

## A Survey of Security Challenges in Internet of Things

Anass Sedrati\*, Abdellatif Mezrioui

Telecommunication Systems, Networks and Services Lab, RAISS Team, INPT, Rabat, Morocco

---

### ARTICLE INFO

*Article history:*

*Received: 25 September, 2017*

*Accepted: 18 January, 2018*

*Online: 30 January, 2018*

---

*Keywords :*

*Internet of Things*

*Challenges*

*Security*

*Privacy*

*Lightweight*

---

---

### ABSTRACT

*Internet of things (IoT) is an innovative technology subject to all kind of imaginary and science fictional solutions. Dreams and speculations are still possible about it. A technology combining real life objects and virtual life (Internet) is indeed a fertile pitch of fantasy and original ideas. However, IoT has in practice to face several challenges to ensure its function and operability in a near future. This paper defines first some technical challenges of IoT today, before focusing on security-related ones via a layered architecture of IoT that we suggest. Finally, a number of actions and required future work is presented to enhance IoT security (Privacy, Lightweight crypto, etc.).*

---

## 1. Introduction

Nowadays, billions of people are active using Internet for all kinds of purposes on a daily basis. People send in fact emails, use social networks, share voice and image, transfer money, watch events, and perform many more actions with it. It is estimated that by 2020, there will be 50 to 100 billion devices connected to Internet [1]. If what is happening now was difficult to conceive 20 years ago, one can easily imagine that future will be as unpredictable, if not even more.

In this context, even Internet itself is set to change from its classical network infrastructure to a more flexible one: The Internet of Things (IoT). IoT will allow most objects to be connected to Networks and interact in different scales. This opens doors to new applications in all domains one can think about. A new way of living and working is emerging by embedding electronics into everyday physical objects. IoT is the next step of the development of communication tools. As a new technology allowing many “things” to be connected for the first time ever, IoT marks a clear difference with the classical Internet where only given devices could do so. This difference is the driver of this article. Given the specificity of IoT and the uniqueness of the “things” it involves, technologies used in Internet might be incompatible in many aspects. This incompatibility is the new challenge facing IoT, affecting many areas, mainly security. To have a functional and secure IoT technology in the future, issues as sensors/actuators and privacy should be looked into and solved.

The aim of this article is to first summarize the challenges of IoT nowadays, before focusing then about our interest area: security issues that are facing the Internet of Things.

The article is organized as follows. In Section 2, we will introduce IoT and define it along with its main related concepts. In Section 3, we will list the differences between IoT and the “traditional” Internet. This comparison will lead us to Section 4, where IoT challenges are presented. Section 5 describes a model of IoT Architecture on which we are going to argue. This model will help us to identify security challenges. Section 6 will be a continuation of the previous Section, highlighting mainly security issues, and describing them a little bit more in detail. In Section 6, we will also refer to our model architecture when detailing security challenges, and link each security challenge to its place in the model. Section 7 will finally be the conclusion and an opening to the future and new work that research could dig into.

## 2. Internet of Things

Formally defined, the Internet of Things is a link between “objects” of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and not only anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time” [2]. According to this definition, one can already note the complexity of the transition from an Internet used for interconnecting end-user devices to an Internet used for interconnecting physical objects that communicate with each other

---

\*Corresponding Author: Anass Sedrati, Email: [sedrati@inpt.ac.ma](mailto:sedrati@inpt.ac.ma)

and/or with humans [3]. IoT combines anything in many thinkable ways. Through its definition, IoT suggests different areas of application: From smart cities to transport or health, all domains are expected to enable IoT in different extends. Agriculture, industry, aeronautics, and even daily life would use it. One can e.g. call his self-driving car to pick him up at the door, and warm up coffee at the work desk while still sitting in traffic jam. Clothes can also with help of weather forecast “decide” how thin they shall be when a person is to wear them. From the most basic and common applications to the most complex and fanciest ones, IoT will be present in our lives very soon. In order to enable IoT, each “thing” should have the ability to support three pillars [3]: (i) The object should be identifiable (anything identifies itself), (ii) The object should be able to communicate (anything communicates), and should be able to (iii) interact (anything interacts). If they fulfill those pillars, “things” can be considered as “smart objects”.

In addition to the three pillars, each “thing” should contain a set of technical components that will enable IoT technology into it. Two essential components of IoT are sensors and actuators. A sensor is a little electronic component able to fulfill the three pillars defined above. In order to make a thing “smart” and able to realize the three pillars, a sensor or an actuator should be attached to it. Through this linking, the thing will be able to send and receive data, and become part of the IoT. A set of sensors form a network called “Sensor network” where they can interact with each other or with Internet. When the networks are wireless, they can be referred to as WSNs (Wireless Sensor Networks). An actuator is an element that converts energy into motion. There are three types of actuators: Electrical, hydraulic and pneumatic [4]. The interest of actuators in as IoT context is that they allow smart objects to trigger actions having an effect on the physical reality [3]. Actuators can be combined with sensors and connected in a network structure called SANET (sensor/actuator network).

To summarize, we can then say that IoT is the network gathering all “things” having a sensor/actuator, and connected with each other in all possible ways and forms. These objects can exchange data to different extends depending on variables that we will see later on.

### 3. Technical Differences Between IoT and Internet

As we have seen in the definitions, IoT can be considered as the next generation of Internet, allowing all sorts of objects to be connected. The first difference is then that not only specific devices can access networks, but basically all of them. The only condition is having a sensor/actuator that can communicate and support the three pillars (being identifiable, communicate and interact). A list of major differences between IoT and Internet will contain:

- **Sensors/Actuators:** Because “things” are not initially set to be connected, they have to be implemented with sensors/actuators. In classical Internet, devices (PC, Smart Phone, TV...) have a complicated electronic system. In IoT, things have a main role that is not always technological. Clothes role is to keep warm, and roofs’ is to protect houses from rain and snow. When these objects will be connected, sensors/actuators should not constitute a major part of them (because they still have to fulfill their initial aim). These technological elements must however be present in order to make the objects labelled as “smart”. A solution is to have

smaller sensors and actuators. This means that they will be limited in resources and capacity, unlike devices used in Internet. Moreover, Internet Enabled devices do not have power consideration, and use chargers.

If sensors are also used in classical Internet such as in IP cameras, the difference is that in IoT, sensors have usually to be on low-power. Their charging (or being self-charging) is still a hanging issue. This difference creates many challenges that will be discussed in the next section.

- **Autonomous “Things”:** In IoT, Things are expected to be more autonomous than our usual devices. Some objects should be able to perform a number of duties themselves, and to communicate with each other without human interaction. But not only that, some specific cases in IoT imply that things are directly connected with each other in their network (Fridge and a car in the smart home network), which creates an extra complexity knowing that no human intervention should be in this network.
- **Difference in nodes [5]:** IoT can be composed of Radio-frequency Identification (RFID) and WSN nodes, whose resources are limited, while the Internet is composed of PC, servers, smart phones whose resources are rich. This means that combinations of complex algorithms can be used in Internet, while IoT is limited in this aspect. Then, other alternatives for security need to be found for IoT.
- **Heterogeneity:** IoT involves very heterogeneous objects which can have different standards. In Internet, data formats and standards are similar even in different operative systems. Managing this heterogeneity in contents and formats is an important milestone for IoT enabling.

The difference between Internet and IoT can be summarized in the Figure 1 in the next page. Figure 1 shows the evolution of networks with respect to the type of connected devices and objects. Internet of Things is gathering not only traditional “technical” devices, but extends even to daily life objects such as cars, fridges or houses. It can be considered as the evolution of Internet towards a connected daily-life objects.

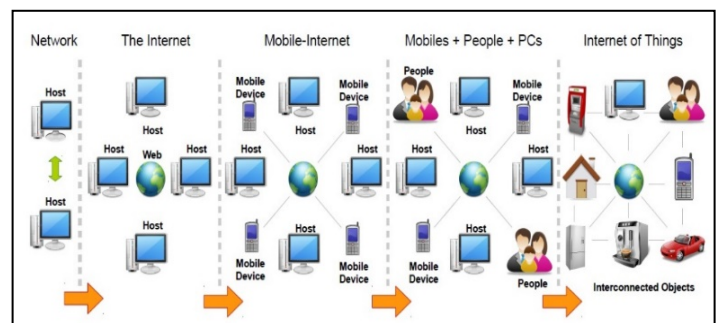


Figure 1. Evolution from Internet to Internet of Things [2].

Given the differences between IoT and Internet that we saw in this section, a preliminary list of what IoT needs to support can be established [3,5]:

- **Manage devices heterogeneity**
- **Scalability:** Naming, addressing, managing information...

- **Spectrum Availability:** Taking into consideration that the number of IoT connected devices will be much higher than in current Internet.
- **Self-organization capabilities:** As “things” will be autonomous and make decision by themselves in some situations.
- **Context awareness:** A device can have different modes and roles depending on the context. The device should be aware about it by its own.
- **Security and Privacy:** As IoT has to find new ways of securing, different from the complex algorithms used in the Internet. IoT devices have in fact less resources (power, CPU, etc.).

#### 4. Internet of Things Challenges

The differences that we have seen between IoT and classical Internet in the previous Section are the main reason of today’s IoT challenges. Internet is in fact an established technology, and a number of its critical issues were already solved. Those challenges can be the same ones facing IoT. The problem is that IoT with its differences in components and way of working creates a new “versions” of these challenges. The difference with Internet implies in fact to find new innovative ways of solving, instead of the “traditional” ones, which only work with Internet. In order to be operational in the future, IoT needs to solve the most critical of them at least.

Considering what we have seen about IoT, we can already list the following challenges:

- **Sensors/Actuators:** As all items (things) will be connected to Internet, they will need a tool to link them to the network: It is the sensors/actuators. Those elements implemented in all sorts of “things” (clothes, walls, fridge...) must be ready to work at any time. Internet is indeed working real-time, and information ought to arrive at almost the same time it is sent. This scenario supposes that all connected “things” have charged sensors at every moment to allow their discovery and be able to send and receive data (resp. actuators in order to be able to perform actions). The challenge is then an energetic one. Low-power wireless sensors which do not need battery replacement over their lifetimes are needed. How will those sensors be charged? Are they sustainable? Energy and power management is a principal issue within the IoT research area.
- **Identification:** In IoT, not all “things” have the same role. In the example of a smart house, a Fridge and the security camera both must be connected, but they do not have the same role and access specificities. This means that Objects should be identifiable in order to allow each one of them to perform its own duties. Identification can be either by being part of a certain class (desk objects, kitchen tools...) or by unique identification. Identification is a notable challenge in IoT. Miorandi et al. [3] have suggested identifying objects in IoT in two ways: “The first one is to physically tag one object by means of RFIDs, QR code or similar (...) returning an identifier that can be looked up in a database for retrieving the set of features associated to it. The second possibility is to provide one object with its own description: if equipped with wireless communication means it could communicate directly its own identity and relevant features. It is however

important to mention that description is not enough to make an object unique. Other elements as ownership have to be added and updated in order to preserve the privacy aspect. This is particularly relevant in scenarios regarding two cars of the same brand parked aside.

The two approaches cited above are not mutually exclusive and can complement each other”.

The identification problem is not entirely solved and is always holding.

- **Scalability:** Given the expected huge number of objects that will be connected with IoT, network and frequency have to anticipate the enormous flow coming in soon, by scaling the network at different levels. Addressing is one example of scalability issues in IoT. The standard commonly used today with internet is the Internet Protocol (IP), and the biggest chances will be that addressing in IoT will also be in this protocol. Even the IPv6 protocol, a candidate for addressing, can face this challenge. But in This situation other questions are raised such as: Should each “thing” have an address at every moment? Should it be allowed a temporary/permanent address? What is the best scheme to identify each “thing” in the IoT?

Scalability in not only related to addressing. Other challenges regarding the size can be about data and networking, information and knowledge management, and even service provisioning and management [3].

- **Heterogeneity:** IoT involves different “objects” ranging from the smallest chip to the big airplanes and buildings. It is not sure that all those items use the same set of protocols and data formats, due to their different capacities and size. However, if we want all those objects to communicate with each other, standards need to be implemented. Standardization does not only apply to addressing, but even to other areas in the IoT. One of the important institutions working to solve it is the IEEE. Challenges face indeed packets that will be routed through different sorts of networks. All those networks must follow the same norms and specifications to be synchronized and understand each other. Standards of IoT must cover nowadays many areas such as security, privacy, architecture and communications.
- **Governance:** The smarter “things” become, the most autonomous they are, and thus the more governance is needed. The question of regulation and how users will be protected are important in that matter. Which organizations will care about law enforcement for IoT? Should new ones be created? How should personal data be protected? Who can see what? How to prevent third party apps from accessing this data?
- **Security:** Security is a major and critical issue in IoT. Therefore, it will be separately presented in detail in the next two Sections.

#### 5. An IoT reference Model

In order to analyze security aspects of IoT, a reference model would be of a good use. Many IoT reference models have been widely discussed in academic publications and these reference models distinguish different levels [6-8]. Providing detailed descriptions of all these IoT reference models is beyond the scope of this paper. But in order to analyze and summarize IoT security issues level-by-level we will use a simple three-level reference

model as depicted in Figure 2. This architecture is our starting point and it will be the architecture that we will consider in this article.

Thus, as shown in Figure 2, IoT can be broken down into three major layers: Devices collect data, gateways and communication units relay the data collected, applications and services analyze the data, and take actions. This architecture highlights also some security aspects that are related to the three main layers:

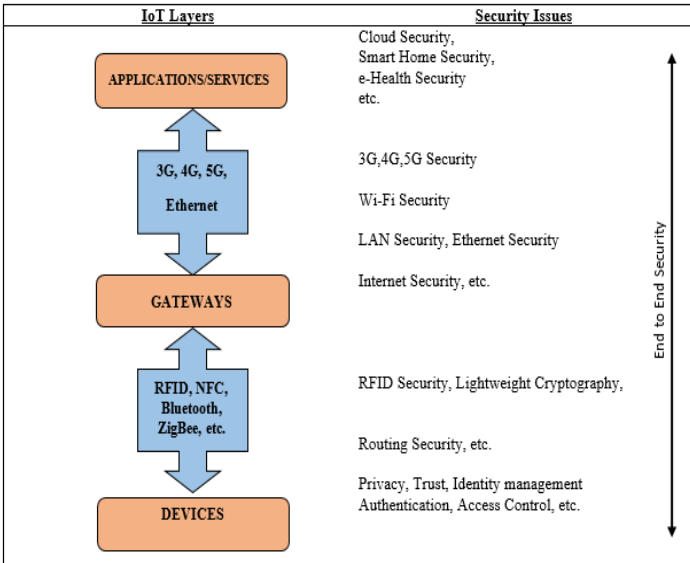


Figure 2. A reference Security Architecture for IoT.

- **Devices:** The Devices Layer is divided between nodes and network. It includes Radio-frequency Identification (RFID) security and Wireless sensors network (WSN). Wireless Sensor Network, which we have defined in Section 2, face in the IoT context many issues that we will define, such as heterogeneity, Cryptographic algorithms or Node trust management.
- **Gateways:** It is the layer responsible for the transport of data and the transmission of commands between the first and third layer (applications and services). This layer gathers security tools and protocols that are responsible of transporting, in a secure manner, data in 3/4/5G, WIFI and LAN/WAN networks.
- **Applications/Services:** This layer provides user applications and services. They can be accessed via cloud computing. These IoT applications and services are subjects to many attacks. Usual attacks to be stopped are Denial of Service (DDoS) attacks and Third-Party attacks. Security should be guaranteed into IoT applications (such as smart home or intelligent traffic), and platforms for support, such as cloud computing should be monitored and secured.

## 6. Security issues in IoT

### 6.1. IoT Security Requirements

Traditionally, security requirements can be broken down into three main categories: (i) confidentiality, (ii) integrity, and (iii) availability, referred to as the CIA-triad [9]. Confidentiality

means limiting the access of certain information only to authorized parts. It is necessary in the IoT context especially regarding applications where information is critical, e.g. Health, finance. Integrity ensures that the received commands and information have not been changed. In case of an error, dramatic consequences could happen, mainly in Things working closely with human lives. Finally, availability ensures that all system services are available, when requested by an authorized user. These basic security principles (Confidentiality, Integrity and Availability) must be ensured by services and mechanisms adapted to the field of IoT.

Table 1. Security threats facing objects by lifecycle [15].

	Manufacturing	Installation	Operation
<b>Applications / Services</b>		Eavesdropping & Man-in-the-middle	Eavesdropping & Man-in-the-middle
<b>Gateways</b>		Eavesdropping & Man-in-the-middle	DDoS Attack, Routing attacks
<b>Devices</b>	Device cloning	Substitution	DDoS attack, Privacy threat, Extraction of security parameters

When investigating IoT security, there are also important requirements that need to be taken into consideration such as privacy, identity management, trust, End-to-End Security, authentication and access control. They are the main security issues which are to be addressed [10-13]. IoT implies “things”. They are the principal component of this technology. Heer et al. [14] have defined the lifecycle of a thing. Each object has three cycles which are: Manufacturing, installation and operation and there are vulnerabilities and threats facings objects during their lifecycle. Table 1 below summarizes different threats affecting the objects during each cycle with respect to the architecture we have defined in Figure 2.

On another side, when talking about security, an important related notion must be also introduced; Context awareness. In order to define different degrees of security, the context is an important factor to be taken into consideration. The object might indeed be secure in a given context, but exposed to threats in another. As objects are set to be autonomous in IoT, they should be aware of their context themselves. This is context awareness. Formally defined “a system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user task “[2]. When relating to security, we must think that as “smart” objects, security standards for things should vary depending on the context, as those objects are supposed to be context-aware. It is also important to know that context-awareness raises privacy issue. A device that is in fact aware of its context possesses a number of information that can

be valuable. Moreover, context-awareness poses an energetic challenge since the device needs to have constant and updated information, which affects its energy consumption.

Let us now study in deep those issues with the help of the architecture that was introduced in the previous section (Figure 2).

## *6.2. Applications/Services security issues*

### **Attacks on the cloud**

Clouds are nowadays mobile databases. Moving to cloud technology is more and more frequent, and even IoT follows this trend. Many IoT solutions have already connected platforms to the cloud such as Bolt [16] providing data management for the Lab of Things (LoT) [17] by using Amazon S3 or Azure for Data storage. Ninja Sphere [18] and Smart-Things Hub [19] do also deploy their solution of the cloud. It seems in fact easier and more practical to have a database on the cloud for IoT applications, in order to access data wherever the objects are. However, clouds are more subject to various kinds of attacks, given their centralizing role.

Many critical reports (Internet of Crappy Things, Internet of Fails, FTC technical reports) have emphasized security in IoT spaces [20]. By centralizing IoT in clouds, and given the present vulnerabilities, the risk of accessing information that can be confidential is even bigger. This might be of negative consequences especially if it is on a big scale or sensitive information (military, financial, etc.).

### **Service Interruption**

DDoS attacks are a very common issue on the Internet, but they need also to be solved in an IoT context. Sonar et al [21] have surveyed these attacks on IoT. DDoS attacks on IoT can affect different layers, (perception, network or application). These attacks cause service interruption, as the cloud server becomes unresponsive, but they can also end on extremely slow response that leads to a deterioration of service quality.

Service interruption in IoT can also happen due to different other factors. Some of these interruptions have been investigated, such as trojans in IoT [22] and various viruses (Stuxnet [23]).

### **Third party attacks**

Weber [24] defines Privacy Enhancing Technologies (PET) as technologies developed in order to achieve information privacy goals. They include Virtual Private Networks (VPN), Transport Layer Security (TLS), DNS Security Extensions (DNSSEC) or Peer-to-Peer (P2P). These technologies are not completely protective in the case of IoT. Certain situations of IoT such as positioning do still present privacy problems [25]. Some malicious third party can in fact access a user's location information and use it for malicious activities. Location information can be extracted for example from sensors and actuators while communicating.

Not only location can be hacked, but more sensitive information: Income or health status...As IoT chips can rely on RFID, they can also be subject to attacks getting private information.

## *6.3. Gateway related security issues*

The gateway is related to the network and how data is transported. Network security is an essential part in protecting data in IoT. Regarding transport aspect, IoT is using the same standards as Internet, issues will then be similar. It presents the following security issues:

### **Wi-Fi security**

The most used wireless standard is Wireless Fidelity (Wi-Fi). Wi-Fi users can encounter different kind of security threads, such as phishing websites. DDoS attacks can also happen on Wi-Fi and flood the network [21].

Access is also important for Wi-Fi. Not everybody can access a Wi-Fi network, but only those having the password. The problem is as we saw that in IoT not all "objects" have a user interface, or keyboard. How could we write a password in a smart T-shirt that only contains a chip with sensor?

Moreover, if the Wi-Fi network is not properly securitized, there is a risk that a connected object in a given network can access to other objects in the same network. It is a very frequent issue on Internet nowadays, and is certainly threat even for IoT security.

### **Other standards**

Third Generation (3G) networks present also certain vulnerabilities. They are for instance subject to DDoS attacks, phishing attacks and identity attacks [5].

## *6.4. Devices security issues*

### **Heterogeneity in technologies**

As we have seen earlier, IoT is a technology that allows all sorts of objects to connect. By doing so, heterogeneity issue is raising even in Security matters. There is for example no uniform international encoding standard for RFID tag; this can create access problems or errors in reading process for the user [2]. Not only tags are different, but even data itself. Data can come with different or even incompatible formats. This can result in data loss or destruction, causing privacy exposure. There should be a process of unification of formats and protocols in order to guarantee a better security in IoT.

### **Encryption**

Encryption is one of the fundamentals of the modern internet security. Information cannot be send directly (or it can be intercepted on the way and be potentially misused from malicious parties). Encryption is the part where information is coded with the help of a key into another series of characters. Only parts with

the key can retrieve the original message and read it. Unfortunately, the classical encryption algorithms and standards cannot be applied for the IoT.

Many “things” do not support those algorithms that require a big memory. The “things” were in fact not designed in the first term to be connected, but rather to fulfill their natural function (clothes, walls, fridges...). This does not mean that those objects do not need to be protected, on the contrary, it is necessary. One of the suggestions given to encrypt data in IoT is then Lightweight cryptography.

The term “lightweight” should not be mistaken with weak (in terms of cryptographic protection), but should instead be interpreted as referring to a family of cryptographic algorithms with smaller footprint, low energy consumption, and low computational power needs, which will resolve both energy and security challenges.

Examples of uses of lightweight cryptography in IoT are authentications schemes [26-27] or device management [28-29]. Lightweight cryptography contains different sorts of algorithms that can be used, all of them are under studies, one can give as examples: Symmetric ciphers for lightweight crypto, asymmetric ciphers and homomorphism.

**Trust Management**

Trust is an important and necessary criterion in all transactions. It is defined as “the measurement of the belief from a trusting party point of view (trustor) with respect to a trusted party focused on a specific trust aspect that possibly implies a benefit or a risk” [30].

Technology and IoT are not an exception, and exchanges in IoT should all come from and to trusted parts. However, heavy encrypting and complex computing are not possible in IoT. This means that the trust system should be simple, but efficient. During the authentication period, user should easily be able to login, while having a secure system in front of him. This can be difficult as it looks as a paradox.

A secure system is usually complicated and difficult to use for a novice user, while a four number PIN code is rather easy to break and presents a weak security model. Then, one challenge research is highlighting is to invent new rich authentication mechanisms, that can be used for IoT, having a better security, but also being simple for use for any costumer and supported by the sensors.

**Secure Routing Protocols**

As IoT is limited in power and computing abilities, classical routing protocols can unfortunately not be used. One of the most important challenges is to design new secure routing protocols for Wireless Sensor Networks, as routing is a vital part of networking, and attacks toward a weak routing protocol can lead to the whole network collapse.

*6.5. IoT Security Threats and Attacks*

In Section 5, we have defined a reference model to analyze IoT security aspects. The model proposed to break down IoT into [www.astesj.com](http://www.astesj.com)

three different layers: Devices, Gateways and Applications / Services. In the current section, we have separately presented threats and attacks related to each specific layer.

Table 2. IoT Security Attacks by layer.

	Device Layer	Gateway Layer	Applications / Services Layer
<b>Threats / Attacks</b>	Heterogeneity in technologies	Wi-Fi related Attacks	Attacks on the Cloud
	Encryption	3G related Attacks	Service Interruption (DDos Attacks, Virus, Trojan, etc.)
	Turst Management	RFID Attacks (Spoofing , Cloning, Unauthorized Access)	Third Party Attacks
	Secure Routing Protocols	Man in the Middle [33]	Spyware, Adware [36]
	Node Tampering [31]	Sybil Attack [34]	Side Chanel Attacks [37]
	Physical Damage	Sinkhole Attack [35]	Cryptanalysis Attacks [32]
	Social Engineering [32]		

In order to summarize our work, we present Table 2 below that gathers different attacks and security threats facing IoT through its different layers. The table includes also some attacks that were not presented in this work. Due to constraints, we have in fact chosen to limit us to a number attacks for this article. Readers wishing to deepen their knowledge about the other attacks can investigate the references attached to them in the table.

**7. Conclusions and future work**

Internet of Things is for sure an amazing and exciting area, with many challenges ahead. We have first defined formally IoT and discovered its specificities. Then we detailed its main differences with the classical Internet. Understanding those differences is the key to specify the areas of challenges that IoT will face. After a general presentation of those challenges, we went into a suggested reference model to analyze security of IoT. The architecture of this model helped us to exhibit security issues that are hanging until now.

In this article, the aim was to give a general image of IoT, with a special focus on security. Our planned future work will be on the Lightweight security solutions. As objects in IoT do not support complex computing, and as cryptography is still important to securitize data, we would like to study on the future Lightweight cryptography algorithms. This is in fact an ongoing research issue that can be of high interest for the scientific community, and we would like to participate with our little contribution in this huge project of IoT.

## References

- [1] C. Perera, A. Zaslavsky, P. Christen, D. Georakopoulos, "Context Aware Computing for The Internet of Things: A Survey". *IEEE Communications Surveys & Tutorials* (May 2013).
- [2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelffl, "Visions and challenges for realizing the internet of things, Cluster of European Research". *Projects on the Internet-of-Things (CERPIoT)*, 2010).
- [3] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, "Internet of Things: Vision, Applications and Research Challenges". Volume 10, Issue 7, pp. 1497-1516, *Ad Hoc Networks*, (September 2012).
- [4] S. Madakam, R. Ramaswamy, S. Tripathi "Internet of Things (IoT): A Literature Review". *Journal of Computer and Communications*, 2015, 3, pp. 164-173
- [5] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, "Security of the Internet of Things: perspectives and challenges". Volume 20, issue 8, pp. 2481-2507. *Wireless Networks* (November 2014).
- [6] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [8] "The Internet of Things reference model." CISCO, 2014. [Online]. Available: [http://cdn.iotwf.com/resources/71/IoT\\_Reference\\_Model\\_White\\_Paper\\_June\\_4\\_2014.pdf](http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf)
- [9] A.M. Nia, N.K. Jha, "A Comprehensive Study of Security of Internet-of-Things". Volume: PP, Issue: 99, *IEEE Transactions on Emerging Topics in Computing* (September 2016).
- [10] N. Parikshit Mahalle, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things", *Journal of Cyber Security and Mobility*, Vol. 1, 309–348. 2013.
- [11] Guanglei Zhao, "A novel mutual authentication scheme for Internet of Things". In *Proceedings of 2011 IEEE International Conference on Modelling, Identification and Control (ICMIC)*, pp. 563–566, 26–29 (June 2011).
- [12] C. Mayer. "Security and privacy challenges in the IoT". *WowKivs, Electronic Communications of the EASST*, Volume 17, Germany (2009).
- [13] "Internet of Things: privacy and security in a connected world", *US Federal Trade Commission, Staff report*, 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>
- [14] T. Heer., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S. and Wehrle, K., 2011. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, 61(3), pp.527-542.
- [15] C. Lu, "Overview of Security and Privacy Issues in the Internet of Things", May 2014
- [16] T. Gupta, R.P. Singh, Mahajan, A. P. J. J. R. Bolt: Data management for connected homes. In *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)* (2014), pp. 243–256.
- [17] A. Brush, E. Filippov, D. Huang, J. Jung, R. Mahajan, F. Martinez, K. Mazhar, A. Phanishayee, A. Samuel, J. Scott, Et al." Lab of things: a platform for conducting studies with connected devices in multiple homes". In *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication* (2013), ACM, pp. 35–38
- [18] Ninja Blocks. <https://ninjablocks.com/>.
- [19] SmartThings. <http://www.smartthings.com/>
- [20] B. Zhang, N. Mor, J. Kolb, D.S. Chan, K. Lutz, E. Allman, J. Kubiawicz, (2015, July). "The Cloud is Not Enough: Saving IoT from the Cloud". In *HotCloud*.
- [21] K. Sonar, H. Upadhyay (2014). A survey: DDOS attack on Internet of Things. *International Journal of Engineering Research and Development*, 10(11), 58-63.
- [22] C. Liu, P. Cronin, C. Yang (2016, January). "A mutual auditing framework to protect IoT against hardware Trojans". In *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific* (pp. 69-74). IEEE.
- [23] M.M.M. Dakhani, M.Z.A.I. Dakhani,(2017). Another Way to Deal with Research Privacy in the IOT: Threats and Assaults on IOT and its Solutions.
- [24] R. H. Weber,"Internet of Things – New Security and Privacy Challenges", *Computer Law & Security Report* (January 2010).
- [25] M. Elkhodr, S. Shahrestani, H. Cheung (2013, April). The Internet of Things: vision & challenges. In *TENCON Spring Conference, 2013 IEEE* (pp. 218-222). IEEE.
- [26] M.A. Jan, P. Nanda, X. He, R-P. Liu (2016). A lightweight mutual authentication scheme for IoT objects. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, "Submitted".
- [27] J.Y. Lee, W.C. Lin, Y.H. Huang (2014, May). A lightweight authentication protocol for internet of things. In *Next-Generation Electronics (ISNE), 2014 International Symposium on* (pp. 1-2). IEEE.
- [28] T. Perumal, S.K. Datta, C. Bonnet (2015, October). IoT device management framework for smart home scenarios. In *Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on* (pp. 54-55). IEEE.
- [29] Y. Jin, M. Tomoishi, N. Yamai (2017, July). A Secure and Lightweight IoT Device Remote Monitoring and Control Mechanism Using DNS. In *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual* (Vol. 2, pp. 282-283). IEEE.
- [30] R. Neisse, M. Wegdam, M. Van Sinderen "Trust management support for context-aware service platforms". In: *User-centric networking, lecture notes in social networks*. Springer international; 2014. p. 75-106.'
- [31] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks." *Communications of the ACM* 47, no. 6 (2004): 53-57.
- [32] I. Andrea, C. Chrysostomou, G. Hadjichristofi, 2015, July. Internet of things: Security vulnerabilities and challenges. In *Computers and Communication (ISCC), 2015 IEEE Symposium on* (pp. 180-187). IEEE.
- [33] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges." *International Journal of Computer Science and Information Technology & Security (IJCSITS)* 1, no. 2 (2011): 136-146.
- [34] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259-268. ACM, 2004.
- [35] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network." *International Journal of Application or Innovation in Engineering & Management* 2, no. 2 (2013).
- [36] Y.J. Jia, Q.A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, A. Prakash, S.J. Unviersity, 2017. ContextIoT: Towards Providing Contextual Integrity to Applified IoT Platforms. In *Proceedings of the 21st Network and Distributed System Security Symposium (NDSS'17)*.
- [37] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer Verlag, 2007.