The Internet of Things (IoT): Characteristics, Applications and New Challenges

Konstantinos Mavrommatis

October 26, 2022

TITLE

The Internet of Things (IoT): Characteristics, Applications and new Challenges

Author: Konstantinos I. Mavrommatis

School of Engineering, Informatics Computer Engineering Department, University of West Attica, Greece, kmavrom@uniwa.gr

Abstract

The Internet of Things (IoT), also called the Internet of Everything or the Industrial Internet, is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other. The IoT is recognized as one of the most important areas of future technology and is gaining vast attention from a wide range of industries.

Additional Keywords and Phrases: IoT, Sensors, Security, Scalability, Designation, Compatibility

Introduction

In the last decade, the development of the Internet of Things technology has experienced a great boom and development, taking into account the mergers and acquisitions between the companies active in the specific field, the appearance of new innovative technologies and the financings made for the further development of the Companies giants in the industry, such as IBM, Cisco and Ericsson, seeing the potential and the direction of the market, focused their interest on the Internet of Things, increased resources on it and proceeded with large educational initiatives but and marketing.

The main reasons for the rapid and large development of IoT technology in this period are the ever-increasing attention and direction of the industry towards it as well as the government initiatives, especially in the developed regions.

Mode of Operation

In order for a device to connect and exchange information with others, it must first contain the appropriate hardware, i.e. sensors and internet connection hardware. These devices collect data from the environment, then connect to Internet of Things platforms, in which platforms the data is stored, and finally this data is combined and used to perform a specific task.

It is important to note that not all data is useful and necessary. The devices, depending on the final task to be performed as well as to optimize their operation, filter the data they finally collect and select them carefully.

Let's analyze the basic components of Internet of Things technology to further deepen and enrich our so far knowledge of how it works.

The four stages of how an Internet of Things process works are:

- Data Collection
- Connect and Send
- Data Processing
- Take Action and Notify User

Data Collection

Sensors, such as the one shown in the image above which is a passive infrared motion sensor, are undoubtedly the main component of an IoT process.

The functionality of sensors includes the observation of environmental changes, from the most obvious to those that are sensitive and imperceptible, which contributes to the great security of the Internet of Things. These sensors are integrated into the devices from which the data that will ultimately be used is collected. An example of such a device is of course our mobile phone, which incorporates many and varied sensors such as camera, GPS, accelerometer, gyroscope, magnetometer and biometric sensors.

Connection and Submission

The next step is to send the collected data to cloud infrastructures, or as we mentioned before Internet of Things platforms. To achieve this mission, connections such as Wi-Fi, Bluetooth, WAN, as well as mobile networks are necessary. The specific connections have fundamental differences in terms of their type of operation as well as their capabilities, and for this reason they must be selected with the appropriate criteria for optimal results.

The connection is particularly important, as the effectiveness of the Internet of Things technology depends on its availability and speed. Therefore, the selection criteria of the connection technology to be used should be strict and documented.

Data processing

Once the data reaches the cloud infrastructures, at this stage of the process it should be processed, which includes analyzing it to perform the appropriate and correct action that will ultimately lead to the completion of the desired task.

However, this specific stage is complex and multi-layered, as the analysis of this data is an action that is included in a wide range of difficulty, from the simplest such as the measurement of an environmental change, to the most complex such as the recognition of persons through cameras [1].

It is extremely important that the data is processed as quickly as possible, as it must take immediate action to reflect the changes that occur at a similar rate but also in an unpredictable manner.

Action and User Notification

The final stage is to perform the action and notify the user. This stage is implemented either through a notification, or through a sound sent to the corresponding application installed on our mobile. The user thus knows that his order has been executed through the systems.

Nevertheless, the degree of difficulty of this stage is a little higher than it seems in theory. A very important factor is how the Internet of Things technology has been developed and adapted in each case. Manually setting up a system is in many cases a necessary implementation and can prevent unwanted results. For example, if the temperature of the refrigerator is not low enough to freeze the ice cubes, the user should be able to manually adjust it without the risk of spontaneous combustion.

The Characteristics of the Internet of Things

The Internet of Things, for its correct and orderly operation, has certain characteristics that govern it. Each act like a link in a chain. If even one of these features is absent, the Internet of Things cannot be achieved in its operation.

For example, if the sensors are missing, the devices will not be able to gather the data. If connectivity is missing, the collected data will not be able to be sent. In addition, if it is not secure and we have a data leak, then its operation is not as desired and should be changed. Therefore, each feature has its own distinct meaning and plays its respective important role.

So let's examine the features one by one to investigate their exact role and contribution to the whole process.

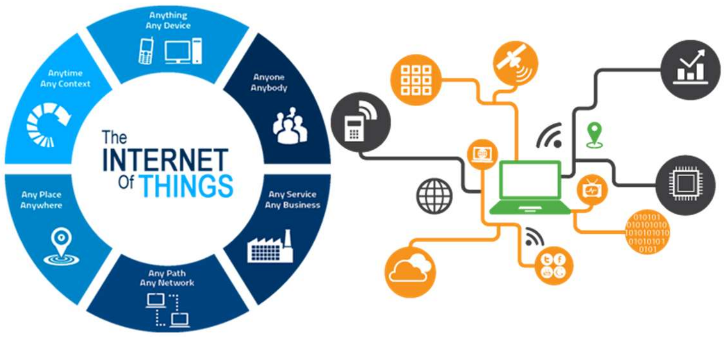

Figure 1 Characteristics of the Internet of Things (via www.pngegg.com)

Connectivity

Naturally, connectivity is one of the most fundamental yet important features of the Internet of Things. Without connectivity, i.e. seamless communication between devices, such as sensors, computers and smartphones, it would be impossible to achieve any action.

Connectivity technologies are Wi-Fi, Bluetooth and radio waves. Various Internet connectivity protocols can be leveraged to maximize functionality and efficiency. In some cases, the Internet of Things is "built" on an intranet.

Communication between devices must be fast, direct and stable. In order for such communication to work smoothly with the aim of achieving a specific task, some devices cannot "wait" for others. All must be ready and have the ability to draw or supply, depending on their role at the given time, with information and data to the rest. The slow communication implies less data from the other devices, which can lead to a wrong "perception" of the system for the information that has been collected and ultimately lead to the implementation of a different type of action than the one expected by the user [2].

So, in order to avoid such unexpected developments in the process of the Internet of Things, the connectivity needs to be characterized by stability, fast speed, immediate response and seamless operation.

Some well-known connectivity technologies are Wi-Fi, Bluetooth and radio waves. Let's dig a little deeper into them to understand how they work.

Sensors

Just as humans have their own senses, such as sight, hearing, touch, smell and taste, which help them interact with the environment, so IoT devices must have their own senses, in order to achieve interaction with the environment and other devices. Through the various types of sensors included in these devices, it is possible to "read" analog values from the environment and convert them into an understandable form, which can be used by the Internet of Things platform.

It is extremely important that these sensors can accurately and immediately read the correct values of the environment and share them directly and successfully. In addition, the choice of sensors must be documented according to the required needs so that the project has the best possible function.

As we mentioned before, the sensors used in an Internet of Things process are many and varied. Let's examine some of them.

Temperature Sensors

The function of temperature sensors, such as the one shown in the image above (Figure 1) showing a Siemens temperature sensor, is to measure the amount of thermal energy coming from a source. Therefore, they have the ability to observe and detect any changes in temperature, and ultimately convert these changes into data to be processed.

For example, the machines used in a manufacturing process have as a necessary requirement that the temperatures of both the environment and the devices have specific values and levels. Another example is the temperature of the soil in agriculture, which naturally is a key factor for the growth of a crop.

Figure 2: Temperature Sensors (via www.pngegg.com)

Humidity Sensors

These sensors measure the amount of water vapor present in the air or other gases. We find them in ventilation and air conditioning systems, in heating systems, both in industries and in domestic installations. Other facilities where we are most likely to encounter them include meteorological stations for forecasting the weather, or even in hospitals.

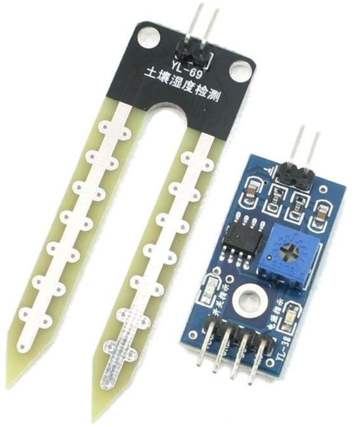

Figure 3: Humidity Sensors (via www.pngegg.com)

Accelerometers

These sensors have the ability to detect acceleration, i.e. the rate of change of speed as a function of time. In addition, it is possible to detect changes related to gravity. Another clever use of accelerometers is their anti-theft function, alerting the system to the movement of an object that should normally remain stationary at all times.

Security

Security is undoubtedly one of the features of IoT that if it does not work properly, the whole project cannot continue, as information about the users that is sensitive personal data is distributed. This information is passed from the endpoints to the analysis layer through connectivity elements. For this reason, it is extremely important from the design stage of even an Internet of Things device to include all the necessary firewalls.

Moreover, as we have seen before, Bluetooth, a connectivity technology widely used in such systems, contains keys to ensure the secure transfer of this data. Similar firewalls are included in WiFi, as well as in the hardware part [3].

Therefore, in terms of security, extensive tests should be carried out for its smooth operation, in order to avoid unpleasant situations, interception and leakage of personal data. The devices, before they go on the market, it is necessary and necessary to meet these security conditions so that in the event of a malicious attack, they are ready to deal with the specific threats in an effective way so that the information and data of the users are not put at risk.
In addition, many technology companies have reward programs for those developers who can identify such security holes and propose an effective solution to close them.

Of course, everything that locks, unlocks, so the question is ultimately how to deal with these situations as effectively as possible, and how to increase the security of the devices so that only in extreme cases can they be hacked.

IoT Device Security Issues

Security issues in an IoT system can be:

- Vulnerabilities: IoT devices are more vulnerable than other electronic devices as they lack the computing power and functionality to have a built-in security system. Another reason that leads an IoT device to have vulnerabilities is the specific and limited budget, which ultimately leads to correspondingly limited security testing. The problem ultimately affects, beyond the devices themselves, the system in general.

- Mismanagement and Device Misconfiguration: Many factors related to the management of a device can lead to its being compromised, including security lapses, weak passwords, and incomplete and sloppy device management in general.

- Malware: Although Internet of Things devices have reduced computing capabilities, as mentioned earlier, they remain susceptible to malware infections.

- Escalating Cyber-Attacks: Infected devices can often be used for so-called Distributed-Denial-of-Service (DdoS) attacks. Additionally, compromised devices can be used as a springboard to infect more devices.

- Information Theft and Exposure: The interception of information and its exposure on the internet is one of the big problems that are likely to happen, since the Internet of Things is about devices connected to the Internet. For this, end users should be informed about such issues regarding the management part of a device, but even in the event that such a thing does not happen, the manufacturing companies should provide technical support and assistance to their customers [4].

Ways to Strengthen the Security of IoT Devices

Below, we will examine some ways and methods through which strengthening the security of the devices of an IoT system can be achieved, if implemented successfully. The specific ways are as follows:

- Designation of an Administrator (Administrator): The existence of a person who will assume the position of the administrator of IoT devices will most likely lead to the minimization of oversights and exposures in terms of security.

- Monitor Typical Network and Device Behavior: Cyber-attacks are sometimes very difficult to detect, for this reason it is extremely important to know the typical behavior of both the network and the device. Device and network behaviors, such as speed and typical bandwidth, can alert users to malware infection of a device.

- Strong Passwords: It goes without saying that the passwords we choose must be strong, contain no names or dates, and include many and varied symbols.

- Code Update and Upgrades: The aforementioned vulnerabilities are unfortunately an ongoing security issue when it comes to the Internet of Things. They can exist at any level of IoT devices. Also, even older vulnerabilities are being used by cybercriminals to infect devices, reminding us that devices connected to the internet must always be updated.

- Network Segmentation: Minimizing cyber-attacks can also be achieved if users create a separate and independent network for IoT devices, different from the one that guests use to connect.

- Secure Wi-Fi network: As Wi-Fi connectivity technology is an important part of IoT, enabling security locks on this part is a very good solution to strengthen security. These safeguards include enabling a firewall, disabling WPS, using a strong password, and enabling the WPA2 security protocol.

- Knowledge of Communication Protocols: In addition to the well-known protocols used by IoT devices to communicate, such as Bluetooth and NFC (Near Field Communication), less well-known ones are also used. Communication protocols, such as for example nRFxx, LoRA, LoRaWAN and 443MHz, are also used, and for this reason, administrators should have knowledge of these protocols and be technically skilled in these matters to prevent potential threats.

- Network Security: While Internet of Things devices can compromise the system's network, the network in turn, if configured correctly and effectively, with security as the main priority, can protect the devices connected to it.

These were some ways, which can make an Internet of Things system more secure. Of course, there are others, but the above are the most basic and common ones, which if implemented correctly, are sure to rapidly increase system security.

Scalability

In IoT systems, the amount of data exchanged between devices can increase greatly in a short period of time. Therefore, in order for the system to be able to adapt to the new data, it is necessary that the levels of infrastructure, cloud services and connectivity expand accordingly. Scalability, as far as the software part is concerned, is certainly important, but the hardware part is just as critical. Because the Internet of Things involves many and varied devices, the ability to rapidly iterate the hardware design and ultimately scale it around the world under different mobile networks while maintaining certification requirements is extremely important. Naturally and to be expected, such a process has many obstacles in its way, including different suppliers and carriers and pieces of hardware. Such scalability of an IoT system inevitably includes the search for regional certifications, which is a time-consuming and costly process.

Compatibility

Another characteristic that should govern an Internet of Things project is compatibility. As the devices are numerous and therefore have a multitude of technical features and components from many companies, maintaining compatibility seems difficult, but at the same time necessary for the correct and orderly operation of an IoT system.

Functional Compatibility Between Products of Different Companies

Because end users will interact with Internet of Things devices, the user experience is especially important. As a user experience, it is defined not only the graphical environment of the mobile applications from which this interaction will largely take place, but also how easy the whole process will be. The end user should therefore use as few applications as possible, and not spend time reading which devices he was going to buy are compatible with the devices he already owns. For this reason, it should either buy products from a specific company, to ensure maximum compatibility, or companies support cooperation between their products for the convenience of their customers.

Let's take an example to understand how important this feature is. Let's say a smart home has been implemented. The door is a product of company X, the refrigerator is a product of company Y, and the lights are a product of company Z. If the user needs three different apps on their mobile phone to interact with all three of these products, that makes the user experience of the IoT system unpleasant and counterproductive.

Conclusion

The Internet of Things, as we have thoroughly seen in this work, has many applications that aim to improve everyday life and the lives of citizens in general. A historical review was made to be able to have a global picture of the roots of this Internet of Things and the birth of its idea. In terms of features that distinguish this technology, such as connectivity, security, sensors, compatibility and scalability, they all work as a complement to each other, thus creating a seamless collaboration between IoT devices, capable of serving many needs and applications. Of course, the features are not the only ones, but the specific ones are the most important for the implementation of an IoT system, without which such a system would be doomed to fail. The applications examined, i.e. the smart home, autonomous vehicles, health applications but also the use of IoT in agricultural production, reflect in the best possible way, the evolution and possibilities of the Internet of Things technology. Seeing all these leaps and bounds of course, one cannot help but wonder what the future holds for this technology, a future that is sure to be bright.

References

[1] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, ‘‘Middleware for Internet of Things: A survey,’’ IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, Feb. 2016.

[2] T. N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, ‘‘Fog computing in healthcare Internet of Things: A case study on ecg feature extraction,’’ in Proc. IEEE Int. Conf. Comput. Inf. Technol., Oct. 2015, pp. 356–363.

[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ‘‘A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[4] A. Mosenia and N. K. Jha, ‘‘A comprehensive study of security of Internet-of-Things,’’ IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586–602, Dec. 2017.