# 

# 

**Internet of Things**

Maurici Abad

Mohamed Chait

Agustín D'Acunto

Meir Mouyal

April 5th of 2019

Facultat d’Informàtica de Barcelona

Universitat Politècnica de Catalunya

Index

[**1. Introduction**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.35syjopf1f8p) **to IoT** [**2**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.35syjopf1f8p)

[**2.**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.kib3wkf6ayi2) **History of IoT** [**3**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.kib3wkf6ayi2)

[2.1](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.1vsbfkrzooh1) How does it work? 4

[**3.**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.imyp5k1yw390) **Possible threats 6**

[**4.**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.n7bxzo6aoppc) **Examples of breaches** [**7**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.n7bxzo6aoppc)

[**5.**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.c66z62h6020n) **Security in IoT** [**8**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.c66z62h6020n)

[5.1](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.vude04khm0zh) Dealing with security 8

5.1.1 Security challenges 8

5.1.2 Security measures 9

[5.2](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.12vw8bm643nv) Tools/Techniques 10

**6.** [**Conclusion**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.k295hwdwt8y3) **11**

**7**[**. References**](https://docs.google.com/document/d/1ge7R2k95mVPb7wVF7aB-QcgSDJDodU0jU_fN_wTHqBA/edit#heading=h.d74xskw5lvqx) **12**

**Presented in class by**

Maurici Abad

Agustín D’Acunto

# 1. Introduction to IoT

Internet of Things, *IoT*, is a concept that refers to the expansion of Internet connexion from conventional platforms like personal computers or mobile cell phones to objects, *things*, that are not traditionally thought as having internet connection.

It refers to the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. The main difference between IoT and Internet is the lack of human interaction, the IoT devices can create information about individuals’ behaviours, analyse it, and take action.

The examples can come from different areas of transporting, such as smart vehicles, to smart cities or health components like a pacemaker. The advancements in medicine, power, gene therapies, agriculture, among others, makes us see how IoT is strongly established.

What is the main goal of IoT? To make humans’ lifes easier. And how does IoT do that? We can interconnect everything in our home, car, workplace, and everything connecting each of those places to make the better way for us to have a satisfactory day. Just imagine, as a little example, that we connect our phone to our coffee maker at home, and everyday, when the alarm goes off, we can have our coffee ready automatically. This is just a little example of what is possible with Internet of Things.

All of these connections can make our life easier, but it also means that mostly everything that surrounds us is gathering information about us, and this will happen more each time, since the number of IoT devices is growing significantly.

Because of its lack of the human role, maintaining efficient security can be really challenging. The need of having all the devices permanently connected to the network for it to be useful as a smart object can be also a good entry point for breaching into our systems. Therefore, security in IoT is a main issue that has to be dealt with. We need to know where all the information goes, and how is it used. There are different strategies, tools and technologies to ensure that there is a confirmation that our IoT devices are properly secured and can make our life actually easier without having any concerns

2. History of IoT

There are some devices that can be considered by many to be made as an IoT device, meaning that can be turned on and off by the network, previous to the term of Internet of Things per se, but it is not accurately defined.

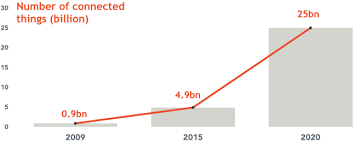
For example, in the early 1980s, the programmers at Carnegie Mellon University could check the status of a Coke machine, and determine whether there would be a drink available, and if it was cold, helping them decide whether they should make the trip to the machine.

The actual term Internet of Things was firstly coined in 1999 by Kevin Ashton, executive director of Auto-ID Center, and was originally used as the title of a presentation he gave when he was working as a brand manager. He wondered whether it would be possible to have products tracked more accurately so that anyone could know where they are and if they were available at that moment or not.

By the year 2000, LG launched the first internet connected refrigerator, that could keep track of the kinds of food items that were stored in it as well as their respective quantities, although it didn’t sell well because people thought it was too expensive for what it offered. Not surprisingly, this kind of fridge could be in any smart house currently, since it has the potential to be a perfectly working IoT device.

Nowadays, there’s consumer, commercial and industrial applications working with IoT in different kind of devices. Smart homes including lightning, heating and security features, transport improvement with traffic routing and smart parking, and even in the health department with better patient care or elderly monitoring, makes us see how the Internet of Things technologies have landed into our world, that is why security in IoT is so important.

To show all this growth, the technology consulting firm Gartner projects that 6.4 billion connected things were used worldwide in 2018, up 30 percent from the previous year. And Gartner forecasts that number will grow by more than three times, to nearly 25 billion by the year 2020.



*Figure 1: Garner forecast of IoT devices evolution*

2.1 How does it work?

There are two ways of building IoT systems: by forming a separate internetwork including only physical objects, making it more local to work, or by making the Internet ever more expansive, enabling it to reach further devices, but this requires hard-core technologies such as rigorous cloud computing and rapid big data storage.

IoT is build using four main components:

* Low-power embedded systems: These systems make the device consume less battery without making it lose performance.
* Cloud computing: Using cloud computing is how the device stores the data it collects, since the amount of data is significantly big and has to be stored on a reliable storage server.
* Availability of big data: IoT relies on sensors and other kind of real-time enablers, and these electronic devices spread throughout every field, therefore, using them will trigger a massive flux of big data. The main enablers used by IoT devices are sensors, nanotechnology actuators, that can be used, for example, for data exchanging, and RFIDs Tags (Radio Frequency Identification), for unique identification.
* Networking connection: The essential part of IoT devices is that they are connected through the network, in order to communicate with the computer controlling them. They also require an IP address, and due to the growing number of devices, it is being studied if it is required a different naming system for these kind of devices.

Main characteristics of IoT:

* Scalable and efficient
* Devices consume little power, due to their low-power embedded systems, and when they are not in use, they are usually put automatically to sleep.
* Intermittent connectivity, devices are not always connected, in order to save bandwidth and battery consumption.

IoT has many different applications, going from Smart cities, with some examples like controlling the electrical distribution, surveillance of places of the city, utilities, emergency services and Smart Grids, to Smart Homes, taking care of its security, the light bulbs, alarms, fridges and other home appliances. There is also an improvement in transport and buildings infrastructure, and even in the health department.

3. Possible threats

A lot of IoT manufacturers don’t spend enough time looking at security, so a lot of IoT devices may be exploitable. In addition manufacturers don’t tend to update their products as fast as they should, and sometimes the software never gets updated.

That opens the door to attackers to sneak into your most intimate place, your home.

IoT attacks may have very different effects depending on the characteristics of the device:

* If it has a microphone, it can record your conversations.
* If it has a camera, it can know when you are at home.
* If it has a speaker, it can give you false information and scam you.
* If it is connected to your Wi-Fi, it can give access to your network, allowing the attacker to steal any unencrypted information or use phishing techniques.
* If it is locking something, like your bike, it can be stolen.

This list keeps going until the hacker runs out of ideas. So it’s very important to take special care of security in IoT devices, because in the end those devices are the ones that store our most intimate information.

4. Examples of breaches

Let’s see several examples from Pen Test Partners of insecure IoT devices and explain the process and techniques of hacking them:

1. Our first example is a smart lock that opens with your fingerprint called tapplock. Some ethical hackers wanted to test this device and reverse engineered the source code of the phone app. They discovered that you could unlock it by using a ‘secret key’, but the key happened to be the Bluetooth MAC address of the lock. So you can easily unlock it with just a bluetooth connection. That’s like leaving the keys next to the lock.  
   But most surprisingly they looked at the cloud services the app talked to, and realised that you can discover where all the locks were!
2. The second example is a Wi-Fi Kettle, the Smarter iKettle 1st gen. They discovered that you could connect to the kettle with telnet command, but it required a password. Then they disassembled it and found out the network microcontroller it used. Next they found it’s data sheet and got the default password. That password happened to be the one used in the Kettle. So the next step was getting the wifi password of the router it’s connected to, and gain access to your home’s Wi-Fi network, leading to any kind of hack.
3. Next we have My Friend Cayla, a child's doll that is able to respond to questions and maintain a conversation. The doll uses the internet to search what the child said which then answers with what it collected online.  
   Ken Munro discovered that to connect to the doll there’s no pin required, so anyone in range can listen and talk with your kids.
4. Finally there are Google Dorks that find home security cameras connected to the internet that have not been configured to be private, so they are reachable from any place. The worst part is that you can listen or even move some of them.

5. Security in IoT

As we have mentioned before, IoT devices gather a lot of information from everything that surrounds them everyday, and they are not being monitored 100% of the time, so security in these devices is critical. For any IoT application, it is crucial to protect data, user privacy, and safety. Breaches can harm production continuity and business processes, customers’ trust, and, worst of all, human health and life.

5.1 Dealing with security

5.1.1 Security challenges

There is a considerable amount of challenges when security of IoT is discussed. Because the idea of networking appliances and other objects is relatively new, security has not always been considered top priority during a product's design phase. In addition, a lot of product designers are more interested in selling their products quickly, therefore, getting them to market before thinking whether they have taken the necessary steps to build security from the start, and all of this because IoT is a nascent market that is growing fast.

One of the biggest issues is the use of hard-coded or default passwords, or even not strong enough, which can lead to security breaches, due to not being strong enough to prevent infiltration.

As we have mentioned before, IoT devices use low-power circuits, which lead to them having less cost and consuming less battery, but that also has the downside that they do not possess the resources needed in order to implement strong devices or cannot offer advanced security measures.

Since most of the devices are sensors that are placed in the field or on a machine and just left there, they seldom receive security updates. Also, from a manufacturer's viewpoint, building security in from the start can be costly, slow down development and cause the device not to function as it should.

There is also an important challenge brought by the lack of industry-accepted standards. There are large companies that may have their own specific standards, but they vary among proprietaries or segments of industry, and even though many IoT security frameworks exist, there is not one that is agreed-upon. The variety and disagreement on this standards makes it really difficult to secure systems, and even more to ensure interoperability between them.

Every organization that uses IoT must start to be aware about all these different challenges and try to face it as a unit, to view security as a shared user, from creation, to service provider and to end user. Security always should be a top priority on all the products, providing encryption and authorization, and refreshing this authorization by changing passwords, updating security measures and taking other precautions.

5.1.2 Security measures

IoT security methods vary depending on your specific IoT application and your place in the IoT ecosystem. For example, IoT manufacturers, from product makers to semiconductor companies, should concentrate on building security in from the start, making hardware tamper-proof, building secure devices, ensuring secure upgrades, providing firmware updates and performing dynamic testing.

A solution developer's focus should be on secure software development and secure integration. and for those deploying IoT systems, hardware security and authentication are critical measures. Likewise, for operators, keeping systems up to date, mitigating malware, auditing, protecting infrastructure and safeguarding credentials are key.

With any IoT deployment, it is critical to weigh the cost of security against the risks prior to implementation, putting security in a critical priority. When security is put in the first place and the correct measures are applied, there is a high chance of defeating the challenges exposed previously.

Some of the most typical measures in IoT are the following:

One of the most important measures is to incorporate security in the design phase. As it is explained before, most of the developers try to put the product in the market as soon as possible, leaving security off. Therefore, enabling security by default is critical, as well as using the most updated security technologies as possible and adapting them to the environment. Also, it is very important to add hardware security in order to protect sensors in the different environment they are going to be placed, making them tamper-proof or tamper-evident.

It is also crucial that hard-coded or default passwords are part of the design process. Always require credentials when updating device software by an end user, and use strong passwords or multifactor authentication. With this being said, using digital certificates will provide trust and control to distribute public keys, and more importantly, verify identity over the network.

To communicate data, and also when it is stored, using strong encryption will make the system more secure. To do the communication, it is essential to protect the integrity of the data being sent from IoT devices, so there has to be strong API security.

Since most of the actions performed by IoT devices are done by the network, it is of huge importance to have great network security. This can be done by using anti-malware, firewalls and intrusion detection, blocking unauthorized IP and using network access control (NAC) to help identify and monitor IoT devices connected to a network.

As a last measure, to avoid being outdated, it is very important that there are continuous software updates as soon as possible. There can also be security teams integrated in the software team for them to have a better idea of which measures to apply.

And not less important, it could be really useful to educate consumers in order for them to realize the cruciality of security in the devices they own, as a measure of prevention.

5.2 Tools/techniques

In IoT security issues are problem specific

Among the most common IoT security issues, experts mention:

* Vulnerability of the network of smart devices.
* Authentication problems.
* Lack of data encryption and security analytics.
* Problems with IoT API and PKI.
* A tendency of launching Io
* Tendency of launching IoT solutions in a rush.

We can differentiate five main directions of security solutions for IoT.

1. **Networks**: To archive a safe network experts recommend combining traditional tools of data protection (like antiviruses and firewalls) with protocols, standards, and complex device capabilities.
2. **Authentication**: Use of two-factor authentication, biometrics, and digital certificates when possible.
3. **Data encryption**: addresses the issue by using a complete encryption algorithms, for example SHA-2 instead of MD5 and SHA-1 for Hashtag operations.
4. **Security analytics**: the need to monitor all the smart devices and check their performance indicators is outstanding. Indegy is a comprehensive Industrial Cyber Security Suite that helps solve this issue.
5. **API and PKI**: A secure API includes an ability to authenticate and authorize the flow of information within the protected IoT network, including smart devices, back-end system, and third party applications.   
   X.509 digital certificate along with cryptographic life-cycle capabilities allow preventing a threat of using PKI.

6. Conclusion

Internet of Things is a growing technology and can be very useful in humans’ lives, and make their lives significantly easier. Nevertheless, since it is a new technology and there is a will to sell fast, security is not a top priority, when it definitely should. As of 2019, IoT is not secure, and it has to continue working so it improves its condition, and take into consideration the measures and challenges this report explains, and hopefully, there will be a considerable improvement soon.

7. References

**Introduction to IoT:**

Nayyan Mujadiya (Mar 31, 2018) Introduction to Internet of things, Available at: <https://medium.com/iot-with-raspberry-pi/chapter-1-introduction-to-internet-of-things-c8c459f4f961>

**History of IoT:**

Jessica Porter (Nov 12, 2018) The History of IoT (Internet of Things) and How It’s Changed Today, Available at: <https://www.techprevue.com/history-iot-changed-today/>

**How does it work and Introduction:**

CUTigress (Feb 4, 2019) Introduction to Internet of Things (IoT), Available at: https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/

**Possible threats & Examples of breaches:**

Pen Test Partners website, Available at: <https://www.pentestpartners.com/>

Pen Test Partners LLP (18th June 2015) 'Infosecurity Europe 2015: Wifi Kettle SSID Hack Demo', *YouTube*. Available at: <https://youtu.be/GDy9Nvcw4O4>

(2nd March 2019) 'My Friend Cayla', *Wikipedia*. Available at: <https://en.wikipedia.org/wiki/My_Friend_Cayla>

(17 February 2017) 'German parents told to destroy Cayla dolls over hacking fears', *BBC News*. Available at: <https://www.bbc.com/news/world-europe-39002142>

(22 October 2016) ''Smart' home devices used as weapons in website attack', *BBC News*. Available at: <https://www.bbc.com/news/technology-37738823>

**IoT Security and security measures:**

1. (Feb 4, 2019) Enabling trust for IoT, Available at: https://www.nexusgroup.com/solutions/iot/
2. (Mar 28, 2019) Un mundo hiperconectado de forma segura, Available at: https://www.elevenpaths.com/es/tecnologia/iot-security/

**IoT security challenges and measures:**

(Feb 4, 2019) IoT security (internet of things security), Available at: <https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security>

**Tools/techniques:**

Intellectsoft IoT Lab website, Available at: <https://iot.intellectsoft.net/>

Indegy website, Available at: <https://www.indegy.com/>

Paul Stokes (25th September 2018) '6 Internet of Things (IoT) security technologies on the contemporary market', *Medium*. Available at: <https://link.medium.com/ENdPmUp2vV>