Higher Nationals in Computing

Unit 43: Internet of Things

ASSIGNMENT 1

Learner's name: Ta Thai Bao
ID:GCS18186
Class:GCS0705A
Subject ID: 1690
Assessor name: VanHH

Assignment due: June 20, 2020 Assignment submitted: June 20,2020

ASSIGNMENT 1 FRONT SHEET

Qualification	**TEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 43: Internet of Things**		
Submission date	June 20, 2020	**Date Received 1st submission**	June 20, 2020
Re-submission Date		**Date Received 2nd submission**	
Student Name	Ta Thai Bao	**Student ID**	GCS18186
Class	GCS0705A	**Assessor name**	Ho Hai Van

Student declaration
I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature	

Grading grid

P1	P2	P3	P4	M1	M2	M3	M4	D1	D2

☼ Summative Feedback:		☼ Resubmission Feedback:
Grade:	Assessor Signature:	Date:
Internal Verifier's Comments:		
Signature & Date:		

ASSIGNMENT 1 BRIEF

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number	Unit 43: Internet of Things		
Assignment title			
Academic Year	2020		
Unit Tutor	Ho Hai Van		
Issue date		**Submission date**	June 20, 2020
IV name and date	Ta Thai Bao		

Submission Format:
Format: This assignment is an Individual assignment and specifically including 1 document: You must use font *Calibri size 12, set number of the pages and use multiple line spacing at 1.3. Margins must be: left: 1.25 cm; right: 1 cm; top: 1 cm and bottom: 1 cm.* The reference follows Harvard referencing system. The recommended word limit is *2.000-2.500 words*. You will not be penalized for exceeding the total word limit. The cover page of the report has to be the Assignment front sheet 1.   *Submission* Students are compulsory to submit the assignment in due date and in a way requested by the Tutors. The form of submission will be a soft copy posted on http://cms.greenwich.edu.vn/   *Note:* The Assignment *must* be your own work, and not copied by or from another student or from books etc. If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style. Make sure that you know how to reference properly, and that understand the guidelines on plagiarism. *If you do not, you definitely get fail*
Unit Learning Outcomes:
LO1 Analyse what aspects of IOT are necessary and appropriate when designing software applications   **LO2** Outline a plan for an appropriate IOT application using common architecture, frameworks, tools, hardware and APIs   **LO3** Develop an IOT application using any combination of hardware, software, data, platforms and services.   **LO4** Evaluate your IOT application and detail the problem your IOT application solves, the potential impact on people, business, society and the end user and the problems it might encounter when integrating into the wider IOT ecosystem

Assignment Brief and Guidance:
You currently work as a product developer for a new startup where you design IOT products for the consumer, corporate, government and defence clients. As part of your role your manager has tasked you to plan and develop a new IOT product, service or application for a potential client. You are required to identify a target user and conduct tests with this user and include this feedback into multiple iterative versions of your product. **Part 1 (Assignment 1)**:: For the first part, you must: • Plan an IOT application for a specific target end user and the tests you intend to conduct with this user. This plan will be in the form of a document and will include supporting evidence and material, such as user personas and customer journey maps. • Create multiple iterations of your application and modify each iteration with enhancements gathered from user feedback and experimentation. This will follow the pathway outlined in your plan.(log book,) **Part 2 (Assignment 2)**: For the first part, you must: • Show evidence about Developed IOT application using any combination of hardware, software, data, platforms and services (video or images of your IOT system with code snippet) • Evaluate your IOT application and detail the problem your IOT application solves, the potential impact on people, business, society and the end user and the problems it might encounter when integrating into the wider IOT ecosystem

Learning Outcomes and Assessment Criteria		
Pass	**Merit**	**Distinction**
LO1 Analyse what aspects of IOT are necessary and appropriate when designing software applications		
P1 Explore various forms of IOT functionality. **P2** Review standard architecture, frameworks, tools, hardware and APIs available for use in IOT development.	**M1** Evaluate the impact of common IOT architecture, frameworks, tools, hardware and APIs in the software development lifecycle. **M2** Review specific forms of IOT architecture, frameworks, tools, hardware and APIs for different problem-solving requirements.	**D1** Evaluate specific forms of IOT architecture and justify their use when designing software applications.
LO2 Outline a plan for an appropriate IOT application using common architecture, frameworks, tools, hardware and APIs		
P3 Investigate architecture, frameworks, tools, hardware and API techniques available to develop IOT applications. **P4** Determine a specific problem to solve using IOT.	**M3** Select the most appropriate IOT architecture, frameworks, tools, hardware and API techniques to include in an application to solve this problem. **M4** Apply your selected techniques to create an IOT application development plan.	**D2** Make multiple iterations of your IOT application and modify each iteration with enhancements gathered from user feedback and experimentation.

Table of Contents

Table of images:

LO1 Analyse what aspects of IOT are necessary and appropriate when designing software applications
P1 Explore various forms of IOT functionality.

1.1 Internet of underwater things

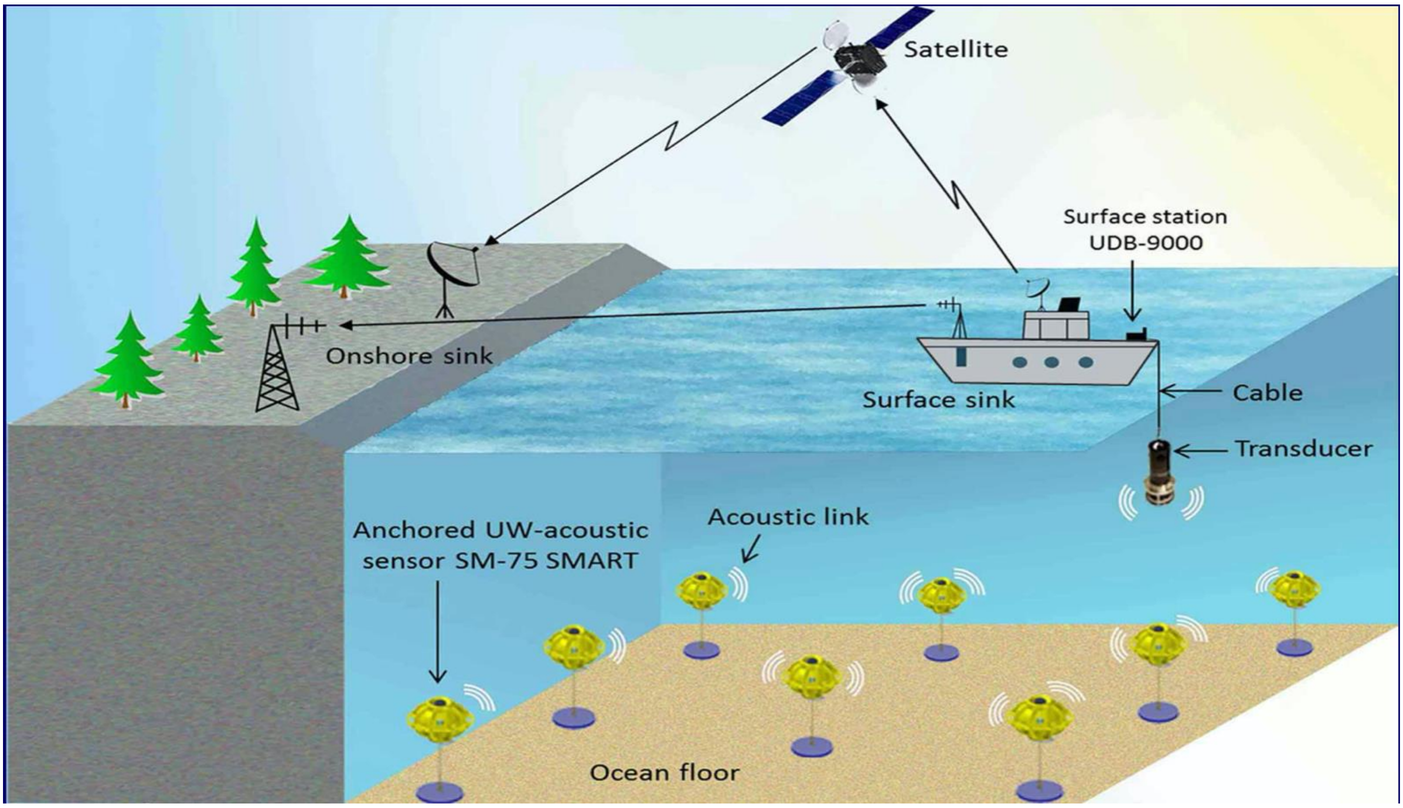

Figure 1: Internet of underwater things (Session 1- Introduction to IOT)

Internet of Things Underwater (IOT Underwater) is a system made of unmanned vehicles that scour the sea while communicating with underwater sensors and sending the information to networks atop the surface. This will be done at a regular internet speed. This information can be used to effectively manage the planet's resources. Also, it can be used for a large number of varying tasks that include:

- Detecting early signs of tsunamis.
- Monitoring the health of animals.
- Surveying shipwrecks and crashes.
- Establishing interactive real-time aquatic education, ecological monitoring applications, and archaeological expeditions.
- This kind of IOT that senses and transmits data through water would be important in the protection or oceans and lakes. These oceans and lakes cover almost three-quarters of the planet's surface and act as a support to the life of almost half of its species. With the help of an underwater IOT, these

vital marine environments can be managed by monitoring offshore oil and gas pipelines – while also scouring the seabed for pollutants.

1.2 Internet of underground thing.

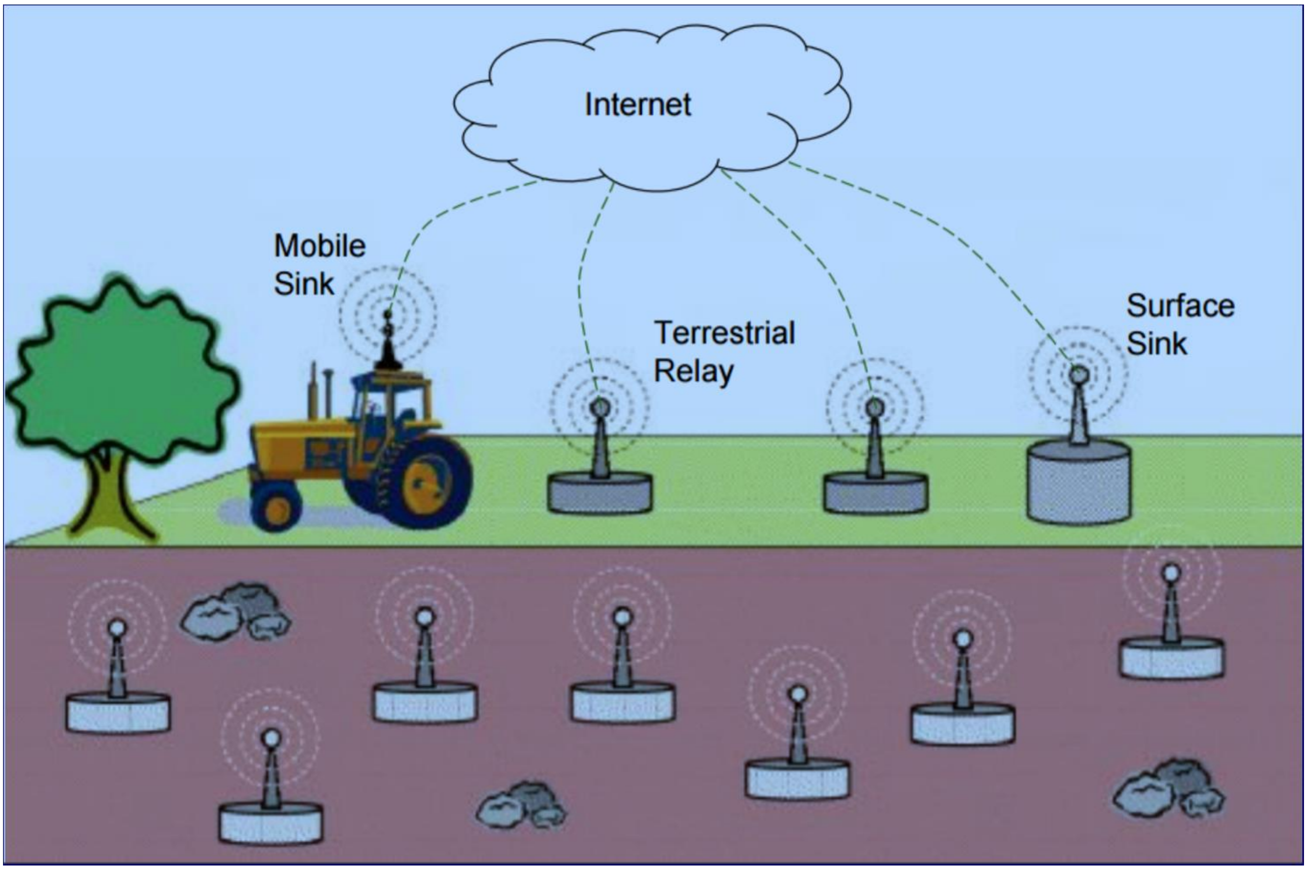

Figure 2: Internet of underground things (Session 1- Introduction to IOT)

The ever-increasing demand for the natural resources needs novel technologies to improve the underground exploration and to produce more crops. The subsurface environment and agricultural lands provide various natural resources such as earth minerals, fossil fuels, metal ores, groundwater, and food. To monitor and improve the production of all of these resources, Internet of Underground Things (IoUGT) is an enabling technology which can provide smart oil and gas fields, smart agriculture fields, and smart seismic quality control . However, implementation of IoUGT is a challenging task due to the harsh underground propagation environment which requires low power and small size underground sensors, long-range communication technology, efficient networking solutions, and accurate localization techniques.

1.3 Internet of battlefield thing

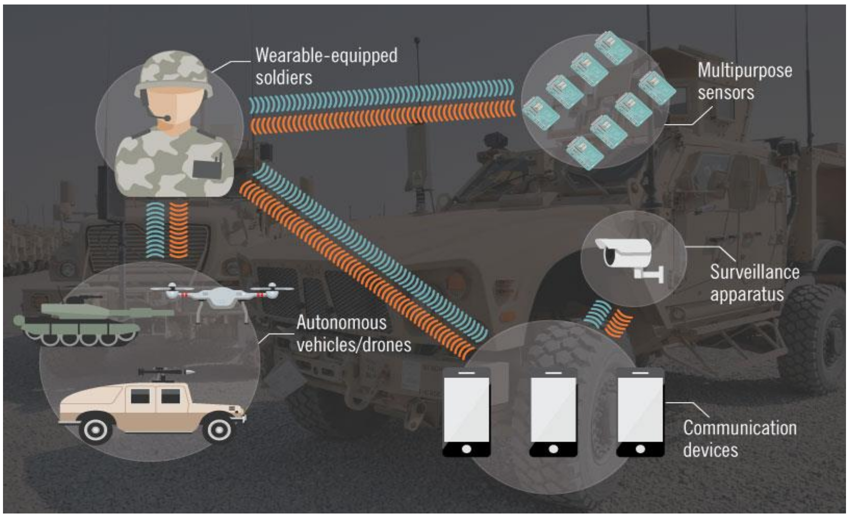

Figure 3: Internet of battlefield things (Session 1- Introduction to IOT)

In the future, military operations will rely less on human soldiers and more on interconnected technology, leveraging advancements in embedded systems and machine intelligence in order to achieve superior defense capabilities. The Internet of Battlefield Things will connect soldiers with smart technology in armor, radios, weapons, and other objects, to give troops "extra sensory" perception, offer situational understanding, endow fighters with prediction powers, provide better risk assessment, and develop shared intuitions.

1.4 Internet of space things

Figure 4: Internet of battlefield things (Session 1- Introduction to IOT)

Today, approximately 60% (4.5B) of the world's population cannot access the internet. Consequently, there has been a renaissance in interest and investment in space- and suborbital-based high-data-rate communications networks.

These networks will have global impact on humanity by affordably delivering high bandwidth information to every part of the world. This area cuts across multiple hardware-oriented fields of interest including: aerospace systems; antennas; autonomous systems; communications; electronics; microwave/mm-wave technology; photonics; position, navigation and timing; power electronics, etc.

1.5 Internet of nano-things.

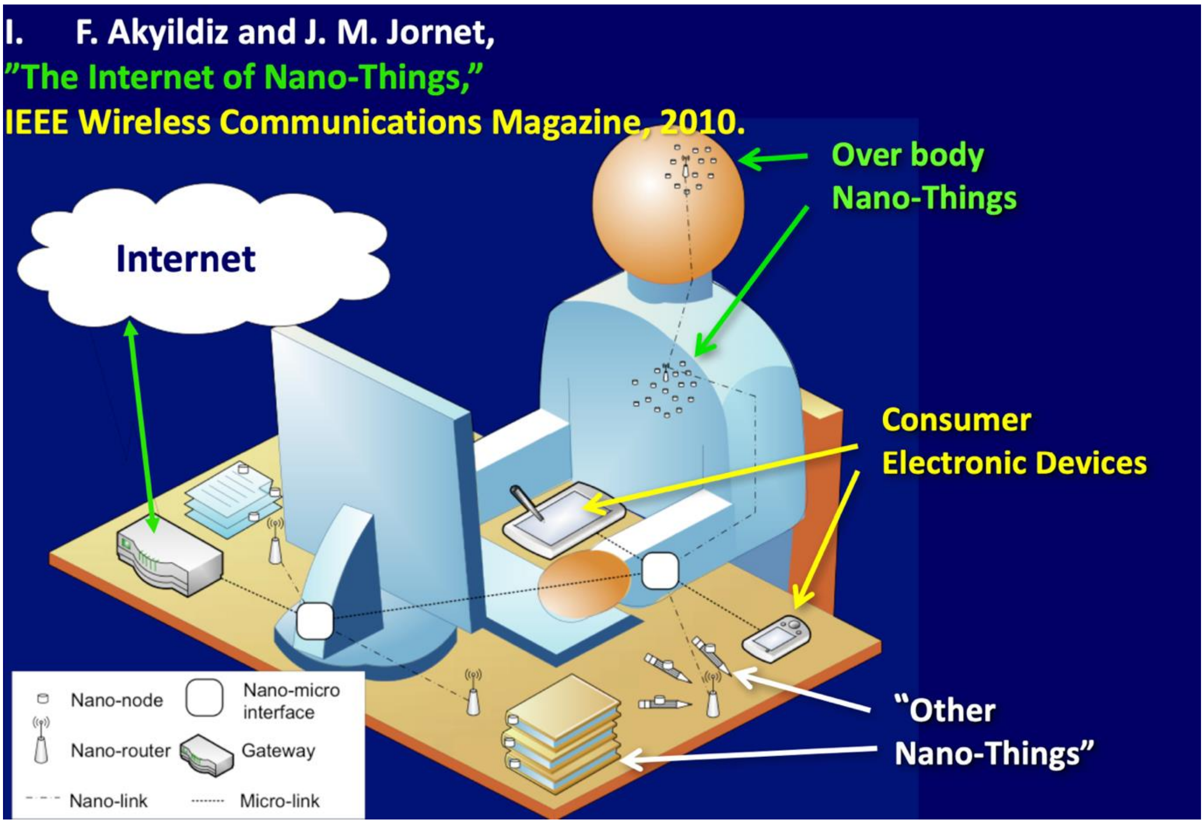

Figure 5: Internet of nano-things (Session 1- Introduction to IOT)

The internet of nano-things isn't very different from IoT, except in the sense that devices interconnected within IoNT are miniaturized and small enough to be termed nanoscale, which is around .1 to 100 nanometers -- with a nanometer measuring at one-billionth of a meter.

Most technologies currently in use -- such as sensors in cars and homes that report environmental conditions, or accelerometers and gyroscopes in smartphones that help people use navigation or location services -- are all examples of very small devices that can be miniaturized to fit within very small volumes. Almost all modern automation depends on nanoscale devices that can communicate with each other in order to provide smarter technical options. These technical integrations will drive innovation in all spaces imaginable, from the automotive industry to the healthcare industry, as well as for regular home goods for daily use.

The types of nano-technologies being integrated into an IoT system are highly specific to the application. For instance, a smart factory will employ IoNT devices to monitor temperature, humidity, gaseous fumes, water quality and perhaps carbon emissions from systems' exhaust. In another example, connected vehicles with similar miniaturized sensors could predict proximity, environmental conditions and location information to help ensure the safety and accuracy of vehicle-assistance systems.

1.6 Internet of bio-nanothings

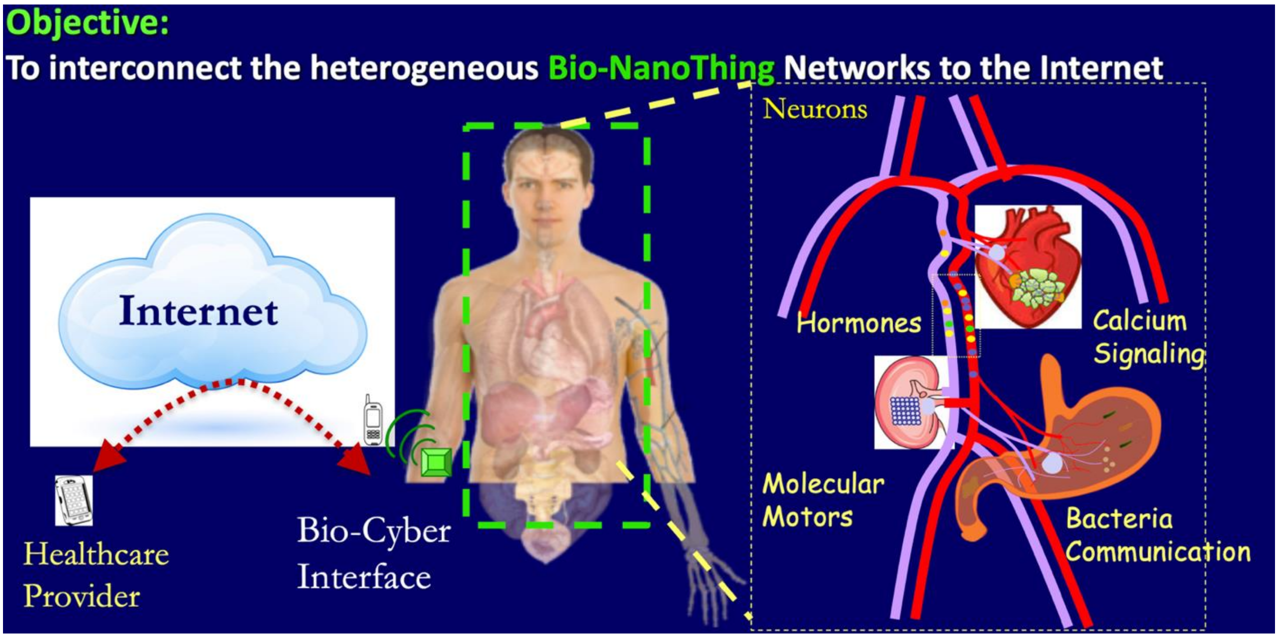

Figure 6: Internet of bio-nanothings (Session 1- Introduction to IOT)

The internet of nano-things isn't very different from IOT, except in the sense that devices interconnected within IoNT are miniaturized and small enough to be termed nanoscale, which is around .1 to 100 nanometers -- with a nanometer measuring at one-billionth of a meter.

Most technologies currently in use -- such as sensors in cars and homes that report environmental conditions, or accelerometers and gyroscopes in smartphones that help people use navigation or location services -- are all examples of very small devices that can be miniaturized to fit within very small volumes. Almost all modern automation depends on nanoscale devices that can communicate with each other in order to provide smarter technical options. These technical integrations will drive innovation in all spaces imaginable, from the automotive industry to the healthcare industry, as well as for regular home goods for daily use.

The types of nano-technologies being integrated into an IOT system are highly specific to the application. For instance, a smart factory will employ IoNT devices to monitor temperature, humidity, gaseous fumes, water quality and perhaps carbon emissions from systems' exhaust. In another example, connected vehicles with similar miniaturized sensors could predict proximity, environmental conditions and location information to help ensure the safety and accuracy of vehicle-assistance systems.

P2 Review standard architecture, frameworks, tools, hardware and APIs available for use in IOT development.

1. **IOT architecture.**

1.1 Three-layer architecture

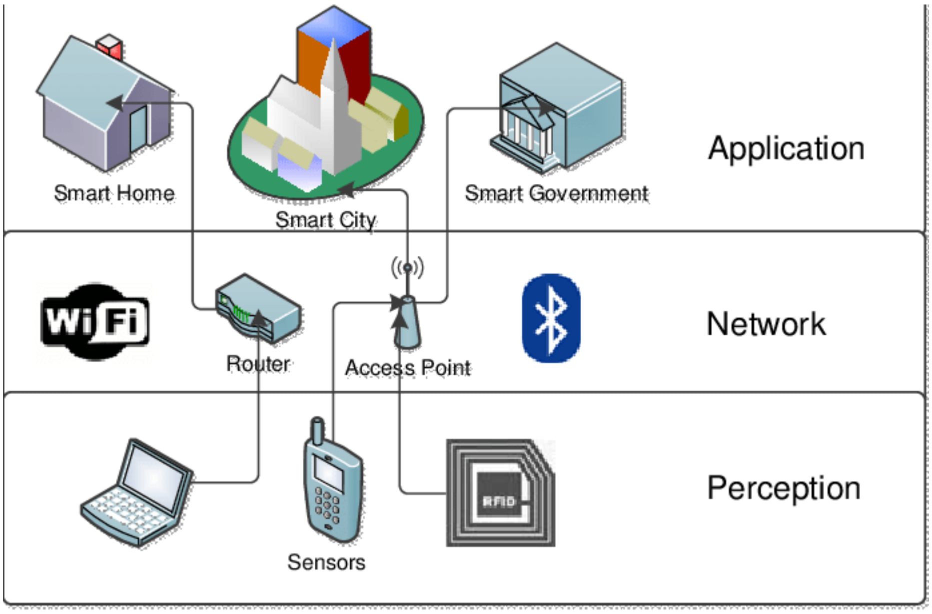

Figure 7: Three-layer architecture

It is a very basic architecture and fulfills the basic idea of IoT. It was proposed in the early stages of development of IoT. It has three layers. The names of these three layers are perception, network and application layer as shown in figure 7.

1.2 Four-layer architecture

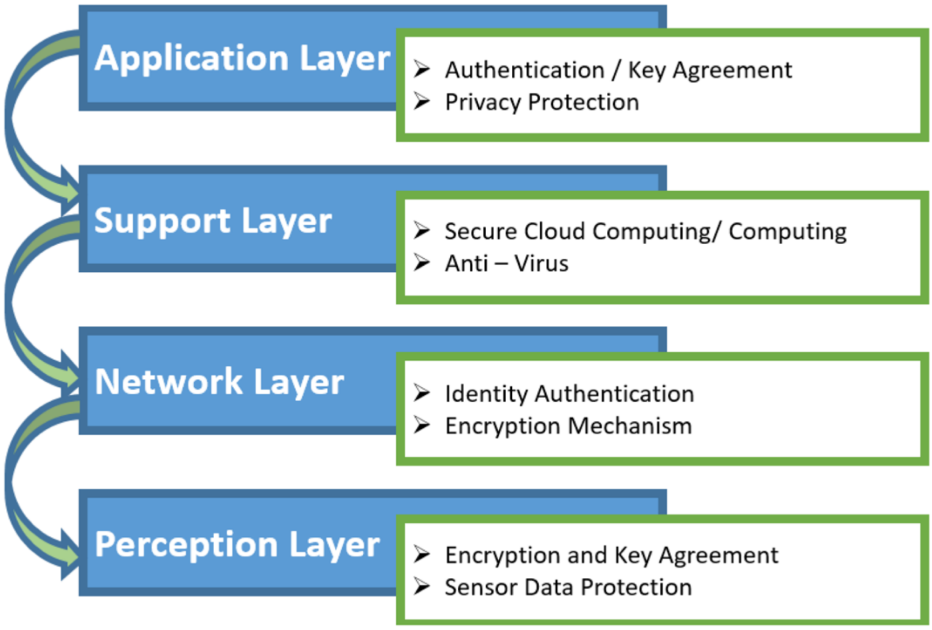

Figure 8: Four-layer architecture

The three-layer architecture was most basic architecture. Due to continuous development in IOT, it could not fulfill all the requirements of IOT. Therefore, researchers proposed an architecture with four layers. It has three layers like the previous architecture, but it also has one more layer called a support layer. Figure 5 presents the layered architecture of it along recommended security mechanisms used to make it secure from intruders. The three layers have the same functionality as the three-layer architecture that we have already discussed such as the three-layer so the functionality of the support layer along security attacks is as follows:

1.3 Five-layer architecture

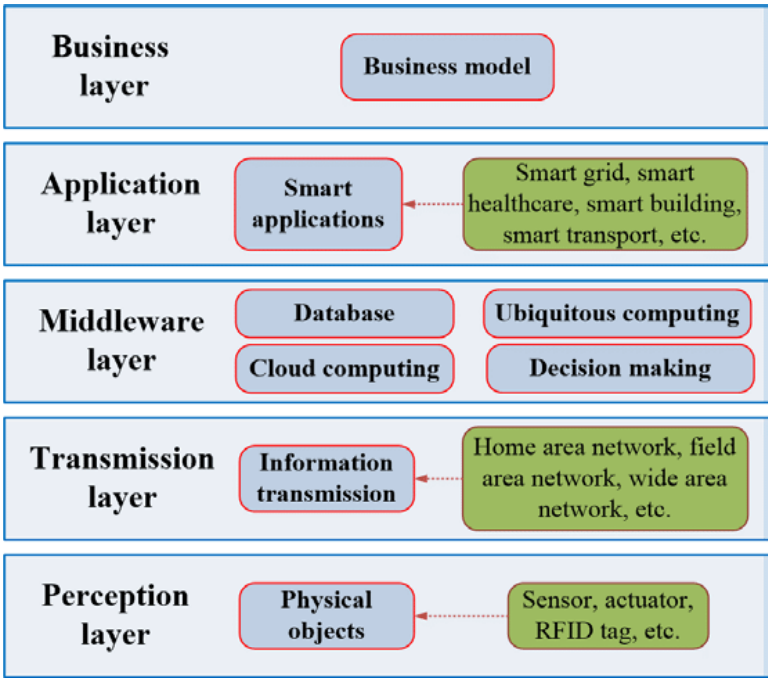

Figure 9: Five-layer architecture

The four-layer architecture played an important role in the development of IoT. There were also some issues regarding security and storage in four-layer architecture. Researchers proposed five-layer architecture to make the IoT secure. It has three layers like previous architectures whose names are perception layer, transport layer and application layer. It also has two more layers. The names of these newly proposed layers are processing layer and business layer. It is considered that the newly proposed architecture has the ability to fulfill requirements of IoT. It also has the ability to make the applications of IoT secure.

2. Framework.

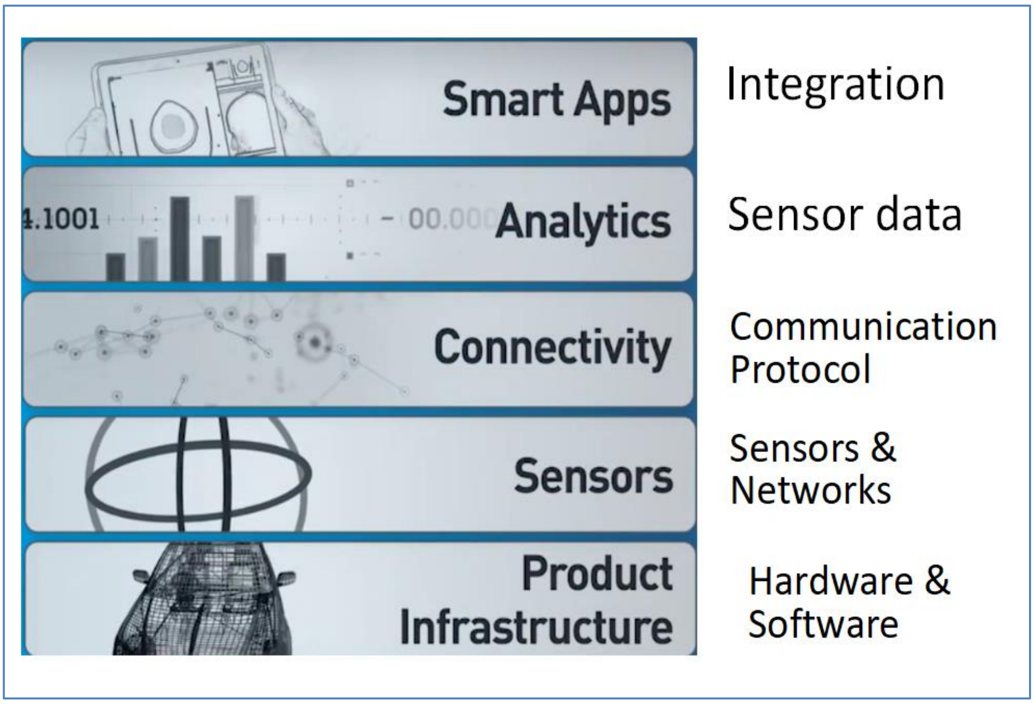

Figure 10: Framework

For an IOT framework to be reliable and dependable, some minimal set of measures should be satisfied to achieve integration and interoperability in IOT. These frameworks span across the IOT research communities ranging from academic research to organisational research which focus on integrating things in IOT.

3. Tools.

3.1 Tinkercad

Figure 11: Tinkercad

Tinkercad is a great tool to start 3d modelling. Even though you are an advanced 3d designer, you might be found yourself using it. It simplifies the process of 3d design. Tinkercad mainly solves primitive design needs. It is not a full design suite. But it contains a lot of feature for a maker or a STEM teacher. Tinkercad consists of multiple modules such as electronics(Arduino), coding, classroom, Minecraft, Lego bricks etc.

If I needed a simple 3d object to print out from my 3d printer, I definitely first tried designing it on Tinkercad. It is easy to use and compatible with 3d printers. In many cases, I use it for my 3d file repair tool. Just upload the file to Tinkercad, and then download it repaired.

3.2 Arduino

Figure 12: Arduino

Arduino IDE is a lightweight, cross-platform application that introduces programming to novices. It has both an online editor and an on-premise application, for users to have the option whether they want to save their sketches on the cloud or locally on their own computers.

While Arduino IDE is highly-rated by users according to ease of use, it is also capable of performing complex processes without taxing computing resources.

With Arduino IDE, users can easily access contributed libraries and receive up-to-date support for the latest Arduino boards, so they can create sketches that are backed by the newest version of the IDE.

3.3 Packet tracer

Figure 13: Packet tracer

Cisco Packet Tracer is the simulation software for CCNA and CCNP, but it could be handy for anyone who is interested in Computer Networking and wants to learn it thoroughly. If you want to learn something very good then you need great practice.

Cisco Packet Tracer provides simulation so a computer networking student could actually create a medium size wide network or LAN and visualize the whole network in front of his / her eyes and could test whether the end user machines are actually communicating with each other or not.

4. **Hardware.**

4.1 Microcontroller(Ardiuno Uno)

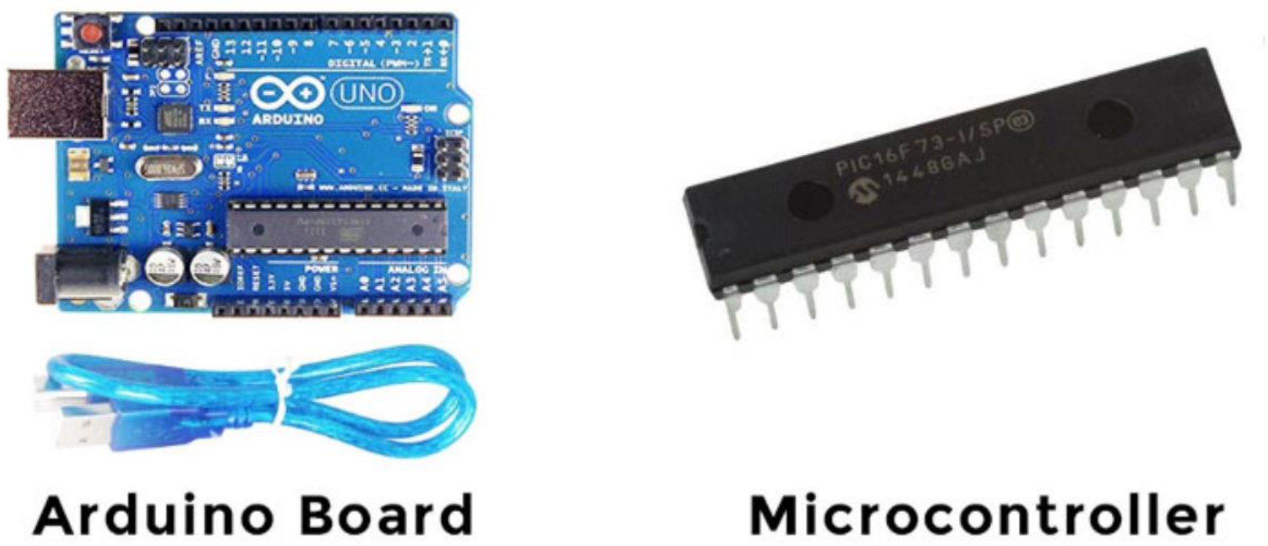

Figure 14: Microcontroller(Ardiuno Uno)

The UNO board is a type of a microcontroller board which is based on the ATmega328. It allows more memory and higher transfer rates. The board has 14 digital i/o pins from which 6 pins can be used as PWM outputs, a USB connection, 6 analog inputs, a 16MHz quartz crystal, an ICSP header, a power jack, and a reset button. Just connect the board with a computer using a USB cable (you can also use an AC-to-DC adapter or battery to give power to the board) and you are good to go. The Arduino UNO R3 board has everything that needs to support a microcontroller.

4.2 Microprocessor(ARM processor)

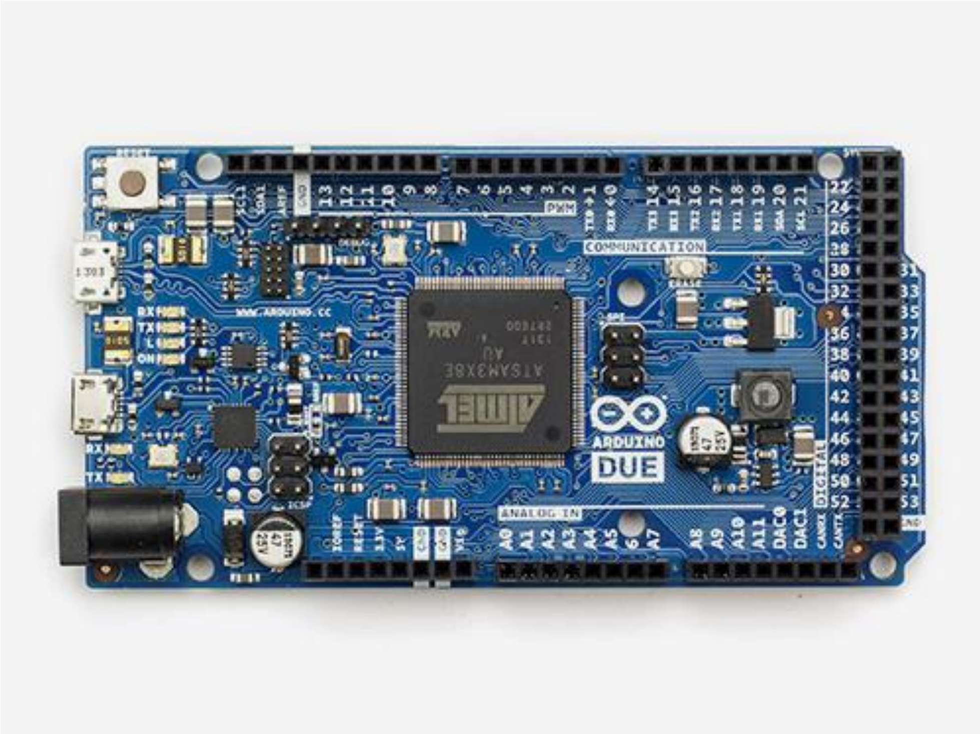

Figure 15: Microprocessor(ARM processor)

A microprocessor is a single chip integrating all the functions of a central processing unit (CPU) of a computer. It includes all the logical functions, data storage, timing functions and interaction with other peripheral devices. In some cases, the terms 'CPU' and 'microprocessor' are used interchangeably to denote the same device. Like every genuine engineering marvel, the microprocessor too has evolved through a series of improvements throughout the 20th century. With the development of microprocessor the number of transistor, clock rate width of bus, Addressable memory increases.

5. **APIs.**

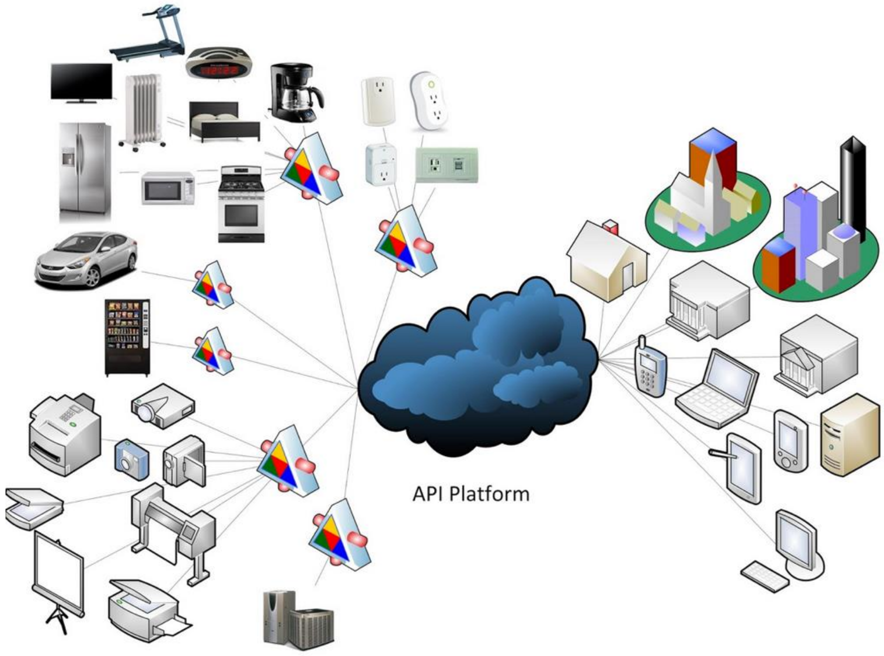

Figure 16: API

The application program (or programming) interface, or API, is arguably what really ties together the connected “things” of the “internet of things.” IoT APIs are the points of interaction between an IoT device and the internet and/or other elements within the network.

As API management company Axway puts it, “APIs are tightly linked with IoT because they allow you to securely expose connected devices to customers, go-to-market channels and other applications in your IT infrastructure.”

Why are IoT APIs important?

IBM called IoT APIs one of its top IoT trends for this year.

“APIs are the market enabler, and ‘internet of things’ devices would be useless without them. By exposing data that enables multiple devices to be connected, APIs provide an interface between the internet and the things to reveal previously unseen possibilities,” said Chris O’Connor, IBM’s GM for IoT, in a blog entry. “In the year to come, the power and importance of APIs will be at the forefront of the conversation around enabling—and more important—monetizing the ‘internet of things.'”

LO2 Outline a plan for an appropriate IOT application using common architecture, frameworks, tools, hardware and APIs

P3 Investigate architecture, frameworks, tools, hardware and API techniques available to develop IOT applications.

3.1 IOT architecture

3.1.1 Three-layer architecture

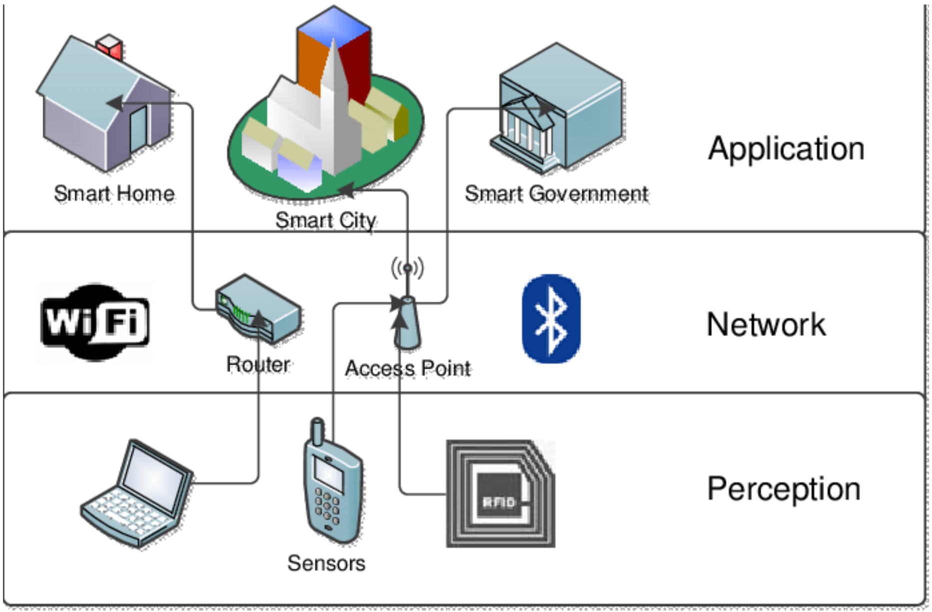

Figure 17: Three-layer architecture

Based on the image above, we see that there are 3 layers with the most copies:

Application layer - defines all applications that use the IOT technology or in which IOT has deployed. The applications of IOT can be smart homes, smart cities, smart health, animal tracking, etc. It has the responsibility to provide the services to the applications. The services may be varying for each application because services depend on the information that is collected by sensors. There are many issues in the application layer in which security is the key issue. In particular, when IOT is used in order to make a smart home, it introduces many threats and vulnerabilities from the inside and outside. To implement strong security in an IOT based smart home, one of the main issues is that the devices used in smart homes have weak computational power and a low amount of storage such as ZigBee.

Network layer is also known as transmission layer. It acts like a bridge between perception layer and application layer. It carries and transmits the information collected from the physical objects through sensors. The medium for the transmission can be wireless or wire based. It also takes the responsibility for connecting the smart things, network devices and networks to each other. Therefore, it is highly sensitive to attacks from the side of attackers. It has prominent security issues regarding integrity and authentication of information that is being transported in the network.

Perception layer is also known as a sensor layer. It works like people's eyes, ears and nose. It has the responsibility to identify things and collect the information from them. There are many types of sensors attached to objects to collect information such as RFID, 2-D barcode and sensors. The sensors are chosen according to the requirement of applications. The information that is collected by these sensors can be about location, changes in the air, environment, motion, vibration, etc. However, they are the main target of attackers who wish to utilize them to replace the sensor with their own.

3.1.2 Four-layer architecture

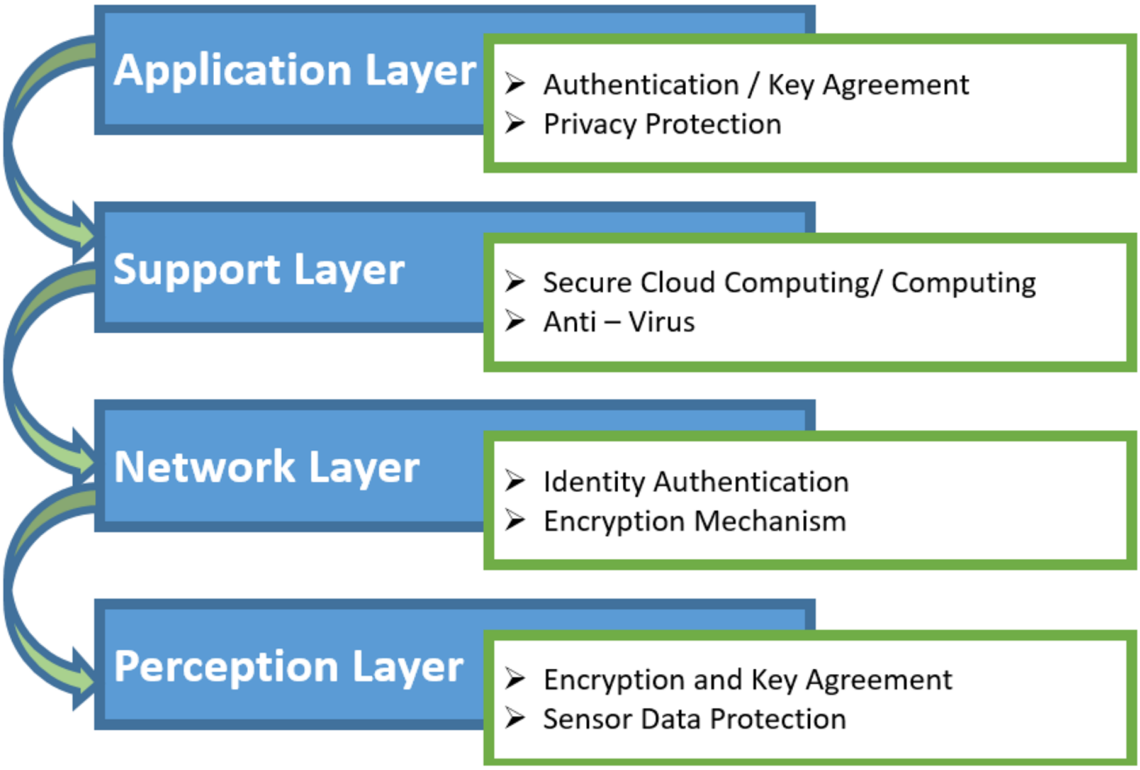

Figure 18: Four-layer architecture

Based on the image above, we see the architecture of IoT has appeared another layer:

Support Layer - The reason to make a fourth layer is the security in architecture of IOT. Information is sent directly to the network layer in three-layer architecture. Due to sending information directly to the network layer, the chances of getting threats increase. Due to flaws that were available in three-layer architecture, a new layer is proposed. In four-layer architecture, information is sent to a support layer that is obtained from a perception layer. The support layer has two responsibilities. It confirms that information is sent by the authentic users and protected from threats. There are many ways to verify the users and the information. The most commonly used method is the authentication. It is implemented by using pre-shared secrets, keys and passwords. The second responsibility of the support layer is sending information to the network layer. The medium to transmit information from the support layer to network layer can be wireless and wire based. There are various attacks that can affect this layer such as DoS attack, malicious insider, unauthorized access, etc.

3.1.3 Five-layer architecture

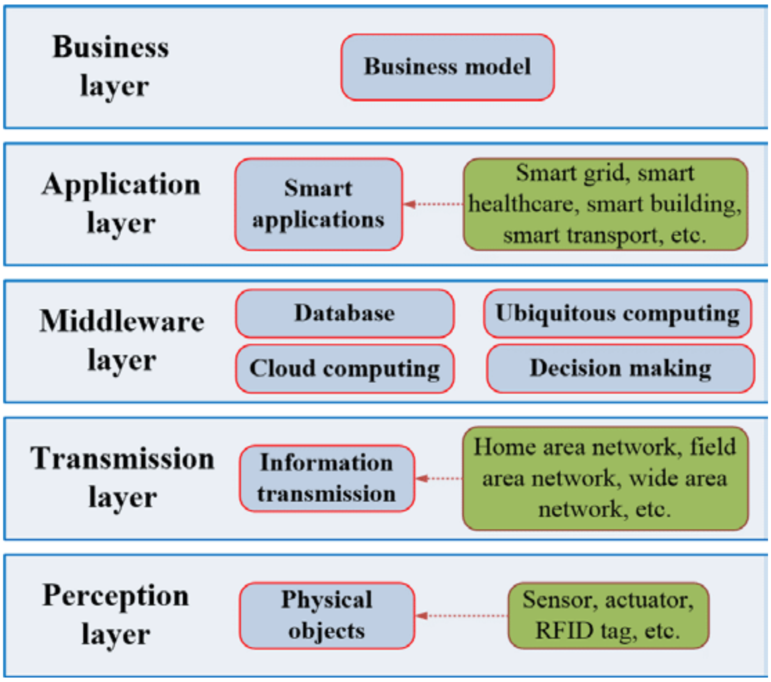

Figure 19: Five-layer architecture

Based on the image above, we see the architecture of IoT appear another layer:

Processing Layer

The processing layer is also known as a middleware layer. It collects the information that is sent from a transport layer. It performs processing onto the collected information. It has the responsibility to eliminate extra information that has no meaning and extracts the useful information. However, it also removes the problem of big data in IoT. In big data, a large amount of information is received which can affect performance of IoT. There are numerous attacks that can affect the processing layer and disturb the performance of IoT. Common attacks are:

- Exhaustion: An attacker uses exhaustion to disturb the processing of IoT structure. It occurs as an after-effect of attacks, such as DoS attack in which an attacker sends the victim many requests to make the network unavailable for users. It could be a result of other attacks that aim to exhaust the system resources, such as battery and memory resources. IoT has a distributed nature; therefore, it does not have a high amount of hazards. It is much easier to implement protecting procedures against it.
- Malwares: It is an attack on the confidentiality of the information of users. It refers to the application of viruses, spyware, adware, Trojans horses and worms to interact with the system. It takes the form of executable codes, scripts and contents. It acts against the requirements of system to steal the confidentially of information.

Business Layer

The business layer refers to an intended behavior of an application and acts like a manager of a whole system. It has responsibilities to manage and control applications, business and profits models of IoT. The user’s privacy is also managed by this layer. It also has the ability to determine how information can be created, stored and changed. Vulnerability in this layer permits the attackers to misuse an application by avoiding the business logic. Most problems regarding security are weaknesses in an application that result from a broken or missing security control. Common problems regarding security of business layer are:

- Business Logic Attack: It takes advantage of a flaw in a programming. It controls and manages the exchange of information between a user and a supporting database of an application. There are several common flaws in the business layer, such as improper coding by a programmer, password recovery validation, input validation, and encryption techniques.
- Zero-Day Attack: It refers to a security hole or a problem in an application that is unfamiliar to a vendor. This security hole is exploited by the attacker to take control without user’s consent and without their knowledge.

3.2 Framework.

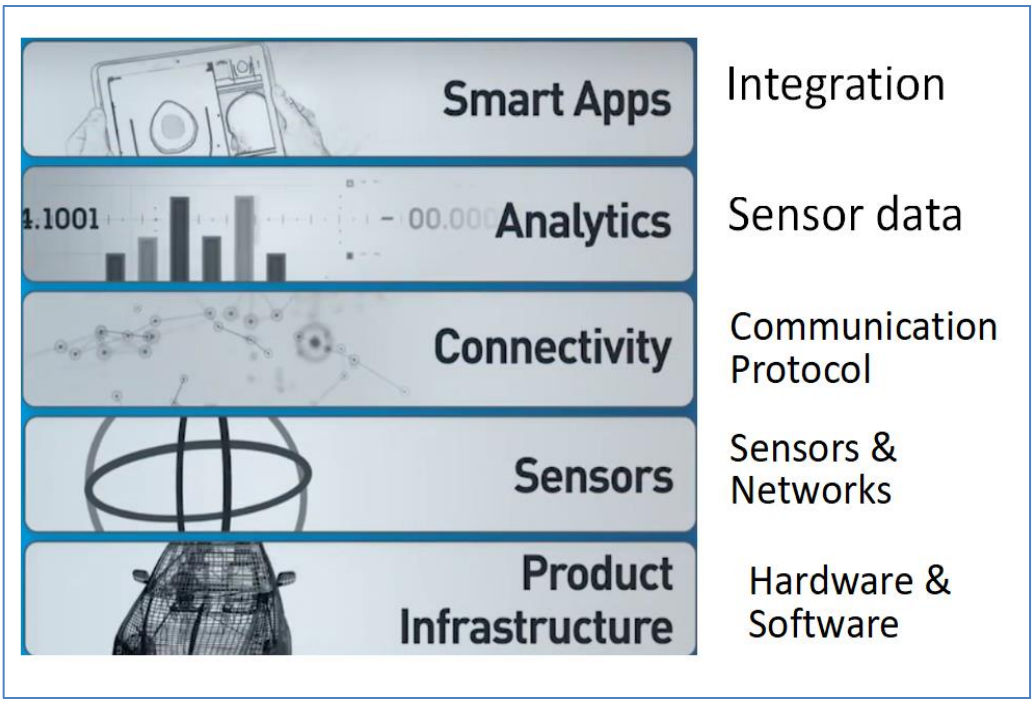

Figure 20: Framework

Smart Apps layer: integrates all of other layers together and support different business decisions.

Analytics layer: translating the sensor data into the meaningful information

Connectivity Layer: Communication protocol necessary to send information from the product to the cloud.

Sensors layer: sensors & the networks that support them

Product Infrastructure layer: Hardware & Software of the product

Design Framework example :

Product: Quad-copter

Including the main equipment:

- 4 Motors

- Circuit board that forms the structure
- Video camera
- Antenna for transmitting sensor data

Figure 21: Flycam

Framework	Value	Description
Smart app	Remote control Video + Sensor information display	I control the flycam with a remote control, camera control and image display.
Analytics	Convert data from gyroscope into optimal motor speeds	The program will calculate the tilt angle and height to balance for the flycam
Connectivity	Radio communication components to stream sensor data	Flycam and remote control device are connected by wireless transmission line
Sensors	Gyroscope for orientation Camera for visual data	The camera device captures the image and sends it to the control unit

Product infrastructure	Hardware [Propellers + Frame], Software [Control Algorithms]	The drone will use the Arduino hardware as well as the part programming for the remote control

3.3 Tools.

3.3.1 Tinkercad

Figure 22: Tinkercad

As we know, Tinkercard is a great tool for creating 3d models and designing adruino models. The tool supports users to create virtual models and test them before they execute on real devices. It helps users to learn more and interact with virtual devices.

Example of Tinkercad:

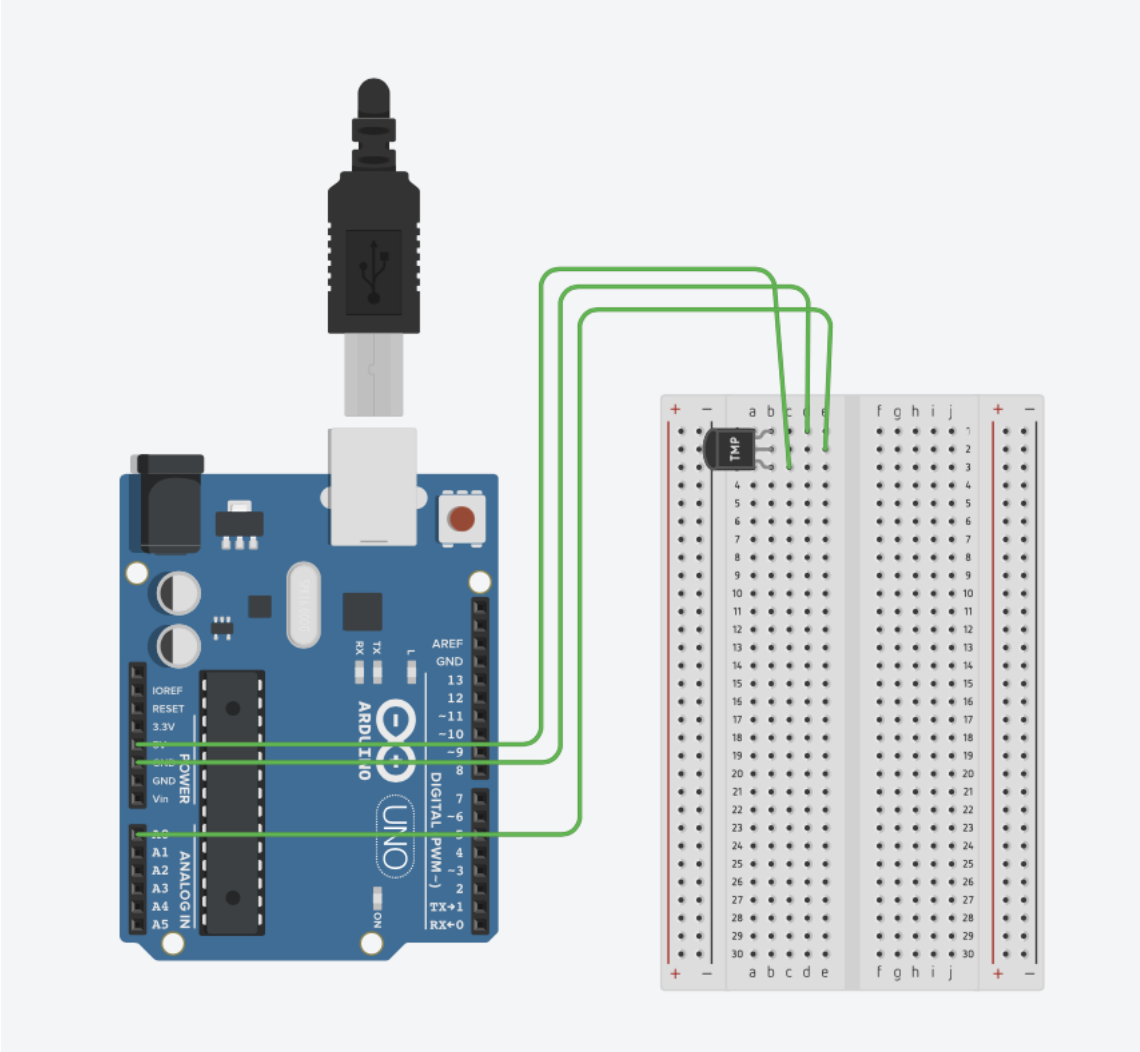

Figure 23: Example design of Tinkercad

As shown above, I used Tinkercad to create a small model of temperature measurement using the Arduino Uno circuit and the Temperature Sensor (TMP 36). Models that help measure the surrounding ambient tissue temperature include (C, F). From there we can rely on the above model to develop systems such as fire alarms, watering plants, ...

Text | 1 (Arduino Uno R3)

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


const int temperaturePin = 0;
float voltage, degreesC, degreesF;

void loop()
{
 voltage = analogRead(A0) * 0.004882814 ;

  degreesC = (voltage - 0.5) * 100.0;

  degreesF = degreesC * (9.0/5.0) + 32.0;

  Serial.print("voltage: ");
  Serial.print(voltage);
  Serial.print("  deg C: ");
  Serial.print(degreesC);
  Serial.print("  deg F: ");
  Serial.println(degreesF);
}
```

Serial Monitor

```
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltage: 0.75  deg C: 24.71  deg F: 76.47
voltag
```

Send | Clear

Figure 24: Example code of Tinkercad

This is the result after the program has been executed and I have measured the temperature around the virtual environment. As we can see, the program measures the temperature (C, F) and displays it on the screen below.

3.3.2 Arduino

Figure 25: Arduino

The Arduino tool is used exclusively for arduino circuits. The main function is to load the code into arduino circuit. The tool has a C programming language support to help customize the programs for Aruino circuits.

Example of Arduino tool:

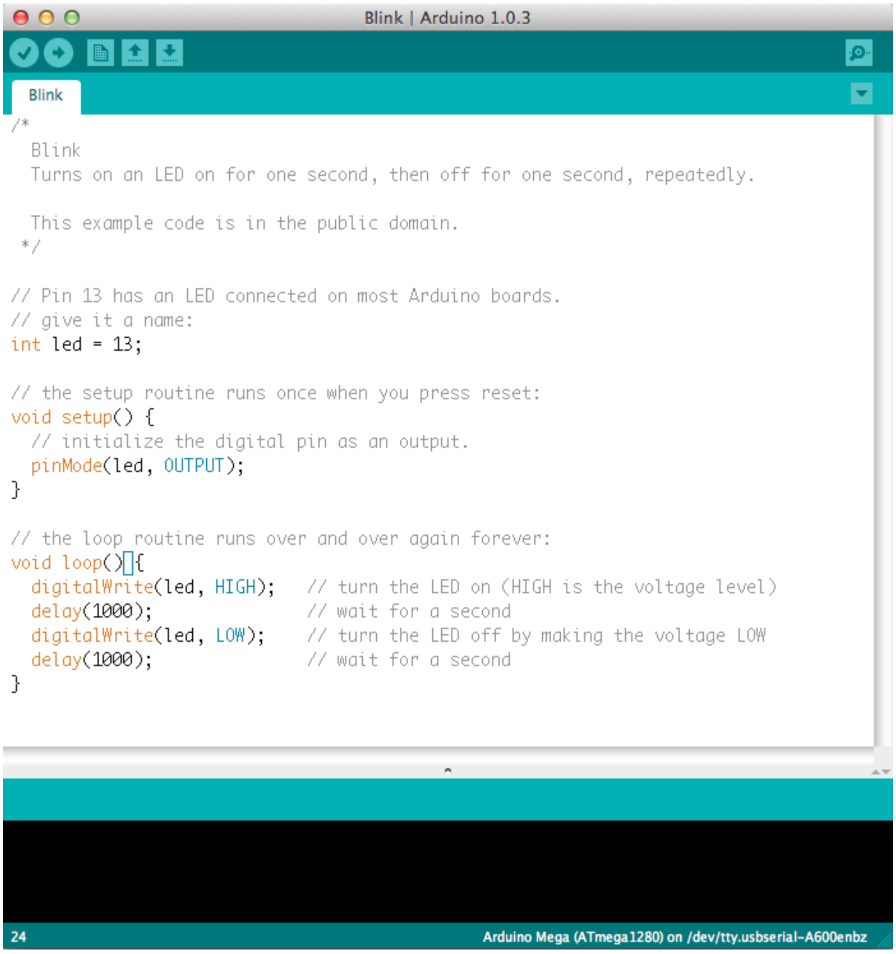

Figure 26: Example code of Arduino

As shown in the picture above, we see the program to turn on and off the lights over time. And somehow the user will load that program into the Arduino circuit to execute the lighting on and off over time. From there we can take advantage of this idea to develop projects such as: alarms, traffic light systems, ...

3.3.3 Packet Tracer

Figure 27: Packet Tracer

As we all know, Packet Tracer is a tool that supports CCNA and CCNP simulations, it helps people to better understand computer networks and can create and test IoT models before execution. Tools can also help us learn and interact with virtual devices.

Example of Packet Tracer:

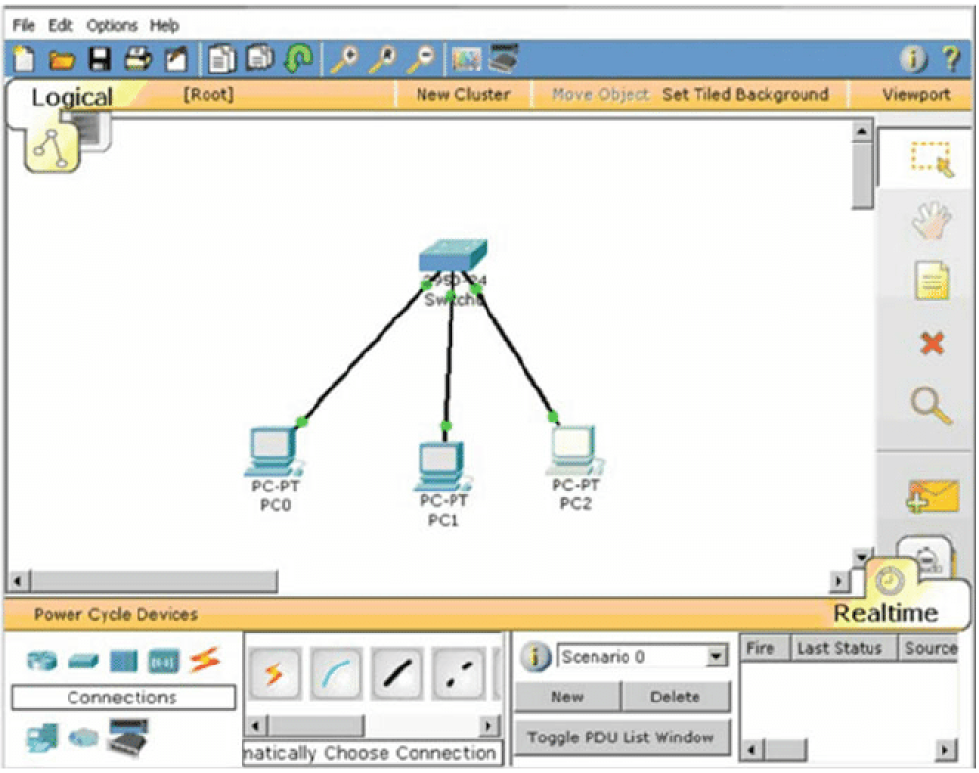

Figure 28: Packet Tracer

As shown above, the Packet Tracer tool has helped users to set up how to connect 3 PCs to each other. From the above, we can take advantage to do many different applications, such as: remote control of remote devices.

3.4 Hardware.

3.4.1 Microcontroller(Ardiuno Uno)

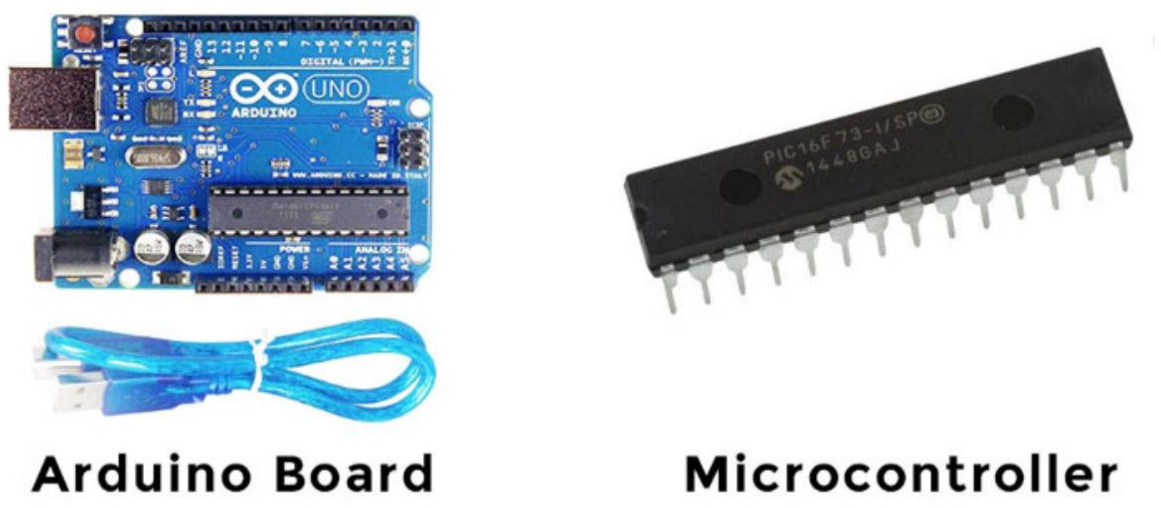

Figure 29: Microcontroller(Ardiuno Uno)

As we all know, Arduino Uno circuit is the central processor when receiving signals from INPUT devices and executes on OUTPUT devices based on the CODE segment that the user has loaded into Arduino Uno.

Example of Arduino Uno:

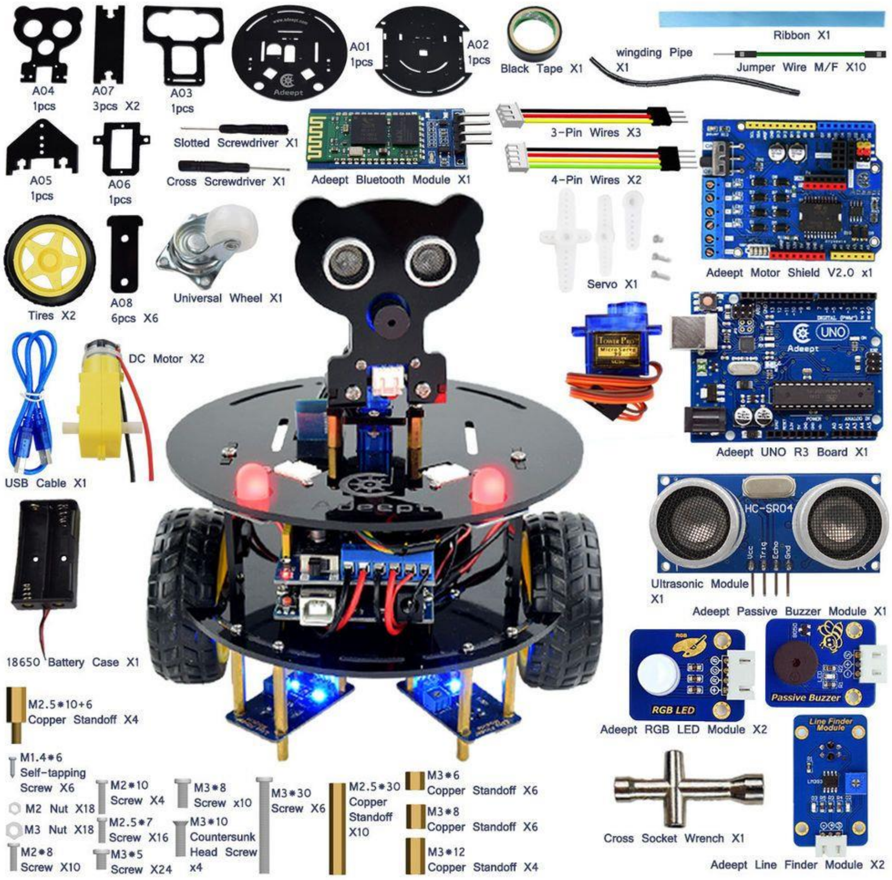

Figure 30: Example of Arduino Uno

As shown above, we saw that it was a project that used the Arduino circuit to develop a path-finding robot. Robots will move on previously drawn lines or find their way in labyrinth models. When an obstacle is encountered, the robot will automatically avoid the obstacle and return to the path it wants.

3.5 API.

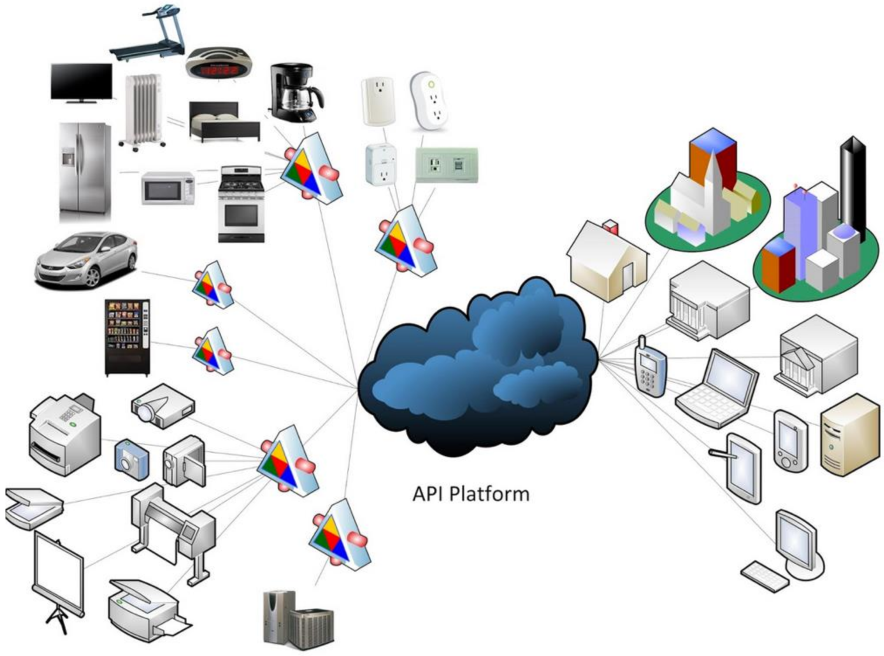

Figure 31: API

As we all know, API is a market support tool, enabling companies to disclose authorized data. From there the API helps connect things together, such as IoT.

Example: API Builder and MQTT for IoT

MQTT is a machine-to-machine (M2M)/Internet of Things (IoT) connectivity protocol and is the de facto communication protocol for IoT. While you could use HTTP(S) on an IoT device, it is pull-based only, while MQTT is push-based (actually subscribe/publish). So, for example, with HTTP, the IoT device would need to constantly ask (pull) if a change is required instead of being told (push) about a desired change. Also, MQTT requires a much smaller payload for communication and connection so using HTTP is both data and power intensive as compared to MQTT.

Axway's AMPLIFY Platform with API Builder, MBaaS and it's NoSQL Database and ability to integrate and orchestrate disparate data sources is ideal for complex IoT applications. API Builder does not contain out of the box MQTT support, but since API Builder is based on Nodejs, we can easily leverage the MQTT npm and a small amount of Javascript code to leverage API Builder and MQTT communication with IoT devices. Furthermore, you will also be able to leverage API Builders API features for non IoT devices, such as connecting to back end data sources, web sites and mobile applications.

API Builder, as well as the IoT devices are all MQTT Clients that communicate through the MQTT Broker as shown below:

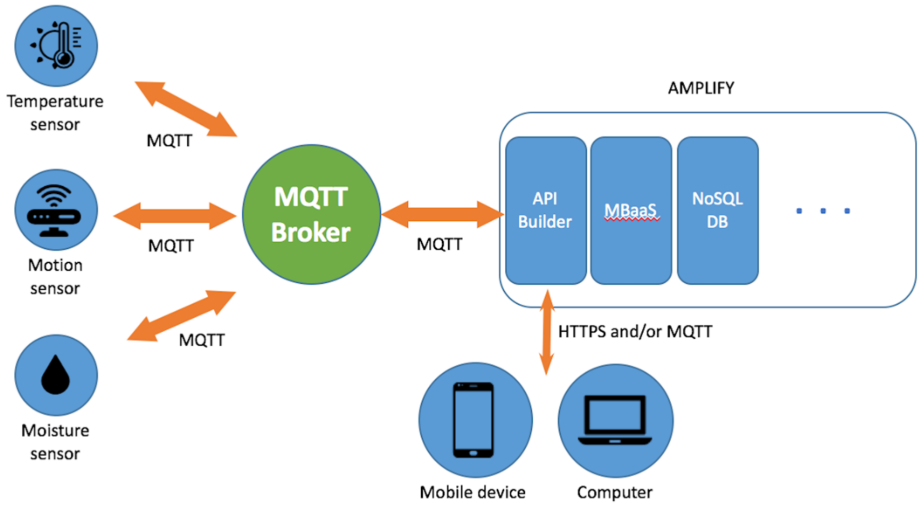

Figure 32: Example of API

The basic concept is to:

- Stand up an MQTT Broker or use a managed service, such as CloudMQTT
- Use MQTT npm in your API Builder project
- From API Builder and your IoT devices, subscribe to and Publish on topics that facilitate in implementing your IoT system
- Listen for and publish messages
- Use programatic access to API Builder Models to store and retrieve data from the AMPLIFY's NoSQL database and/or external data sources
- Use API Builder's integration with AMPLIFY's MBaaS to send Push notifications to mobile devices

So, in order for an IoT device to send data to API Builder, API Builder needs to subscribe to a topic, e.g. temp, and the IoT device needs to publish on that same topic, temp.

P4 Determine a specific problem to solve using IOT.

4.1 Design thinking

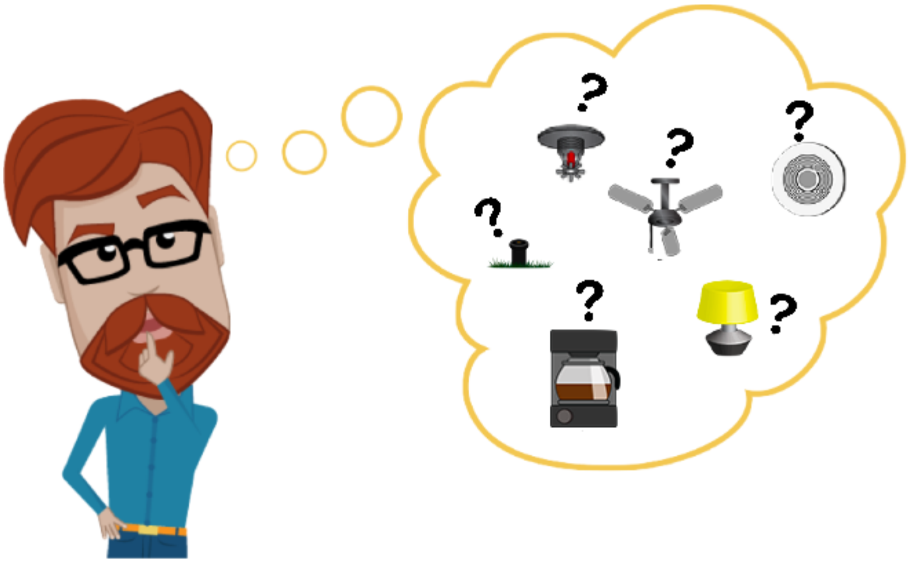

Figure 33: Design thinking

Because at present, Dat's house is very inconvenient. If he wants to use devices, such as: fans, lights, air conditioners, etc., then he has to go directly to the device and turn on them. But now, due to a car accident, I have to be in a wheelchair for about a few months if he wants to use the equipment indoors. He was forced to come close to the device and turn on their switches. So Dat wants to develop a system that helps control devices using the internet, for example: Dat uses a smartphone or laptop to access the home's general website to control devices.

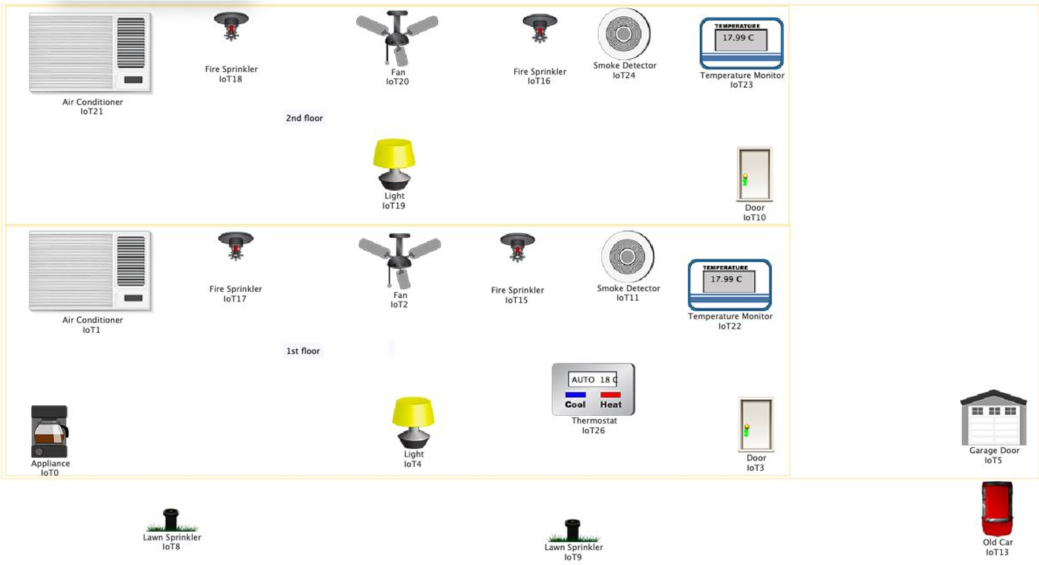

Figure 34: Home

The image above is a house model that has not been used IoT.

4.2 Questions for Defining a Problem

What is the Problem?	The house was very inconvenient, Dat could not control the devices remotely but had to come close to control them.
Who has this problem, and what do we know about them?	Dat could not move due to accident.
What are their concerns and needs?	Dat wants to control home appliances with the internet and know the house becomes smarter.
How do they interact with their environment?	Dat always had to sit in a wheelchair.
What causes the problem?	Dat cannot move but when he wants to use the devices indoors, he must be near to use them.
When does this problem occur?	When Dat needs to use appliances in the house.

Can you turn this problem into a question?	How to control home appliances using the internet?

4.3 Example of Smart home solution.

What is the Problem?			
Control home appliances with internet			
Available solutions to this problem or similar, including those discovered through research	**Pros and Cons of this solution? Cost and practicality?**	**How is it relevant, innovative and/or disruptive?**	**What are the limits of this solution?**
- Devices are connected to the internet and controlled by a mobile phone	- The network must be redesigned indoors and costly.	- Dat can control home appliances remotely and more easily. The house itself can solve frequently repeated problems.	- Costs - System designers need to have good knowledge of IoT.
What can you identify as the key factors of success?			
Control devices easily, conveniently, control devices by internet.			

4.3 Process Diagrams

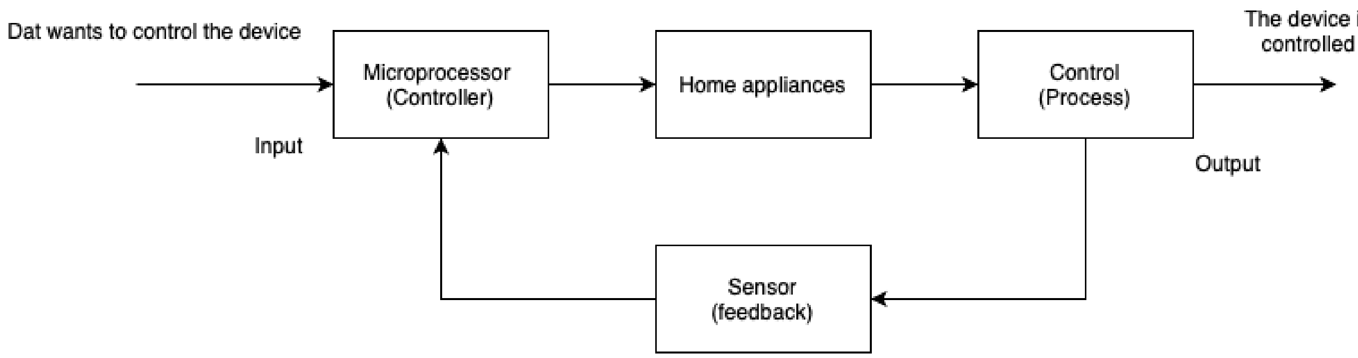

Figure 35: Process diagrams

4.4 Design a system: Choosing sensors

- Sensors are an integral part of IoT, I choose sensors for my smart home system

Sensors	**Durability and stability**	**Power consumption**	**Connection range**	**Cost**
Smoke detector	1-1,5 year	12- 30VDC.	1-2m	$17
Temperature monitor	1-2 year	15- 20VDC	1-2m	$29,79
Home gateway	3-4 year	12- 30VDC	15-30m	$28

4.5 Design a system: Connecting devices

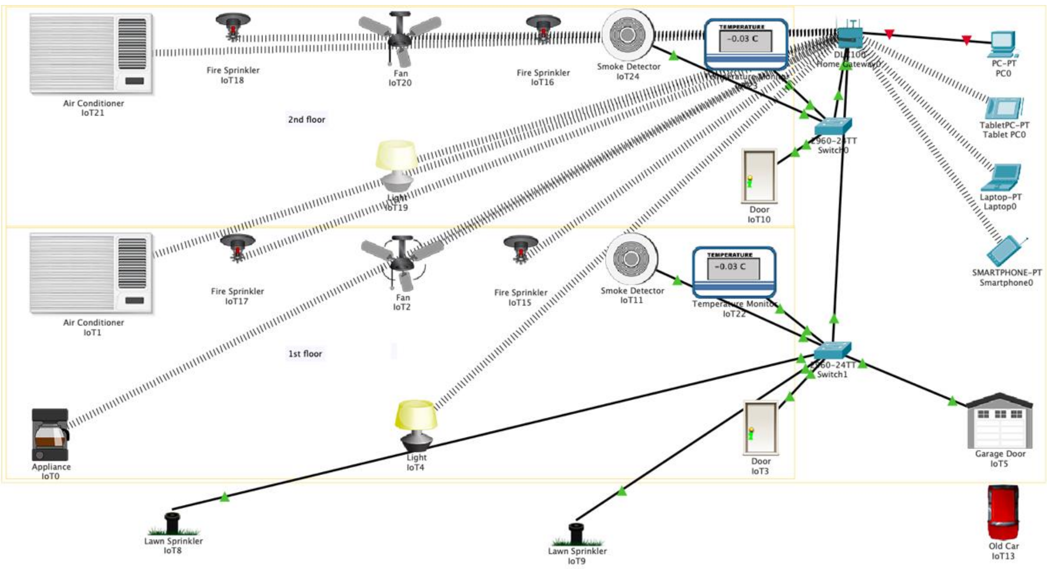

Figure 36: Design a system: Connecting devices

- As the picture above, I have connected the devices together by wireless and wired connection.

- First, I use the home gateway as a central system to connect devices in the house.

- Second, I connect devices that support wireless connectivity to the home gateway.

- Third, for devices that do not support wireless connection, I use the copper cord to connect the devices.

- Finally, when Dat wants to use appliances in the house, Dat needs to use a phone.

4.6 Design a system: Local storage and processing.

- The data collected from the sensors will be transferred to the home gateway and then processed based on the conditions designed on the system.

- Besides, I create a syslog server to store historical information when I use devices in the house.

4.7 Design a system - Security requirements

- Based on the designed system, users need to have an account and a password to be able to control devices in the home, in case the user does not have an account and password cannot control.
- Besides, I also create another type of account with the main function is to configure the devices in the house.

4.8 Summary

- I have designed Dat for a smart home model, after a period of use. Dat responded that thanks to the IoT system, Dat was able to use devices in the home more easily without having to move back almost.
- Through the design of the smart home system, I realize that the system is still very limited, with indoor devices and indoor sensors is still too few. Currently, the system is still very simple, it needs to develop more in the future.

References

[1] Unit 43 - Internet of Things 2019, *Session 1- Introduction to IOT*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[2] Unit 43 - Internet of Things 2019, *Session 2 - Design Framework for IOT system*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[3] Unit 43 - Internet of Things 2019, *Session 3 - Basic of IOT System*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[4] Unit 43 - Internet of Things 2019, *Session 4 - Sensors and Actuators - Introduction*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[5] Unit 43 - Internet of Things 2019, *Session 5 - Digital Sensors Practices*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[6] Unit 43 - Internet of Things 2019, *Session 6 - Analog Sensors Practices*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[7] Unit 43 - Internet of Things 2019, *Session 7- Communication Packet Tracer*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[8] Unit 43 - Internet of Things 2019, *Session 8 - Intermediate Devices - Microprocessors*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[9] Unit 43 - Internet of Things 2019, *Session 9 - Programming and Big Data*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[10] Unit 43 - Internet of Things 2019, *Session 10 - Design IOT System*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[11] Unit 43 - Internet of Things 2019, *Session 11 - IOT Standards and Protocols*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[12] Bwn.ece.gatech.edu. 2020. The Internet Of Space Things (Cubesats) | Broadband Wireless Networking Lab. [online] Available at: <https://bwn.ece.gatech.edu/projects/iost/index.html - :~:text=The Internet of Space Things (CubeSats),sensors to unmanned aerial vehicles.> [Accessed 20 June 2020].

[13] Jariego, V., 2020. The Internet Of Bio-Nano Things. [online] Mind the Post. Available at: <https://pacojariego.me/2019/11/10/the-internet-of-bio-nano-things/> [Accessed 20 June 2020].

[14] NewGenApps The technology company with integrity. 2020. Iot Ecosystem Components: The Complete Connectivity Layer - Newgenapps. [online] Available at:

<https://www.newgenapps.com/blog/iot-ecosystem-components-the-complete-connectivity-layer/ -:~:text=IoT is a network of,connecting enterprises and vendors together.> [Accessed 20 June 2020].

[15] Team, D., 2020. How Iot Works - 4 Main Components Of Iot System - Dataflair. [online] DataFlair. Available at: <https://data-flair.training/blogs/how-iot-works/> [Accessed 20 June 2020].