Received <day> <Month>, <year>; | Revised <day> <Month>, <year>; | Accepted <day> <Month>, <year>

DOI: xxx/xxxx

ARTICLE TYPE

Smart certification: protecting the originality of the product in the eyewear sector

Sabrina Sicari* | Alessandra Rizzardi | Alberto Coen-Porisini

[1]Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria, Varese, Italy

Correspondence
*Corresponding author Sabrina Sicari, Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria, via O. Rossi 9, 21100 Varese (Italy). Email: sabrina.sicari@uninsubria.it

Abstract

The growing diffusion of the technologies related to the Internet of Things (IoT) paradigm not only facilitates the connectivity among a huge amount of different devices, but also the variety of applications and services which can be provided to users. Everyday objects, equipped with the technologies involved in such a paradigm, become smart and are able to guarantee users who own them to be connected *"always, in any place, at any time and with any object"*. Consequently, the opportunity of communicating in real time enables the design and development of novel customizable functionalities, which are even closer to the needs of the users. Different application domains can benefit from this innovation, including the ophthalmology and eyewear sector. In such a context, the lenses and the eyeglasses frames become smart, thanks to the adoption of IoT paradigm. A relevant application in such an area concerns the definition of a system able to guarantee the originality of the product (and, so, verify the certification), as well as preventing the spread of imitations and counterfeit products, recognizing them in real time. In this paper, a preliminary approach for solving such emerged issues is proposed. More in detail, the main requirements and involved functionalities are pointed out and represented in a coherent flow, through Node-RED, which is a flow-based programming tool targeted to support the design and development of IoT applications.

KEYWORDS:
Internet of Things; Security; Eyewear Sector; Eyewear Counterfeiting; Eyewear Certification; Node-RED

1 | INTRODUCTION

Since the last decade, the spread of smart services in different application scenarios (home automation, logistics, transport, agriculture, industry 4.0, etc.) has been increasing, thanks to the growing use of technologies related to the Internet of Things (IoT) paradigm (1). Such an innovation is achieved by introducing electronic equipment into real objects, even for everyday use, thus making them *smart*. They are equipped with sensors, actuators, RFID (Radio-Frequency IDentification), NFC (Near Field Communication), etc., and are connected through protocols and standards, including MQTT (Message Queue Telemetry Transport), CoAP (Constrained Application Protocol) , ZigBee, 6LowPAN (IPv6 over Low-Power Wireless Personal Area Networks), Bluetooth, Wi-Fi, cellular networks etc. (2)

Thanks to the integration and interaction of such technologies and protocols, a network infrastructure is created with the aim of sharing information at a global level; moreover, the availability of the Internet connection also fosters the spread of the so-called *smart objects*. They are able to acquire heterogeneous data from the environment where they are placed in, and to perform

actions, in response to certain situations that may occur in a given application context. Therefore, an ever-growing set of smart objects acquires a digital identity, and, as a consequence, it has an active role thanks to their connection to the network. The final goal is to provide various types of services to interested users. To this end, the acquired data must be processed and properly integrated into useful services(3).

As expected, in the near future, an ever-increasing amount of contents and services will be available in real time, through the use of *smart* devices. Note that the *smart* nature will be a feature of everyday objects, paving the way for new applications. In such a perspective, the traditional concept of the Internet is replaced by the notion of *interconnected smart objects*, which underlies the IoT paradigm (4).

The features just described are the basis for the design and development of innovative systems, in different application fields. In particular, in the ophthalmology and eyewear sector, the possibility of guaranteeing the originality and certification of each product is of great importance (5). Note that, in this case, the eyewear field is the ideal candidate to become the *smart object*. Different brands put on the market every year products that have unique technical features and design aspects. Hence, it is fundamental to ensure consumers that the product purchased through the various distribution chains is original and not, for example, an imitation (even illegally) sold by some competitors or by counterfeiters.

This paper aims to provide a preliminary approach for solving such emerged issues in the eyewear sector. More in detail, the main requirements, which must be taken into account for ensuring the originality of glasses or part of them (i.e., lenses/frames), will be clearly pointed out. Then, an IoT platform, with the related system's flow will be defined and represented by means of Node-RED (6), which is a flow-based programming tool by IBM, targeted to support the design and development of IoT applications.

The paper is organized as follows: Section 2 presents the background on the security issues related to the eyewear sector; Section 3 details a possible solution to the analyzed issues, which is further represented and described in Section 4, with the support the Node-RED tool; Section 5 ends the paper and draws future research directions.

2 | BACKGROUND ON THE EYEWEAR SECTOR AND MOTIVATION

All over the world, the eyewear sector is among those most affected by the phenomenon of counterfeiting, as regards trademarks, patents, designs and models (7). This is due to the fact that eyewear is a sector having a great commercial success.

The damage, resulting from the spread of lower quality or counterfeit products than the originals, is not only economic (it is estimated that in the eyewear sector, counterfeiting is responsible for the loss of about 15%-20% of the market every year (7)), but an important impact is also on the health of users who buy them. In fact, glasses (both prescription glasses and sunglasses) are considered as a personal protective medical device and, therefore, they must be compliant with certain regulations, in several states and countries (8). The damage deriving from the use of non-compliant glasses regards both the sight, since the lenses would not respect the features imposed by the standards, and the skin, since the frames could be made with toxic materials.

Hence, the importance of providing robust solutions for guaranteeing the originality of the products in the eyewear sector is twofold: (i) on the one hand, the producers must be able to control and prevent counterfeiting of their brands, to avoid financial loss; (ii) on the other hand, consumers must be sure that the products they buy do not harm their health.

Currently, original prescription glasses or sunglasses should be recognizable, for example according to EC directive 2007/47/EC (9), by the fact that: (i) they have the *CE marking* in a visible, legible and indelible way; (ii) they are denoted by an information note, which contains the manufacturer's name and address, the instructions for use and maintenance, several warnings; (iii) they have a warranty on possible manufacturing defects or damage caused thereafter.

Such information are not enough to ensure the originality of the products, as they can be easily tampered or replicated. Hence, new approaches must be defined, in order to address the following goals: (i) ensuring that the data associated to the products about their originality are kept secure, in the sense that they cannot be altered or replicated; (ii) allowing the real time verification of such data; in such a way, a capillary control on the certificate related to the product can be conducted, as better explained in Section 3. Taking in mind the peculiarities of the investigated scenario, the IoT principles perfectly fit its requirements, due to features such as mobility, real time communications, heterogeneity of devices, and so on. The adoption of IoT technologies in the eyewear sector is not new (5), but, in this paper, a novel focus is dedicated on the products' reliability, both from consumers' and from producers' viewpoint.

In fact, as emerged from the aforementioned analysis, the security and privacy for protecting the originality of the product in the eyewear sector still represent open challenges. No solution is available to solve such issues yet, but the introduction of IoT technologies and functionalities seems to be a viable solution. Another important aspect concerns the methodology adopted

for designing the new envisioned approaches, since a system and, in particular a complex IoT platform, must be conceived and preliminary tested in a controlled and *easy of use* environment, before the real deployment, in order not to waste time and resources. Nowadays, different programming languages and tools are chosen for validating and testing purposes. Often researchers make also use of existing data-sets in order to operate with real data. The main drawback, mainly in presence of IoT environments, is that often the whole system is not tested, but only a part of it. This is due to the lack in the use of a comprehensive tool, able to represent the new-defined IoT architecture close as much as possible to the future real working system. To cope with such an issue, the adoption of Node-RED tool is proposed hereby. The main advantages of Node-RED are the following: (i) the easy-of-use, due to its web-based interface; (ii) the data flow-programming paradigm; (iii) the event-driven approach; furthermore, it facilitates the interoperability among different protocols and standards to realize complex systems. The application's behavior is represented as a network of black-boxes, which may communicate with each others and regulate the flow of the information within the designed system. A visual browser-based representation supports designers and developers in better understanding the happening interactions within the whole IoT network. In fact, Node-RED flows can directly run on IoT devices or can be connected to real devices, thus involving both hardware (e.g., sensors) and software (e.g., services), thanks to available libraries. Moreover, Node-RED is written in Node.js, whose lightweight nature allows it to also be deployed on constrained devices, such as Raspberry PIs or other similar ones.

Other web-based platforms, targeted to IoT, have been proposed in literature (10). The most similar to Node-RED is *WoTKit*, written in Python (while Node-RED uses Javascript language), whose main limit, with respect to Node-RED, is that it never accesses local sensors or OS services. Finally, *Yahoo Pipes* allows no real-time data processing. Instead, *LabVIEW* is more focused on the hardware layer. Other tools provide no data flow-programming features, targeted to IoT applications. Such considerations motivate our choice.

3 | REQUIREMENTS AND APPROACH

A possible solution to deal with the issues, emerged in Section 2, consists in conceiving an IoT-based system as automatic as possible, capable of recognizing, in real time, the originality of the product itself. Note that the implementation of such a platform would also allow to prevent the spread of the imitations themselves, since the counterfeiters should be threatened by the possibility of being recognized before the purchase of the illegal products themselves.

Thanks to the miniaturization capabilities provided by innovative technologies, such as the use of NFC (11) or RFID (12), it would be possible to equip glasses with miniaturized devices, named *tag*, inside the frame and/or inside the lenses themselves. Such miniaturized devices are in charge of storing information, possibly encrypted, regarding the product itself, such as an identification code. Such information can be read by proper readers or by more powerful devices, such as smartphones or tablets, at any time, always connected to the Internet, so as to create the IoT network. Therefore, data can be received in real time, to verify the authenticity of the glasses or of part of them (i.e., lenses/frames) from a generic remote place. If a product does not have any legible tag, it would, of course, be a counterfeit object (only in several unusual cases it could be considered a system's failure); the same is for a tag containing information not corresponding to that established by the manufacturer.

The fundamental components of the envisioned platform are the following: (i) the smart objects, represented by the glasses or by part of them (i.e., lenses or frames); (ii) the tags; (iii) the tags' readers; (iv) a cloud. The following steps must be taken into account towards the realization of a robust and reliable IoT system for verifying the originality of products in the eyewear sector:

- Starting from the national regulations and considering the medical directives, a set of requirements to be owned by the products must be draw up. Such information can then be outlined to create a sort of identikit of the product and will be used to define the content of the tags (e.g., RFID tags) to be applied to the considered smart objects (i.e., the lenses or the eyeglasses frames). Note that different manufacturers can (and should) implement different strategies for establishing the content of the tags; in this way, it would be more difficult to put in act further attempts of counterfeiting and unfair competition among different partners. Several solutions, already available in the literature in the field of security and privacy, ensure that the information contained in the tag cannot be violated by unauthorized entities (13) (14), thus increasing the reliability of the whole system. Such solutions include key agreement management (e.g., distribution, update, revocation) or authentication procedures. Note that the conceived platform allows the glasses to communicate with external devices, such as the aforementioned readers connected to the Internet, thus fully underlying the IoT paradigm.

- Taking into account the needs of manufacturers in terms of the requirements and physical dimension of the different products, the best suited IoT technology to be adopted can be further identified. Note that the involved devices are expected

to make available short-range communications, probably in a range from few centimeters to few meters. For example, technologies such as NFC and RFID are already used in various applications, including: file sharing, electronic credit cards to make payments (contactless POS), mobile gaming, purchase and use of travel tickets, boarding pass, traceability of goods, and so on.

- Conducting an assessment of the whole product's chain, from the product design and production process, to the purchase and use by the consumer, allows, then, to establish the impact of the new approach for guaranteeing the products' originality. In particular, it is important, at this stage, to identify the new hardware and software components to be added to the current products. In such a direction, it would be desirable to establish proper agreements or joint initiatives among the interested manufacturers, in order to address the technical difficulties in implementing the proposed infrastructure.

- Considering that, compared to traditional networks, IoT networks also involve mobile devices and a huge amount of smart objects, possible threats to the security of the proposed system must be evaluated and, possibly, prevented. In fact, there is a risk that the data, stored and transmitted by the involved devices, may be transferred to unauthorized entities or, even worse, an intrusion from the outside towards the the IoT network itself may be carried out. As a result, each single IoT device that joins to the proposed IoT platform can represent a new potential attack vector. To this end, the proposed solution must take into account possible violation attempts and provide adequate security countermeasures (15). In this way, the trust of producers and consumers towards the products themselves will ensure a greater diffusion of the adopted IoT technology. In particular, different cryptographic solutions must be evaluated, comparing their performance, in order to adopt the technique that best suits the actual application context. Moreover, mechanisms for the management of cryptographic keys (such as revocation or update) must be defined, in order to guarantee the confidentiality and integrity of the information transmitted. Finally, proper security and privacy policies must be set up within an enforcement framework, in order to automatically manage possible violation attempts.

Figure 1 summarizes the identified IoT system's flow, which will be put in relation with the Node-RED flow in Section 4.

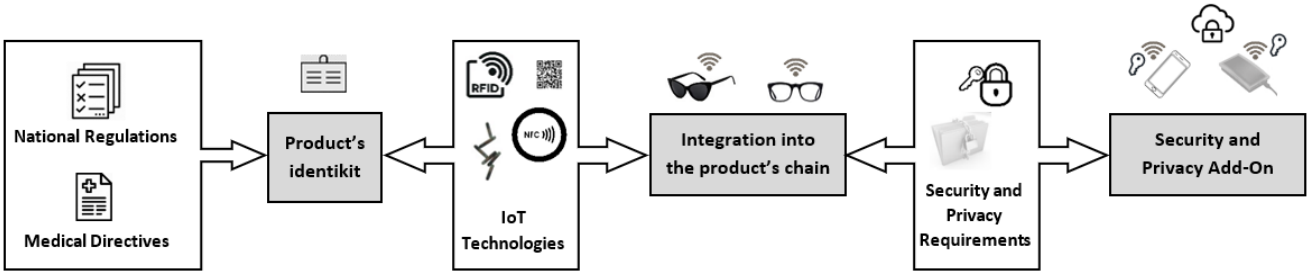

FIGURE 1 IoT system's flow

4 | NODE-RED DESIGN TOWARDS DEVELOPMENT

Once identified the requirements and the main steps to be considered towards the realization of a comprehensive solution for the investigated scenario in Section 3, a high-level overview by means of Node-RED tool is proposed hereby, detailing the management of product's originality. It is worth to remark that the system's components now presented are well-structured following the chosen flow-based approach, so as modules can be independently adapted, depending on the need of the manufacturer which may decide to adopt the envisioned solution. Hence, the conceived flow must be adjusted by the interested manufacturers, according to the specific features of their products.

Products are supposed to be tracked and identified by means of proper tags; while the "tags' reading" functionality may run both on dedicated devices (e.g., readers such as the RFID readers) and on mobile devices, such as smartphones or tablets, equipped with the proper hardware and software required by the application. The actions undertaken by the readers are executed in real time and, automatically, when the reading is performed and depend on the information contained in the tag associated to the product. The products can be associated with the following status, after a reading: (i) *ORIGINAL*, if the corresponding product is recognized to be original; (ii) *COUNTERFEIT*, if the corresponding product is recognized to be counterfeit, on the

basis of the information contained (or not present) in the tag; (iii) *ERROR*, whether there had been any issue while reading, which prevents a correct classification of the product.

Figure 2 shows the Node-RED flow, which represents the steps related to the tag generation, which contains the information which will be used for checking the originality of the associated product. The first step, named *Read Product Feature*, starts from the product's identikit, as defined in Figure 1 . Then, proper security measures (*Security Functions* in the figure) are applied to the generated product's identikit itself (*Generate Product Identikit* in the figure) and the result is registered on the cloud service (*Cloud Connection* and *Log Product/Tag Registration* in the figure), while the production of the tag itself is authorized (*Confirm Tag Generation* in the figure). It is worth to remark that also the information stored in the cloud must be protected; such a field is well-investigated in literature and many solutions regarding transport/storage ciphering, and access control, are available (16) and, therefore, can be applied to protect the stored data as well as the communications among smart devices and the cloud, taking place thanks to the Internet connection. Instead, products' tags and smart devices communicate among themselves by means of short-range protocols, which depend on the technologies adopted, but also on the required range of transmission. In that sense, various protocols can be involved, such as 6LoWPAN, ZigBee, BLE, NFC, Z-Wave, RFID's radio waves, etc., which offer different primitives for data protection. In particular, encryption and authentication mechanisms are specified, such as: (i) Advanced Encryption Standard (AES) block cipher for 6LoWPAN, ZigBee, BLE, NFC, Z-Wave; (ii) RC4 for RFID (17).

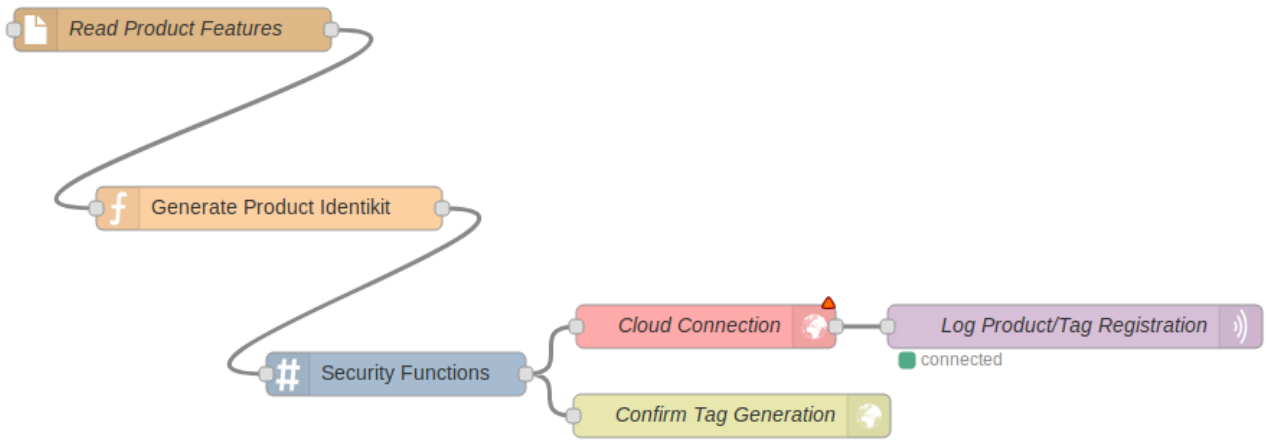

FIGURE 2 Node-RED Flow - Product's originality tag generation

Once the product is put on the market, depending on the chosen IoT technology, the consumers must be able to: (i) read the tag's content (*Read Product Tag* in the figure); (ii) perform the security checks (*Security Checks* in the figure); (iii) verify the originality (*Verify Originality* in the figure); (iv) notify the cloud service of the response (*Cloud Connection* in the figure) and register the outcome of the verification check (*Log Tag Verification Check* in the figure).

In fact, despite the readings are supposed to take place in short-range communications, it is also fundamental that the readers are connected to a cloud service, in order to log and, so, to keep trace of the products' checks. In fact, each manufacturer should be aware of the results of the checks related to its products, so that the manufacturer or other involved actors can make further controls on the products recognized as counterfeit.

Figure 3 shows the Node-RED flow, which summarizes the interactions just described.

Starting from the conducted analysis, the high-level flows proposed hereby can be associated with the IoT technologies, the security add-ons, and the cloud service that better fit the needs of the manufacturer. Note that the fundamental requirement for the eyewear sector is miniaturization, in order to avoid to compromise the usability and aesthetics of the products themselves. It worth to remark that the proposed approach can also be adapted to support a secure and privacy aware tracking system, in case of product's loss or theft.

5 | CONCLUSION

The paper presented an overview of the issues related to the realization of an IoT system, able to support the verification of the originality of the products made within the eyewear sector. Towards the definition of well-suited solutions, a high-level approach

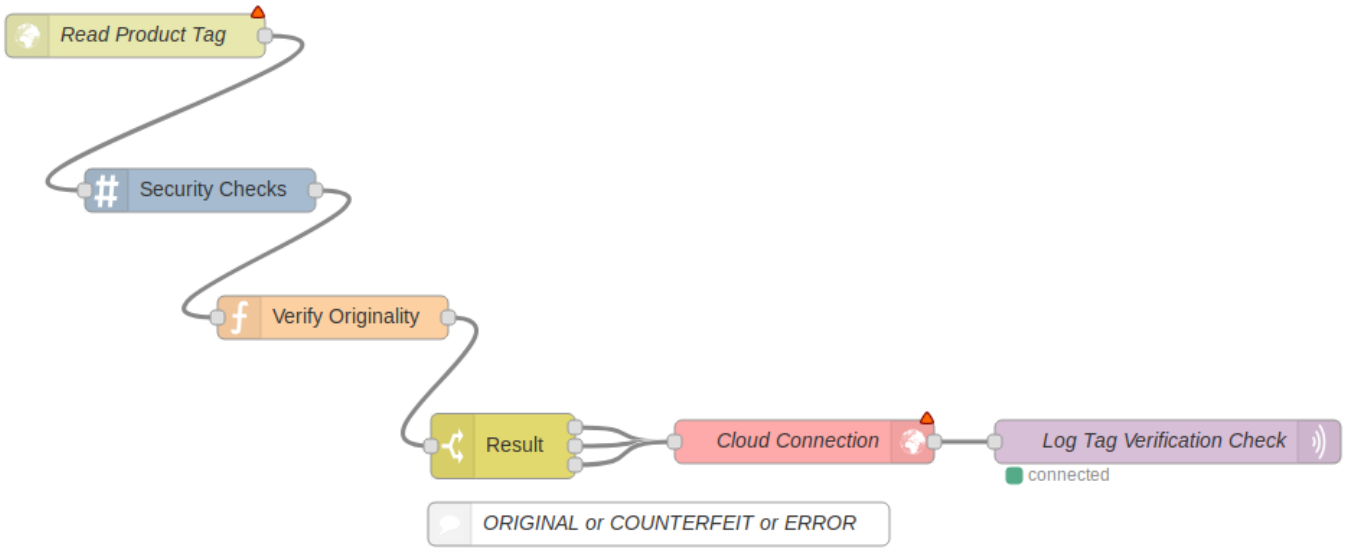

FIGURE 3 Node-RED Flow - Product's originality tag verification

based on the Node-RED tool is proposed, paving the way for the design and development of new solutions in the investigated field.

References

[1] Jazdi N.. Cyber physical systems in the context of Industry 4.0. *IEEE Intern. Conf. on Automation, Quality and Testing, Robotics.* 2014;:1-4.

[2] Al-Fuqaha Ala, Guizani Mohsen, Mohammadi Mehdi, Aledhari Mohammed, Ayyash Moussa. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials.* 2015;17(4):2347-2376.

[3] Miorandi D., Sicari S., De Pellegrini F., Chlamtac I.. Internet of things: Vision, applications and research challenges. *Ad hoc netw.*. 2012;10(7):1497-1516.

[4] Atzori Luigi, Iera Antonio, Morabito Giacomo. The internet of things: A survey. *Computer networks.* 2010;54(15):2787-2805.

[5] Wang Yu-Hui, Hsieh Chia-Ching. Explore technology innovation and intelligence for IoT (Internet of Things) based eyewear technology. *Technological Forecasting and Social Change.* 2018;127:281-290.

[6] https://nodered.org/ Accessed online on 31st January 2020.

[7] https://www.securingindustry.com/clothing-and-accessories/eyewear-firms-lose-15-20-per-cent-of-revenues-to-counterfeiters-/s107/a2533/#.XhCvQUdKhPY Accessed online on 31st January 2020.

[8] https://www.thevisioncouncil.org/members/standards Accessed online on 31st January 2020.

[9] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32007L0047 Accessed online on 31st January 2020.

[10] Blackstock R.. Toward a distributed data flow platform for the web of things (distributed node-red). *5th Intern.l Workshop on Web of Things.* 2014;:34-39.

[11] http://nearfieldcommunication.org/ Accessed online on 31st January 2020.

[12] Weinstein Ron. RFID: a technical overview and its application to the enterprise. *IT professional.* 2005;(3):27-33.

[13] Haselsteiner Ernst, Breitfuß Klemens. Security in near field communication (NFC). In: :12-14sn; 2006.

[14] Knospe Heiko, Pohl Hartmut. RFID security. *Information security technical report.* 2004;9(4):39-50.

[15] Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A.. Security, privacy and trust in Internet of Things: The road ahead. *Comp. Netw.*. 2015;76:146-164.

[16] Vaquero Luis M, Rodero-Merino Luis, Morán Daniel. Locking the sky: a survey on IaaS cloud security. *Computing.* 2011;91(1):93-118.

[17] Al-Sarawi Shadi, Anbar Mohammed, Alieyan Kamal, Alzubaidi Mahmood. Internet of Things (IoT) communication protocols. In: :685-690IEEE; 2017.