The ISC Int'l Journal of Information Security

August 2019, Volume 11, Number 3 (pp. 9–17)
http://www.isecure-journal.org

Selected Paper at the ICCMIT'19 in Vienna, Austria

Role and Application of RFID Technology in Internet of Things: Communication, Authentication, Risk, and Security Concerns☆

Saadi Hadjer [1,2,*], Yagoub Mustapha C.E. [3], and Touhami Rachida [1]

[1] *Faculty of Electronics and Informatics, University of Science and Technology Houari Boumediene, Algiers, Algeria*
[2] *Laboratory of Research, INPTIC, Algiers, Algeria*
[3] *School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada*

ARTICLE INFO.

Keywords:
Architecture, Authentication, Communication, IoT, RFID, Security, Sensors.

Abstract

The Internet of Things (IoT) is a very encouraging and fast-growing area that brings together the benefits of wireless systems, sensor networks, actuators, etc. A wide range of IoT applications have been targeted and several aspects of this field have been identified to address specific issues, as well as technologies and standards developed in various domains such as in radio frequency identification (RFID), sensors, and mobile telephony, to name a few. This article aims to talk specifically about the RFID technology and its accompanying communication, authentication, risk, and security concerns while applied to the IoT field. An important part of this work is indeed focused on security aspects that derive from the use of RFID in IoT, especially in IoT networks. The results of our research work highlighted an excellent integration of RFID in the field of Internet of things, particularly in healthcare systems.

1 Introduction

Nowadays, the Internet of Things (IoT) has invaded our daily life; the entire world has to be linked through inter-connected objects via the Internet and through appropriate protocols. Applications in various fields have demonstrated the effectiveness of this new vision of the world, which makes human life so much easier. Since objects must be identified, tags are pasted with a unique identifier and can be wirelessly identified by Radio Frequency using different technologies, the most widespread technology being the RFID or Radio Frequency Identification which, in turn, has experienced a great deal. evolution and large propagation with wide applications. Therefore, our work focused on all aspects of using RFID as a foundation in the field of IoT.

In 1999, Kevin Aston coined the term "Internet of things," which was used for the first time by the MIT's Auto-ID Center, a network of academic laboratories concentrated on RFID and IoT [1]. But what exactly the Internet of things (IoT) means?

The Internet of Things is a new technology that makes objects themselves identifiable when they exchange information. It lets persons and objects to become connected at anytime, anywhere, with anything and anyone, whatever the nature of the objects

☆ The ICCMIT'19 program committee effort is highly acknowledged for reviewing this paper.
* Corresponding author.
Email addresses: hadjer_saadi@yahoo.fr, myagoub@uottawa.ca, rachida.touhamib@gmail.com
ISSN: 2008-2045

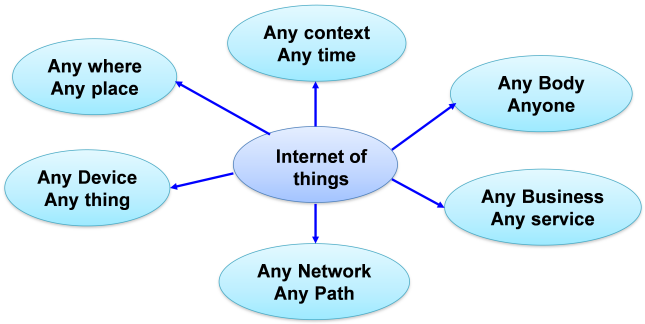

Figure 1. IoT issues

to be connected [2]. So, this technique forms a system which is the linkage of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, that allow objects to amass and exchange data to further automate the human life, as summarized in Figure 1.

The Internet of Things offers an interface between the real and the virtual worlds. Physical objects have virtual representation, which allows them to become familiar with a context in which they can detect, communicate, interact, and share data, information, and knowledge. Using intelligent decision algorithms in software applications, suitable fast responses can be given to a physical entity based on the most recent information collected on physical entities in databases and taking into account historical data trends, whether for the object itself or for similar objects. This opened new horizons for the notion of IoT in many areas such as supply chain management, transport, logistics, aerospace, automotive, intelligent environments (homes, buildings, and infrastructure), energy, agriculture, retail, etc [3]. Most frequently used case in RFID technology as a method of communication, sensor technologies, other wireless technologies, etc.

This paper is organized in seven sections, after this introduction and related work we talked about the principle and architecture of IoT in Section 3. In Section 4, we coted the RFID as the main communication technology linked to IoT and focused on the relationship between them. In Section 5 some application domains of IoT are highlighted in Section 6, we summarized some difficulties and challenges inherent to their combination and finally, we made the accent on the aspects of security, authentication, and risks related to the implementation or use of the emergent RFID-IoT technology. Then, we ended this paper with a conclusion.

2 Related Works

To make any application more efficient and for the purpose of facilitating our human life, the combination of the two very powerful technologies, RFID and IoT, has a significant impact in the current technological revolution, such as in smart cities, smart roads, smart medicine, making them intelligent thanks to the use of RFID technology, but also efficient thanks to this technological combination.

Several papers have been written taking this vision in mind, i.e., the use of RFID in the technological world of IoT. Xiaolin Jia et al. [4] talked about RFID technology and its applications in Internet of Things, the concept of IoT, its architecture and design goals with a good description of all layers, RFID concepts and fields of applications. Other researchers studied the IoT applications in several domains like in logistics and supply [5], manufacturing, agriculture management, health care and medicine [6] as further detailed in this paper, smart homes [7], and intelligent community security system (smart cities) [8]. J. Sathish Kumar et al. [6] raised another field of applications, i.e., Vehicle Management [9], where the information of the cars are sent by RFID tags, read by RFID readers and incorporated in a large network of sensors to give all necessary information to improve security aspects of environment when the car live his position in the parking.

3 Principle and Architecture of IoTs

We can see the IoT as a massive network of devices and microprocessors connected through a series of midway of interfaces where numerous technologies can be used as RFID, wireless connections may facilitate this connectivity. RFID is used with tags attached to objects to identify and follow them, which is called traceability. Sensors then are used as principle device to collect data from the environment around such objects, all being embedded, thanks to miniaturization and nanotechnology with embedded intelligence which give them the advantage to be smart while achieving intelligent control of every thing. To better understand the functionalities of IoT, Figure 2 shows the main blocks constituting a real IoT system (detailed in Figure 3 along with related services [10]).

Based on the information presented above, the architecture of the Internet of Things can be schematized by a model of three main layers, namely perception, network, and application. As illustrated in Figure 4, the perception layer (also called recognition layer) aims to collect information and data identifies the physical world. The network layer, the intermediate layer, performs processes such as initial processing and dissemination of data. The upper application layer provides the services. Among these layers, the inter-mediate network layer is the most important and can be considered as the "central nervous system" responsible for performing global services in con-

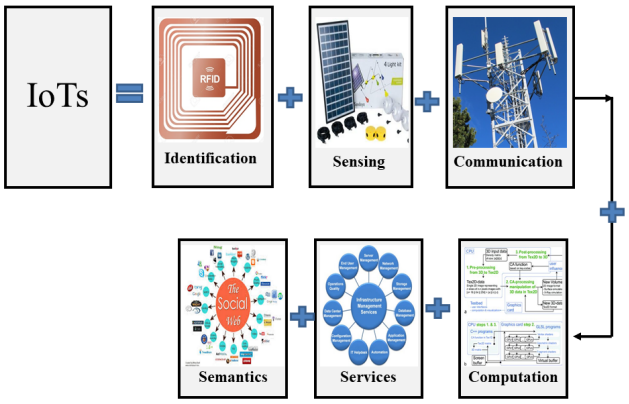

Figure 2. Principle and different component and functions of IoTs

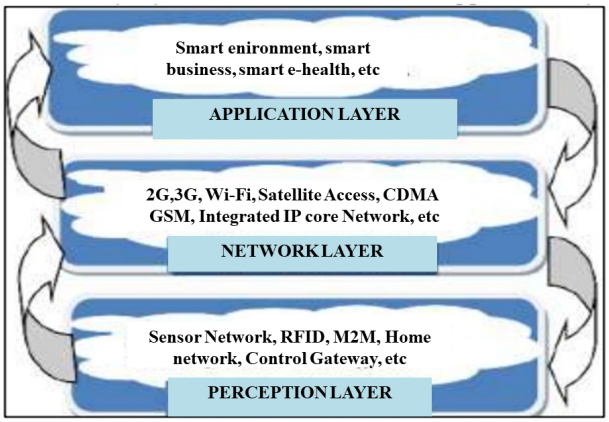

Figure 4. Architecture of IoT with most used technologies in each layer

IoT elements	Identification	Sensing	Communication	Computation		Service
Samples	Naming	Smart sensors, wearable sensing devices, embedded sensors, actuators, RFID tags	RFID,NFC, UWB, Bluetooth, BLE, IEEE 802.15,4, Z-wave, WiFi, WiFidirect, LTEA	Hardware	Software	Identity-related (shipping), Information aggregation (smart grid), Collaborative-Aware (smart home), ubiquitous (smart city)
	EPC, µCode			SmartThings Arduino, intel Galileo, raspberry Pi, Gadgeteer, BeagleBone, SmartPhones	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc	
	Adressing					
	IPv4, IPv6					

Figure 3. Building blocks and technologies of the IoTs

nected objects through the connection between the two extreme layers, perception and application [10].

4 Communication Technologies in IoTs

The rapid development of wireless technologies and the ever-increasing enhancement of information technologies and networking, coupled to miniaturization of embedded systems, give a powerful mean to guarantee efficient communication between several devices, objects or things. The main technologies enabling communications in the IoT domain are summarized below [10].

4.1 RFID

RFID is a technology that emerged with the beginning of the 21st century. From that, it shows a very quickly spread. Its signals are used to establish a point-to-point connection between objects. RFID comprises three major components: (i) a transponder (also called tag or label) for carrying data pasted on the element or thing to be identified, (ii) an interrogator or reader reading the information or data transferred, and (iii) a communication channel that transfers data to a database, a processor or another system. RFID standards concern both the frequency ranges (for data communication) and the data format (for data storage on the label). The principal shortcut of this technology is the serious problem of collisions between tags or between readers. Some of the IoT applications using RFID are smart shopping, smart chips, arts and games, smart environment, security enhancement, intelligent waste management and health care. So we can even claim that IoT is one of the direct and widely-used applications of RFID technology.

4.2 Sensors

Sensors are an essential building block of IoT, they can have a widespread range of applications. The sensor is the first element of the measurement chain; it measures and transforms the physical quantities at its entry into electrical quantities measurable by an electronic device in an analog or digital form. The sensors can be subcutaneous, implanted in a purse or on clothes. Despite their very small dimensions, they can still receive data from quite long distances. Sensors are indispensable in human life and offer services in thousands of applications in so various areas such as in military, environmental, health, construction, commercial/domestic applications, etc.

As for its physical entity, a sensor can be used alone or be part of a sensor network (in which case, it is called “node”). The hardest task is to ensure connectivity between multiple nodes that can be connected

by a wired or wireless link. A sensor node in a wireless sensor network can be considered as a small, low power device devoted to exchange information with data storage units, microprocessors, low power devices, analog-to-digital converters, data transceivers, controllers, etc.

4.3 Combination of RFID and Sensor Technologies

Combining different technologies can strongly reduce the gap between the real world of objects and the virtual world of networks. For instance, a RFID tag can provide accurate information about the object to which it is attached such as its nature or position. The sensor, on the other hand, can provide information about the surrounding environment. The combination of these two technologies, RFID and sensors, on mobile objects can indeed give a real image about the position and state of the concerned object. So, an RFID tag sensor can, comparatively to a conventional RFID tag, act on the data assembled by the sensor. Combined with wireless technology, these two technologies can offer a widespread variety of applications in biomedical, military, smart cities ....

4.4 Sensors and Mobile Phones

Mobile telephony is a key element in our daily life, especially with the explosion of new functionalities of highly evolved and evolving mobile networks. Mobiles can be, in fact, considered among the most widespread communication and data transmission tools. Combined with sensor technology, they can provide accurate environmental information, motion recognition, and so more.

4.5 Near Field Communication Norm

Near Field Communication (NFC) is a conventional group of criteria and norms for smart and mobile phones to realize the communication with each other on a centimeter scale. NFC devices can be used in many applications, such as contactless payment systems, credit cards, smart cards and others.

4.6 ZigBee

ZigBee is a requirement standard for a group of high-level communication protocols used to construct personal networks made from small, low power digital radios. The performance of this standard is its long range despite of its low power, and that through intermediate devices mesh. Mainly reserved for low data rate applications, long battery life, and secure network.

Table 1. Technology standards (Radio-Frequency Identification - RFID, Wireless Fidelity - Wi-Fi, Wireless Sensor Network - WSN; Personal Area Network - PAN, Local Area Network - LAN, Peer-to-Peer - P2P)

	RFID	Wi-Fi	Bluetooth	WSN
Network	*PAN*	*LAN*	*PAN*	*LAN*
Topology	*P2P*	*Star*	*star*	*Mesh, star*
Power	*V.low*	$Low - High$	*Low*	*V.low*
Speed	$400Kbs$	$11 - 10Mbs$	$700Kbs$	$250Kbs$
Rang	$< 3m$	$4 - 20m$	$< 30m$	$200m$

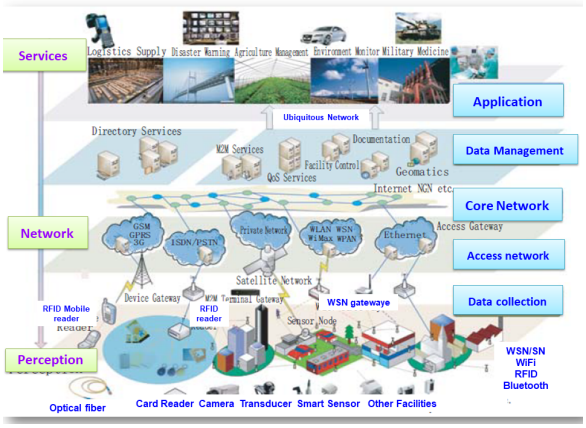

Figure 5. System architectures of IoT and applications at each layer

Table 1 recapitulates and compares widely used communication technology standards and characteristics.

5 Application Domains of IoTs

IoT applications are very plentiful and varied in all areas of people's daily lives. They cover large domains of society, industry, and environment. Most IoT applications are developed around the following areas: intelligent vehicles, intelligent life and intelligent cities. More precisely, in daily lifestyle, merchandizing, agriculture, smart factory, supply chain, emergency, healthcare, tourism, and energy, to name a few [11]. Figure 5 summarizes both the IoT system architectures and the different applications and technologies related to each layer.

6 RFID and IoTs Relationship and Applications

Almost of IoT applications are based on RFID communication or sensors technology. To understand the relationship between these two technologies, we can summarize it in three types of IoT applications explained below [11]: The smart cities IoT applications are based on several technologies: RFID, Wireless Sensor Networks as well as single sensors as IoT elements. Other examples of IoT applications using RFID are in warehouse and city sense [12]. We can also cite

the use of RFID in logistics as part of an IoT system with WSN and single sensors [12]. In healthcare in particular, several technologies associated with the IoT (e.g., RFID, NFC, WSN, WiFi, and Bluetooth), which considerably enhance the measurement and control procedures of dynamic functions such as temperature, blood pressure, heart rate, cholesterol level, blood glucose, etc [12].

6.1 RFID Communication in IoT

One of the major technologies used in IoT is RFID, as it allows the storage of complex data, wireless communication without line of sight and automatic identification and traceability of objects. RFID technology was used for the first time during the Second World War to distinguish between ally and enemy aircrafts. Compared to the outdated barcodes, obvious advantages make RFID a better and more practical technology to use with objects of different surfaces, providing read/write capabilities without any visual contact and the option to read multiple RFID tags at the same time [13].

6.2 Application of RFID in IoTs for Healthcare System

Health applications using the RFID technology in IoT systems are much diversified, from the location of medical equipment, to the identification of newborns and patients, to the monitoring and validation of medical treatments, to the location of patients, to the management of procedures in medical centers as well as to the management of surgical processes. The widespread and rapid use of RFID technologies in the health field requires the achievement of three main conditions: reliability of access and management, security of sensitive health information when transmitted via RFID systems connected to the IoT infrastructure, and secure authentication against hostile interferences and/or attacks in the communication links between RFID tags and servers. Figure 6 illustrates a typical healthcare system with the different applications in RFID [11].

A typical example of the application of RFID-IoT combined technology in a healthcare system is illustrated in Figure 7, where a mobile cardiac telemetry-monitoring platform is presented. With this system, the patient freedom is significantly improved, since he/she is connected 24/7.

6.3 WSN-RFID in Oil and Gas Industry

The use of Wireless Sensor Networks (WSN) associated to sensors, RFID and IoT in the oil and gas industry, is a promising field of application, where a large number of sensors is used to form a WSN as shown in Figure 8.

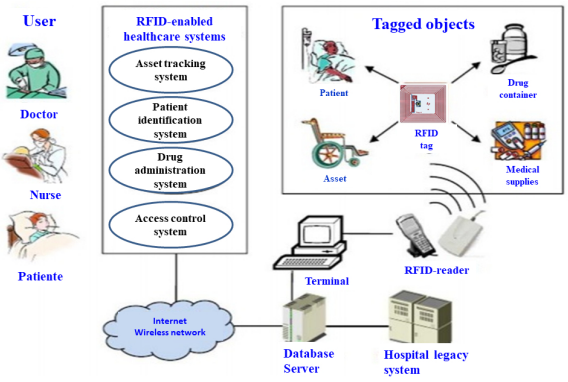

Figure 6. Typical RFID-based healthcare system [11]

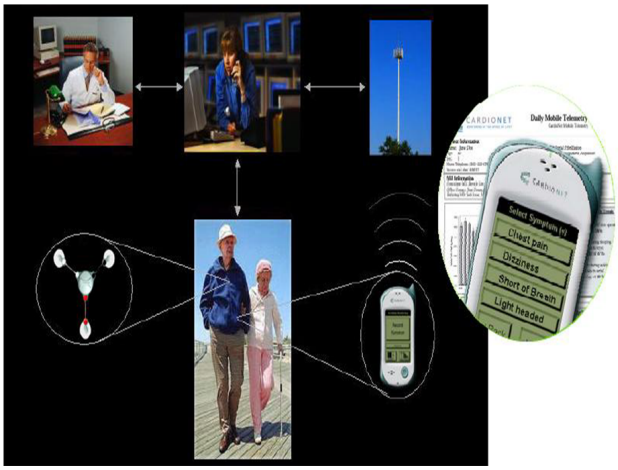

Figure 7. Mobile cardiac telemetry monitoring platform [11]

In wireless instrumentation, WSN-RFID are used in installations in remote and hostile areas, in temporary installations, in ease of scalability, and in redundant data collection for production optimization.

RFID and WSN are also widely used for sensing and traceability of personnel, equipment, containers, drilling tools, monitoring, and maintenance.

6.4 Defies and Issues of IoTs

Although technologies adopting IoT have become more and more numerous in the last few years, a multitude of problems must be addressed, which opens new directions for researchers of this field. The concerns and defies of IoT deal with complex architectures, privacy and security, data intelligence, quality of service, communication protocols, GIS-based visualization, and more. Furthermore, we have to mention the challenges inherent to scalability, technological standardization, interoperability, discovery, software

Figure 8. WSN RFID in Oil and Gas Industry

Figure 10. Application domains and defies of IoTs [10]

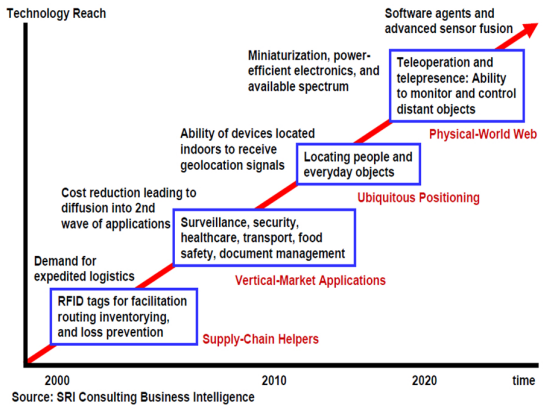

Figure 9. Evolution steps of IoTs [11]

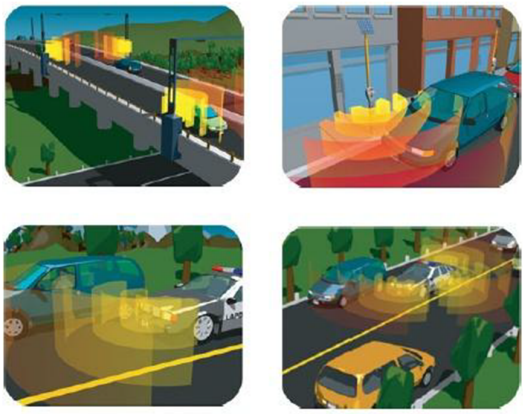

Figure 11. RFID for Inter-vehicular Communication

complexity, data volumes and interpretation, power supply, interaction and short-range communication. Also, some of the major challenges in IoT are related to collision issues due to the use of RFID technologies, security and privacy concerns, cost, design, and integration into existing systems.

Figure 9 represents the different steps and evolution of the use of IoT in several domains, like RFID, according to the evolution of defies.

IoT is intended as a network of a billion people interacting with a million of e-businesses, with a trillion intelligent devices interconnected thus, leading to a large number of application domains (as illustrated in Figure 10 that represents a big challenge to deal with, i.e., is there a limitation to this defy?

To give a response to this question, a statistics demonstrated that since 2015, one trillion sensors linking the physical and digital worlds have been merged to become the "Internet of Things", which implies that the list of applications of smart wireless is limited only by our imagination.

7 Security Requests for RFID Communication

A basic RFID system is composed of a tag, a reader and a data management system. Certain requirements must be taken to realize a secured system or secured mutual transfer of data. Therefore, to be built, a secured communication should deal with an important concept, which is RFID authentication. The main conditions of secured authentication are a mutual authentication between the RFID components (tag, reader, and server), confidentiality, forward security, scalability, and attack resistance [14].

An example that requires a lot of security aspects is the use of RFID for inter-vehicular Communication as shown in Figure 11. It includes RFID for communication between vehicles or Vehicle Identification Systems, where the aim is to determine if a vehicle registration has expired, to monitor traffic and vehicle speed in construction zones or other pertinent areas, to ticketing parking, etc.

In this section, we will detail the major axes related to this primordial aspect, i.e., security, with which we

can assure confidentially of data exchanged between the different connected objects of an IoT network.

7.1 Main Challenges in IoT security

The IoT can give rise to a multitude of applications in diversified fields with a great financial impact. Nevertheless, a great number of challenges have to be addressed for their good functioning, for which we can quote some as follows [15]:

1) Management of objects with unique identifier: IoT aims to connect billions of physical objects. So, a successful identification requires a unique ID number, or Unique Identifier (UID), to avoid any kind of misidentify or confusion between products. Therefore, a proper and planned identity management is essential for the dynamic allocation of UIDs for billions of products or physical objects. This function can be ensured by the introduction of RFID communication protocols in the IoT system.

2) Standardization and interoperability: In order to have a common communication language between multiple objects from different providers, an international standardization is required to ensure an unified language and operating mechanism understandable by all physical objects and sensors in a global environment including an IoT network, a RFID system, and a WSN, as well as to improve interoperability and communication flexibility between them.

3) Privacy and confidentiality of information: The main identification technology used in IoT is RFID because of its advantages compared to other technologies. For reasons of security and to avoid any kind of unauthorized access, especially because of the wireless nature of the communication link between RFID tags carried by the objects to be identified, it is essential to guarantee the confidentiality of the information exchanged. Again, the information from the different sensors in a wireless system is subject to different possible attacks and must therefore be secured by means of encryption algorithms to ensure the integrity of the data at the information processing system level.

4) Security of physical devices: one of the major challenges is also the guarantee and protection insurance of all IoT objects arranged in different positions, and regardless of their location, against any kind of attack, physical damage or vulnerability to non-secure accesses.

5) Network security and autonomy: with the significant number of big data from large wired or wireless sensor networks, the processing units must guarantee these tasks without loss of information and without external intervention; all these functions must be ensured by the IoT network, so not only a security challenge is needed, but also autonomy.

7.2 RFID Authentication Mechanism

The encryption algorithms used in the RFID authentication system can be classified into two categories of cryptosystems: non-public key (NPKC) and public key (PKC). NPKC-based RFID authentication schemes are much preferred since they offer better performance because of their simplicity. This simplicity comes precisely from their structure and architecture that are very simple to reimagine, such as the schemes based on the NPR (cyclic redundancy code) check which is based on simple operations at the XOR, AND, and OR bits [16].

Nevertheless, research has shown the inefficiency of NPKC-based schemes due to the lack of implementation of certain attributes to guarantee secure communication. With the evolution of microelectronic technology, some PKC algorithms have been directly implemented in RFID chips.

7.3 Security Necessities for RFID Communication

As mentioned above, a conventional RFID system consists of a tag, a reader and a communication management system or a server. So because the communications between these three components are wireless, it is not secure by nature, which then raises high risks of spying or loss of data exchanged between tags and readers. To solve this problem, authentication is necessary. Note that between the reader and the server the communication is secured thanks to the use of a security mechanism and an encryption key.

According to the literature, various research papers have identified the requirements for secure RFID communication as well as strong and effective authentication mechanisms [16].

1) Mutual authentication: an authentication between the reader and the RFID tags is necessary to secure the communication in this transmission channel (as already stated, between the reader and the server the communication is much secure).

2) Anonymity: Tag ID must be encrypted to satisfy better mutual authentication.

3) The information exchanged between the tags and the readers must be confidential against any kind of illegal access by means of encryption before being transmitted.

4) Availability: The RFID authentication must be realized during the lifetime of an RFID tag, and the synchronization of the different functions must be

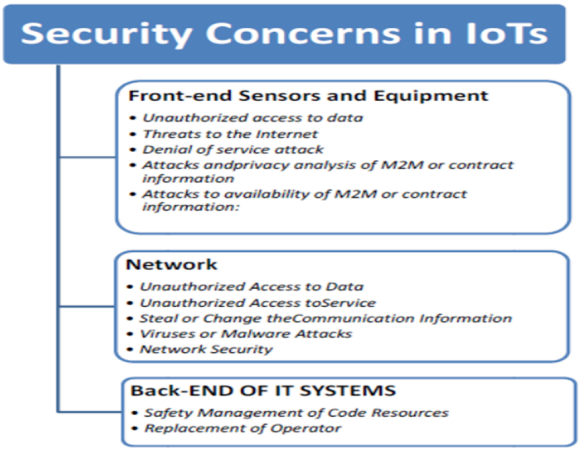

Figure 12. Security risks and threats [6]

performed, otherwise, the authentication mechanism will be invalid.

5) Transfer security: the authentication mechanism must ensure the security of data transfer so that it is protected from any kind of illegal access, which leads to a violation of the private lives of people.

6) Resistance to attacks: The RFID authentication process must be secure against various attacks to ensure the security of communications within the RFID system.

Figure 12 summarizes the main risks and menaces that can be encountered in IoT communication systems.

8 Conclusion

The IoT is the new direction of actual life and researches. It uses a diversity of information sensing identification devices and information processing equipment. It can be associated with several technologies such as RFID, WSN, etc. to form a widespread network that deals with intelligent and automated objects or things thus, facilitating our daily life. This paper investigates the main applications and challenges of RFID technology, and more particularly in healthcare, with a focus on this technology as an important and fundamental part of an IoT network as well as on how to guarantee a secure communication link between all components involved in this network.

References

[1] Sadia MazharA M. U. Farroq, Muhammad Waseem. Review on internet of things (iot). *International Journal of Computer Applications*, 113, 2015.

[2] Drashti Hirani Vishal Kansagara, Darshan Thoria. Overview on internate of things (iot). *International Journal of Advance Research in Engineering, Science and Technology*, pages 1–4, 2016.

[3] Xin He Jian An, Xiao-Lin Gui. Study on the architecture and key technologies for internet of things. *IACR Cryptology ePrint Archive*, 11:329–335, 2012.

[4] Xiaolin Jia, Quanyuan Feng, Taihua Fan, and Quanshui Lei. Rfid technology and its applications in internet of things (iot). In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, pages 1282–1285. IEEE, 2012.

[5] Y.Meng Y.X. Lu, T.B. Chen. Evalution guideling system and intelligent evaluation process on the internet of things. *American Journal of Engineering and Technology Research*, 11:537–541, 2011.

[6] Dhiren R. Patel J. Sathish Kumar. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90:20–26, 2014.

[7] Long Chen Shervin Erfani, Majid Ahmadi. The internet of things for smart homes: An example. In *8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, 2017.

[8] RK Pateriya and Sangeeta Sharma. The evolution of rfid security and privacy: A research survey. In *2011 International Conference on Communication Systems and Network Technologies*, pages 115–119. IEEE, 2011.

[9] Jihong Liu and Li Yang. Application of internet of things in the community security management. In *3rd International Conference on Computational Intelligence, Communication Systems and Networks*, pages 314–318. IEEE, 2011.

[10] V. Bhuvaneswari R. Porkodi. The internet of things (iot) applications and communication enabling technology standards: An overview. In *International Conference on Intelligent Computing Applications*, 2014.

[11] Debiao He and Sherali Zeadally. An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal*, 2015.

[12] Chunling Sun. Application of rfid technology for logistics on internet of things. In *AASRI Conference on Computational Intelligence and Bioinformatics*, pages 106–111, 2012.

[13] Fuquan Sun Xu Cheng, Minghui Zhang. Architecture of internet of things and its key technology integration based-on rfid. In *in Fifth International Symposium on Computational Intelligence and Design*, pages 294–297, 2012.

[14] U. Kumar T. Borgohain and S. Sanyal. Survey of security and privacy issues of internet of things. *Internationl Journal of Advanced Network Applications*, 6:2372–2378, 2015.

[15] Kavita Khanna Rishika Mehta, Jyoti Sahni. Internet of things: Vision, applications and challenges. In *International Conference on Computational Intelligence and Data Science ICCIDS 2018, Procedia Computer Science*, page 1263–1269, 2018.

[16] Hemalatha D and Afreen banu El. Development in rfid (radio frequency identification) technology in internet of things (iot). *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, 4:4030–4038, 2015.

Hadjer SAADI received the DEUA Diplôme d'Etudes Universitaires Appliquées in Electronics, Option communication in 2000 from institues of higher techniciens from Université des Sciences et de la Technologie Houari Boumediene, Algiers, Algeria, then Dipl-Ing. degree in Electronics option contrôle de processus et robotics in 2003, Magister degree in Electronic instrumentation in 2006, and Ph.D. degree in 2018 all from the Faculty of Electrical and Informatics Engineering, Université des Sciences et de la Technologie Houari Boumediene, Algiers, Algeria. She joined the Institute National de la Poste et des Technologies de l'Information et de la Communication, Algiers, Algeria, as Lecturer during 2007-2017 and then as Assistant Professor during 2018 till today. She is a member of the Laboratory of Instrumentation (LINS) and Laboratory of Research in TIC (LABORTIC). Her research interests include telecommunication, mobile communication and networking, RFID anti-collision algorithms, architecture design. She has authored around 20 publications in these topics in international journals and referred conferences.

Mustapha C.E. Yagoub received the Dipl.-Ing. degree in Electronics and the Magister degree in Telecommunications, both from the École Nationale Polytechnique, Algiers, Algeria, in 1979 and 1987 respectively, and the Ph.D. degree from the Institut National Polytechnique, Toulouse, France, in 1994. After few years working in industry as a design engineer, he joined the Institute of Electronics, Université des Sciences et de la Technologie Houari Boumédiene, Algiers, Algeria, first as Lecturer during 1983-1991 and then as Assistant Professor during 1994-1999, holding the position of Head of the Communication Department from 1996 to 1999. In 2001, he joined the School of Electrical Engineering and Computer Science (EECS), University of Ottawa, Ottawa, ON, Canada, where he is currently a Professor. His research interests include RF/microwave CAD, RFID design, antenna design, active device modeling and characterization, neural networks for high frequency applications, and applied electromagnetics.

Rachida TOUHAMI received the Diplôme d'Ingénieur degree in Electronics in 1985, the Magister degree in Telecommunications in 1990, and the PhD degree in 2001, all from the Ecole Nationale Polytechnique, Algiers, Algeria. She joined the Institute of Electronics, Universit e des Sciences et de la Technologie Houari Boum ediene (USTHB), Algiers, Algeria, first as Assistant during 1986– 2001 and then as Assistant Professor from 2002. Since 2007, she is working as Professor in the Faculty of Electronics and informatics, USTHB. She is working as Professor in the Ecole Nationale Polytechnique, Algiers, Algeria from 2016. Her research interests include microelectronics, RF/microwave device modeling and Microsystems.