Internet of Things: Security Between Challenges and Attacks

Benali Cherif, Zaidi Sahnoun, Maamri Ramdane, Bouchemal Nardjes

Internet of Things: Security Between Challenges and Attacks

Benali Cherif[1], Zaidi Sahnoun[1], Maamri Ramdane[1], Bouchemal Nardjes[1,2]
[1]*Lire Laboratory- A. Mehri* ,Constantine, Algeria
[2]*University Center Abdelhafid Boussouf of Mila, Algeria*
cherif.benali@univ-constantine2.dz, zaidi.sahnoun@univ-constantine2.dz,
ramdane.maamri@univ-constantine2.dz, n.bouchemal.dz@ieee.org

***Abstract*— In recent years, the fast developments in hardware, software, networking and communication technologies have facilitated the big emergence of many technologies such as Internet of things. Measurement and collecting data from physical world, and then sending it to digital world is base of this technology. The transmitted data are stocked, processed and then possibly used to act upon the physical world. IoT adds intelligence and autonomy to many domains (e.g. health care, smart transportation and industrial monitoring). As a result, it makes human life more comfortable and simple. However, as all emerging technologies, IoT is suffering from several security challenges and issues, especially that most of IoT devices and sensors are resources- constrained devices. As security issues and attacks could put systems in dangerous and could threat human life too, this paper treats these problems. We will provide an overview about IoT technology, and we will present various security issues that target the perception and the network levels. Moreover, we will discuss how each layer is damaged by harmful and malicious purposes. Most of recent papers use the three layers architecture (which is an old architecture) to present security problems; but this paper uses one of the new reference architectures to study security threats and attacks.**

Keywords*— *IoT architectures, security, challenges.

I INTRODUCTION

The internet of things (IoT) could be seen as the second version of Internet, where large number of physical objects (e.g. intelligent devices, sensors, actuators etc.) have the ability to sense, collect data, and communicate with each other without any human assistance .This technology gives many services in several application domains such as health care, smart industry, and smart homes [12]. Nevertheless, with the great benefits of IoT, there are many problems, challenges and issues of security which require deep and serious thinking. Nodaway, security problems are increasing seriously [03], where IoT has not only the same security issues of its construction technologies, but it has more [01].

Today, IoT architecture is very important, because a good architecture is the main key to create a secure IoT system. But, there is no universal architecture used by all the constructors to shape an IoT system [08].

For that, this paper provides an overview about IoT technology and presents the key problems of security. It reposes on three main phases: In the first one we give an overview about IoT technology and we present two main IoT architectures. The second phase presents IoT security challenges that face the implementation of security policies. It presents also the security feathers in IoT (CIA security triad).Finally, the third part is reserved to present the most important security attacks and issues of perception (sensing) and network levels. In order to analyze the IoT security issues and attacks in more details, this part presents and classifies them using IBorgia et al [15]. ++ this paper is organized

II IOT OVERVIEW

In 1999, Kevin Ashton was the first person that used the term Internet of things (IoT). IoT uses a set of sensor nodes and intelligent devices to collect data from physical world (environment), and then send it to the digital world. RFID and WSN are the two main technologies used to collect and send data in network level. After that, the data get processed and delivered to final application and end-users [05].

IoT may be defined as a dynamic worldwide network infrastructure of intelligent devices and sensor nodes, which are able to configure themselves automatically and they can make their own decisions without human intervention. Each IoT device has a unique identifier that allows this device to communicate with others (IoT devices use many types of communication protocols) [13].
There are many application domains of IoT such as the following: [07]

- Smart energy, smart homes, Smart Buildings, smart cities.
- Internet connected cars and buses (smart transportation) ,health care and fitness monitoring(smart watch and bracelets)
- Earth supervision and environment monitoring (water quality, fire detection, air pollution monitoring etc.), industrial monitoring.
- Smart devices like tablets and smart phones.

A. The Three layers Architecture

It presents the first IoT architecture which is composed of three layers: Perception layer, Network Layer and Application layer [06], Fig.1.

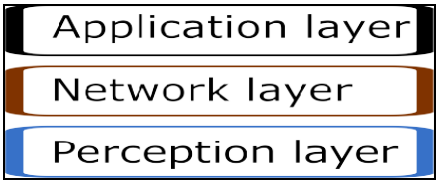

Fig. 1. Three Layers Architecture of IoT.

1. *Perception layer*: Known also as physical layer, is the responsible layer of interconnecting and identifying the different IoT devices [07].It uses a very large number of smart devices and sensor nodes to collect data from physical word (environment) [05, 06] . To connect with other devices, each device must be identified with unique identifier [07].

2. *Network layer*. The main objective of this layer is gathering information that is obtained from physical layer, and then transfers it to application layer. WSN and RFID are the main two technologies used to collect and send data.
   This layer is the responsible of the communication between different devices, using many communication protocols (e.g. MQTT, CoAP…) and technologies (e.g. ZigBee, Bluetooth, WI-Fi...) [05, 06].

3. *Application layer*. It presents the top layer of this architecture, which takes two main responsibilities: data storage and processing, and provide a set of services to different applications (final users) [06].This layer is service-oriented that offers data to different kind of final users and applications, to satisfy their needs. There are many applications domains such as smart transportation and healthcare [07, 04].

B. IoT layered Architecture of IBorgia and al.

Borgia and al. propose an IoT architecture that is very helpful to solve the interoperability and security issues . It has six different layers, presented in figure Fig. 2. [8, 15].
From the bottom to up we have:

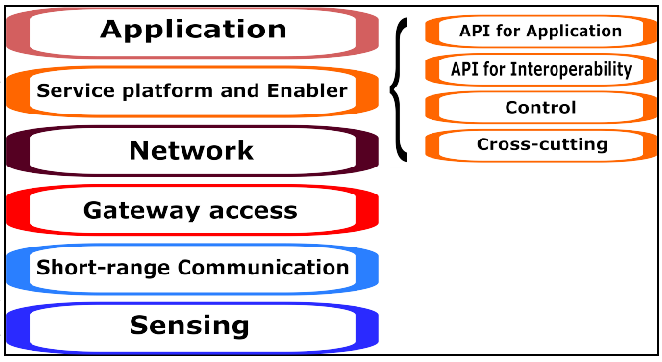

Fig. 2. IBorgia and al IoT architecture.

- Sensing layer is responsible layer to percept and collect data from physical world using a large number of sensor and device nodes.

- The three layers *Short-range Communication*, *Gateway access* and *network*, serve as Communication Bridge between *Sensing* and *Service platform and enabler* layers. They use many standards and technologies to exchange data [11]. The idea of splitting the network level into three layers comes from the fact that the existing internet protocols (such as HTTP) require a memory size and power capabilities, which is an issue for small devices, We have to point out that most of IoT devices are

small and weak devices [10].

- Most of IoT devices and sensor nodes are characterized with low processing capabilities, limited storage and constrained memory.

  Moreover, they usually implement only two or three bottom layers of OSI, and they are mostly not directly compatible with TCP/IP. Gateways can solve this problem, because they use HTTP protocol to communicate with each other and they support specialized protocols and technologies to interact with physical sensor and devices [09].

  They enables their connection with high bandwidth networks (the network layer) [08], and they support aggregation, processing, and bridging [10]. In Short-range Communication, IoT devices are usually interconnected through a short range wireless network (WSN), where several technologies are used (e.g. Bluetooth, Z-wave, ZigBee).

- IoT Service platform and Enabler: The fifth layer includes software and services to control the IoT system (storage, processing etc.).It guarantees many non-functional requirements such as security, safety, and availability.

- Application layer is the top layer of this architecture. It is a service-oriented layer that offers services to final applications and users, such as services and software devoted to smart transport, Health care and energy monitoring.

III SECURITY CHALLENGES IN IOT

This section will present the main challenges that face implementation of security policies. Security trends in IoT will be also presented.

A. IoT security challenges

Security in IoT domain has many challenges that complicate the construction of security solutions and policies, such as the following:

- The limitation of resources: IoT devices have usually limited resources such as low processing power, limitations of energy and memory. These limitations complicate the implementation of powerful encryption algorithm in IoT systems [13, 09]. Moreover, most of devices are resource constrained and they have not enough hardware and software to support TCP/IP protocol and security protocols [12].

- Heterogeneity of devices and network technologies: IoT use many types of sensors, devices and network technologies and this can result many security problems. It complicates also the creation of powerful security policies [12].

- Lack of standardization: there are not unique standards that all the constructors of IoT devices use. Each vendor uses his own standards, protocols and technologies [12].

- The integration of the physical and cyber domains exposes the system to attacks. Cyber attacks may target the cyber domain and paralyzes the physical domain (IoT devices) [14].

- IoT devices are placed everywhere, so they can easily be damaged, stolen, and get unauthorized access [11].

- The proposed techniques and security methods are essentially based on traditional network security methods. However, IoT system is more challenging than traditional networks, due to the heterogeneity of devices and protocols [14].

- Millions of devices could be used in an IoT system (e.g. a system to measure the temperature all around

the country), which result unmanageable amount of data [02].

B. Security trends and feathers in IoT

Security includes many trends or feathers, but in this section we present the three main trends and the security triad CIA (confidentiality, integrity and availability) [11, 04].

1. Confidentiality

It is a security characteristic and it means that just the sender and the receiver can read the exchanged information. So, data must be protected in all communication process: in sender and receiver sides, and during data transportation in network. [11].

2. Integrity

It refers to the absence of unauthorized data changing (modification) .So, in all process of communication; the data must not get modified in the sender side, the receiver side and between them. The unauthorized data modification compromises this security trend [11].

3. Availability

It means that the system or the service (or a device) is available and accessible to his clients, and everything is offered correctly. The availability is stolen if the target system or service is inaccessible, or the client couldn't even make a communication with it [11].

IV RELATED WORK

This section will present three propositions to solve the security problem in IoT.

A. Ioannis Andrea and Al classification of IoT security attacks

According to the authors [7], this contribution is a new classification of different types of attacks. Compared to other classifications, this one is unique, because it uses four distinct classes to divide the current different attacks. The four classes are: Physical, Network, Software and Encryption attacks. We have to note that this classification is based on the target point of attacks to classify them. So the attack can target the system physically (IoT devices), or its network, or from applications (that are running on devices) on the system, and finally from encryption schemes.

1. Physical Attacks:

In this type of attacks, the physical components (devices or things) are the target of attacker. The goal of this type of attack is to compromise security feathers as availability. It can be just to harm the target component(s) (the functional roles) or as an enter point to harm all the system. To make the attack works, the attacker has to be in the IoT system (as a foreign element) or physically close. Many attacked could be mentioned such as: Malicious Node Injection, Physical Damage*, and Node jamming (in WSNs).*

2. Network Attacks

Contrary to the previous type, the attacker doesn't have to be close or near the IoT system, he can make the attack works remotely. This class contains a set of attacks which threat the level network of the IoT system. The communication between the different physical devices is guaranteed by the network level (layer), so network attacks are very dangerous for information confidentiality and privacy. There are many attacks but the most important are: Traffic Analysis Attacks, Routing Information Attacks, RFID Unauthorised Acces.

3. Software Attacks

In this type of attack, the software part of IoT system is the source of vulnerabilities. The attack is basing of the use of deferent types of malicious programs to steal information, change and tamper the system data, deny of service and even harm the IoT system devices. The main tools (malicious programs) that are used in this class are: worms, Trojan horses, spywares, viruses and malicious scripts. The main attacks in this class are: *Phishing Attacks Malicious, Script Attack,* and *Denial of Service.*

4. Encryption Attacks

The IoT system uses encryption scheme to protect the exchanged data between devices. This class gathers a set of attacks that try to break the encryption scheme of IoT system (generally, the goal of attack is to obtain the encryption key that has being used for encrypting and decrypting data. *Side channel Attacks* and *Cryptanalysis Attacks are the main* encryption scheme *attacks.*

A summarized representation of this classification is shown in table below:

CLASSIFICATION OF IOT ATTACKS

Physical Attacks	Network Attacks	Software Attacks	Encryption Attacks
Node Tampering	Traffic Analysis Attacks	Virus and Worms	Side Chanel Attacks
RF Interference	RFID Spoofing		Cryptanalysis Attacks: a) Ciphertext Only Attack b) Known Plaintext Attack c) Chosen Plaintext or Ciphertext Attack
Node Jamming	RFID Cloning	Spyware and Adware	
Malicious Node Injection	RFID Unauthorised Access		
Physical Damage	Sinkhole Attack	Trojan Horse	
Social Engineering	Man In the Middle Attack		
Sleep Deprivation Attack	Denial of Service	Malicious scripts	Man In the Middle Attack
Malicious Code Injection on the Node	Routing Information Attacks	Denial of Service	
	Sybil Attack		

Fig. 3. A summarized representation of AIoannis A and Al's

B. Abdul W.A and Al classification of IoT security

In this classification, the four layers architecture of IoT has been used to classify the different attacks (the aim of the paper is to discuss security of four layered architecture of IoT). So, in each layer, this classification presents the possible attacks that could be, as shown in the next figure: [5]

The four types of attacks are: [5]

1. Physical Layer attacks

The *Physical Layer* is the responsible layer of collecting information from the physical word by using a set of sensor nodes and intelligent devices, and ensures the communication between these physical equipments. Those devices (hardware parts of an IoT system) are the target of the physical layer attacks to: cause damages on the physical node, steal the data confidentiality and integrity, and deny the access to services. To achieve his attack, the adversary has to be close to IoT system. There are many physical attacks such as *Node Tempering*, Unauthorized Access to the Tag and Tag cloning.

2. *Network Layer attacks*

In this type, the attacker concentrates on the network level of the IoT system, which presents the communication bridge between different physical devices and sensor nodes. The network layer gathers information which is obtained from physical layer (collected by devices), and then transfers this data to processing layer, so attackers find it as a good part or level to steal information. There are many network attacks such as: *RFID Spoofing, RFID Unauthorized Access.*

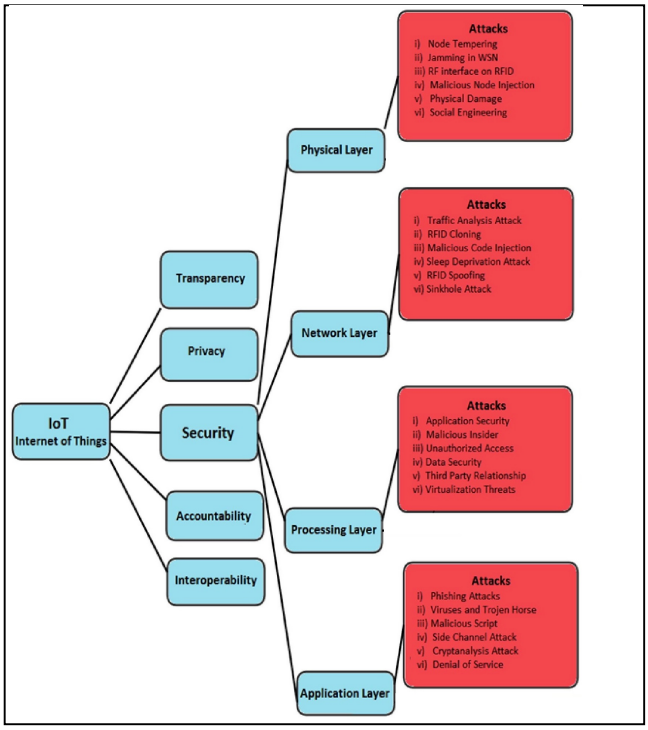

Fig. 4. Abdul W.A and Al classification [5]

3. *Processing Layer attacks*

The processing layer is the responsible of the storage, the processing, and data analysis, as a result, this qualifies it to be a good level to practice several malicious activities by attacker. Most of attacks are inherited from the used technologies (such as cloud computing attacks).This type of attacks gathers many attacks
such as: *Malicious Insider, Virtualization threats.*

4. *Application Layer attacks*

The application layer is service oriented layer which provides the processed information to the final users (applications such as healthcare, smart homes etc.) as services. In this layer, the attackers use malicious programs to harm the systems, such as viruses, spywares, Trojan horse and worms. The application layer attacks present a serious type of attacks, they are used to: steal private and confidential data, altering data, damage the IoT devices, and get unauthorized access. There are many attacks like: Virus, Worms, Trojan Horse and Spyware attacks, Malicious Scripts attacks, and Denial of Service.

C. A systemic approach for IoT security

In the paper [16], the aim of authors is the exploration of a new approach to design security mechanisms and deployment in IoT context. They propose a systemic (and cognitive) approach to ensure the IoT security, and to explore each actor's role and its interactions with the other principal actors of the proposed scheme. The paper [16] sees the IoT system as a complex system in which people interact with intelligent devices.

In this proposed approach, the set of connections between different nodes have a specific character depending on complex nature of IoT environment. Moreover the paper [16] takes into consideration the dynamic and complex nature of this proposed model. It presents its perspective in respect of the main elements illustrated in the approach which are "nodes" and "tensions".

The interactions between nodes are represented by tensions. The nodes are the origination and destination actors of a tension. This approach takes into consideration the environment complexity. The approach is presented in the figure 5.

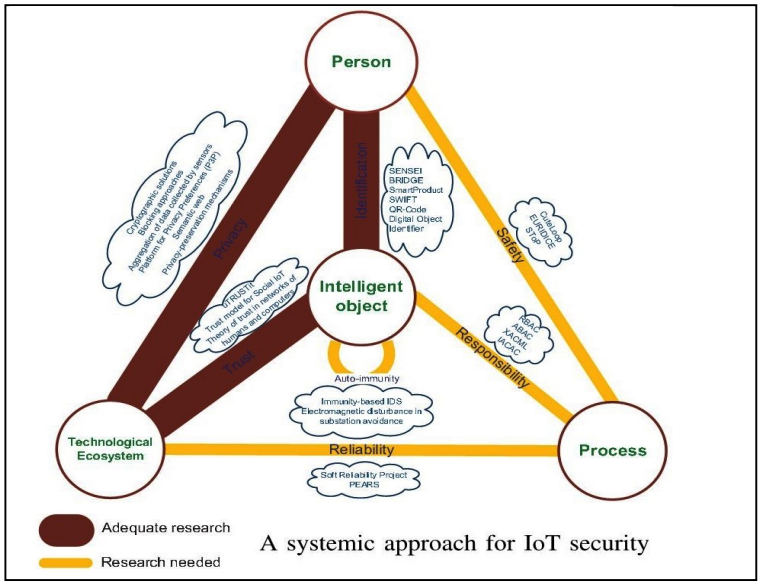

Fig. 5. A systemic approach for IoT security [16]

In order to explain this model, we will describe each node and its functions briefly .The tensions between different nodes need a special study and discussion; we will try just to explain them shortly:

1. Nodes

There are four nodes: Person, Process, Intelligent Object, Technological ecosystem[18]

- *Person.* The human resources play a principal role in the IoT security, because they are responsible for security rules management that includes: the definition of security rules and practices, ensure efficiency of rules, auditing and verification practices. This vital node plays an essential role in the management and enhancement of security. So, the person node should be able to analyze all the context of IoT.

- *Process.* This node refers to a resources or a means that are used to accomplish tasks, and to guarantee security requirements. In order to ensure the security of the environment at different levels, the process has to be conformable and compliant with the security policies. Furthermore, there is a big difficulty to implement security processes, because the model is complex and the existence of several interactions originating from the process node. According to practices, security process has to face many requirements such as requirements of standards, requirements of strategies, requirements of policies etc.

- *Intelligent Object.* This node presents the heart of this approach; it refers to an "object" enhanced with electronic capabilities to communicate with other objects in his environment (intelligent devices). An object can exchange information, cooperate and connect with other objects.

- *Technological ecosystem.* The technological choices (technologies) that have been made to ensure the security of IoT is represented by this node. There are many categories of information security technology (or technologies) such as Identification and Authorization, and Security Design and Configuration.

2. Tensions

Tensions represent the interaction between nodes. The paper [18] presents 7 tensions: Identification and authentication, Trust, Privacy, Responsibility, Autoimmunity, Safety, and Reliability. This part wills discuss them: [18]

- *Identification and authentication.* This tension attaches the two nodes: *intelligent object* with the *person.*In IoT context, each entity must be identified, to ensure a correct communication between entities, and to guarantee the absence of unauthorized access. Radio Frequency Identification (RFID) is the main technologies used in IoT to connect different devices.

- *Trust.* The "Trust" tension attaches the technological ecosystem node with the intelligent object node. Basically, we can say that Trust represents the level of confidence that the environment can grantee to the intelligent object (if the level is reliable and dependable or not).

- *Privacy.* The tension that attaches the person with the technological ecosystem is "privacy". The ubiquitous characteristic of the IoT environment make the privacy an important tension in the systemic model of IoT security.

- *Responsibility.* The "Responsibility" tension attaches the *process* node with the intelligent object. It means the set of access rights and privileges, which have to be clearly specified and defined evidently, depending on privacy constraints. Moreover, in order to avoid dangers when the object regulates a process; the set of rules of liabilities and responsibilities for each entity must be taken in consideration.

- *Autoimmunity*
  The tension that attaches the *intelligent object* in self loop (with its self) is "Autoimmunity". Proposing an artificial immune system solution for IoT is the aim of this tension.

- *Safety*
  The "*safety*" tension attaches the two nodes: person with process. Ensuring safety when an unexpected problem (egg: failure, attack …) appears, is one of the main security challenges that the IoT system has to face (and overcome it).So, the reduce damage possibility is considered by safety

- *Reliability*
  The tension that attaches the process node with the technological ecosystem node is "Reliability". The goal of this tension is to guarantee the availability of data and information, using efficient ways of managing data repositories. It deals with communications management and data

V. SECURITY ATTACKS AND THREATS IN IOT

IBorgia and al. architecture offers an interesting functional view for IoT system, and it satisfies the recent requirements of IoT system. It catches the main features of an IoT system that are: the interaction between the local and personal networks of sensors nodes on one side and the interaction between high- bandwidth networks with computation power systems in the other side.
Basing on these considerations, we adopt this architecture as a mould (model), to analyze security issues and attacks in IoT system. The main security attacks are presented in the figure *Fig.3*

Sensor-based threats present a serious family of IoT security threats [02], which could be classified into four categories, basing on intentions and nature of these threats. These categories are: (1) Information Leakage (2) Transmitting malicious sensor commands (3) false sensor data injection (4) denial of-service (DOS) [01].

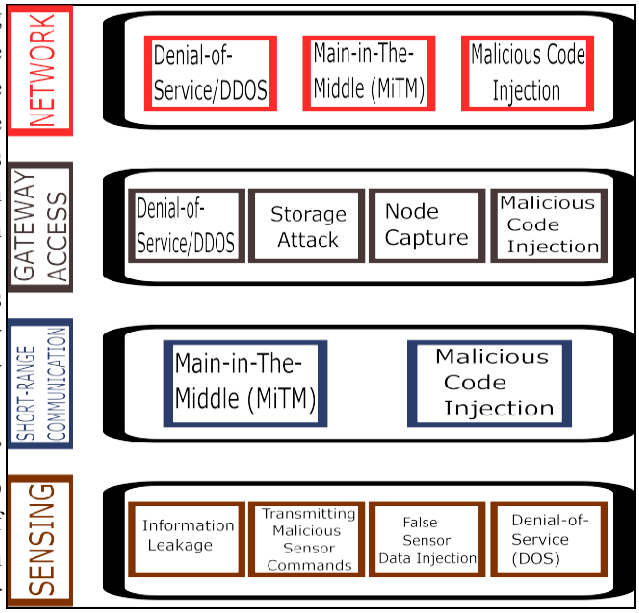

Fig. 6. Some Security attacks in IoT (using IBorgia Architecture)

1. Information Leakage

IoT sensors could stock sensitive data like login, passwords, and credit card information; and the steal of this data puts the user privacy and IoT system security in danger. IoT attacker can use a sensor information to achieve his attack (or information from multiple sensors to achieve a more complex attack).
In this category, four methods could be used: keystroke inference, task inference, location inference, or eavesdropping [01], *Fig. 7.*

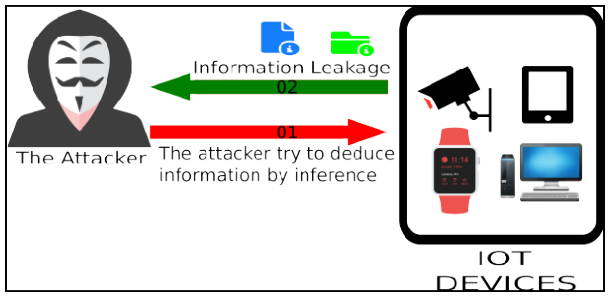

Fig. 7. Information Leakage method Sensing layer

- *Keystroke Inference.* In this method, the attacker try to deduce the keystrokes entered in the IoT device.
  When a user types (or gives) inputs to his device, tilts it, or turns it, a set of deviations are resulting. These deviations are used later by the attacker to infer the entered data. Keystroke Inference can be performed on the device itself or by using nearby sensor.
  This attack can be performed using magnetic Sensors, light Sensors, audio Sensors, and video Sensors [01].

- *Task Inference.* This type of attack is based on the deduction (the reasoning), in which the attacker tries to extract information about the ongoing task or application inside the target device. This information presents the state of the device and used to start an attack, without alerting the device security policies.
  The idea of this attack starts from the fact that sensors show deviation in the reading process for various tasks running on the devices, and this deviation can be used to infer the running process or application inside this device.
  Task inference can be performed using magnetic Sensors, Power Analysis etc. [01].
  For example, Timing Attack is a task inference attack, which enables the discovery of vulnerabilities and extracting information about security policy.
  Timing attack is done by observing the responding time for different inputs and queries to determine the cryptographic algorithms implemented in the system.
  It is usually used with small devices that have weak computing capabilities [03, 05].This attack threats the data confidentiality.

- *Location Inference.* This type of attack is used to determine the victim location, which is private and sensitive information in itself, and use it to launch another attack.
  This attack steals the location-privacy. The attacker use acoustic information embedded in an audio source (e.g. audio messaging) to identify sensitive locations of the target entity. For example, this attack could be used to compromise location privacy of participant in anonymous session. This information is used to produce a location fingerprint [01].

- *Eavesdropping.* in this type of attack, a malevolent application uses an audio sensor (e.g.: microphone) to listen to a private conversation secretly. After that, the attacker tries to extract confidential information from this conversation (e.g. social- security number and credit card information).
  The attacker can record the conversation on a storage device or listen to it in real-time [01,03].
  For example, replay attack (or play back attack) uses the eavesdropping to steal authentication information from the sender and then use it to send a request message (Identity stealing) [03]

2. Transmitting Malicious Sensor Commands

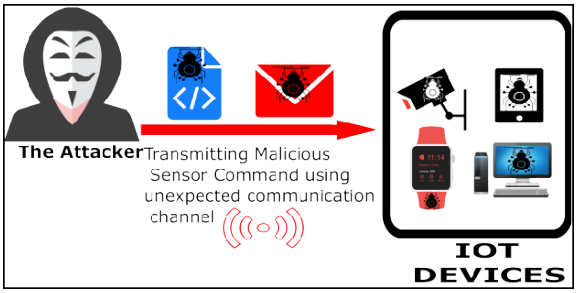

Fig. 8. Transmitting Malicious Sensor Commands method

Today, most of IoT devices and sensors allow the creation of unexpected communication channel with other entities. This weak point could be used by attacker to create a communication channel, and then he launches his attack. This attack could change critical parameters of the target sensor (e.g. light intensity), or even transmit malicious commands (trigger messages) to activate a pre- planted malware [01]. The malicious program (virus or malware) could be inserted into the device physically, or via Malicious Code Injection attack. As a result, the attacker gains a full access to that node, and then he can control all the IoT system [01]. There are many methods to transmit signals and malevolent commands such as using a audio sensors, light sensors, or a magnetic sensors [01], *Fig.8.*

3. False Sensor Data Injection

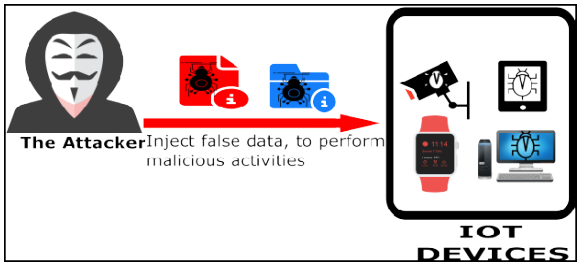

Fig. 9. False Sensor Data Injection method

IoT system uses different devices and sensors to collect very important and sensitive data. We could not imagine the results if a patient data in a hospital have been altered or faked.

False sensor data injection is an attack where the sensor data is forged (faked), or even to inject false data. It's used to perform malicious activities. The attacker use specific commands to change the real information or to modify the device's actions. This attack needs a physical access to the target device or a remote access by using various communication medium (Wi-Fi, Bluetooth, etc.) [01]. For example, Malicious Fake Node attack belongs to this type, in which the attacker uses a fake node to inject false data [03], *Fig.9.*

4. Denial of-Service (DoS)

	Confidentiality	**Integrity**	**Availability**
Information Leakage	YES	NO	NO
Transmitting Malicious Sensor Commands	YES	YES	YES
False Sensor Data Injection	NO	YES	YES
Denial of-Service (DOS)	NO	NO	YES

TABLE I. THE STOLEN SECURITY TRENDS OF EACH ATTACK TYPE

In this section, we talk about Denial-of-Service (DoS) for a sensing and perception device. DoS for a device is a type of attack to deny maliciously the normal operation of this device, and to forbid the access to it.

There are two types of DoS attacks: active and passive attacks. In active attacks, the access to an application, a task or a device is refused effectively. However, if one application has been attacked to stop another ongoing task on the device, we call this a passive attack [01]. DoS attack could have an after-effect to exhaust the system resources, such as battery and memory resources [03]. For example, DoS attack is used with gyroscopes of drones and accelerometers to shut the device down [01].This attack will be more explained in a next part.

From the explication above for each method, we conclude that each type can threat one or more security trends. This is represented in the next table TABLE I.

Note that, results of a type of attack (or all the attack) could be used to launch another attack (The second attack can threat another security trends). That is called composition of attacks.

A. Short-range communication, Gateway access and Network layers

Short-range communication, Gateway access and network represent together the network layer of the three layers architecture [08, 11]. They have many common attacks, but with some specifications in each one.

That is why this section treats them together, and it presents the attack specification in each layer. The network level has many attacks but the main ones are:

1. Denial of Service (DoS)

It is an attack to deny authentic users to access a device or a network resource. The attacker accomplishes this attack by flooding the targeted component with redundant requests. He inundates the network traffic by sending a large amount of data, and this results massive consumption of system resources. The flooding process makes the system or the target device inaccessible or difficult to use by some or all authentic users [03], Fig.10.

The DoS attack has a distributed version called distributed DoS (DDoS). DDoS attack is defined as a set of concurrent DoS attacks. The attacker could use botnet army, which is an army of IoT devices that are infected with malwares. DoS and DDoS attacks may cause energy dissipation issues and physical damage [04], Fig.11.

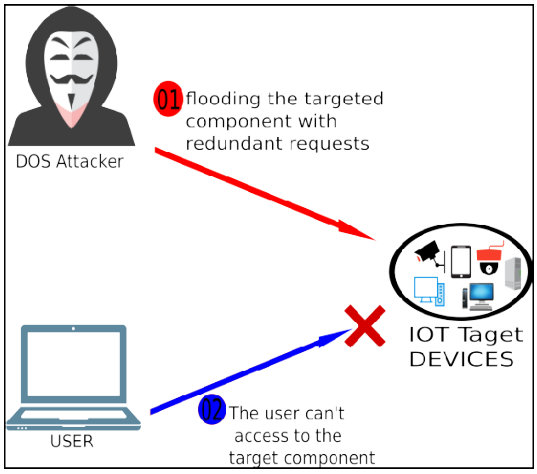

Fig. 10. Denial of-Service (DOS) attack

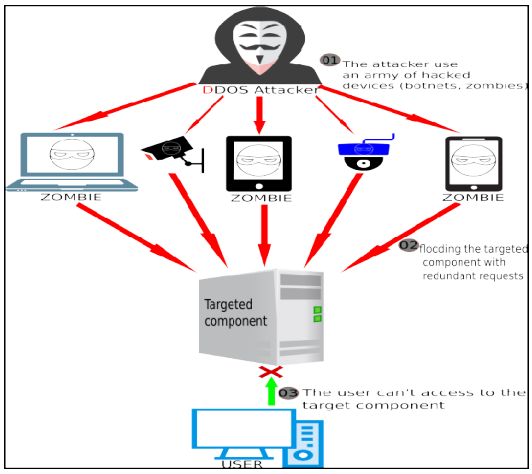

Fig. 11. Distributed Denial of-Service (DDoS) attack

2. Man-in-The-Middle (MiTM)

In this attack, the hacker plays secretly a role of a mediator between the sender and the receiver who believe they have a direct communicating with each other.
He becomes the controller of all the communication; therefore he can capture, change and manipulate the communication information in real time according to his needs.
It is a serious security threat that steals the integrity of information [03]. MITM is also known as Malicious Node Injection because the attacker injects (plants) a new malicious node between the sender and receiver, to control all the exchanged data [05], Fig.12.

3. Storage Attack

In this attack, the hacker tries to get the stored data and information inside the target node. For example, the gateway node can store sensitive user information, and that make it a good target for attackers. The gateway can be attacked to change or delete his stored information [03], Fig.13.

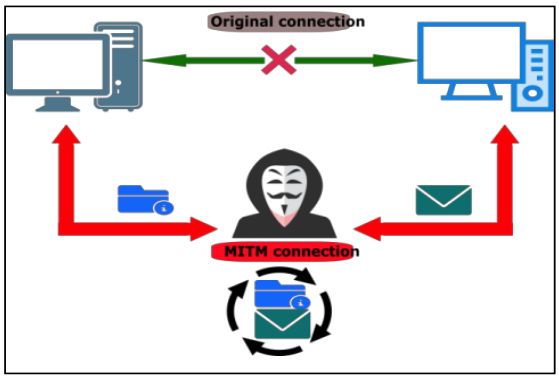

Fig. 12. Man-in-The-Middle (MiTM) attack

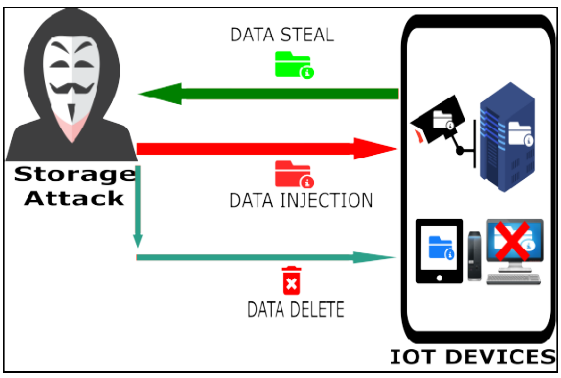

Fig. 13.Storage attack

4. Node Capture

is a serious attack faced the IoT system, in which an attacker gets the full control over a key node, like a gateway node. The attacker can steal many private information such as communication information between a device and the gateway, a communication security key, and many sensitive information stored in the gateway's memory [03]. Moreover, the attacker can add a duplicate node to the network to send malicious data; as a result he threats the data integrity and confidentiality [05], Fig. 14.

5. Malicious Code Injection

As we presented earlier, the injected malicious code (or malware) gives the attacker the full control over the infected node. He could activate the injected malware by *transmitting malicious command attack*. The attacker can use the infected nodes (devices) to gain a full control over the IoT network, affect the IoT network, or even block it completely. This type of attack can really cause serious problems in the IoT system [05], *Fig.15*.

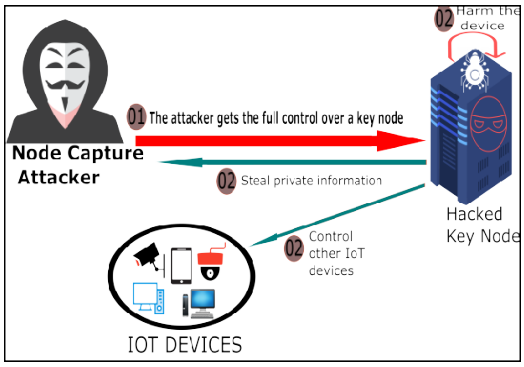

Fig.14.NodeCaptureAttac attack

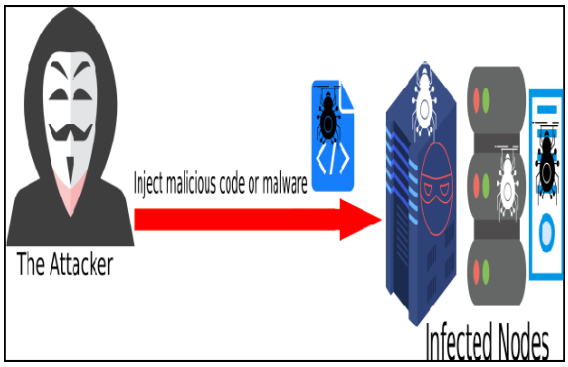

Fig. 15. Malicious Code Injection attack

B. Discussion

As we said earlier, the three layers Short-range communication, Gateway access and network have many common attacks, but with some specifications or differences in each one. The next table explains the specifications (properties) of each attack in each layer (if the Attack could be per formed), TABLE II.

	Short-range communication layer	**Gateway access layer**	**Network layer**
DOS/D.DOS (attacks to compromise the availability)	----------	Deny the access to the gateway (devices could not access to the gateway).	Deny of access to the gateway from ''service platform and enabler layer''(or the opposite sense)
Main-in-The-Middle (MiTM)	The attacker Intercepts and alters the communication information, which is sent between a device and the gateway.	----------	Intercepts and alters the information between the gateway and capabilities of ''service platform and enabler layer'' (e.g. cloud).
Storage Attack	----------	Steal, change, or delete the gateway's stored information.	----------
Node Capture	----------	Get the full control over the gateway.	----------
Malicious Code Injection	The attacker affects and controls the communication. He could block it completely.	The attacker could control or block the Gateway node (as a result all the IoT system)	The attacker affects and controls the entire network. He could block it completely

I. CONCLUSION

The increasing popularity of IoT and its applications is bringing attention towards their security issues, threats and attacks. This paper has presented the IoT technology and its main architectures and then it focused a very important aspect in IoT: the security.

As a perspective of this paper, some points will be discussed in an extension paper for this work such as:

Security issues in the last two layers of IBorgia and al architecture.

- Current security mechanisms to prevent security threats and attacks.
- Several security solutions and approaches.
- Some security implementation attempts, counter measures like Software Defined Networking (SDN) and Blockchain.

REFERENCES

[1] Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac , "A Survey on Sensor-based Threats to Internet-of- Things (IoT) Devices and Applications" , PP. 01-08

[2] Qi Jing , Athanasios V. V , Jiafu Wan , Jingwei Lu , Dechao Qiu , "Security of the Internet of Things: perspectives and challenges" Wireless Netw (2014)Springer , PP. 01,02 (2481, 2482).

[3] Muhammad Burhan , Rana Asif Rehman, Bilal Khan,Byung-Seo Kim , "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey" , PP. 03,06,07,09

[4] Diego Mendez, Ioannis Papapanagiotou, Baijian Yang , "Internet of Things: Survey on Security and Privacy" , PP. 02,09,10,11,12

[5] Abdul Wahab Ahmed;Mian Muhammad Ahmed;Omair A.K;Munam A.S , "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT" , in IJACSA jornal , PP. 01,02, 03,05

[6] A.Vithya Vijayalakshmi, Dr. L. Arockiam "A STUDY ON SECURITY ISSUES AND CHALLENGES IN IoT", in jornal: IJESMR , PP. 01,02

[7] Ioannis Andrea , Chrysostomos Chrysostomou , George C. Hadjichristofi , "Internet of Things: Security vulnerabilities and challenges" , PP. 01,03

[8] B. Di Martino , M. Rak , M. Ficco , A. Esposito , S.A. Maisto , S. Nacchia , "Internet of things reference architectures, security and interoperability: A survey" , journal : Elsevier , PP. 02,03

[9] Sergey Efremov, Nikolay Pilipenko, Leonid Voskov , "An Integrated Approach to Common Problems in the Internet of Things" , PP. 05

[10] WSO2 WHITE PAPER by : Paul Fremantle , "A Reference Architecture For The Internet of Things" , PP. 02,04

[11] Mihael Radovan , Boris Golub , "Trends in IoT Security - MiPro 2017" , in Daimler AG, Stuttgart, Germany , PP. 01,02,03

[12] Tabassum Ara, Pritam Gajkumar Shah,and M. Prabhakar , "Internet of Things Architecture and Applications: A Survey" , PP. 01,06

[13] Mohammed A.M.Sadeeq , Subhi R. M. , Zeebaree Riyadh Qashi , Sarkar Hasan Ahmed , Karwan Jacksi , "Internet of Things Security: A Survey" , in ICOASE conference PP. 01

[14] Mardiana binti Mohamad Noor, Wan Haslina Hassan , "Current research on Internet of Things (IoT) security: A survey" , in jornal Elsevier , PP 01,03.

[15] E. Borgia, The internet of things vision: Key features, applications and 560 open issues, Computer Communications 54 (2014) 1–31. arXiv:1207.0203, doi:10.1016/j.comcom.2014.09.008. URL http://dx.doi.org/10.1016/j.comcom.2014.09.008

[16] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal , Zied Chtourou , "A Systemic Approach for IoT Security", PP 01-04