Towards Understanding Internet of Things Security and its Empirical Vulnerabilities: A Survey

Salim El Bouanani[1], Omar Achbarou[2], My Ahmed Kiram[3], Aissam Outchakoucht[4]
Computer Science Dept, Cadi Ayyad University, Marrakesh, Morocco[1, 2, 3]
LISER laboratory, Hassan II University, Casablanca, Morocco[4]

***Abstract*—The Internet of things is no longer a concept; it is a reality already changing our lives. It aims to interconnect almost all daily used devices to help them exchange contextualized data in order to offer services adequately. Based on the existing Internet, IoT suffers indisputably from security issues that could threaten its evolution and its users' interests. Starting from this fact, we try to define the main security threats for the IoT perimeter and propose some pertinent solutions. To do so, we first establish a state of the art concerning the IoT definition, protocols, environment, architecture and security. Then, we expose a case study of a standard IoT platform to illustrate the impact of security on all IoT layers. Furthermore, the paper presents the results of a security audit on our implemented platform. Finally, based on our evaluation, we highlight many solutions as well as possible directions for future research.**

Keywords—Internet of things; IoT security; security audit; IoT architecture; IoT protocols

I. Introduction

After Ashton introduced the internet of things (IoT) for the first time [1], the concept really took shape with the MIT Auto-ID [2] and their presentation of the IoT vision. In the IoT world, any daily device can be transformed to a "smart thing" or "smart device" if it could be equipped by an IP address [3], thus accessible like any other connected computer. According to Cisco Internet Business Solutions Group [4], IoT is simply defined as the point in time when more "things" were connected to the Internet than people. In fact, IoT connects humans and a huge number of devices as never before, basically sensors and actuators. In this sense, the group predicts that there will be 50 billion connected devices by 2020. This great number of "things" tends to transform the three dimensions related to information processing [5], namely "location, time and manner", since information can be processed by people, devices or services.

This democratization (i.e. openly available to almost everyone) and interconnectivity helps provide processes with precise data to make optimal decisions. From this point, we notice that several new realities emerged such as smart grids, smart homes, smart cities, etc. "Smart environments" are made possible thanks to the IoT paradigm which helped the emergence of communication protocols, embedded sensors, and smart physical objects that collect and process data in real time. In this context, the Internet with billions of connected devices gathering contextualized data and having actuating ability can be considered as sensory, which means that it provides the ability to become more proactive thanks to their ubiquitous connectivity to the Internet.

However, this evolution doesn't remain without weaknesses; the pervasive paradigm established by the IoT can be seen as a huge, complex and risky zone where the previously cited advantages can quickly become drawbacks. Actually, this technology is facing serious challenges [6] such as heterogeneity, security, privacy, access control, IPv6 transition, power supply, massive data storage and processing, etc.

This paper mainly answers the following fundamental questions:

- What are the most significant IoT security challenges to address?
- To what extent the usual audit techniques can be used in IoT environments?

To the best of our knowledge, there is no paper that answered these questions from a practical perspective. This article is implementing an IoT based platform, on which we performed an audit to come up with empirical solutions.

Focusing on security issues in the IoT, we can assert that they are not only related to threat diversity, but are also the results of the various vulnerabilities. To secure IoT environments, many studies have to be led in order to enumerate risks that have to be covered. In fact, many researches were focused on tracking not only the vulnerabilities of IoT devices but also the potential threats that can exploit them [7, 8, 9, 10] and the conclusions of these researches were alarming.

The pervasive aspect of the IoT environments make them present everywhere with many interconnected devices whose security and privacy issues could have a significant impact in our daily life.

In the following sections, we will define the IoT, then we will focus on detailing the IoT environments and security. Moreover, we choose a case study of a generic IoT infrastructure on which we will apply a security audit, a risk analysis and several attacks to finally come out with solutions and recommendations as a concrete and logical result to ameliorate IoT security.

II. Overview of the Internet of Things

Day after day, the Internet is getting larger due to thousands of newly connected "smart objects". In this section, we take a deep look at this paradigm, its standards, protocols and application domains, all from a security perspective.

A. The Internet of Things Paradigm

There is no unique accepted definition for IoT. In this paper, we tried to propose a definition that seems relevant and global, based on literature review [5, 11, 12, 13] we define IoT as a global infrastructure of networked physical and virtual objects. These intelligent electronic devices ("smart things") should have a unique identity as well as the ability to transfer/receive data over networks using interoperable technologies offered by Internet protocols. The IoT as a ubiquitous network is founded on four major pillars namely sensing, communicating, processing and actuating.

In the next subsection, we will explore how IoT will be present almost everywhere in our daily life: smart cars, smart cities and E-Health applications, etc.

B. Application Domains

One aspect of the Internet transformation is that it benefits from sensory abilities that help it become more proactive. This goal is achieved through the cooperation of many sensors – measuring temperature, motion, pressure, etc. – and actuators that perform the right tasks according to the situations – turning on an air conditioner, ringing an alarm, weight sorting, etc.

In Table I, we modified three mostly used application domains categories [5] into four by adding "Healthcare" to "Industry", "Environment" and "Society". The importance of this category is due to the growing interest in healthcare applications based on huge investments to develop objects that take care of people's health.

Given the intersections between IoT and all these diverse domains, several protocols and standards were proposed to facilitate and simplify their implementations. Below, we focus on some commonly used ones.

C. Protocols and Standards

It is known that most IoT devices are constrained devices, these latter will require energy saving, less computations and a minimum of network connectivity, thus, using HTTP protocol [12] is no longer convenient since its request needs at least nine TCP packets, even more when we consider packet loss from poor connectivity. HTTP is not the only protocol that can no longer be used in IoT environments.

In Fig. 1, we present some protocols and standards IoT oriented that can replace traditional network protocols organized following the TCP/IP Layers.

TABLE. I. IoT CATEGORIES AND SUB CATEGORY DOMAINS

Category	Application domains
Industry	Retail, transportations, manufacturing, logistics, industrial control, telecommunications
Healthcare	Smart Health, e-Health, activity monitors
Environment	Smart environment, smart agriculture, smart animal farming, domestic automation
Society	Smart cities, security and emergencies, social networking

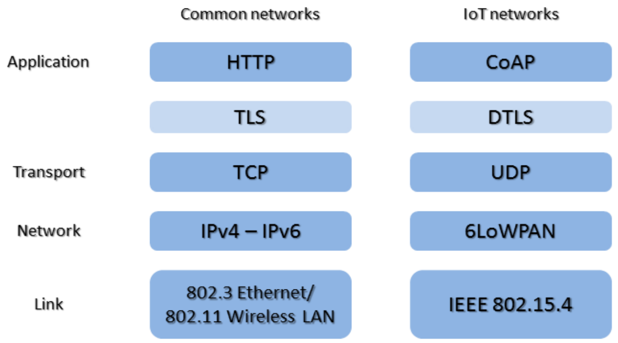


Fig. 1. Difference between Traditional and IoT Networks.

Depending on the need, both TCP and UDP could be used in the transport layer; however, we recall that UDP is simpler and faster than TCP. Consequently, using UDP is advantageous in the environments where reliability is not a priority; nevertheless, there are numerous situations where TCP is mandatory. Also, we mention that both TCP and UDP segments are not encrypted so it is strongly recommended to use TLS/DTLS for communication security (Note that DTLS is a TLS-like protocol, but unlike this latter, DTLS is based on UDP).

In the application layer, many IoT-oriented protocols are available; e.g. CoAP for Constrained Application Protocol [14] as an alternative to HTTP in IoT environments, or MQTT for Message Queuing Telemetry Transport [15] that can replace HTTP too when TCP is required. Here is an overview of these two widely used protocols:

CoAP [16]: It is a web transfer protocol for resource constrained devices and networks. It is built on top of UDP and follows the REST paradigm. There exist many implementations of this extremely lightweight protocol, each of these with its own particular features and requirements.

MQTT [17]: It is a publish/subscribe messaging protocol based on a client/server model where a broker (server), receives messages from all the other nodes. Its resulting flexibility and simplicity enable the connection of embedded devices to middleware and applications.

At the network layer level, there is the 6LoWPAN standard for IPv6 Low Power Wireless Personal Area Network [18] and we find the IEEE 802.15.4 standard [19] in the link layer. The increasing number of objects can no longer be managed by the IPv4's address ranges, also the IoT devices (sensors, actuators and constrained objects) need an internet protocol that could manage low-power devices with limited processing capabilities. That is why the transition to IPv6 is an evidence. The importance of 6LoWPAN as an application reside in allowing IPv6 packets to be sent and received over IEEE 802.15.4 based networks.

Hereafter in Table II, the previous cited protocols and standards with their security options.

Undoubtedly, IoT systems could be built over familiar web technologies, though the result would not be as efficient as the newer protocols and standards that are adapted to the IoT.

TABLE. II. IoT PROTOCOLS AND STANDARDS

Protocol & Standard	Description	Security
MQTT	- Simple and lightweight messaging protocol - Publish/subscribe architecture - Relies on TCP as transport protocol - Use broker - More mature and stable	- No encryption by default - Username and password are required for authentication - TCP connection may be encrypted with SSL/TLS
CoAP	- RESTful application protocol for constrained nodes and networks - Client / server architecture - UDP-based transport protocol - Still evolving	- No encryption by default - SSL/TLS are not available to provide security - Use Datagram Transport Layer Security (DTLS) for encryption - DTLS permit CoAP devices to support RSA and AES or ECC and AES
6LoWPAN	- Allow transmission of IPv6 Packets over IEEE 802.15.4 Networks - Guarantee the encapsulation and compression of IPv6 packets.	- Security of 6LoWPAN is defined at the link layer by IEEE 802.15.4. -Unlike in IPv6, IPsec is not suitable to use in IoT/6LoWPAN environments given their constraints.
IEEE 802.15.4	- Communication protocol for low rate wireless personal area networks (LR-WPAN) - Used by many implementations based on proprietary protocols such as ZigBee or 6LoWPAN. - Its architecture is defined in terms of layers; each layer is responsible for a part of the standard and offers services to the higher layers.	- The 802.15.4 specification provides security functions at the link layer: access Control, messages integrity, messages privacy and protection against replay attacks. These elements are set at the security-enabled field in the MAC frames. We can enable one, several or all the functions, based on encryption algorithms AES.

III. Internet of Things Environments

The IoT relies on open architecture to maximize interoperability among heterogeneous systems and distributed resources. This architecture has to fulfil some security requirements, especially confidentiality, integrity and availability. In this section, we present the basic IoT architectures as shown in Fig. 2:

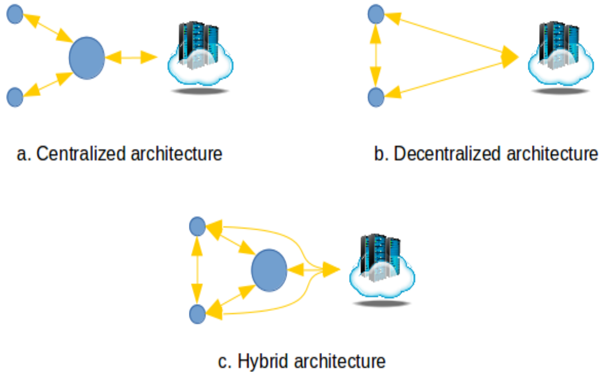
A. *Internet of Things Architectures*

In IoT environments, three main IoT architectures are frequently adopted [20]:

Centralized architecture (Fig. 2(a)): where end devices pass through gateways (more powerful nodes) for every communication whether with other objects or with the Cloud.

Decentralized architecture (Fig. 2(b)): every end device is autonomous; it is fully capable of managing its communications without any intermediate device.

Hybrid architecture (Fig. 2(c)): combines the two previous ones [21], gateways manage some features (i.e. security mechanisms) while the end device deals with the rest.



a. Centralized architecture

b. Decentralized architecture

c. Hybrid architecture

Fig. 2. IoT Architectures.

B. *Standard Internet of Things Architecture*

On the basis of conducted literature review, hybrid architecture is used in the case study that we are presenting in this paper. This architecture provides more flexibility, reliability and availability, which are mandatory requirements for reliable platforms. Fig. 3 details the various components of this architecture [22], which are the cloud, the mobile and the IoT devices.

Actually, in the cloud component, four layers are defined. First, the application layer then the repository layer for files; next we find the middleware to manage communications and finally the link layer where communication protocols are used.

For the gateway sensor, it was pertinent to add a device API layer below the middleware, where sensor and actuator protocols will be defined, and the optional embedded OS layer. Finally, the link layer hosts several protocols and standards such as Bluetooth, Wi-Fi, IEEE 802.15.4 for constrained devices/networks, etc.

It is worth noting that BT, BT LE (Bluetooth Low Energy), Zigbee, and NFC are lightweight standards and protocols.

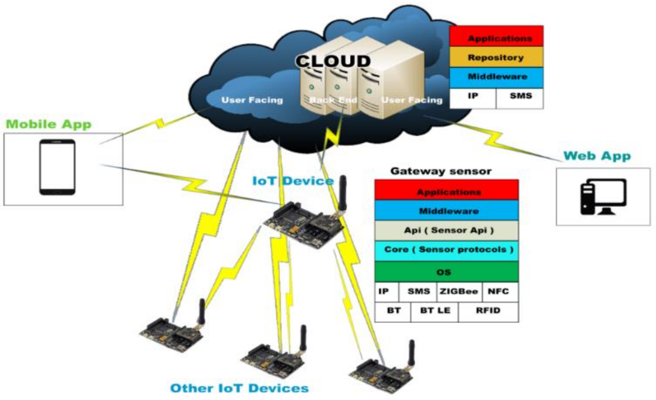


Fig. 3. Internet of Things Standard Architecture in Detail.

C. Internet of Things Security

Jointly to the IoT exponential evolution, threats in IoT remain critical and various. Indeed, many security issues have to be solved in network protocols, data and identity management, user privacy, access control models, etc. These vulnerabilities are mainly due to the fact that connected devices are designed to be easily and quickly deployed (reducing the Time-to-Market) and accessed by users who are little informed on the IoT risks. Hence, reducing the costs of research and development on security makes this domain an accessory where it should be a priority.

Recently, academic research targeting the privacy and security for IoT environments has gained more momentum. The survey papers [23], [24], [25], [26], and [27] evaluate the possible threats to IoT systems according to the layers and the available countermeasures. The present paper focus on IoT security with a more methodical and formal tools beginning with the proposition of a standard IoT architecture suitable for security needs, then by conducting a security audit covering the whole environment and finally by the reputed EBIOS risk analysis. Up to our knowledge, there is no paper that has adopted this procedure to evaluate and recommend solutions to IoT security issues in such a holistic manner.

In order to discuss security issues, we introduce the CIA model, which relies on three pillars "Confidentiality, Integrity & Availability" [10] briefly explained hereafter:

Confidentiality refers to the ability to protect data from unauthorized parties.

Integrity refers to the ability to prevent our data from being changed or deleted in an unauthorized or undesirable manner.

Availability: It is the ability to access our data when and where it's needed.

Concretely, we will distinguish three main areas in the IoT environment to facilitate our security audit, namely:

- The IoT device (e.g. sensor, actuator, smartphone, people)
- The Network (e.g. LAN, Internet)
- The Cloud: platform for storing, treating and analyzing data.

IV. Case Study of a Standard Internet of Things Platform

To be more concrete, and without losing generality, we decide to focus on one (generic) scenario and to work methodically to explore its security requirements.

In Fig. 4, we expose the fundamental components of our standard IoT environment. We tried to have a generic IoT platform with basic operations very similar to the majority of existing platforms to be able to have global results. For our case, our platform can be considered as a temperature detection platform with actuating and notifying abilities.

We have objects collecting temperatures continuously – unavailability is not tolerated, in addition to the cloud platform responsible for managing and analyzing collected data and sending notifications when temperatures exceed some thresholds. To increase availability, we placed a central less-constrained node allowing us to have hybrid architecture. More components are added to the architecture to enrich it – smartphones, PCs, a router etc.

A. Environment Architecture

We opted for the standard IoT architecture as mentioned in the subsection B.2 due to its availability and flexibility advantages. Indeed, if the cloud platform fails, the external entity (a minimum level of service) will be guaranteed by the nodes, in order not to paralyze the whole IoT environment. Also, we can use the central node, more powerful than other IoT devices, for tasks that require more computing and to orchestrate our environment.

We used ThingSpeak as an IoT cloud platform. It helps us to visualize the behavior of temperature data, to use various mobile applications in order to control our objects (e.g. Blynk), and to view data behavior (e.g. ThingView on Android).

B. The Components

During the implementation of the platform, we made some technical choices that are shown in Fig. 5. This latter presents a sample of the IoT constrained nodes, IoT less constrained ones, sensors and actuators that we actually implemented in our architecture:

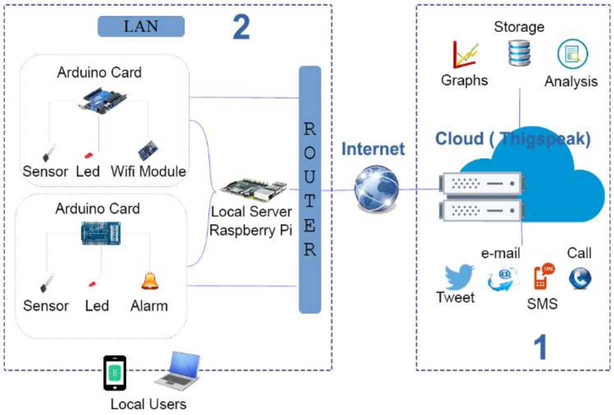


Fig. 4. Environment Architecture of the Case Study.

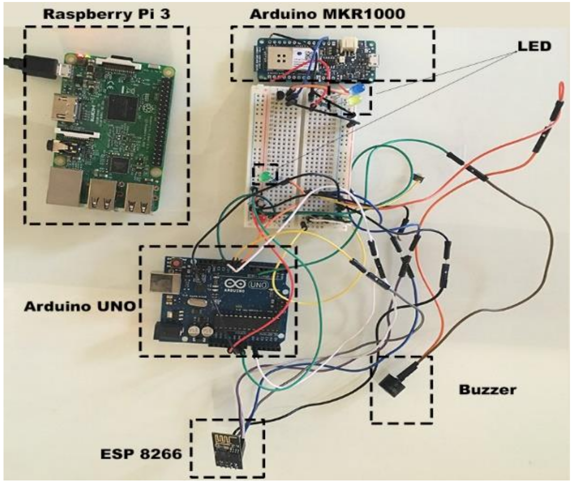


Fig. 5. Our IoT Environment Components.

1) The micro-controllers: They are integrated circuits that gather the essential elements of a computer: processor, memory, peripheral units and input-output interfaces. Micro-controllers are characterized by a high degree of integration, lower power consumption, lower operating speed and reduced cost compared to microprocessors used in personal computers. We opted for Arduinos.

2) The central node: The Raspberry Pi is a nano-computer board that allows the execution of several operating systems GNU/Linux and compatible software. The operating system used in our case study is the Raspbian. In the Raspberry, we installed our local server that will be discussed in following subsections. In Table III, we expose a brief comparison between the investigated nodes and a smartphone as reference, in terms of performances and capabilities. It shows clearly that the Raspberry has similar computational capabilities, which is the reason why it is a central node in our architecture, as a device that can be considered less constrained compared to the Arduinos or microcontrollers.

C. The Organogram

In this section, we present how the whole IoT environment works in (see Fig. 6). We can identify three sections in our system:

1) Object-level: An internal process within the IoT node determines if the temperature exceeds the threshold value; if so, the alarm sounds and a red LED light up.

2) Central node level: The data sink collects information, then applies some availability and integrity verification functions. An SMS is sent to the administrator in an error context.

TABLE. III. COMPONENT PERFORMANCES IN COMPARISON TO A SMARTPHONE

Objects	RAM	CPU
Arduino UNO	2KB	16 MHz | 8-bit architecture
Arduino MKR1000	32KB	48MHz | 32-bit architecture
Raspberry Pi	1GB	Quad-core | 1.2 GHz | 64-bit architecture
iPhone 6	1GB	Dual-core | 1.4 GHz | 64-bit architecture

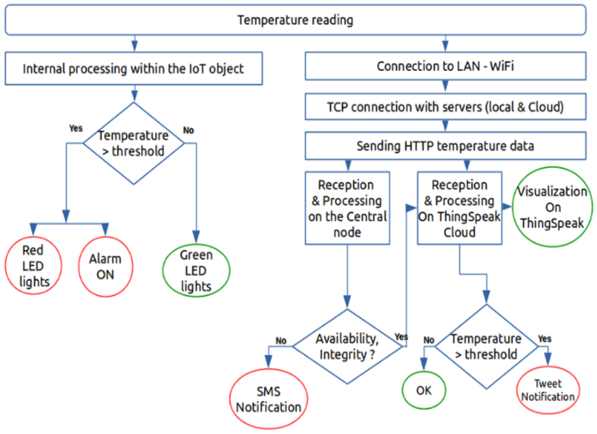

Temperature reading
Internal processing within the IoT object
Connection to LAN - WiFi
TCP connection with servers (local & Cloud)
Sending HTTP temperature data
Yes
Temperature > threshold
No
Reception & Processing on the Central node
Reception & Processing On ThingSpeak Cloud
Visualization On ThingSpeak
Red LED lights
Alarm ON
Green LED lights
No
Availability, Integrity ?
Yes
No
Temperature > threshold
Yes
SMS Notification
OK
Tweet Notification

Fig. 6. Organizational Chart of the Case Study.

3) Cloud: On ThingSpeak cloud platform, we also configured actions of sending tweets to the accounts dedicated to our IoT environment, the manager will be tagged in the tweet mentioning that the temperature exceeds the threshold.

You can refer to our repository in GitHub [28] for the code of this implementation and other technical details.

V. SECURITY AUDIT AND RISK ANALYSIS

In this section, we introduce and lead a security audit jointly with a risk analysis on our case study. This approach will provide us with a transparent exploration of the IoT environment security.

A. Importance of the Security Audit

In the IT domain, people always pretend that their systems are secure; however, one of the most effective ways to determine whether this is true is by performing a thorough audit of the whole system. Thus, audit and information security should work together synergistically. The information security designs, implements and applies various procedures and protocols to protect the organization's information resources, while audit provides periodic feedback and suggestions in order to improve that security.

Symantec considers that security audits do not take place in a vacuum [29]; they are part of the on-going process [30] of defining and maintaining effective security policies. Otherwise, security audits provide such a tool as a fair and measurable way to examine how secure an “IT system” really is. These audits become more exigent when these systems are much more complex and interact with various other domains opening larger surface vulnerabilities, which is the case for our IoT environments.

B. Risk Analysis

It is hard to study and manage the systems’ security without using a risk management methodology. In fact, security measures are not able to assure 100% protection against all threats. Therefore, risk analysis, which is the process of evaluating system vulnerabilities and the threats facing it [31], is an essential part of security management as it provides concrete results based on a scientifically approved approach.

In our study, we opted for EBIOS (Expression of Needs and Identification of Security Objectives) methodology since it provides a global and consistent view of information systems security. Moreover, EBIOS [32] has a uniform vocabulary and concepts; it also allows exhaustive coverage with determination of suitable security objectives and requirements. It is a method for analyzing, evaluating and acting on risks relating to information systems. It generates a security policy adapted to the needs of an organization and includes the five following steps:

The first step handles the context establishment, the relationship between the business context and the IS, contribution to business goals, boundary, decomposition, etc. Then, security requirements are determined based on the feared security events. Next, a risk study is conducted in order to identify and analyze threat scenarios. In the fourth step, information from the previous phases is used to identify risks and describe the necessary and sufficient security goals relating to these risks. Finally, the essential security requirements are determined as well as the exhibition of the perfect coverage of security objectives. These steps are described according to our platform in the next subsections:

C. Context Study

As mentioned before, our case study consists in setting up an environment, which includes all the elements taking part in an IoT ecosystem. First, it is necessary to identify the sensitive elements and the zones presenting security. The environment defines a hybrid architecture where smart objects are connected to each other, to a local central node and to a Cloud platform. The communication protocol used for sending the temperature values to the Raspberry Pi and ThingSpeak is HTTP. Smart devices can be controlled by smartphones and the system can autonomously trigger actions in an emergency context: alarms, SMS, Tweets. This environment is considered critical, so no unavailability or alteration is tolerated.

1) Expression of security needs: The target system being identified, we will express here the security needs. This step contributes to risk estimation and definition of risk criteria; it is based on the development and use of a needs scale as well as the identification of unacceptable impacts on the system.

In our study we treated confidentiality, integrity and availability as security criteria. For the first, we defined four levels (public, restricted, reserved and secret), then we opted for an integrity scale of three levels (no need for integrity, mastered and integrated). For the availability scale, we fixed four levels (no need for availability less than 72 hours, less than one hour and a real-time availability). In order to evaluate the risks, we have defined a 4-level gravity scale (negligible, limited, important and critical) and another for the probability (minimal, significant, strong and maximum).

We have divided our perimeter to six surfaces, which we evaluate according to the three security criteria fixed above, making 18 feared events with three criteria for each surface, namely:

The IoT object (1), information collection (2), local storage/treatment (3), information transfer (4), storage and processing of information on the Cloud (5) and actions (6). One of the first observations in this assessment is the criticality of the unavailability and alteration in most of the studied surfaces compared to confidentiality. This latter does not have a significant weight given the nature of the information exchanged (temperature) in our case.

2) Threat study: We estimated that threat scenarios will affect the following sub perimeters:

- IoT devices: consists of an Arduino board equipped with a temperature sensor, an actuator (LED / alarm) and a wireless module.
- Central Node: Raspberry board which hosts an apache web server.
- The staff: represents those who have access to the company buildings, namely the director, employees and trainees.
- The Wi-Fi LAN.
- Location: the location of the objects.
- Internet.
- Mobile applications: thanks to which the client can act on the object and where it will receive notifications describing the behavior of temperature values.
- The platform (ThingSpeak) that stores and analyses data and sends notifications by SMS, e-mail or Tweet.

Our evaluation allowed us to reach the most probable sources of the threats on our IoT environment, namely the mobile, LAN, staff and Cloud.

3) Risk analysis: We have established a list of 18 risks of unwanted events and previously appreciated threat scenarios. 12 unacceptable risks, 4 significant and 2 negligible. Risks previously analyzed (identified and estimated) are shown in Table IV. The risk matches those reduced by existing security measures, like use of surveillance cameras, use of WPA2, etc.

4) Determination of security requirements: Many security measures may be recommended, we cite the most relevant here: access control for IoT objects, passwords policy, encrypted protocols (HTTPS, CoAPS…), IDS/IPS and firewalls on LAN, updates, upgrades, choice of a Cloud platform, awareness, and qualifications and training of information security staff.

Once applied, we estimate that the risk levels will decrease in a considerable way, so that no unacceptable risk will remain. 14 will become negligible and only four significant risks remain, namely, the risk related to the modification of transferred information, which must stay unmodifiable; risk related to the modification of information in storage and treatment, which must stay unmodifiable; risk related to the modification of the IoT device, which must stay unmodifiable; and risk related to the unavailability of actions in real time.

5) IoT attack perimeters: Based on the OWASP's report, we were able to gather and limit these surfaces to four as shown in Fig. 7.

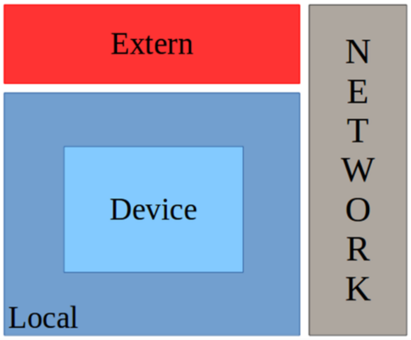


Fig. 7. IoT Attack Surfaces.

TABLE. IV. RISK EVALUATION

GRAVITY	4. CRITICAL		- Risk related to the unavailability of the IoT device in real-time. - Risk related to the modification of the central node. -Risk related to the modification of transferred information. - Risk related to the modification of information in storage and treatment. - Risk related to the modification of the action.	- Risk related to the unavailability of the IoT device in real time. - Risk related to the modification of the IoT device. - Risk related to the unavailability of captured information in real time. - Risk related the modification of captured information. - Risk related to the modification of the central node. - Risk related to the unavailability of the information transferred in real time. - Risk related to the modification of the information transferred. - Risk related to the modification of the information in storage and treatment - Risk related to the unavailability of actions in real time.	
	3. IMP		- Risk related to disclosure of secret central node contents. - Risk related to disclosure of reserved transferred information.	- Risk related to disclosure of reserved transferred information. - Risk related to the unavailability of the central node more than 1 hour. - Risk related to the unavailability of the information in storage and treatment, more than 1 hour.	
	2. LIMITED		- Risk related to disclosure of limited information in Cloud storage and treatment.	- Risk related to disclosure of public captured information. - Risk related to disclosure of limited information in Cloud storage and treatment.	- Risk related to disclosure of the IoT device beyond the stuff and the device owner. - Risk related to disclosure of public captured information.
	1. Neg.				- Risk related to disclosure of public actions.
		1. Min	2. Significant	3. Strong	4. Maximal
		Probability			
Negligible risks				Significant risks	Intolerable risks

Neg. stands for negligible; Imp. for important; *Min*. for minimum.

The Device: the key of any IoT architecture and its weak link, this surface regroups device memory, its physical/web interfaces, its firmware and its network services.

Local treatment: includes local storage, treatment and control.

Network: all communication traffic whether in LAN, MAN or WAN including ad-hoc networks and internet.

External treatment: includes all services that are traded outside the local network, especially Cloud and Third-party APIs, web-services, remote access and applications.

D. Security Attacks

Table V exposes the four IoT security layers summarized in the previous subsection. For each layer, we listed some well-known attacks, their impacts and then our recommendations to improve the security of the IoT environment related to these layers.

E. Security Solutions

Due to the generic aspect of our platform, we come up in Table VI with concrete suggestions and tangible recommendations towards a more secure IoT system. The implementation of these recommendations will satisfy the security goals of the whole IoT environment according to the CIA triad. The recommendations are categorized by their impact on one or more of these three pillars: confidentiality, integrity and availability.

Other solutions and best practices could be added [33,34] from the application of security standards as PCI-DSS, ISO/IEC 15408 and 2700x, etc. if the IoT environment is part of an information system already governed by established standards.

In addition to these recommendations, IoT environments should have an Information Technology Security Evaluation to ensure that their platform and things go through a formal security evaluation process, such as Common Criteria. An evaluation from a certified lab could enable the manufacturers of the IoT products to obtain an international security certificate.

TABLE. V. IOT ATTACKS BY LAYERS

Layers	Attacks	Impacts	Recommendations
Device layer	- IoT object theft / USB access - Disconnect the power - Run malicious software during the initial start-up process - Side channel attacks - Reverse engineering	- Malfunction of the smart object - Get hold of critical information - Sending incorrect information	- Implement secure booting so that the system only runs trusted software during the initial start-up process - Implement physical anti-theft solution (locks, cameras…) - Secure storage / tamper resistance
OS layer	- Break simple passwords - Privilege escalation - Buffer overflows - OS fingerprinting	- Uninstalling the system - Critical configuration changes	- Eliminate as many known vulnerabilities as possible (e.g. error configuration, simple passwords, improperly obtained higher permissions, buffer overflow) to minimize external intrusions to the system
App. layer	- DoS, DDoS - Backdoor / SQL injections - XSS - Virus / Trojan horses - Logic bombs / Worm	- Paralyze the whole system - Unauthorized access - Information steal - Sending false information	- Design security as part of the product, not separately - Apply secure coding principles, which minimize security vulnerabilities - Port optimization / firewall
Net-work layer	- Man in The Middle - Break simple passwords - Sniffing / Spoofing - DoS, DDoS/replication attacks - Routing attacks	- Critical information disclosure - Information alteration during transfer - Power cut - Use the identity of a legitimate user maliciously	- Integrate authentication and secure network access - Incorporate authentication and secure communications to prevent eavesdropping and ensure trusted communications between connected devices

TABLE. VI. SUGGESTED SOLUTIONS

Solutions	C	I	A
Access control to devices, network and Cloud	*	*	*
Security by design	*	*	*
Validation by a certified third-party trough evaluation process, such as Common Criteria	*	*	*
Encryption SSL/TLS, DTLS, ...	*	*	
Long, complex and periodically changeable passwords	*	*	*
Principle of least privilege	*	*	*
Internet protocol security (IPsec) and digital signature (e.g. ElGamal).	*	*	
Firewall, IDS/IPS and router control			*
Apply secure coding principles to avoid XSS, SQLI, buffer overflow…	*	*	*
Secure local network: WPA2 activation	*	*	*
Redundancy			*
Logging		*	
Hybrid architecture			*
Updates and upgrades	*	*	*
Choosing a secure Cloud platform	*	*	*
Disabling physical input-output: USB, SSD Cards …	*	*	*
Secure company building: authentication, cameras, fire protection devices			*
Administrator machine security	*	*	*
User and administrator awareness	*	*	*

VI. Conclusions and Perspectives

The IoT paradigm is certainly a big part of Internet evolution. Its main vision is to interconnect physical and virtual things based on evolving interoperable technologies. Nowadays, IoT is developing much faster than ever before; it will bring us opportunities in everyday aspects of life. However, it has also raised several new challenging issues, especially security problems that will slow down this evolution until we find the right solutions.

In this paper, we first presented the concept of the IoT paradigm, its application domains, protocols and standards. Then we detailed the main IoT architectures. After that, and to illustrate the impact of security in IoT environment, we opted for a standard case study on which we applied a security audit followed by a risk analysis as well as several attacks in order to provide adapted solutions to improve IoT security.

In our future work, we will explore the access control in IoT environments; first by analyzing the existing AC models and eventually we will propose a new one focusing on IoT context.

References

[1] K. Ashton, “That ‘Internet of Things’ thing in the real world, things matter more than ideas,” RFID Journal, 2009.

[2] MIT AUTO-ID Center, “Vision, Technology, Applications, ” Retrieved May 21, 2019, from http://web.mit.edu/supplychain/www/sp-iscm/repository/auto-id_103001.pdf, 2001.

[3] R. Want, S. Dustdar, “Activating the Internet of Things [Guest editors’ introduction],” Computer (Long. Beach. Calif), 2015.

[4] D. Evans, “How the Next Evolution of the Internet Is Changing Everything,” Cisco Internet Bus. Solut. Gr., 2011.

[5] H. Sundmaeker, P. Guillemin, P. Friess, Sylvie Woelfflé, “Vision and Challenges for Realising the Internet of Things,” Cluster of Europ. Research Projects on the Internet of things, 2010.

[6] O. Salman, I. Elhajj, A. Chehab, A. Kayssi, “IoT survey: An SDN and fog computing perspective,” Computer Networks, 2018.

[7] R. A. Rahman, B. Shah, “Security analysis of IoT protocols: A focus in CoAP,” ICBDSC, 2016 [The 3rd MEC International Conference on Big Data and Smart City].

[8] HP Fortify, “Internet of Things Security Study : Smartwatches,” Hp, 2015.

[9] Cisco, “IoT Threat Environment,” with risk-based Secur. Progr. Recomm. A White Pap. , 2015.

[10] K. Michael, “The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice,” Comput. Secur. , 2012.

[11] S. El Bouanani, M. A. El Kiram, O. Achbarou, A. Outchakoucht, “Pervasive-Based Access Control Model for IoT Environments,” IEEE Access, vol. 7, pp. 54575–54585, 2019.

[12] R. Minerva, A. Biru, D. Rotondi, “Towards a definition of the Internet of Things (IoT),” IEEE IoT Initiative white paper, 2015.

[13] M. Gyu Lee, “The Internet of Things - Concept and Problem Statement,” 2012.

[14] C. Bormann, “Block-Wise Transfers in the Constrained Application Protocol (CoAP),” 2016.

[15] OASIS (Organization for the Advancement of Structured Information Standards), “MQTT Version 3.1.1,” 2014.

[16] M. Iglesias-Urkia, A. Orive, A. Urbieta, D. Casado-Mansilla, “Analysis of CoAP implementations for industrial Internet of Things: a survey,” Journal of Ambient Intelligence and Humanized Computing, 2018.

[17] M. A. Prada, P. Reguera, S. Alonso, A. Morán, J. J. Fuertes, M. Domínguez, “Communication with resource-constrained devices through MQTT for control education,” IFAC-PapersOnLine, 2016.

[18] N. Kushalnagar, G. Montenegro, C. Schumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals,” 2007.

[19] IEEE P802.15 Working Group, “IEEE 802.15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs),” 2011.

[20] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” Comput. Networks, 2013.

[21] I. Bouij-Pasquier, A. A. Ouahman, A. A. El Kalam,M. O. de Montfort, “SmartOrBAC Security and Privacy in the Internet of Things,” 2015.

[22] P. Friess, “The Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems,” 2013.

[23] M. binti Mohamad Noor, W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” Comput. Networks, 2019.

[24] F. A. Alaba, M. Othman, I. Abaker, T. Hashem, F. Alotaibi, “Author’s Accepted Manuscript Internet of things Security: A Survey,” J. Netw. Comput. Appl., 2017.

[25] A. Tewari, B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Generation Computer Systems, 2018.

[26] A. Riahi Sfar, E. Natalizio, Y. Challal, Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” Digit. Commun. Networks, 2018.

[27] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things J., 2017.

[28] S. El Bouanani, https://github.com/esalim/IOT-STANDARD-PLATFORM, last visit 26-08-2019.

[29] R. Garrett, “INSECURITY in loT,” Supply Demand Chain Exec., 2016.

[30] B. Hayes, “Conducting a security audit: an introductory overview,” Symantec Connect, 2003.

[31] B. D. Romero M, H. M. Haddad, “Asset assessment in web applications,” ITNG2010, 2010, [7th International Conference on Information Technology: New Generations].

[32] ANSSI agency, “EBIOS risk management methodology, ” p. 13, 2010.

[33] M. Hossain, R. Hasan, A. Skjellum, “Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems,” ICDCSW, 2017 [IEEE 37th International Conference on Distributed Computing Systems Workshops].

[34] Cisco, “The Internet of Things : Reduce Security Risks with Automated Policies,” 2015.