IOT

INTERNET OF THINGS

تسنيم جمال202120221

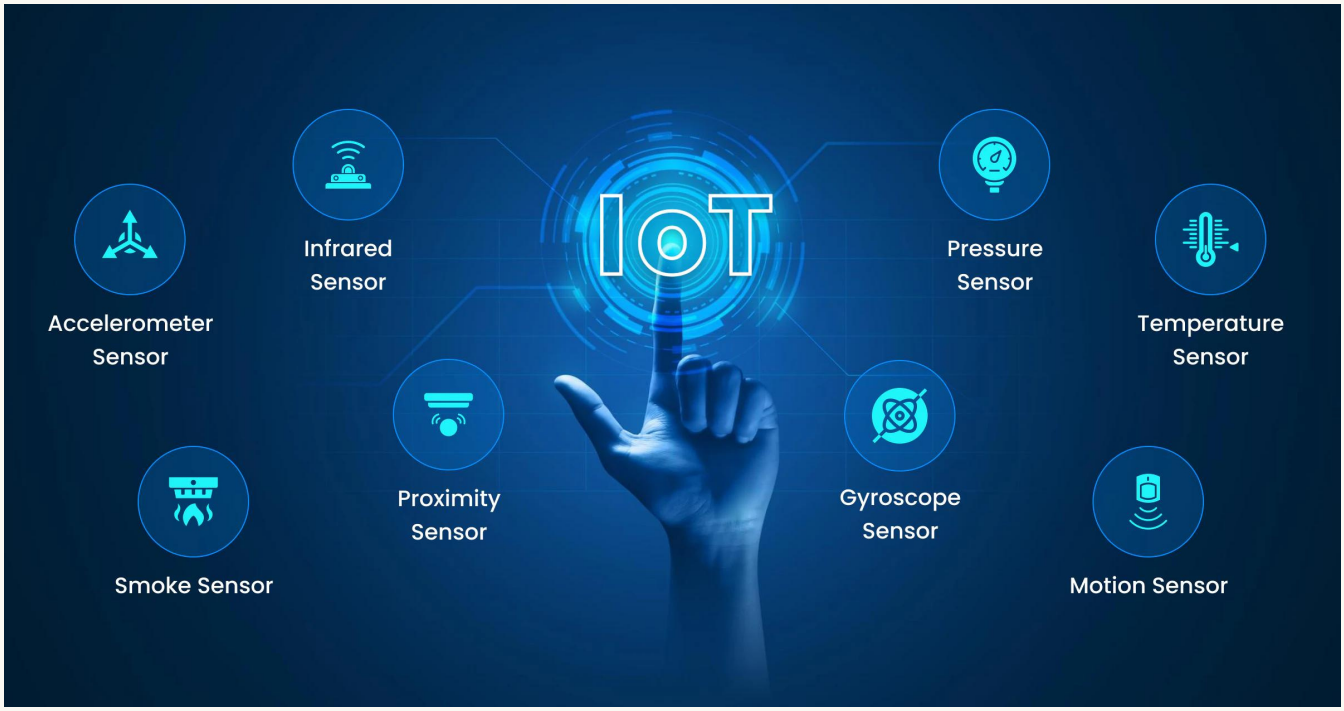
سارة طارق202120228

مي وليد 202120159

زهراء محمود202120218

ENG: Mohamed Karam

TABLE OF CONTENT



INTRODUCTION

As an overview of this huge field if this is the first time you hear about it, the Internet of Things can be explained simply as follows: the connection of the devices we use in our daily lives to a cloud network with some software that receives the information sent from these devices and processes them and returns orders to these devices to act according to these data without any interference from the owner of the devices.

DEFINITION OF IOT

it is a relatively modern term, which only emerged in 1999.

It was then merely a hypothetical term referring to machines' interaction with each other, and is now intended to connect different devices with each other using the Internet for data transmission and analysis.

We are witnessing this day – in one form or another – from smart watches, to smart lighting that interacts with a person's presence in the room that lights or grievances.
The Internet of Things is like the normal Internet we use daily, but it connects all devices to each other and not just the phone and computer. Television, refrigerator, washing machine, fireplace and car are all tied together through the Internet.
But what if the things we use on a daily basis are given these possibilities through sensors and cameras and moreover these devices are connected to the Internet?
In this case, it would not be unusual for a car to feel your presence, for example through a camera, to give an order to turn off the lighting at your home (the connection between the lighting of the house and the car is done through the Internet).

So we're saying the Internet of Things, not the Internet of Machinery, not the Internet of Devices, because we can actually connect everything we use to the Internet, even cookware, refrigerator shelves, even roads, waste boxes.

COMPONENTS

User Interface
Delivering information to user

Devices/Things: Physical objects embedded with sensors, actuators, and connectivity to gather and transmit data.

Connectivity: Communication protocols and networks (like Wi-Fi, Bluetooth, or IoT-specific protocols) enabling devices to share data

Data Processing
Making data useful

Data Processing: Edge computing or cloud servers process and analyze the collected data.

Connectivity
Sending data to cloud

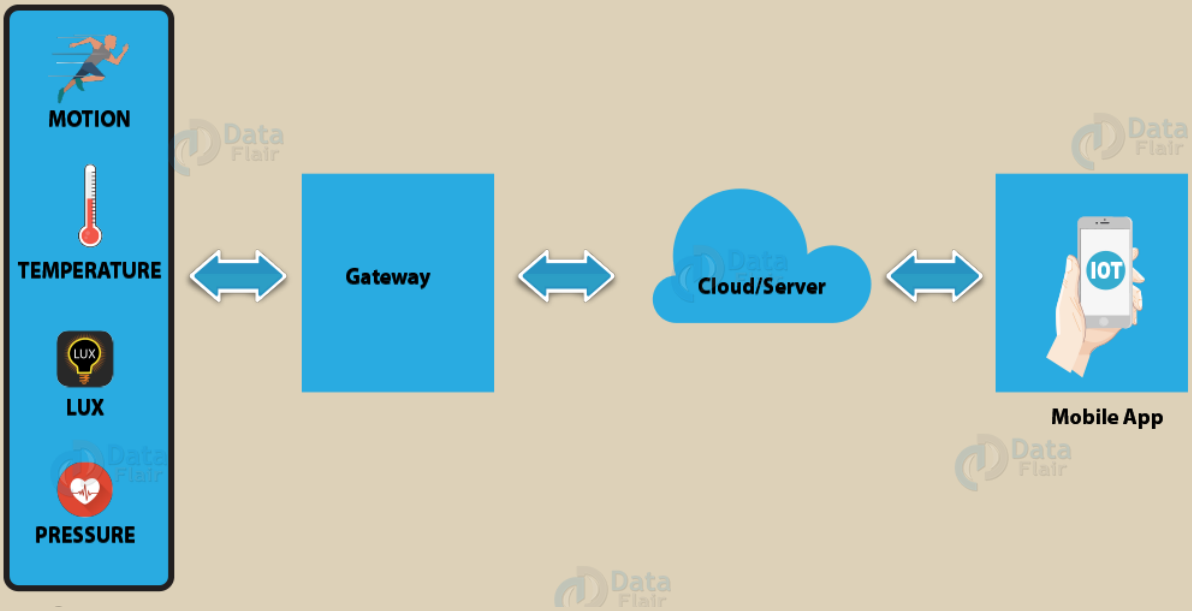
User Interface: Interfaces for users to interact with IoT systems, often through applications or dashboards.

Sensors
Collecting data

Security: Measures to protect data, devices, and networks, including encryption and authentication.

Middleware: Software facilitating communication between devices and enabling data management.

HOW TO WORK



01 Data collection from devices and sensors

02 Connecting devices to each other

03 data processing

04 Interaction and user interface

1. **At this point the devices or sensors embedded in them collect data from the environment around them, and this data may vary according to the type of sensors**

There is a great variety of sensors whether for heat, sound, light or pressure and humidity sensors.... etc.

It is possible to calculate your mobile phone within these devices, it also has a number of sensors capable of collecting, marking and transmitting data, but IoT devices are usually more specialized and focused than your mobile phone.

The outputs of this process may be very different, they may be complex or simple, they may be just numbers showing temperatures or atmospheric pressure, and they may be images or videos as needed.

---

2. **All data collected through devices and information is sent via the Internet to the electronic cloud, which you store, process and organize their transfer to other devices according to a particular protocol.**

This phase is the most important stage because it affects the rest of the stages, affecting the safety of the process and the efficiency and effectiveness of the Internet of Things.
It is also a cause of the biggest IoT critics; They are the possibility of being hacked, and the complexity of communication between devices and each other.

---

3. **Data collected by sensors is processed and stored by the cloud at this stage, and this is the effective step by which the machine or device understands the meaning of this data.**

This stage is also the one that determines how intelligent these devices are, as the more sophisticated and smarter technologies are used.

Such as Machine Learning, Deep Learning, Artificial Neural Networks, the smarter they are, and better able to successfully perceive the environment around them.

---

4. **At this stage data and outputs are converted into a form that can be evaluated and understood by the user; Whether this method is through an app or through text messages, alerts or others.**

Often, this UI not only informs people about what it has done or will do, it may even show them the data and make them choose from several options.

IOT USES

health

The field of medicine and health care has been highly sought after by IoT technology, because it can provide higher quality and efficient health care both for patients and for the infected. One of the most famous examples of this smart watch is measuring blood pressure, heart rate and sleep style in individuals.

Homeware Field

Perhaps one of the most popular ideas and perceptions of IoT is being a way to connect all home devices and machines to a single network. Besides these traditional and well-known benefits, IoT also helps to save and rationalize energy consumption by monitoring the functioning of devices, lighting, conditioners and others.

transport

This technology aims to reduce or reduce road accidents, as well as make car journeys more fast, effective and of course safe.

industry

Various industries have met with tremendous developments thanks to IOT technology, as the factory has become fully automatic by connecting machines and machines of manufacturing to each other, and putting man only as an observer.

farming

IOT is much more useful in large-scale agriculture; It can help farmers to follow changes in soils and plants from drought or alteration of their ingredients and increased acid or basement, which will help farmers to intervene quickly and find solutions as soon as possible.

ADVANTAGES

security and protection

It will significantly reduce the incidence of crimes or even completely erase them

save a lot of time

We humans will help us focus on important things, allocate leisure time to rest or enjoy.

Reduce our energy consumption

Spectacular amounts of energy can be provided, especially those related to lighting or human neglect

Reducing accidents and health problems

TIn transport, communications and the health sector, people's age will increase, and death rates will decrease.

Automation of everything that can be automated

IoT technology will help us to make all periodic and routine tasks done without our intervention and without any mistakes. This will provide a comfortable lifestyle for humans, and will help individuals become more productive.

Providing a lot of data

It will contribute to creating a very strong wave of improvement and development both from the service side and products

DISADVANTAGES

lack of privacy

It is very difficult to maintain privacy and security, everything is monitored and recorded in boring detail

Changing Human Nature

Psychologists and behaviors expect man to become emotionally cold, and to lose the ability to feel gradually changed as a result of prolonged handling of the machine... Which will bring him into a state of emotional dullness.
Besides, the frequent use of these machines will also result in a total reliance on them, and the loss of some skills that we consider essential today. Leaving these tasks to the machine to take over fully will mean our inability to do them in case the machine breaks down for any reason or another.

Millions of job losses

It will cause significant and complex economic impacts, but fortunately economists tell us that it will create millions of other jobs.

Hack and data theft

It will cost a person a heavy loss, and it will leak very accurate information.

This accurate information makes it as if this hacker penetrated the human person and his psyche and not only the device, but another technique that might save us from this predicament is the blockchain technique.

CHALLENGES

- Bandwidth
- Remote access
- security
- Scalability
- Coverage
- Limited battery life

Bandwidth availability

when too many of devices use the same frequency bands in the same location, their signals interfere with each other.

A common example of this is WiFi in apartment buildings. Every resident with a WiFi router creates a separate network that uses the same frequencies (usually 5GHz or 2.4GHz). Since they're so close together (in some cases on either side of the same wall), their signals can easily interfere when everyone tries to use these frequencies simultaneously

solution

MNOs worldwide pay for a license that essentially privatizes segments of the RF spectrum, like a toll lane on a highway, making it so that only their customers can access this bandwidth. Different MNOs who operate in the same area each have their own licensed bands, which helps decrease the likelihood of interference.

Remote access

The type of connectivity an IoT device uses can change how you're able to access the device. For example, using your customers' WiFi or ethernet requires support personnel to either have VPN privileges or be on the premises. On-site visits are extremely expensive, but if that's the only way a technician can troubleshoot or update your device, you're stuck paying the additional costs.

Solution

A common option is to utilize cellular networks to provide updates even when WiFi internet access is unavailable. This can also be effective in situations where the existing WiFi is not effective, such as when it limits data transmissions or blocks large updates.

Another option is to also ensure as much work is done online as possible. In other words, utilizing the cloud, IoT routers and other devices that do the processing and heavy lifting instead. This way, the major updates can be deployed in the cloud. This software-light approach also helps conserve power, too, as an added bonus.

Scalability

A quick-scaling nature is both one of the biggest benefits and challenges of IoT development. More devices mean more data, and the ability for businesses to gain deeper insights and subsequent actions.

However, it also creates more data to process, more infrastructure to manage, and more connections to maintain. When making your first steps into the Internet of Things, you should prepare with scalability in mind. You may very well end up adding additional devices or technologies, after all.

solution

Global IoT solutions like emnify circumvent this challenge by creating agreements with carriers all over the world. With a single emnify SIM card, your devices can connect to more than 540 networks in over 195 countries.

security

From the beginning, IoT devices have been notoriously vulnerable to cyber attacks. There are countless examples of IoT devices being incorporated into botnets (like the infamous Mirai botnet) or being hacked to misuse or access other parts of a network. This problem isn't going to just go away because, unfortunately, it stems from some inherent issues with IoT devices.

IoT devices often have a limited power supply and need to last for years in the field on a single charge. As a result, they need to transmit and receive data with little power. Adding encryption, authentication, and security protocols can significantly increase the power consumption of basic transmissions, so many IoT devices don't have these capabilities.

solution

Thankfully, low-power connectivity solutions continue to implement new security technologies. And this is an area where cellular IoT is particularly valuable. Cellular networks authenticate devices through SIM cards, and security features like IMEI locks ensure that only the intended device can use a particular SIM card. Cellular networks also allow you to perform remote firmware updates as needed while consuming minimal power. Finally, providers like emnify can help close security gaps with virtual private network (VPN) capabilities and greater control over your devices' communications.

Coverage

To transmit and receive data, IoT devices need a network connection. Lose the connection, and you lose the device's capabilities. While there are numerous IoT connectivity solutions, they're all best suited for different types of coverage. The solution you choose can severely limit where you can deploy. This makes coverage a constant IoT challenge.

For example, WiFi is a common choice for IoT connectivity. But your devices can only operate within a short range of a router, and you can only deploy your devices at locations that have WiFi. When the infrastructure isn't available, you have to either pay to build it or outfit your devices with a backup solution that already has coverage.

solution

Several technologies provide wide coverage, enabling IoT devices to operate within a few miles of the network infrastructure. While cellular is the most popular option, there are also Low Power Wide Area Networks (LPWANs) like Sigfox and LoRaWAN. In the years to come, satellite connectivity will likely become more common as well.

Limited battery life

Most IoT devices have small batteries. This is mainly because the devices are often incredibly small—and new generations of IoT technology are trending smaller and more efficient devices and components.

solution

Newer networking technologies like NB-IoT and LTE-M have power-saving features like Power-Saving Mode (PSM) and Discontinuous Reception (DRX). These features can help extend the battery life of IoT devices to 10 years or more. But many older technologies still in use today don't have these capabilities, leaving businesses to choose between too little data throughput and too much power consumption.

Another way manufacturers can make more efficient use of their batteries is with specialized IoT routers and gateways. These pieces of network infrastructure can serve as intermediaries between IoT devices and the applications and network entities they need to communicate with. The gateway or router can support the more complicated protocols and security processes like encryption and authentication, keeping devices secure while minimizing their power consumption.

SKILLS REQUIRED

• Business	• Biomedical Engineering
• Electronics	• Computer Science and Security
• Design	• Sales
• Telecommunication	• Packaging

We can not be perfect in everything!!!

Top platforms

- cisco
- google cloud
- Blynk
- IFTTT

CONCLUSION

The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.