and intrusion detection in wireless sensor networks, in: Proceedings of IEEE ICON 2008, New Delhi, India, December 2008.
[80] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, Guidelines for Securing Radio Frequency Identification (RFID) Systems, NIST Special Publication 800-98, April 2007.
[81] R. Kumar, E. Kohler, M. Srivastava, Harbor: software-based memory protection for sensor nodes, in: Proceedings of IPSN 2007, Cambridge, MA, USA, April 2007.
[82] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997.
[83] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, Strong authentication for RFID systems using AES algorithm, in: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, MA, USA, August 2004.
[84] B. Calmels, S. Canard, M. Girault, H. Sibert, Low-cost cryptography for privacy in RFID systems, in: Proceedings of IFIP CARIDS 2006, Terragona, Spain, April 2006.
[85] L. Cranor, et al., The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Group Note, November 2006.
[86] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Computer 36 (10) (2003) 103–105.
[87] J. Wickramasuriya, M. Datt, S. Mehrotra, N. Venkatasubramanian, Privacy protecting data collection in media spaces, in: Proceedings of ACM International Conference on Multimedia 2004, New York, NY, USA, October 2004.
[88] C.M. Medaglia, A. Serbanati, An overview of privacy and security issues in the internet of things, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[89] O. Savry, F. Vacherand, Security and privacy protection of contactless devices, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[90] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, J. Reverdy, RFID noisy reader: how to prevent from eavesdropping on the communication? in: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems 2007, Vienna, Austria, September 2007.
[91] G.V. Lioudakis, E.A. Koutsoloukas, N. Dellas, S. Kapellaki, G.N. Prezerakos, D.I. Kaklamani, I.S. Venieris, A proxy for privacy: the discreet box, in: EUROCON 2007, Warsaw, Poland, September 2007.
[92] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 2009.
[93] C. Thompson, 25 Ideas for 2010: Digital Forgetting, Wired UK, November 2009.
[94] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K.H. Kim, S. Shenker, I. Stoica, A data-oriented (and beyond) network architecture, in: Proceedings of ACM SIGCOMM'07, Kyoto, Japan, August 2007.
[95] T. O'Reilly, J. Pahlka, The 'Web Squared' Era, Forbes, September 2009.
[96] S. Tedjini, E. Perret, V. Deepu, M. Bernier, Chipless tags, the next RFID frontier, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.

**Luigi Atzori** is assistant professor at the University of Cagliari (Italy) since 2000. His main research topics of interest are in multimedia networking: error recovery and concealment, IP Telephony, video streaming, network QoS management. He has published more than 80 journal articles and refereed conference papers. He has been awarded a Fulbright Scholarship (11/2003–05/2004) to work on video at the University of Arizona. He is editor for the ACM/Springer Wireless Networks Journal and is involved in the organization of several International Conferences on Multimedia Networking.

**Antonio Iera** is a Full Professor of Telecommunications at the University "Mediterranea" of Reggio Calabria, Italy. He graduated in Computer Engineering at the University of Calabria in 1991; then he received a Master Diploma in Information Technology from CEFRIEL/Politecnico di Milano and a Ph.D. degree from the University of Calabria. From 1994 to 1995 he has been with Siemens AG in Munich, Germany to participate to the RACE II ATDMA (Advanced TDMA Mobile Access) project under a CEC Fellowship Contract. Since 1997 he has been with the University Mediterranea, Reggio Calabria, where he currently holds the positions of scientific coordinator of the local Research Units of the National Group of Telecommunications and Information Theory (GTTI) and of the National Inter-University Consortium for Telecommunications (CNIT), Director of the ARTS – Laboratory for Advanced Research into Telecommunication Systems, and Head of the Department DIMET. His research interests include: new generation mobile and wireless systems, broadband satellite systems, Internet of Things. Elevated to the IEEE Senior Member status in 2007.

**Giacomo Morabito** was born in Messina, Sicily (Italy) on March 16, 1972. He received the laurea degree in Electrical Engineering and the Ph.D. in Electrical, Computer and Telecommunications Engineering from the Istituto di Informatica e Telecomunicazioni, University of Catania, Catania (Italy), in 1996 and 2000, respectively. From November 1999 to April 2001, he was with the Broadband and Wireless Networking Laboratory of the Georgia Institute of Technology as a Research Engineer. Since April 2001 he is with the Dipartimento di Ingegneria Informatica e delleTelecomunicazioni of the University of Catania where he is currently Associate Professor. His research interests focus on analysis and solutions for wireless networks.

# Computer Networks

1. What is the term IoT means? Mention some of the application of IoT in modern life with Example.
   **Answer:**

   **IoT :** The internet of things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.

   **Some Applications in modern life:**
   - Transportation and logistics domain – Autonomous car
   - Healthcare domain – Remote Patient Condition Check
   - Smart environment (Home, Office, Plant) – Google Home
   - Personal and Social Domain – Smart Watch / Auto updating activities in social media
   - Enterprise – Environmental Monitoring
   - Utilities – Smart Meter By Electricity supply Company
   - Futuristic Application Domain: Enhanced Game Room.

2. Suppose your grandmother is a patient who lives alone and she doesn't know which medicine she needs to take at which time.For this particular scenario how could you use Iot to solve it? Which domain or application you should chose to solve this problem and Why?

   **Answer:**
   For this particular situation I use Healthcare domain of IoT.There will be a device which have four functionality like Tracking, identification and authentication ,data collection sensing which can assure to track the timing of taking medicine and collect the data and give a notification about to take the medicine at a particular .

3. What is IoT? Who introduced this term and when.

   Answer:

   IoT means Internet of Things the Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals

   The term internet of things was first coined by Kevin Ashton in 1999.

4. Say your kid who is under age is home alone and prohibited to drink cold water from the refrigerator. How can you remotely control this situation from your office using IoT technology and which domain you think will go with this situation?
   Answer:
   For this current situation we can use smart environment domain of IoT.
   There will be a system that has functionality of comfortable home and remotely control home appliances using that we can control our home appliances access.