A Study of Modelling IoT Security Systems with Unified Modelling Language (UML)

Hind Meziane*, Noura Ouerdi
LACSA Laboratory, Faculty of Sciences (FSO)
Mohammed First University (UMP), Oujda, Morocco

***Abstract*—The Internet of Things (IoT) has emerged as a technology with the application in different areas. Hence, security is one of the major challenges that has the potential to stifle the growth of the IoT. In fact, IoT is vulnerable to several cyber attacks and needs challenging techniques to achieve its security. In this paper, the use of a UML (Unified Modelling Language) aims at modeling IoT systems in various views. The purpose of this study is to discuss the need for more modeling in terms of security. For this reason, this paper focuses on modeling security of IoT systems. The objective is to make a comparison in terms of layers by describing the IoT architecture and presenting its components. In other words, the research question is to look for the modeling of security in the IoT layers. There is no standard that takes into account the security of the IoT architecture, there are different proposals of IoT levels, which means that each author has his own vision and own proposition. Moreover, there is a lack of modelling languages for IoT security systems. The main interest of this study is to choose the layer on which we should be interested. The question then is as follows: "which is the layer whose modeling is relevant?" The obtained results were conclusive and provided the best insight into all the specifications of each layer of the IoT architecture studied.**

Keywords*—Internet of things (IoT); IoT systems; IoT security; modelling; Unified Modelling Language (UML); UML extensions; IoT applications

I. Introduction

IoT or Internet of Things is a big area. The general idea of it is to make objects connected or linked together in order to communicate and exchange information via communication technologies like LoRa, LoRaWan, 4G, 3G, 2G, etc. IoT was coined by Kevin Ashton (pioneer of Radio Frequency Identification (RFID) technology (Automatic Identification Technology)) in 1999 [1]. IoT is a vast domain [1][2]. The IoT aims at enabling things to be connected at anyplace, anytime with anyone and anything using any network/path and any service. IoT is now used in multiple fields like Healthcare, Transportation, Factory, Building, City, Retail, Surveillance, Manufacturing, Agriculture, Logistics, Lifestyle, Industrial, etc.

Software engineering goals include gaining the greatest knowledge of the problem and modeling complicated systems utilizing tools such as UML (Unified Modelling Language) diagrams. The UML diagrams can be used for modelling the complex systems. In this sense, realistic IoT application scenario modeling on a wide scale with various operating conditions necessitates/requires a mix of edge devices, sensors, and actuators [3]. The goal of this paper is to review published studies and look into the current state of IoT modelling security. The modelling of security systems for IoT is the main step, thus, security modelization is essential. In the literature, there are two types of tools: modeling languages (UML, SysML (System Modelling Language) and ThingML (Internet-of-Things Modeling Language)) and extensions to these languages (UML4IoT, IoTsec, UMLsec, SysMLsec, SysML4IoT). Various languages with their extensions have been provided to simulate and model IoT systems like IoTsec, ThingML, SysML, UML4IoT, SysML4IoT, etc.

In this context, networking and designing IoT and edge computing layers [3] is a very laborious process because of: (1) end-point networks like Bluetooth, Wi-Fi, and 4G are complex and heterogenous; (2) heterogeneity of edge and software stack and IoT hardware resources; (3) mobility of IoT devices; and (4) the complex interaction between IoT and edge layers [3]. Creating an edge computing and IoT testbed with high verisimilitude is not only difficult or complex, resource-intensive and expensive but also time-consuming. Furthermore, because of the high cost and broad domain expertise necessary to reason about their variety, usability, and scalability in actual IoT and edge computing settings, testing in reality edge computing and IoT environments is not practical [3]. Hence, in this article, we are interested in modelling IoT security systems and we also discuss the modelling challenges in the IoT environment context.

In UML 2.5, there are now fourteen diagrams that developers utilize to build systems. However, for some specific application domains, these diagrams are ambiguous. As a result, specific domain notations are covered by the UML extensions [4]. In UML, there are some extension artefacts that are well defined, these are: tags, values, stereotypes and constraints. These extensions mechanisms allow designers to develop specific models for certain areas/domains, such as modeling security concerns in systems, UML extension for Hypermedia Design [4], profiles to model Internet of Things (IoT) systems, …. [4]. However, security is one of the major issues. Three issues in designing IoT applications are addressed due to the lack of a strategy to develop/model IoT applications, the lack of a model to design security challenges in IoT, and the heterogeneity of different software and hardware devices.

The objective and originality of this paper are as follow: A lot of research work on modelling languages have been provided, but we could not find works on the following question "what is the relevant layer to model that really contributes to the security of IoT systems?" that is the strong

*Corresponding Author.

point of this research. In the literature, there is a lack and absence of works in the same section/point and this can be considered among the criticisms. The main idea of this work is to choose an IoT layer for which modelling is relevant. The problem to be discussed is as follows: which layer should be specified? The main objective is to look for the modeling of security in these layers, i.e., on which layer we should be interested? To do this, we compare the four layers by considering various parameters. However, there are no answers about the following question: What is/are the relevant layer(s) to model that really contributes to the security of IoT systems?

A. Contribution

The contributions of this survey are summarized as follows:

- This paper presents a state of the art of modelling IoT systems with UML, SysML and ThingML to perform a comprehensive study on modelling IoT security systems.
- This survey defines and describes the challenges that IoT systems are currently facing.
- The architecture of IoT systems is proposed as well as the role of each IoT layer is also described.
- This paper proposes a summary and taxonomy of security attacks and vulnerabilities at different layers. Then, the security issues, problems, vulnerabilities and challenges of each layer were also introduced. It also explores the security requirements for IoT layers.
- The strong point is to define the layer that needs more security in the IoT architecture. The added value is as follows: there is no survey that has been made to confirm "which is the layer whose modelling is relevant?"

B. Outline

This paper is organized as follows: The related works done in IoT security modelling are presented in Section II. Section III provides the IoT challenges. Section IV outlines the proposed methodology including architecture of IoT systems, challenges of each IoT layer, classification of attacks and vulnerabilities in IoT, IoT security requirements, OWASP IoT Project by analyzing security threats and vulnerabilities, followed by an example of modeling IoT security with UML. Results and discussion are covered in section V. Finally, Section VI concludes the paper.

II. Related Works

Currently, modeling the security of IoT systems has become highly important among researchers, each researcher uses a language (whatever its extension, e.g. IoTsec, UML4IoT, SysML-Sec...) to prove the quality of its work. In this section, we review and discuss the literature of some previous papers which are related to our theme in order to keep up with the languages and extensions used. It is extremely difficult to model a real IoT scenario due to several challenges that we will discuss later in the results and discussion section.

There are several simulation environments currently available such as IoTSim-Edge, IoTsuite, SimIoT... For instance, Jha et al., (2020) [3], aims to build a novel simulator, IoTSim-Edge, that allows users to evaluate the edge computing scenario in an easily configurable and customizable environment. Further, the authors give the general architecture of edge computing considered for modeling by IoTSim-Edge simulator. The architecture of the proposed simulator consists of multiple layers. IoTSim-Edge targets to model smart devices using low energy protocols. The authors also consider the simulation of battery power by using a predefined drainage rate. The presented architecture of IoT-Edge computing consists of two components: actuator nodes and sensing nodes. The sensing nodes collect the information of surroundings via sensors and send it for processing and storage. Whereas, the actuators will be activated according to the analysis of the information/data. The communication layer is responsible for transferring data to IoT devices, cloud, and edge devices. Different communication protocols are used for transferring data. Edge infrastructure is the next layer that consists of several types of edge devices (e.g., Raspberry Pi and Arduino). These devices can be transparently accessed through the help of various types of containerization and virtualization mechanisms. It provides an infrastructure to deploy the raw data produced by the sensing nodes. The services or application layer consists of various services which can be accessible directly to the users. These services (applications) will be accessed through a subscription model.

A. Modelling IoT Security System using UML Language

Robles-Ramirez et al., (2017) [4], mention a number of approaches that aim to model IoT systems and security considerations. They used IoTsec, which is a UML extension and another example that includes a notation for security modelling in IoT systems. Furthermore, to model IoT systems, they propose a UML/SysML extension, which attempts to encapsulate security knowledge. In particular, a new UML extension is proposed, which characterises security issues encapsulated within a nomenclature, and UML stereotypes, in order to model common actors and UML notation extensions. The objective is to move IoT development at a previous step from the implementation stage; the designing phase. This work targets security concerns in IoT development. Besides, the authors provide a simple model language to describe security actions and entities. The main aim is to facilitate the representation of security issues using a visual notation [4], even if the developers are unfamiliar to Internet security concepts. To represent an IoT system in terms of security issues/concerns, the authors, adopted the four layers architecture including sensing, network, service, and application layer.

Dhouib et al. (2016) [5], give a highlight to the current status of "Papyrus for IoT". It is a modeling environment that enable to deploy, specify and design complex IoT systems by using an IoT-A lightweight methodology. Furthermore, in order to illustrate the modelling environment, they use the example of a smart IoT-based home automation system, which consists of five steps:

- Step 1: Design the requirements and the purpose of the system by using SysML requirements diagrams and UML use case diagrams in Papyrus SysML Component.
- Step 2: Define the process specification. The IoT system's use cases are described, derived from and based on the requirements and purpose specification.
- Step 3: Define the system's functional architecture based on the IoT domain model.
- Step 4: Define the operational platform for the functional system's execution.
- Step 5: With Papyrus Designer Component, define deployment plans that include information about the allocation/assignment of functional blocks (step 3) to operational ones (step 4).

Moreover, they introduce MDE4IoT frameworks covering more than only a single MDE technique. Moreover, papyrus is an open-source Modeling Environment. In contrast to the other publications, the introduced approach already uses IoT-A in the Papyrus for IoT modelling environment.

Reggio (2018) [6] presents a method (IoTReq) for the elicitation and specification of requirements for IoT systems. The method uses UML for modelling the domain, requirements elicitation and specification of IoT requirements. This method also supports the specification of non-functional specifications. Reggio proposes a UML profile for the requirement gathering for IoT applications.

Ouchani (2018) [7] creates a formal framework for assessing the functional correctness of IoT systems. The suggested framework includes all of the major components of IoT systems, and the process is completely automated. Author describes the IoT architecture by showing its components with their interactions. The suggested IoT architecture enclosed five components which are demonstrated and analyzed subsequently in the next section. (1) Object devices, (2) User devices, (3) Computing services, (4) Social actors (are human agents) and (5) The environment. These components interact via communication protocols of various ranges (ZigBee, WiFi, Cellular, Human-machine, Bluetooth, SSH, IpSec, etc.). However, the proposed work suffers from PRISM's restrictions, and the security proprieties are not described.

(Thramboulidis and Christoulakis, 2016) [8], presented UML for IoT (UML4IoT) domain-specific modelling language to tackle the IAT (Industrial Automation Thing) domain. They presented the UML4IoT approach, a UML profile aimed at modeling cyber-physical components as their integration into IoT systems in manufacturing domain. UML4IoT is an UML profile for IoT, which have been already employed in the domain of real-time and embedded systems. However, UML4IoT extension does not support security modeling. Moreover, the authors didn't provide any reason about their choice.

B. Modelling IoT Security System using SysML Language

Ferraris et al. (2020) [9], present a model-driven approach extending UML and SysML diagrams. The aim of this work is to provide developers with a tool helping them to consider domains such as trust and security during the SDLC (System Development Life Cycle) of an IoT entity.

C. Modelling IoT Security System using ThingML Language

Harrand (2016) [10] introduced ThingML (Internet-of-Things Modeling Language), which is a modelling language that focuses on a distributed and heterogeneous systems, for generating code framework for diverse targets. ThingML is designed to support the development code generation. It can be considered as a DSML (domain specific modeling language). Generally, it has more been applied to IoT and CPS (Cyber-Physical Systems). Nonetheless, the authors do not take security into account.

However, for the existing papers in this field of modeling IoT security systems with UML, SysML, or ThingML, no survey has been made to confirm which is the layer whose modeling is relevant. In other words, there is no answer about the following questions: "Which layer whose modeling is relevant?" This means what is the relevant layer to model that really contributes to the security of IoT systems? Which calls the need for an in-depth comparison on the IoT layers including the upcoming and existing security issues. In general, as another limitation of similar works, modeling IoT security systems is still very superficial.

III. IoT Challenges

The IoT infrastructures and security are still in infant phases. IoT systems have its own specific challenges. Hence, there are several obstacles to the development of the IoT. The following are some challenges and constraints in IoT systems:

A. Interconnectivity

Interconnectivity characterizes the ability of IoT systems and their constituents to communicate and use each other's services in a seamless manner [1], [2], [11]. The global information and communication infrastructure [12] allows for the interconnectivity of anything.

B. Heterogeneity

IoT devices are heterogeneous, since they are based on several networks and hardware platforms [12]. They can communicate with other service platforms or devices via various communication technologies and networks like LoRa, 2G, 4G, etc. Indeed, these IoT protocols are heterogeneous. Therefore, we need to make sure that there is a compatibility between them.

C. Interoperability

Interoperability is a basic value of the traditional Internet, the first criterion of internet connectivity is that "connected" systems/computers "speak the same language" of protocols and encodings. To support their applications, various industries nowadays use various standards. The adoption of common interfaces between these different entities becomes increasingly critical when there are various sources of data and heterogeneous devices. As a result, IoT systems must be able to deal with a high level of interoperability [1], [2],[12].

D. Scalability

In an IoT network, there are a large number of IoT devices [1] and nodes, Cisco estimated that in 2020, 26.3 billion devices were connected to the Internet [13]. Because of this large number (including the number of users and the number of participating IoT things), scalability is a crucial issue for creating effective defensive methods [13].

E. Big Data

Not only the number of smart objects [13] will be enormous, but the data generated by each object will be huge. Because each smart device is supposed to be supplied by too many sensors, each of which generates massive amounts of data over time, and also exchanges it on multiple IoT layers [1], [2], [13].

F. No Standardization

There is a lack of standardization in terms of IoT definition, vision, architecture, attacks, [1], [2]. For the IoT layers architectures, there are several proposals of IoT architecture with three, four, five, and seven layers (for the Cisco IoT model). Further, there is no robust solution that will solve most of IoT security issues.

G. Resource Constraint

Resource constraint (Limited Resources) in terms of energy, storage space and computing capacity. End devices in the IoT have limited resources like memory, storage, CPU, battery, and transmission range [13]. In other words, IoT devices are uniquely identifiable and are mostly characterized by limited processing, small memory, and low power. Furthermore, IoT devices [4] have many constraints like software based, network-based, and hardware based limitations, which depict new challenges for IoT developers. Moreover, implementing conventional security measures is impossible because it would be a very hard and complex process [14]. Since IoT devices have constrained resources, standard encryption algorithms cannot be applied directly for the IoT system. Lightweight cryptographic techniques were suggested by [14]. Therefore, a comparative study of existed lightweight cryptographic algorithms must be required. In addition, due to the rapid growth of IoT devices and the great developpement of new technologies and elements in the market, IoT systems have become vulnerable to several attacks.

H. The Lack of Encryption

The lack of encryption in the cloud which should also be considered [1]. An encryption procedure is important for IoT systems.

I. Security and Privacy

That means provide the necessary protection for data and maintain the privacy of users; this is the biggest challenge of the IoT. This is especially critical in healthcare devices. For applications in personalized medicine, such intelligent devices are becoming more popular. The information gathered is typically highly substantial and frequently includes meta-data like time, place, and context [15]. Besides, it describes the five security features, like confidentiality, availability, integrity, authentication and non-repudiation. Another serious problem is about how to get a secure and an efficient IoT platform to deliver what is required to be delivered.

J. Security Policies

We need to have policy. Policies are operational rules that must be maintained in order to keep data organized, secure, and consistent. Because security is also about how to use this flow of data. Security policies should be followed by users.

IV. Methodology

The objective of this paper is to conduct a comparative study of different layers of the IoT architecture taking into account the specifications of each layer. The layer is a factor among the factors that differentiates the modeling of IoT systems. Thus, to ensure the security of IoT systems, this contribution will compare these layers based on IoT architecture in order to outline the relevant layer to model.

The problem to be discussed is as follows: at which layer we are going to work? Do we combine two layers or we work on one layer? So, the main aim of this section is to choose which layer requires more security. To answer this research question, a systematic review on IoT architecture and security concerns could be done regarding several important axes/points. In other words, we need to do a comparison in terms of layers. By looking for layer modeling, we report the results and findings of this section. Thus, the proposed methodology is based on six steps. We gathered all specifications for each layer of IoT. For this purpose, the author is looking for a detailed description on IoT layers as well as an analysis of each layer was also done by covering the next points:

1) At first we will present the functionalities of IoT architecture to understand how IoT system basically works and underline the architecture we are working on.

2) After that, we will detail in the second step the security issues/problems of the IoT architecture which contains multiple layers, to give a detailed explanation and general understanding of different security challenges in different layers.

3) Then, we will provide a classification of security attacks and vulnerabilities in each layer of IoT systems, to conclude the most security attacks in each layer.

4) Followed by security requirements in IoT to analyze an in-depth the security services that must come with each layer.

5) In the fifth step, we will talk about the OWASP IoT Project as an example of security threats analysis.

6) And finally, we will end with, a comparison that were obtained previously to outline the extension that meet our needs regarding/in terms of security. That is why we took a UML extension as an example for modeling IoT security.

To be clearer, we followed these steps in the methodology section in order to compare the different layers by keeping the results of the six steps.

There are many papers, and researchers have presented different architectures. Some researchers present architecture composed of five layers [1], [2], some architecture composed

of three layers and in our research, we are interesting and we choose the architecture of four layers: physical layer, then, network, middleware and application layer. In this paper, the author adopts four layers architecture to present or choose the relevant layer to model that really contributes to the security of IoT systems and also to reflect the IoT architecture concerns. The proposed model of the IoT system is innovative, that take into consideration all characteristics, concerns, issues and threats of the four layers of the IoT architecture. Therefore, the best IoT architecture is that of four layers. Because, it is very general and presents in a great way the concept of the IoT. Besides, security at the middleware layer (storage/cloud/data) is not the same as security at the application layer (authentication/identification); as more than we separate the problems, we find solutions. In other words, security concepts in the cloud/middleware layer may not be integrated in the application layer. Moreover, we need cloud because we have so much data generated by many connected objects. Therefore, the middleware layer is also provided as a necessary and an integral part of the IoT model. Fig. 1 shows proposed and detailed architecture of IoT systems. It shows various devices and technologies at these layers. In this paper, author is using and describing the functionality of the following layers:

- Physical Layer
- Network Layer
- Middleware Layer
- Application Layer

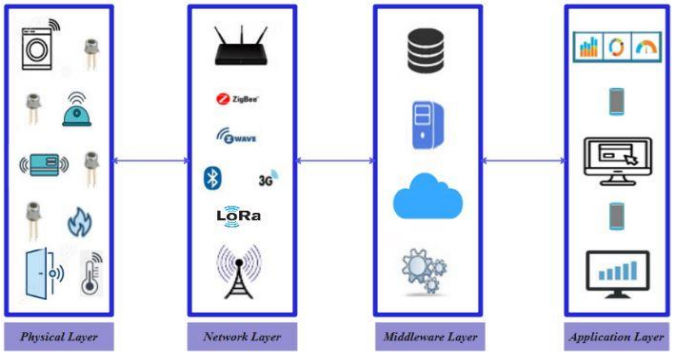

Fig. 1. IoT Architecture based on Four Layers.

A. IoT Architecture

There is not a standard for the IoT architecture, there are different proposals of IoT levels. It consists of different layers. To achieve this goal, and for simplicity, this paper focuses on four IoT layers.

1) Physical/Perception layer: Physical layer, which is also called the Perception layer. In [1] and [2], the first or base layer has been generalized by physical layer, that is not limited to actuators and sensors, it is composed of sensors, controllers, RFID tags and reader, actuators, and devices. IoT devices include mobile devices, single-board computers, and micro controller units [2]. IoT involves objects or things such as sensors, actuators, RFID tags and readers, to permit interaction between the physical and virtual worlds. The capacity of a connected thing to optimize the probability of satisfying/achieving the user's goals may be used to determine its intelligence. Connected things intelligence spans from non-existent to perfectly rational [11]. The sensors may monitor or measure values like temperature, pressure, humidity, air quality, movement, speed, flow, and electricity…. Sensors collect information about their surroundings. This layer's main purpose is to collect useful data from the environment (like humidity, WSN, temperature, and heterogeneous devices, etc), then process, and digitize these information/data [1]. Body sensors, vehicle telematics sensors, environmental sensors, home appliance sensors, are classified according to their specific purpose. The actuator can be used for performing particular action.

The functionalities of this layer include actuating, sensing, actuating and sensing, storage, and processing [11]. Gathering and generating information by devices are the main operations of the physical layer. The collected data with the networks will be sent to the cloud. There are three types of things [11] smart things (or physical objects), sensors or/and actuators, and gateways. Finally, the first layer is "physical layer" also known as recognition, perception. The main function is to identify, generate and collect data from the physical world to perceive their environment by detecting changes using sensors.

The first layer components are: Tag, sensors/actuators, coordinator and network (LAN, PAN). In other words, LAN or PAN can be considered as a form of connectivity between sensors and sensor gateways. While WAN can be considered as a form of connectivity between sensors and servers.

Enabling technologies for the IoT can be grouped into three categories [12]:

- Technologies that enable "things" to acquire contextual information.
- Technologies that enable "thing" to process contextual information.
- Technologies to improve Security and privacy.

2) Network layer: The network layer is the connectivity layer which connects the perception layer to the cloud trough, a gateway using different technologies such as Lora, satellites, 3G, and others technologies. It is responsible for the transfer of this sensitive and massive volumes of data between different layers via network. It contains Router, Internet, Switches, Gateway [1], This layer is used for the connectivity, it defines the different protocols and communication networks or technologies such as Sigfox, 3G, 4G, 5G, WIFI, Zigbee, Bluetooth, LoRaWAN, LoRa, which represent the edge where the collected data can be processed. This layer is responsible for the connectivity of the IoT infrastructure. It also collects data from the physical layer and transmits it to the upper layer. The transmission medium can be wired or wireless.

These technologies include, but not limited to ZigBee, RFID, NFC, WSN, MANET, Wi-Fi. Furthermore, these technologies have their own security issues. Multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration.

IoT communication technologies are based on two different categories [1]: Short-range and Long-range technologies. The first one include Z-Wave, Zigbee, RFID, NFC, 6LoWPan, etc. The second includes LPWAN technologies, among them LoRa/LoRaWAN, Cellular communication (2G/3G/4G/5G), NB-IoT, Sigfox, etc.

3) Middleware layer: The middleware layer contains (data analysis, data visualization, Cloud, API, Datacenter,) [1]. It stores, processes and analyses huge amounts of data, big data processing modules, employs databases, cloud computing, classification and polymerization [1]. In this layer there are different methods, tools and techniques that can be used to analyze the data collected by sensors and network layer in order to visualize it in the next layer (application layer). The stored data will be exploited by users. The main function of this layer is the complete analysis via very robust systems that contain Artificial Intelligence, other models/algorithms to do the analysis of the data. Due to its unlimited processing and storage capacity, cloud computing is crucial for the IoT [14]. It also provides a distributed architecture/infrastructure for processing and analyzing IoT data before pushing it to the application layer.

4) Application layer: The application layer visualizes the data produced by IoT computing. It is responsible for delivering personalized services to all industries and to the user [1]. It is the interface for users to communicate to their IoT things and access data. It supports protocols that can be deployed for IoT like MQTT (Message Queue Telemetry Transport)[1], XMPP (Extensible Messaging and Presence Protocol) [1], CoAP (Constrained Application Protocol) [1], SMQTT (Secure MQTT), AMQP (Advanced Messaging Queuing Protocol), etc. HTTP (Hyper Text Transfer Protocol) is used by [16]. This protocol cannot be employed in the application layer, it is not suitable/appropriate for resource-constrained since it is heavy in weight and therefore requires a large parsing overhead [17]. This layer provides personalized services based on the demands of the user. The IoT application covers “intelligent” environments/spaces in areas such as wearable devices, agriculture, transport, factory, building, health, city, lifestyle, home, commerce, vehicles, emergency, supply chain, environment and energy.

5) Summary: This subsection adopted and introduced four level model. To sum up, the IoT objects and things of the physical layer communicate with each other in order to deliver intelligent applications and services for users or human. These IoT devices collected information/data that need to be secured. Billions of devices (medical devices), sensors, actuators and IoT things are connected to the Network. The number of these connected devices is expected to grow increasingly over the coming years. Sensors, RFID and actuators are the major components of physical layer that can be easily accessed by attackers. These devices need to be managed and secured appropriately, to avoid their significant security risks.

Moreover, IoT involves various communication technologies, which could be affected by different threats. Consequently, for each communication technology, a taxonomy of all possible attacks with their degree of severity/impact/danger must be required. In other words, the communication between these layers need to be secured. Therefore, a secure architecture is needed with some recommended technologies. The first result in this subsection illustrates that the physical and network layer contain the most components that are targeted by attackers. Moreover, because of generating and gathering information by IoT things and devices are the main operations of the physical layer. Therefore, the risk of data theft can be decreased or minimized with physical layer security. Indeed, these data can be stored and processed in local network, so communication technologies and protocols should also be secured. The next subsection will offer insights into the security issues and problems of the IoT architecture. Here, we will give some common issues and challenges of each layer of IoT architecture.

B. The Security Challenges of the IoT Architecture

In this subsection, we analyze security challenges in each layer of the proposed model. Because each IoT layer has its own challenges and security issues.

1) Security challenges and problems of physical layer: At this first layer, the main challenge is the limited resources on IoT devices: storage, memory, CPU, and energy. For instance, sensor is a small equipment with limited resource. Devices of the physical layer are often limited in terms of process and data storage resources, and the applied technologies (such as RFID, NFC, Bluetooth, ZigBee) are being limited in data transmission range and rate. For many IoT devices that are mobile and rely on embedded batteries, energy is one of the most important resources [11]. In terms of energy, the IoT devices need a significant amount of electricity because of their powerful processing capability.

The malicious attack on the identification technology and the sensor is the main challenge for the physical layer [1], which interferes with the collection of data. Things include physical objects (micro-controllers, sensor/sensor nodes, actuators, RFID tags and readers), this physical hardware are targeted by several attacks in the both layers (physical and edge computing layers).

Every IoT devices and Things is linked to the internet in order to talk and communicate to each other. So, there is the possibility of hindering the privacy. Indeed, due to a variety of security vulnerabilities, RFID, and sensors are in threat. Moreover, hardware components and IoT objects are vulnerable to several physical attacks like Object replication attacks, RF Interference on RFID, Hardware Trojan, Object jamming, Physical damage, Camouflage, Malicious node injection, Object tampering, social engineering, Side-channel attack, Malicious code injection, Tag cloning, Outage attacks

[16], False Data Injection Attack, booting vulnerabilities [17], Node Tampering, Node Jamming in WSNs [18] . For instance, the malicious node injection attack targets the physical layer since the node is physically inserted/injected into the network [18]. Besides, side channel attack is conducted at the physical layer because attacker uses side channel information to find the encryption key [18]. At sensors, an attacker can manipulate data, can also do boot attacks, and can capture a node [19].

IoT software are targeted by many attacks. Indeed, hardware components of IoT, like types of RFID tags, sensors, RFID readers, are also vulnerable [16]. The major attacks are targeting the IoT hardware components. Attackers must be located near to hardware or devices in order to launch physical attacks. The attackers may want to physically destroying the devices/hardware, endanger the communication mechanism, tampering the energy source, limiting its lifetime, etc. Also, the attacker can directly access the related attributes of the device through physical attacks, and then start further attack.

The weaknesses of the various devices are exploited in security attacks against IoT systems. IoT devices are subject to well-known vulnerabilities such as the use of unauthenticated requests to conduct/perform actions, broken authentication, sensitive data exposure, infection flaws, XSS (cross-site-scripting), CSRF (Cross Site Request Forgery), missing function-level access control [20].

2) Security challenges and problems of network layer: At the second layer, one of the main/most challenges that face this layer is the heterogeneity of data; for instance, in the network part, there is a huge heterogeneity of data in term of IoT communication technologies (Lora, WI-fi, ZigBee, 4G). This may cause compatibility problems. Compatibility is another major problem. There are some attacks specific to some IoT technologies communication. These technologies of communication include, but not limited to ZigBee, WSN, LoRa, MANET, Bluetooth, RFID, 3G, NFC, Wi-Fi, etc. Moreover, these technologies of communication have their own security concerns and issues. The following are the major security attacks that are faced at the network layer: Phishing Site Attack, Access Attack, DDoS/DoS Attack, Data Transit Attacks, Routing Attacks, unlawful attacks, common attacks [17], Traffic Analysis Attacks, RFID Spoofing, RFID Cloning, RFID Unauthorized Access, Man in the Middle Attacks, Routing Information Attacks [18], Selective Forwarding, Routing Information Attacks, RFID Unauthorized Access, RFID Spoofing, Replay Attack, Traffic Analysis Attack [21].

Additionally, the network attacks consist of manipulating the IoT network system to cause damage. Attack can be started without being close to it (network) [21]. Attacks on networks can have significant consequences, sometimes causing a total shutdown [21]. The software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system. The main attacks in the Network layer, targeting the network protocols. An example of network and software attacks in reality is described in [1].

3) Security challenges and problems of middleware layer: Today, the most significant data attacks that are happening in the IoT world: Data Inconsistency, Data Breach and Unauthorized Access [21]. An example of data attacks was launched in reality in March 2018 [21], Cambridge Analytica had obtained access to the private data of more than 50 million Facebook users. Other major security issues at the middleware layer include cloud and data security as well as database security [17].

In the middleware layer, various possible attacks are discussed in [17] such as: Man-in-the-Middle, SQL Injection Attack, Signature Wrapping Attack, Cloud Malware Injection, Flooding Attack in Cloud.

4) Security challenges and problems of application layer: The application layer has specific security problems and issues such as privacy issues and data theft [17]. In the application layer, major attacks are discussed in [17] like Data thefts, Access Control attacks, Service Interruption attacks, Malicious Code Injection attacks, Sniffing attacks, Reprogram attacks.

5) Summary: In this subsection, we have given of the security challenges and problems being faced in each layer of IoT. In my view, the main challenges of IoT systems mainly relate to the first and second layers which are explained and analyzed previously. Since the influence stemming on IoT as IoT devices limitation (resource constraint) and heterogeneity or compatibility problem is very strong. For instance, limited resources challenge for the physical layer and the second challenge is about the heterogeneity of data for the network layer. So, we have to focus on both layers (Perception/physical, and network layer) due to their big/huge challenges and also for other reasons that will be discussed later.

C. Classification of Attacks and Vulnerabilities in Each Layer of IoT Systems

Based on [1], IoT attacks can be classified into fifteen categories: attacks based on vulnerability, on layers, on behavior, on technology of communication, on impact, on security concepts, on target, on software, on source, on devices, on encryption, etc. It is absolutely important to identify vulnerabilities and attacks against each IoT layer. The identification of IoT security attacks is crucial due to the ever-growing number of threats and vulnerabilities in the IoT domains. It is firstly necessary to identify the IoT attacks and vulnerabilities and then classify them.

1) Vulnerabilities in each layer of IoT systems: In terms of vulnerabilities of physical layer, the work [21] have highlighted the vulnerabilities against physical devices like IP cameras, Amazon Echo. For example, attacks such as device spoofing, device scanning, and brute force may control of the cameras. Attackers can get the password for a camera of any length or combination via a device spoofing attack.

Additionally, the attacker can perform a device scanning attack to discover all online cameras by enumerating all MAC addresses that could exist [21]. The vulnerability issue for the "Things" is caused by careless program design, which opens opportunities for the installation of malware or backdoors [22]. The attacker can attack an IoT system by physically weakening or tampering a node [18].

In terms of vulnerabilities of network layer, the attacker can target an IoT system from their own network by exploiting faults in the routing protocol and other network-related protocols or by employing malicious software. The network layer is highly vulnerable/susceptible to phishing site attacks [17].

In terms of vulnerabilities of middleware layer, XML signatures are utilized in the middleware's web services. By exploiting SOAP (Simple Object Access Protocol) vulnerabilities, the attacker can execute operations or alter eavesdropped messages in a signature wrapping attack, which breaks the signature algorithm [17].

At the application layer, insecure cloud interface is a vulnerability in an IoT system that can be an attack vector. Buffer overflow consists in exploiting a vulnerability of an application resulting in abnormal behavior sometimes leading to access to the system with the rights of the application. Software vulnerabilities that allow resource buffer overflows or pushing an IoT device to exhaustion state by an attacker [23]. For instance, a low battery level may cause the laptop to shut down unexpectedly. Due to the majority of the system being in "sleeping" mode, other "things" could not be interoperable [23].

2) Classification of attacks and vulnerabilities based on Layers: In this section, author proposes to summarize the attacks and vulnerabilities based only on the IoT layers, the list is endless. Moreover, each attack has a degree of severity [1], [2]. According to [1], [2], [16]–[18], [21], the security attacks and vulnerabilities at each layer in IoT system are collected and shown in Table I.

3) Summary: After establishing the taxonomy of security attacks and vulnerabilities in each layer of IoT systems. All of these attacks cause significant harm since they alter data, steal sensitive data, drop packets and encryption key, etc.[18]. According to Table I, we showed that the two first layers have been threatening by many IoT attacks and vulnerabilities compared to middleware and application layers. Most attacks on the IoT often occur in IoT objects and IoT network. In other words, most IoT attacks and vulnerabilities have resided in physical layer and network layer because of the poor security design of these connected objects as well as vulnerabilities in IoT protocols and communication technologies. In the next subsection, we will examine and summarize the security requirements for IoT.

TABLE I. CLASSIFICATION OF ATTACKS AND VULNERABILITIES BASED ON LAYERS IN IOT SYSTEMS

Layer	Attacks and vulnerabilities in IoT	Attacks description
Physical Layer	Social Engineering, Node Capture, DoS (Denial of Service) Attack, Distributed DoS Attack, spoofing attack, Fake Node, Replay Attack, Mass Node Authentication, Tag cloning, Unauthorized Access to the Tags, Denial of Sleep Attack, RF Interference on RFID, Eavesdropping, Man In the Middle, RF Jamming, Routing Threats, Object replication, Hardware Trojan, Object jamming, Camouflage, Object tampering, Sleep Deprivation Attack, Outage attacks, Wormhole and Timing attack. Malicious Node Injection, Malicious code Injection, False Data Injection Attack, booting vulnerabilities, Physical damage, Side Channel Attack, Node Tampering, Node Jamming in WSNs, Data Manipulation, Boot Attack.	Both software and hardware components of IoT are targeted by several attacks. Additionally, attackers must be located near to hardware or devices with different intent to launch physical attacks, which can also directly access the related attributes of the device through physical attacks.
Network Layer	Spoofing, MITM attack, Routing Information attack, Sinkhole attacks, Sybil attacks, DoS, Denial of Sleep Attack, Selective forwarding, Eavesdropping/sniffing, Routing attacks (Worm Hole, Hello Flood, Black Hole, Gray Hole, Sybil attack), Phishing Site Attack, Access Attack, DDoS Attack, Data Transit Attacks, Routing Attacks, Malicious code injection, RFIDs interference, unlawful attacks, common attacks, Traffic Analysis Attacks, RFID Spoofing, RFID Cloning, RFID Unauthorized Access, Man in the Middle Attacks, Replay Attack, Routing Information Attacks.	The network attacks consist of manipulating the IoT network system to cause damage. The software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system.
Middleware Layer	Flooding Attack in Cloud, Malicious Insider, Cloud Malware Injection, Unauthorized Access, Signature Wrapping Attack,Data Inconsistency, Cryptanalysis Attacks, Web Browser Attack, DoS, SQL Injection Attack, MITM, Data Breach, Data Security.	The main challenges are Cloud/data security, and database security.
Application Layer	Buffer Overflow, Botnet, Code Injection, DoS, Sleep Deprivation, Phishing Attack, Sniffing Attack, Authentication and Authorization, DDoS Malicious Scripts, Data Access and Authentication, Trojan Horse, Social engineering, Cryptanalysis Attacks, Brute Force and Cross Site Scripting, Access Control attacks, Service Interruption attacks.	Data theft; Attackers exploit the vulnerabilities of application and programs.

D. IoT Security Requirements

This subsection provides the details about the IoT security requirements. According to [1], [2], [24], the basic security services include authentication, authorization, availability, integrity, confidentiality, and non-repudiation. Therefore, the authors of [24] illustrated only three IoT layers namely Perception, Networking, and Application. Nevertheless, IoT security must also come in the Middleware layer as well as with some other security services including Privacy, Authenticity and Compatibility.

- Privacy needs to be adapted to information as well as devices, this key property must be concerned to the Network and Application layer.
- Compatibility must be concerned to the Network layer.
- The middleware layer must be integrated with confidentiality, integrity and authenticity services [25]. The middleware layer provides these three services to the data exchanged [19].

1) Security services requirements for IoT layers: Generally, security solutions consist of five main objectives as shown in Fig. 2. While, IoT security requirement must be represented by the key properties that are listed below. The IoT security requirements including integrity, availability, confidentiality, authentication, authorization, non-repudiation, privacy, compatibility and authenticity are represented at different layer of IoT as shown in Table II.

a) Confidentiality: It is the property which ensures that only authorized users, under predefined conditions, have access to the information. The IoT system cannot directly apply standard encryption algorithms due to the limited resource of IoT devices. Lightweight cryptographic algorithms are used to guarantee data protection and confidentiality [14].

b) Integrity: It is the property which ensures that information is only modified under predefined conditions. To provide data integrity, a number of cryptographic hash algorithms are utilized, such as MD5 and SH1. However, the majority of these approaches, cannot be used since IoT devices are resource constrained. Many lightweight hash functions were suggested to address this issue [14].

c) Availability: Terminology of the security environment to characterize the proper functioning of the computer system at a given time. IoT device availability is highly necessary. IoT network availability should be handled in both hardware and software. The IoT application's hardware availability refers to every device being present at all times, whereas software availability refers to the capacity to offer services anytime and anywhere[14].

d) Authentication: It is the property that ensures that only authorized entities and users have access to the system or the IoT devices. Authentication protects against identity theft. It is the procedure of validating an identity [14]. Before exchanging data, to connect a device to the network, it needs authenticate itself. Lightweight cryptographic techniques, biometric identification or physical primitives can be used to verify the authentication [14].

e) Authorization: It makes sure that entities have the necessary control permissions to carry out the operation they've requested [13].

f) Non-repudiation: It is the property which ensures that the author of an act cannot then deny having carried it out. The second idea contained in the usual notion of signature is that the signatory undertakes to honour his signature: contractual, legal commitment, he can no longer go back. It is an important element of network security [14]. It is the capacity to assure that an IoT node cannot reject/deny having sent a message and that the recipient cannot deny having received it. Public Key Cryptography can be used to achieve it.

g) Privacy: Attacks on privacy are linked to the unauthorized collection of sensitive information about individuals. When collecting, transmitting, and storing data, data privacy must be considered. The issue of data privacy has received many practical solutions. Stream ciphers, Block ciphers, pseudo-random number generators, and anonymization are some of these methods [14].

h) Compatibility: Of the emerging and the existing IoT protocols in the network layer, the big challenge concerning this layer is the huge heterogeneity of data in term of IoT communication technologies (LoRa, Wi-fi, ZigBee, 4G, etc.).

i) Authenticity: [25] Illegal users are not permitted to access the system or obtain sensitive data.

2) Summary: According to Table II, we showed that generally, the two first layers are missing various security shields. For instance, confidentiality, integrity, authentication, availability, and authorization are the major problems/needs in the physical layer. The network layer requires integrity, availability, authentication, authorization, non-repudiation, privacy and compatibility. If these security requirements have identified in the two first layers, so the risk of unauthorized access can be minimized, this means that if IoT devices and things are secured then, the access control in the middleware and application layers can be achieved.

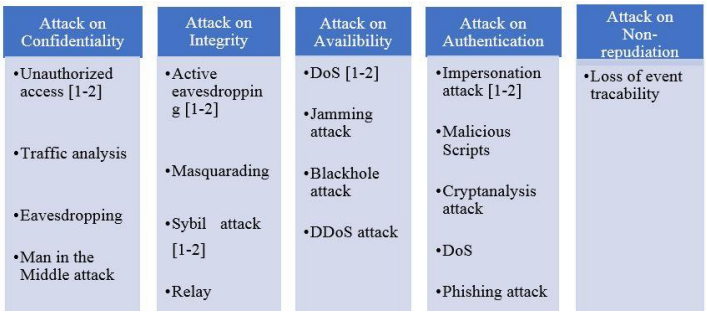

Fig. 2. Taxonomy of IoT Attacks based on Security Concept.

TABLE II. THE BASIC SECURITY REQUIREMENTS FOR IOT SYSTEMS

IoT Layers	**Security Services/concepts**								
	Confidentiality	***Integrity***	***Availability***	***Authentication***	***Authorization***	***Non-repudiation***	***Privacy***	***Compatibility***	***Authenticity***
Physical Layer	✓	✓	✓	✓	✓				
Network Layer		✓	✓	✓	✓	✓	✓	✓	
Middleware Layer	✓	✓							✓
Application Layer		✓		✓	✓		✓		

E. Security Threats and Vulnerabilities Analysis

1) Overview of OWASP Internet of Things Project: Based on an open community and a collection analysis provided by security industry professionals, the Open Web Application Security Project's or OWASP IoT Project released its Top 10 2018 [26], which publish a report that represents the top 10 security problems and issues to avoid when using, managing, creating, deploying an IoT system. This project has listed the main concerns and vulnerabilities of IoT systems based on different IoT architecture levels. The OWASP IoT Project [15] shown that a large number of IoT vulnerabilities are caused by a lack of adoption of existing/common security mechanisms including access control, authentication, role-based access control and encryption. Therefore, because of the complicated characteristics of IoT, establishing and implementing security techniques, measures, practices, and tools is not easy. The Table III represents each security concerns by a number ranged from 1 to 10.

2) Summary: After analyzing this project, author observed that the most of issues and vulnerabilities are surrounding physical layer and most of them target the IoT devices. For instance, "Lack of Physical Hardening" has been identified by this project. This means the lack of physical security measures enables potential attackers to access sensitive data that may be used in a future distant attack or to obtain local control of the device. So, "Lack of Physical Hardening" is the most important concern that tackles the physical layer. In addition, we need to ensure that only the authorized people can access the sensitive data produced by devices or physical objects**.** Besides, if the security will be implemented in the physical layer including IoT things, as well as in the network layer including IoT protocols and communication technologies, then, data theft will be minimized. Consequently, significant enhancements are required to make the IoT framework secure and safe. In the next subsection, we will examine an example of security modeling in IoT systems with a UML extension called IoTsec.

F. Example of IoT Security Systems Modeling with UML

Any artificial language that may be used to convey information, knowledge, or systems in a framework determined by a set of rules is referred to as a modeling language. The UML aims to standardize the various ways for describing object-oriented systems that already exist. IoT interconnects smart entities anyhow and anywhere. Since, IoT rises new issues as well as modeling IoT security systems is a field that lacks the modelling languages for representing IoT systems in several views. The main objective of this subsection is to find the most effective extension instead of a language for IoT security modeling. Based on the characteristic of each tool, we choose two important criteria: (1) specific for IoT systems and (2) System security modeling. The choice of these points depends on our goal which is modeling IoT security. According to the extensions comparison mentioned in [4], we note that UML4IoT and SysML4IoT extensions can model IoT systems, but they lack of security matters. Other extensions like UMLsec, and SysMLsec can be specified for security modeling, but they are not specific for modeling IoT systems. In IoT systems, IoTsec aims at modeling security issues, it is a subset of SysML and UML. It combines UML, SysML, and UMLsec. All these reasons make the IoTsec an ideal example of UML extensions, because it is the only one designed to enable security modeling for IoT systems. In this section, we give an interesting example which used a new UML extension called IoTsec that involves security issues of IoT systems (see Fig. 3). Another example done by [4] shows a layer diagram with IoTsec. Fig. 3 shows a class diagram for an IoT device with IoTsec [4], where an IoTdevice called RapberryPi3. RapberryPi3 uses a relational class N to authenticate a temperature sensor, N means authentication, in this example the attributes N have not been established yet, but they might be any authentication protocol. According to this analysis, we justified the choice of IoTsec as the best UML/SysML extension compared to the existing ones.

TABLE III. OWASP IOT TOP 10 SECURITY CONCERNS –2018 VERSION

N°	The main concerns in IoT systems	Description
1	Weak, Guessable, or Hardcoded Passwords [26]	Use of easily brute forced, publicly available, or unchangeable credentials
2	Insecure Network Services [26]	Unneeded or insecure network services running on the device itself
3	Insecure Ecosystem Interfaces [26]	Lack of authentication/authorization, lacking or weak encryption
4	Lack of Secure Update Mechanism	Lack of ability to securely update the device
5	Use of Insecure or Outdated Components [26]	Insecure software components/libraries that could allow the device to be compromised
6	Insufficient Privacy Protection [26]	All aspects of the IoT architecture that potentially expose sensitive unencrypted data must be taken into account[27].
7	Insecure Data Transfer and Storage [26]	Lack of encryption or access control of sensitive data anywhere within the ecosystem
8	Lack of Device Management [26]	Lack of security support on devices deployed in production
9	Insecure Default Settings [26]	Devices or systems shipped with insecure default settings
10	Weak, Guessable, or Hardcoded Passwords [26]	Use of easily brute forced, publicly available, or unchangeable credentials

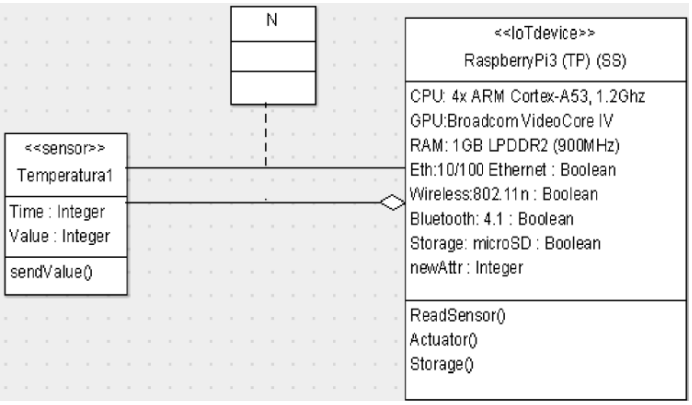

Fig. 3. Example of a Class Diagram for an IoT Device with IoT Sec [4].

For instance, Fig. 4 shows the Ouchani's modeling. For this example, the author suggested IoT architecture enclosed five components:

- Object devices: physical objects embedded with software and sensors.
- User devices: physical objects that collect data from objects and communicate with servers.
- Computing services provided by external, internal, and cloud servers.
- Social actors: human agents that can manipulate and hold devices.
- The environment: the infrastructures which envelops the IoT entities.

These components interact via communication protocols of various ranges (ZigBee, WiFi, Cellular, Human-machine, Bluetooth, SSH, IpSec, etc.). Table IV shows results achieved and describes clearly what has been done before on the problem.

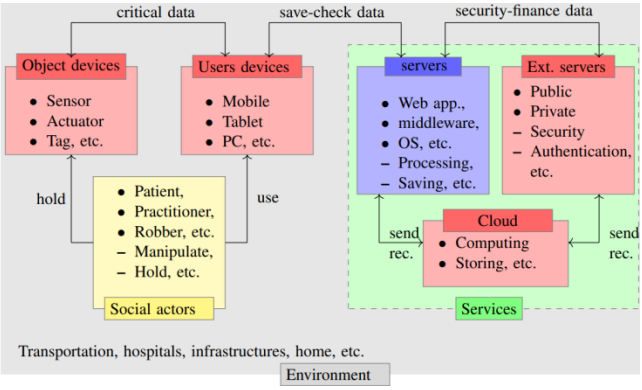

Fig. 4. IoT-SEC Components Architecture [7].

TABLE IV. COMPARATIVE STUDY RELATED TO MODELLING IOT SECURITY

Survey	Modelling IoT security
Jha et al., 2020 [3]	Authors represent the architecture of IoT-Edge computing. Authors modeled an edge infrastructure. So, they implemented and designed numerous new classes.
Robles-Ramirez et al., 2017[4]	Regarding security concerns, authors aim to represent an IoT system. They adopted the four layers architecture including sensing, network, service, and application layer. Moreover, the nomenclature in classes is also shown. Further, this may be reached by the Block Diagram of SysML.
Samir Ouchani, 2018 [7]	The author describes the IoT architecture by presenting the IoT components with their interactions. The suggested IoT architecture enclosed five components including object devices, social actors, user devices, computing services, and the environment.
Proposed	Through this paper, the four-layer IoT architecture (Physical/perception, Network, Middleware, and Application) are proposed. Further, Physical and Network layers are chosen for IoT security modelling, which really contributes to the security of IoT systems

V. RESULTS AND DISCUSSION

In this work, the main idea is to choose the layer whose modelling is relevant. Ensuring security in IoT systems is more difficult due to several challenges. There are four layers generally, so far there is no standardization. So, according to my analysis, we should specify which layer we will work on, otherwise, we model the different layers. Several IoT architectural models have been proposed in the literature. To understand better IoT systems, we choose to work with a four-layer IoT architecture, which is composed with: perception layer, network, middleware, and application layer. Based on all observations and the Tables II and III, author found that there are two layers that must be modelled in IoT security systems, these two layers are called the physical and network layers which contain great challenges, issues, concerns, major attacks and vulnerabilities.

As we discussed in methodology section that security issues and concerns were only designed for both physical and network layers and not for middleware and application layer. In other words, taking the conclusions and results into consideration from each subsection of the previous section, it is fitting that we should only center on physical and network layers, while middleware and application layers are left out. This means that both physical and network layers have specific security concerns, issues, problems, attacks, vulnerabilities, and challenges which are not present in both middleware and application layers. The main focus is on the physical layer and the network layer due to the limitations and constrains brought by the IoT devices as well as the compatibility issue.

In addition, for each layer a detailed analysis has been done in terms of four-layer architecture. The goal is to model IoT security system at the design stage, even if developers are not fully familiar with cyber security concepts. IoT system design is difficult, and UML modeling is proving to be a useful tool for overcoming it. In general, UML, SysML, and ThingML are the three modeling languages. While, IoTsec [4], UMLsec [7], SysMLsec [7], SysML4IoT [7], UML4IoT [8] are some extensions of UML and SysML. Based on extensions comparison which have done in [4], we noticed that, neither UML nor SysML languages can be used for security modeling of IoT systems. Whereas ThingML is the most used language for modeling IoT systems. However, this language only specific for IoT systems and does not model the systems security. The only UML/SysML extension to model IoT security is the "IoTsec".

There are some challenges for modelling/designing IoT applications:

- Heterogeneity: due to its different virtual and physical components with several characteristics that are embedded, forming a complex system; as well as the compatibility problem (communication technologies).
- Interoperability: in terms of infrastructure. Indeed, resources are restricted and limited in the physical layer.

- Distribution: over a large number of processing nodes.
- The absence of a model for addressing security concerns in IoT systems.
- A lack of a design paradigm for IoT applications.
- The lack of standardization in IoT architecture is another restriction.

Thus, the challenge of evolving and deploying software for the IoT is frequently underestimated [28]. IoT applications have two primary characteristics from the standpoint of software engineering. The first factor is the distribution over a large number/range of processing nodes. While, the second one is the high/significant heterogeneity of processing nodes as well as the protocols that connect them [28]. With UML resources, it is possible to represent a small IoT system. UML diagrams and extensions can be used to represent the various views of an IoT environment (security, static, behavioral, etc. [29]). Tables V and VI present the added values and the weakness of each paper to deduce what have been done before on the problem, and what is new.

Therefore, modelling IoT systems is challenging due to their heterogeneity, which is caused by the integration of physical and virtual components, resulting a complex system [29]. Indeed, the IoT is often viewed as a single-issue domain [30]. The UML is a language [29] of general usage for documenting, specifying, visualizing, and constructing artifacts of the software system [29]. Simulating a realistic scenario in IoT is very challenging [31]. The challenge of modeling such complex systems lies in the heterogeneity of these systems, due to their different virtual and physical components that are embedded. Indeed, UML resources are used to represent the various views of an IoT environment or application using its extensions and diagrams [29]. Since security is considered as one of the most crucial quality attributes in networking [32] and also in the field of IoT and software engineering, it is necessary to provide holistic protections for IoT architecture [33].

To answer the research question, author mainly based on the proposed methodology including the results of all subsections and challenges related to the security of IoT systems (IoT layers). As we discussed in the above section, the physical layer can be easily accessed by attackers as well as the main operations of this layer. The IoT communication technologies and protocols of the network layer are susceptible to security vulnerabilities. Both layers impacted differently by the security issues, problems, attacks, threats and vulnerabilities compared to two last layers. Compatibility, heterogeneity and resource constraint of the two first layers made the IoT security worse. All these reasons make security of IoT systems complex and more difficult. Consequently, we need to model the two first layers (physical and network layers).

Finally, the relevant layers to model that really contribute to the security of IoT systems are two layers namely, the physical layer and the network layer. The choice of these two layers poses at least two major and huge problems which may slow down the whole IoT systems development. For that, we should have interested in these two layers more. To sum up, security needs to be modeled in both physical and network layers. According to Table V and Table VI we can notice that a method to design IoT systems with their security issues is required.

TABLE V. COMPARISON OF RELATED SURVEYS

	Objectives	**Results**
[3]	Authors aim to model realistic IoT and edge environments. To model an edge infrastructure, they implemented and designed numerous new classes. IoT & Edge computing	The findings demonstrate that IoTSim-Edge has different capabilities in terms of mobility modeling, heterogeneous protocols modeling, battery-oriented modeling, application composition and resource provisioning for IoT applications.
[4]	For IoT systems the use of the UML was proposed by the authors of [4], with also the suggestion of extensions. Besides, IoTsec was also presented by authors; The aim is to facilitate the representation of security concerns with a visual notation, even if the developers are not totally or completely familiar to Internet cybersecurity concepts.	For modeling common actors, IoTsec uses UML extensions for security encapsulated in UML nomenclature and stereotypes. They aim at detailing the activities developed in three stages.
[5]	Authors aims at modeling environment that enable to deploy, design, and specify complex IoT systems;	The approach introduced by authors uses already IoT-A in the Papyrus for IoT modelling environment.
[6]	Authors suggested extensions and used UML for IoT systems; IoTReq was the proposed method;	The IoT system present peculiar characteristics that necessitate the use of specific approaches to represent their requirements, implementing hardware, software intersection.
[7]	Authors describes the IoT architecture by showing its components with their interactions.	The suggested IoT architecture enclosed five components as shown in Fig. 4.
[8]	Authors aims at using the UML, or UML profiles, for supporting the IoT systems development.	Authors used UML4IoT an UML approach based on the use of UML profile. UML4IoT is an UML profile for IoT

TABLE VI. ANALYSIS OF THE EXISTING SURVEYS

Survey	**Weakness**
[3]	The authors didn't mention some different factors such as storage technology, …
[5]	This paper has not a detailed and comprehensive look;
[7]	The authors don't consider privacy, security and trust domains.
[8]	The mentioned extension does not support Security;
[10]	This paper lacks more experiments. Moreover, the proposed framework suffers from the limitations;

VI. Conclusion

Existing visions have resulted in a lack of knowledge of the architecture of IoT systems. Hence, there is no standardization about the IoT architecture. Moreover, in the previous works, there is no answer about the following questions: Which is the layer whose modeling is relevant? What is/are the relevant layer(s) to model that really contribute to the security of IoT systems? Through this work, several axes have been presented and detailed. Hence, a proposed IoT architecture has also been investigated. Moreover, security concerns at various layers of IoT architecture were described in this study. Then, the challenges of IoT architecture were demonstrated. The chosen or proposed IoT architecture consists of four layers (see Fig. 1), known as the perception, network, middleware and application layer.

This paper covers the modelling of IoT systems. The objective of this article is to model complex systems. Modelling of IoT application in the real environment is difficult, complex, time-consuming and not effective in terms of cost [3]. To facilitate modelling of IoT systems, several languages and extensions have been developed. As a result, this study recommends the use of IoTsec for modeling IoT security because it is the only one that enable us to model IoT systems and security that are our needs/goal. In this paper, we have studied the comparison in terms of IoT layers. Further, a comparison between previous works in terms of modelling IoT security systems have been also made in order to deduce the relevant layer to model that really contributes to the security of IoT systems.

We have studied in detail the architecture of the IoT systems in order to be able to deduce that physical and network layers have many challenges, issues, vulnerabilities, attacks and need more security. In this paper, the physical layer and the network layer are the two layers chosen for modelling. Therefore, the security of IoT systems must be taken and considered in an earlier stage during the design phase.

Our future study will focus on making a comparison between UML and SysML modeling languages to prove the efficiency of SysML with a concrete case of IoT systems which is forest fires.

References

[1] H. Meziane, N. Ouerdi, M. A. Kasmi, and S. Mazouz, “Classifying Security Attacks in IoTUsing CTM Method,” in Emerging Trends in ICT for Sustainable Development, Cham,2021, pp. 307–315. doi: 10.1007/978-3-030-53440-0_32.

[2] M. Hind, O. Noura, K. M. Amine, and M. Sanae, “Internet of Things: Classification ofattacks using CTM method,” in Proceedings of the 3rd International Conference onNeworking, Information Systems & Security, New York, NY, USA, Mar. 2020, pp. 1–5. doi: 10.1145/3386723.3387876.

[3] D. N. Jha, K. Alwasel, A. Alshoshan, X. Huang, R. K. Naha, S. K. Battula, S. Garg, D. Puthal, P. James, A. Zomaya, S. Dustdar, and R. Ranjan, “IoTSim-Edge: A simulation framework for modeling the behavior of Internet of Things and edge computing environments,” Software - Practice and Experience, pp. 1–19, 2020.

[4] D. A. Robles-Ramirez, P. J. Escamilla-Ambrosio, and T. Tryfonas, “IoTsec: UML Extension for Internet of Things Systems Security Modelling,” in 2017 International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE), Nov. 2017, pp. 151–156. doi: 10.1109/ICMEAE.2017.20.

[5] S. Dhouib et al., “Papyrus for IoT—a modeling solution for IoT,” Proceedings l’Internet des Objets (IDO: Nouveaux Défis de l’Internet des Objets: Interaction Homme-Machine et Facteurs Humains. Paris, France, 2016.

[6] G. Reggio, “A UML-based proposal for IoT system requirements specification,” in Proceed-ings of the 10th International Workshop on Modelling in Software Engineering - MiSE ’18, Gothenburg, Sweden, 2018, pp. 9–16. doi: 10.1145/3193954.3193956.

[7] S. Ouchani, “Ensuring the Functional Correctness of IoT through Formal Modeling and Verification,” in Model and Data Engineering, Cham, 2018, pp. 401–417. doi: 10.1007/978-3-030-00856-7_27.

[8] K. Thramboulidis and F. Christoulakis, “UML4IoT—A UML-based approach to exploit IoT in cyber-physical manufacturing systems,” Computers in Industry, vol. 82, pp. 259–272, Oct. 2016, doi: 10.1016/j.compind.2016.05.010.

[9] D. Ferraris, C. Fernandez-Gago, and J. Lopez, “A model-driven approach to ensure trust in the IoT,” Hum. Cent. Comput. Inf. Sci., vol. 10, no. 1, p. 50, Dec. 2020, doi: 10.1186/s13673-020-00257-3.

[10] N. Harrand, F. Fleurey, B. Morin, and K. E. Husa, “ThingML: a language and code genera-tion framework for heterogeneous targets,” in Proceedings of the ACM/IEEE 19th Inter-national Conference on Model Driven Engineering Languages and Systems, Saint-malo France, Oct. 2016, pp. 125–135. doi: 10.1145/2976767.2976812.

[11] F. Alkhabbas, R. Spalazzese, and P. Davidsson, “Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study,” Internet of Things, vol. 7, p. 100084, Sep. 2019, doi: 10.1016/j.iot.2019.100084.

[12] K. K. Patel, S. M. Patel, and P. Scholar, “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges,” p. 10, 2016.

[13] M. Dabbagh and A. Rayes, “Internet of Things Security and Privacy,” in Internet of Things From Hype to Reality, Cham: Springer International Publishing, 2017, pp. 195–223. doi: 10.1007/978-3-319-44860-2_8.

[14] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, “A Review of Security in Internet of Things,” Wireless Pers Commun, vol. 108, no. 1, pp. 325–344, Sep. 2019, doi: 10.1007/s11277-019-06405-y.

[15] A. Alkhalil and R. A. Ramadan, “IoT Data Provenance Implementation Challenges,” Pro-cedia Computer Science, vol. 109, pp. 1134–1139, 2017, doi: 10.1016/j.procs.2017.05.436.

[16] H. Akram, D. Konstantas, and M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model,” ijacsa, vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090349.

[17] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Access, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[18] J. Deogirikar and A. Vidhate, “Security attacks in IoT: A survey,” in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Feb. 2017, pp. 32–37. doi: 10.1109/I-SMAC.2017.8058363.

[19] M. S. A. Reshan, “IoT-based Application of Information Security Triad,” International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 24, Art. no. 24, Dec. 2021, doi: 10.3991/ijim.v15i24.27333.

[20] M. B. Barcena and C. Wueest, “Insecurity in the Internet of Things,” Security response, symantec, vol. 20, 2015.

[21] J. Sengupta, S. Ruj, and S. Das Bit, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” Journal of Network and Computer Applica-tions, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[22] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “IoT Security: Ongoing Challenges and Research Opportunities,” in 2014 IEEE 7th Interna-tional Conference on Service-Oriented Computing and Applications, Nov. 2014, pp. 230–234. doi: 10.1109/SOCA.2014.58.

[23] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, “Internet of Things (IoT): Taxonomy of security attacks,” in 2016 3rd International

Conference on Electronic Design (ICED), Aug. 2016, pp. 321–326. doi: 10.1109/ICED.2016.7804660.

[24] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things Security: Challenges and Key Issues," Security and Communication Networks, vol. 2021, p. e5533843, Sep. 2021, doi: 10.1155/2021/5533843.

[25] C. Ataç and S. Akleylek, "IoT Çağında Güvenlik Tehditleri ve Çözümleri Üzerine Bir Araştırma," European Journal of Science and Technology, pp. 36–42, Mar. 2019, doi: 10.31590/ejosat.494066.

[26] "OWASP Internet of Things | OWASP Foundation." https://owasp.org/www-project-internet-of-things/ (accessed Apr. 13, 2022).

[27] M. M. Anghel, P. Ianc, M. Ileana, and L. I. Modi, "The Influence of Privacy and Security on the Future of IoT," IE, vol. 24, no. 2/2020, pp. 42–53, Jun. 2020, doi: 10.24818/issn14531305/24.2.2020.04.

[28] B. Morin, N. Harrand, and F. Fleurey, "Model-Based Software Engineering to Tame the IoT Jungle," IEEE Softw., vol. 34, no. 1, pp. 30–36, Jan. 2017, doi: 10.1109/MS.2017.11.

[29] M. T. B. Geller and A. A. de M. Meneses, "Modelling IoT Systems with UML: A Case Study for Monitoring and Predicting Power Consumption," American Journal of Engi-neering and Applied Sciences, vol. 14, no. 1, pp. 81–93, Feb. 2021, doi: 10.3844/ajeassp.2021.81.93.

[30] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home envi-ronments," Information, vol. 7, no. 3, p. 44, 2016.

[31] G. Kecskemeti, G. Casale, D. N. Jha, J. Lyon, and R. Ranjan, "Modelling and simulation challenges in internet of things," IEEE cloud computing, vol. 4, no. 1, pp. 62–69, 2017.

[32] K. Ahmed, S. Verma, N. Kumar, and J. Shekhar, "Classification of Internet Security Attacks," in Proc. 5th Natl Comput. Nation Dev., Delhi, India, Mar. 10-11, 2011.

[33] K. Chen et al., "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," Journal of Hardware and Systems Security, vol. 2, no. 2, pp. 97–110, 2018.