Securing the Internet of Things (IoT)

Abla El bekkali [1] [2], Mohammed Boulmalf [1], Mohammad Essaaidi [2], Ghita Mezzour [1]
[1] International University of Rabat, FIL, TICLAB, Morocco
[2] ENSIAS, University Med V, ISRT, Morocco
{abla.elbekkali@uir.ac.ma, mohammed.boulmalf@uir.ac.ma, m.essaaidi@ieee.com, ghita.mezzour@uir.ac.ma}

***Abstract*— Internet of Things is a large network of interconnected "things". IoT refers to the exchange of data and information from real world devices to the Internet. IoT technology will enable breakthrough applications in several areas such as e-Health, smart cities, transportation and industry, and includes multiple technologies, cloud computing, communication, etc. IoT reveals not only the possibilities of high efficiency and low cost, but also scalability. On the other hand, security issues exist and are a major concern for researchers. This article is a systematic literature review (SLR) where show the most basic and common architecture proposed for IoT with a security analysis of each layer. This SLR is also made to present IoT security solutions, as well as a comparison of these solutions. Finally we will present future research directions.**

Keywords*— *Internet of Things, Scalability, Efficiency, Architecture, Layer, Security.

I. INTRODUCTION

Kevin Ashton introduced in 1999 the Internet of Things "IoT" which is an assembly of interconnected devices [1].

Internet of Things is a network of objects, humans, devices, services that are connected and communicate with each other via the Internet. These objects collect and exchange data between themselves, but also with us to achieve a common goal in various areas and applications. Figure 1 presents the general concept of IoT.

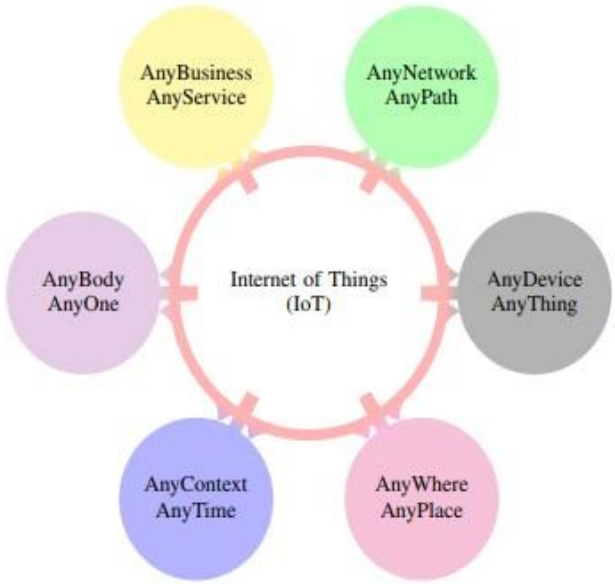

Fig. 1. IoT Definition [2].

There are several IoT applications in all areas, we mention the most important: The smart home, intelligent building, smart grids, smart transportation, and smart health-care. These applications offer an easier life for people. Like the example of smart homes that give people control over remote devices, smart healthcare can also save lives by making advanced disease diagnoses [3].

The Internet of Things is expanding. With the ramp-up of IoT applications, come to a connected whole life, adopting existing revolutions, such as wireless technologies and sensors (Wi-Fi, WiMax, GSM, Bluetooth, UMTS, ZigBee, etc.). Although IoT applications offer the amenities of life to people, and despite the considerable evolution of IoT, there are still uncertainties about the concepts of security of use, which means that the security of privacy cannot be ensured following the risks of disclosure of users' private information. This risk of exposure of personal information increases with the expansion of IoT. Knowing that this security problem is of great concern to researchers, they confirm that to limit the threats of IoT, security mechanisms must be adapted, and that effective solutions must be put in place.

This document is elaborated as follows: Section II, explains the state of IoT, with examples of IoT security issues around the world. Then, a presentation of the most basic architecture of the IoT, as well as an analysis of the security problems of each IoT layer. Section III presents the related work on IoT security solutions. Section IV, presents a comparison of the proposed solutions. Finally, Section V concludes the paper and reveals possible future directions.

II. INTERNET OF THINGS SECURITY

With the development of the Internet of Things market, the security of IoT is becoming more important than ever. To ensure the security of any device, it is necessary to rely on 3 pillars, called "CIAs" suggested by the information security triad: (i) Confidentiality, (ii) Integrity and (iii) Availability. The current CIA triad has expanded over the years to also include significant security goals for IoT such as non-reputation, authenticity, and privacy.

A. Examples of attacks on IoT devices

From the beginning there have been several IoT security issues, we will mention a few.

In 2014 an iot security problems occurred. Considerable damage in an Iranian nuclear project was caused by a Stuxnet attack that is a malicious computer worm, designed primarily to target controllers connected to a Windows OS

978-1-5386-7330-0/18/$31.00 ©2018 IEEE

computer, while taking control. The purpose of this attack is to damage the uranium enrichment facilities. The computers were infected by this attack with a USB device [4].

In 2015, the Jeep was hacked into the Sprint cellular network by researchers who could deflect it from the road, speed up the vehicle or even slow it down. These researchers took full control of a Jeep SUV using the vehicle's CAN bus. They hacked the vehicle by exploiting a firmware update vulnerability. This hacking has been announced by the IBM Security Intelligence website [5].

In 2016, there was the disclosure of a malicious botnet by the security specialists of Sucuri. This botnet is over 25,000 CCTV devices adopted to send distributed denial of service attacks. Sucuri's security experts found that the botnet was using IP addresses in more than 105 countries [6].

B. *Internet of Things architecture*

Several architectures have been proposed in recent years and the most basic architecture is composed of 4 layers: Perception layer, Network layer, Middle-ware layer and Application layer (Fig. 2).

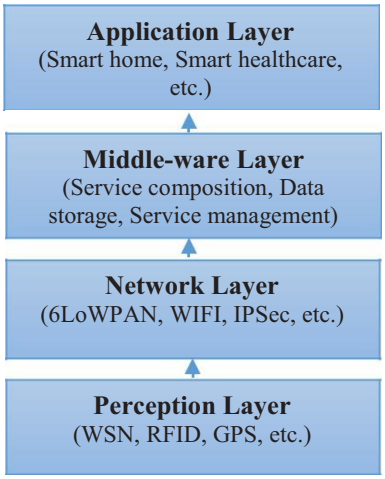

Fig. 2. Architecture of IoT

Perception layer: Also called the recognition layer, designed for collecting information and identifying the physical world via several types of sensors such as (RFID, ZigBee, WSN, Wi-Fi, etc.) [1].

Network layer: The role of the network layer is to transmit the information collected from the perception layer using the sensors, to any information processing system via the different communication networks.

Middleware layer: This layer is between the network layer and the application layer, it is service oriented and provides data storage, service management, and so on. It guarantees the same type of service between connected devices.

Application layer: This layer is responsible for providing applications suitable for users and for different types of industries while taking into account their needs, such as (Smart home, Smart Transportation, Smart healthcare, etc.).

C. *Security analysis in each layer*

Security issues must be taken into account. We need to understand and deal with all the security issues in each layer, even though they are complex and difficult. The IoT security architecture is divided into four layers, the first layer is the perception layer, then the network layer, the middle-ware layer and the application layer. In this section, we analyze these security issues in this three-layer architecture.

i. *Security analysis of the perceptual layer*

This layer includes sensors and physical devices. The sensors are limited by resources and this is a big problem because they have a very small storage capacity as well as a very low computing power. In the perceptual layer, after data collection, their transmission is done with a wireless network. The signals can then be attacked, monitored or even intercepted in the event that protective measures fail because they occur in public. Knowing that the security system is difficult to implement in this layer. As a result, physical devices are vulnerable to multiple attacks. Among the powerful attacks:

- Differential Power Analysis (DPA): Enables the disclosure of the secret key stored in a cryptographic device by correlating the instantaneous power consumed by the device with the input data. To guess the key, DPA uses statistical methods to evaluate power traces with uniform texts [7].
- Gateway Node: This is a sensitive device, which can be easily controlled by attackers. It causes a danger to the security of the entire network, also the leakage of all information as the communication key [6].
- Fake Node & Malicious Data: The injection of data or malicious code is done by the attackers with the addition of a node to the system, which causes the stop of the transmission of the real data. Attackers manage to control or even destroy the entire network.
- Denial-of-service (DoS): A widespread attack on the internet and WSN, its goal is to make a service unavailable and the loss of network resources.
- Routing attack: Data transfer and relay are in the perception stage where data collection takes place. Therefore, during the transmission, the data can be attacked by the intermediate nodes [8].
- Replay: This attack is intended to have the trust of the system and that by launching the packet received by the destination host. Generally this attack is adopted in the destruction and validation of certification or also in the processing of authentication [6].
- Side-channel attack (SCA): The role of the SCA is the disclosure of the secret keys and then assign them to several cryptographic devices during execution as (smart cards, RFID systems, etc.).

Data encryption and node authentication are essential for secure and convenient execution. Authentication is an appropriate technique to prevent access to illegal nodes and the encryption technique is the best for confidentiality [9].

ii. Security analysis of the network Layer

The central Internet network already includes some security measures, so it is relatively secure. Yet there are still attacks that must be analyzed and processed for the future Internet. The biggest problem with IoT over the large amount of data is network congestion. We mention the security issues in this layer.

Communication Network Security Issues: Confidentiality and data integrity are threatened by communications network security issues. Despite existing countermeasures, there are still attacks aimed at harming the communications network, such as: man-in-the-middle, damage to integrity, denial-of-service attacks, eavesdropping attack, sybil attack, sink attack, sniffing attack, etc.

iii. *Security analysis of the middleware layer*

This layer is between the network and application layer, it has several characteristics and its main purpose is to connect several systems, with the extraction of the different hardware components, the communication protocols and also the operating systems, also to bring a multitude of interfaces so that programmers integrate the final application [10]. This layer includes data storage technologies, which can be used by attackers and unauthorized parties.

On the other hand, several attacks can occur, such as the following attacks:

- Jamming: A DoS attack, its purpose is to disrupt the communication between the nodes. The attacker blocks the reception of the radio channel of a node by transmitting on its frequency band to cause radio interference [8].
- DoS Attack: Its goal is to shut down a machine or network, making it inaccessible to intended users. DoS attacks on this layer may cause unavailability of services.
- Node Alteration: Node falsification is the extraction of sensitive data.
- Data attacks: These are attacks on the data service, such as redoing service requests, modifying data on request headers, and so on.
- Malicious Insider: This is an attack on a network or computer system by an inside person with authorized access to that system, which is intended to falsify the data.

iv. Security analysis of the application layer

Security issues in this layer differ by industry or environment. Although the security of the application layer is expensive and complex, we can nevertheless analyze and present these most important security problems:

- Authentication: An effective authentication technology must be in place to avoid any illegal user intervention, knowing that each application has a large number of different users. Spamming, identification and information processing must also be taken into account.
- Privacy leak: The attacker manages to steal the confidential data of users knowing that the IoT application is running on operating systems as well as on common hosting services. According to the results of the query the attacker can also analyze the location of the terminal as well as the confidentiality of the identity [8].
- Social engineering: Following the existing relationship between users of the IoT, attackers manage to manipulate people to bypass security devices, and obtain information from users by exploiting their naivety.

III. RELATED WORK

IoT is spreading rapidly in different areas for individuals and businesses. As a result, the security of connected objects is an immediate and urgent challenge for all. Here are some important security solutions for IoT proposed and presented by different researchers and publisher, as well as a table 1 which presents an analysis of these solutions.

R. Aggarwal introduces a method of security for devices by using RFID (Radio Frequency Identification) that are installed/integrated into smart objects to enable communication between objects and humans [11].

Weiss et al. propose a comparative and comprehensive metric security model (CCM) based on a risk management method, in this model the security is evaluated in terms of incidents and asset losses [11].

Tahir et al. develop a solution to enhance the security of IoT, an ICMetric-based solution associated with the Secure Remote Rabbit protocol that secures entities and their intercommunications. ICMetric is an integrated circuit metric in the field of cryptography that solves the problems related to the major trade-offs in modern systems, using the extraction of the mathematical and statistical characteristics of the device, when combining the characteristics they define the performance of the electronic device. ICMetric consists of two calculation steps: the calibration step and the operation step. ICMetric has several purposes, such as stopping key theft and cloning of devices by adding a layer to cryptographic schemes, another purpose is to prevent tampering with the device and unauthorized access. The protection of the data stored and transmitted between the devices. The authors confirm that this solution guarantees authentication, confidentiality and non-repudiation [12].

Liu et al. suggest a solution for secure IoT. This solution is based on the principles of a biological immune system and adopts a dynamic defense framework, knowing that static defense strategies may be inadequate. They present a circular defense with five links: detection of security threats, calculation of dangers, security responses, formulation of security defense strategies and security defense. The behavior of a biological immune system is realized in order to create links in the proposed schema solution to make this approach adaptable to the IoT environment. The researchers simulated the real environment of IoT using an antigen, auto and immunity-based detector in real IoT. They are used to mimic the mechanisms that are applied to recognize pathogens in biological immune systems. The result of the simulation show that the proposed approach can provide a new and effective method for securing the Internet of Things [13].

Table I. ANALYSIS OF THE SECURITY SOLUTIONS IN IOT

SOLUTIONS	SECURITY REQUIREMENTS		
	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
R. Aggarwal [11] « Method of security for devices by using RFID (Radio Frequency Identification) »	NO	NO	NO
Weiss et al. [11] « Comparative and Comprehensive Metric security model (CCM) based on a risk management method »	YES	YES	NO
Tahir et al. [12] « ICMetric cryptographic keys with SRRP »	YES	YES	YES
Liu et al. [13] « Dynamic iot security based on the principles of a biological immune system »	NO	NO	NO
Zhou et al. [14][15][16] « Media-aware traffic security architecture (MTSA)»	NO	NO	NO
Rose [17][16] « Nano-electronic security primitives and protocols for the emerging IoT devices»	YES	NO	YES
Lessa dos Santos et al. [18] [16] « Datagram Transport Layer Security (DTLS) »	YES	YES	YES
Kothmayr et al. [19] « DTLS and RSA »	YES	YES	YES
Xin [20][16] « Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) »	YES	YES	NO
Zegzhda and Stepanova [21] « Graph topology to enhance IoT security »	NO	YES	NO
WALLIX [22] « Bastion type access management technology »	YES	YES	YES

Zhou and Chao propose a new media-aware traffic security architecture (MTSA) for media-based traffic security. The goal of the MTSA architecture is to meet the challenges and requirements of multimedia system security in the IoT environment. This MTSA architecture provides users with multiple multimedia services at any time and place [14] [15] [16].

Rose introduces PUF (Unclonable Physical Functions), the main goal is that nanoelectronic technologies be used to implement energy-saving security mechanisms with limited resources for IoT devices. PUF can enhance security based on secret key generation or strong authentication. However, PUF may have certain limitations and restrictions, such as unreliable responses [17] [16].

Lessa dos Santos et al. have proposed a security architecture for IoT that grants the constrained devices the communication with internet devices, by adopting Datagram Transport Layer Security (DTLS) with mutual authentication. The architecture is based on Internet of Things Security Support Provider (IoTSSP) and two main mechanisms for the 6LoWPAN front-end router (6LBR) for redirecting DTLS handshaking to IoTSSP. The association of constrained devices and the IoTSSP helps prevent denial of service attacks [18] [16].

Kothmayr et al. also present an IoT security solution that allows security in constrained devices by offering to use hardware that supports RSA and is dedicated for that. This solution involves the use of Trusted Platform Modules (TPMs) that are added to constrained devices. The proposed solution is executable for the emerging IoT knowing that it allows the confidentiality, the integrity and the authenticity of the messages [19].

Xin presented a security solution to use for data transmission in IoT which is a mixed encryption algorithm. This algorithm uses hybrid key technology, which takes into account the characteristics of a symmetric key and an asymmetric key to ensure confidentiality, integrity and non-repudiation of the data. Encryption is of great importance to the security of IoT. For information security, AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography) are used. The proposed algorithm uses the encryption of the AES algorithm for its simplicity, velocity and reliability. Xin argues that hybrid encryption provides better and more efficient information security while information is transmitted over a number of network components [20] [16].

Zegzhda and Stepanova have proposed a solution to enhance IoT security, this approach is a basic theoretical framework its purpose is to prevent security threats intended to disrupt or destroy IoT services and components. This

solution primarily provides protection for IoT nodes against DoS denial attacks, while maintaining a random adaptive d-regular graph topology. The authors claim that this solution takes into account the requirements of IoT and guarantees integrity [21].

WALLIX, a French publisher of computer security software, is a trusted partner in this ecosystem of cybersecurity solutions by protecting datacenters and virtual machines hosted by cloud service providers with access privilege management technology. Bastion type. The Access Management and Privilege Session features offered by the WALLIX Bastion secure, trace, and control the identity and activities of administrators who exploit sensitive data and virtual machines. Thanks to the Bastion, access to sensitive data processed by connected objects is protected with a single sign-on or SSO system and a password safe. Sessions and activities perpetrated on virtual machines are then recorded and monitored in real time to alert fraudulent orders and revert to an incident. The Bastion acts as a barrier between the service provider and the managed machines, which reduces threats from within the systems and protects the data processing of connected objects [22].

IV. Evaluation of IoT Solution

Many researchers analyze and present the security aspects of IoT, but most research typically focuses on a single level of IoT architecture. This survey examines the security of the entire system and treats each layer of the IoT architecture. The security solutions proposed in the previous section are analyzed, compared and presented in Table 1. This assessment is based on the main security requirements: confidentiality, integrity and availability. According to our analysis, we note that only 4 out of 11 solutions that meet basic security requirements.

Although researchers are trying to meet security requirements with their solutions, but the methods presented have limitations in terms of security and reliability for IoT. As for example for R. Aggarwal's solution, although RFID tags are important for IoT security, there are still threats to privacy. Also for the solution of Weiss et al. it guarantees confidentiality and integrity, except that the availability and accessibility of data remains a challenge. The evaluation conducted on these solutions offers unmatched visibility on the consideration of cybersecurity issues.

After a long study we see that the real problem of IoT is data protection. We believe that the concepts of trust, privacy or confidentiality of data can be removed with the intervention of Blockchain technology on data processing. The blockchain by its protocols makes it possible to protect data by encrypting them. This mechanism secures transactions between connected objects and contributes to trust between actors.

V. CONCLUSION AND FUTURE WORK

With the emergence of IoT, personalized security and privacy at all levels is needed. The security of connected objects is starting to fuel debates and is growing in awareness. IoT security is probably one of the major concerns at the moment. The question affects us all (users, manufacturers, companies, etc ...). While some IoT security frameworks are currently being developed by researchers or others, they are still at different stages of advancement. More specifically, they are specific to certain sectors of activity and generally only cover certain security requirements.

This work aims to provide a better understanding of the IoT security issues previously encountered through an IoT security strategy, based on a comprehensive risk analysis. The article also introduces the IoT security architecture with an analysis of security issues for each layer, as well as a presentation of several security solutions for IoT proposed by different researchers to date, as well as their limits in terms of security. In the future, we will propose an innovative approach based on the union of IoT and Blockchain technology to ensure data protection.

References

[1] K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, “A Systematic Literature Review on the Security Challenges of Internet of Things and their Classification”, p. 9.

[2] M. Abdur, S. Habib, M. Ali, and S. Ullah, “Security Issues in the Internet of Things (IoT): A Comprehensive Study”, International Journal of Advanced Computer Science and Applications, vol. 8, no 6, 2017.

[3] I. Yaqoob and al., “Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges”, IEEE Wireless Communications, vol. 24, no 3, p. 10‑16, juin 2017.

[4] (28/05/2018) 5 IoT Security Hacking Instances to Take Note of. Available:https://www.embitel.com/blog/embedded-blog/security-challenges-faced-by-iot-based-industries.

[5] (25/05/2018) The 5 worst examples of IoT hacking and vulnerabilities in recorded history. Available:https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/.

[6] Y. Chahid, M. Benabdellah, and A. Azizi, “Internet of things security”, 2017, p. 1‑6.

[7] S. D. Kumar and H. Thapliyal, “Security Evaluation of MTJ/CMOS Circuits Against Power Analysis Attacks”, 2017, p. 117‑122.

[8] B.Sasikala, M. Rajanarajana, Dr. B. GeethavaniIndia, “Internet of Things: A Survey on Security Issues Analysis and Countermeasures”, International Journal of Engineering and Computer Science, juin 2017.

[9] V. Adat and B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture”, Telecommunication Systems, vol. 67, no 3, p. 423‑441, mars 2018.

[10] M. Gregório, R. Santos, C. Barros, and G. Silva, “Problems in Adopting Middleware for IoT : A Survey,” p. 6, 2016.

[11] S. A. Kumar, T. Vealey, and H. Srivastava, “Security in Internet of Things: Challenges, Solutions and Future Directions”, 2016, p. 5772‑5781.

[12] R. Tahir, H. Tahir, K. McDonald-Maier and A. Fernando, "A novel ICMetric based framework for securing the Internet of Things," 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2016, pp. 469-470.

[13] C. Liu, Y. Zhang and H. Zhang, “A Novel Approach to IoT Security Based on Immunology,” Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, December 2013.

[14] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," in IEEE Network, vol. 25, no. 3, pp. 35-40, May-June 2011.

[15] A.M. Eskicioglu, “Multimedia security in group communications: recent progress in key management, authentication, and watermarking,” Multimedia Systems (2003), 9: 239.

[16] A. Oracevic, S. Dilek, and S. Ozdemir, « Security in internet of things: A survey », 2017, p. 1‑6.

[17] G. S. Rose, "Security meets nanoelectronics for Internet of things applications," 2016 International Great Lakes Symposium on VLSI (GLSVLSI), Boston, MA, 2016, pp. 181-183.

[18] G. Lessa dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 809-815.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, “DTLS based security and two-way authentication for the Internet of Things,” Ad Hoc Networks, vol. 11, no. 8, pp. 2710 – 2723, 2013.

[20] M. Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System," 2015 International Conference on

Cyber-Enabled Distributed Computing and Knowledge Discovery, Xi'an, 2015, pp. 62-65.

[21] D. Zegzhda and T. Stepanova, "Achieving Internet of Things security via providing topological sustainability," 2015 Science and Information Conference (SAI), London, 2015, pp. 269-276.

[22] (28/05/2018) Connected Objects: An ecosystem to secure IoT Available: http://blog.wallix.com/fr/securiser-l-iot-objets-connectes.