# RESEARCH ON THE DESIGNING OF AN ALGORITHM AND CREATING A SOFTWARE APPLICATION FOR A SECURITY SYSTEM BASED ON IOT AND RFID

DOBRE Mihaela Cosmina Daiana[1], TARBĂ Ioan – Cristian[2]
[1]Faculty of Industrial Engineering and Robotics, Study program: Applied Informatics in Industrial Engineering, Academic year: 4, e-mail mihaela.dobre20@yahoo.com
[2]Faculty of Industrial Engineering and Robotics, Manufacturing Engineering Department, University POLITEHNICA of Bucharest

*ABSTRACT: The purpose of the paper is to develop a software application for simulating and testing IoT and RFID systems. The subject studied aims to develop an application with database access to authenticate the users to protect the facility by implementing different security policies. In this paper we have exemplified some ideas about architectures, communication protocols and IoT technologies, designed a smart factory, in which we have connected several IoT devices, which can be remotely controlled using a smartphone or personal computer.*

*KEYWORDS: IoT, RFID, Firebase, Java, Android Studio*.

## 1. Introduction

The purpose of this work is to develop a software application, a database and an experimental model of access control, the communication being carried out through the Internet. The objective of system is to have access and to monitor the records of the personnel entering or leaving an area where access is intended to be controlled. The way this system is wanted to work is by creating a software application and an experimental model that represents the physical access control system, all of which interact with a database developed specifically through the Firebase utility, a platform developed by Google for creating mobile and web applications.

For the realization of the software application, the Java language will be used in the Android Studio development environment, and for the experimental layout, an ESP32 device will be used, programmed via the Arduino IDE in C++, together with an RFID RC522 card reader.

## 2. State of art

RFID is one of the main technologies available that has made the Internet of Things (IoT) come to life. It is a wireless technology for automatic identification and data capture. The RFID technology shown in Figure 2 is a booming communication technology in IoT applications. It is based on a wireless technology in which a label is attached to an object, using contactless communication with a radio frequency reading device through a radio link. [1]

RFID is a system in which this object is uniquely identified by transmitting its identity (unique ID) through radio waves to a middleware responsible for data handling. Free of human error, it guarantees the quick and easy collection of information about a product, time, transaction or place. As a wireless communication protocol for active RFID operating in the Industrial Scientific Medical (ISM) tape is DASH7, which is available at world wide level and is suitable for IoT requirements. DASH7 (DA7) is standardized by ISO 18000-7. [2]

## 3. IoT architectures, communication protocols, and technologies

Objects that we use in everyday life are interconnected, from here we can understand the importance of the Internet of Things (IoT). Given this importance, a flexible architecture for IoT systems needs to be defined. With the advent of IoT, which will connect numerous objects to the Internet, traffic will increase substantially and higher data storage requirements will arise. Such a large network also leads to security and privacy issues [5]. Therefore, the proposed IoT architecture must address various factors such as reliability, quality of service, and scalability.

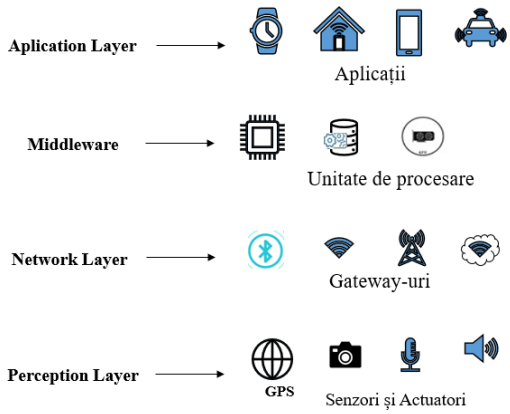


Figure 1 – IoT Architecture

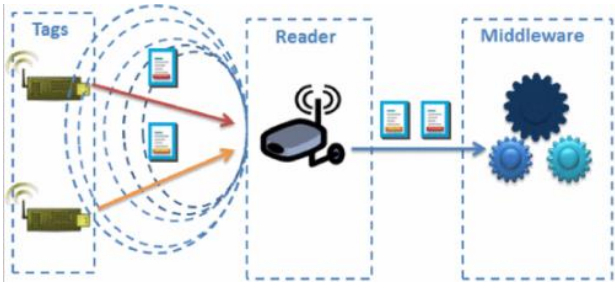


Figure 2 – RFID Architecture [1]

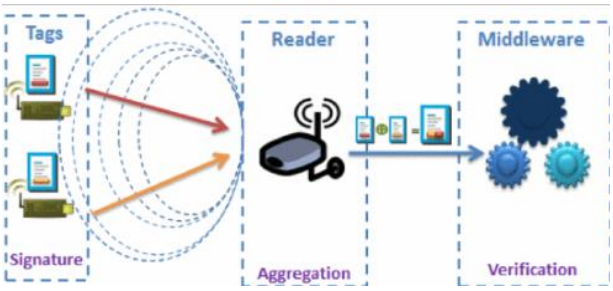


Figure 3 – Secure RFID architecture [1]

Achieving device interconnection requires a communication environment. For example, if a sensor is part of an IoT network, it needs a wired or wireless environment, such as Bluetooth or others, to transmit the data it collects. When it comes to IoT technology, wireless communication is the main focus, and many communication technologies and protocols can be used to connect smart devices, such as Internet Protocol version 6 (IPv6), through low-consumption personal area wireless networks such as: (6LoWPAN), DASH7 (ISO 18000–7 standard), ZigBee, Bluetooth and near field communication (NFC).

- DASH7

The DASH7 Alliance protocol (D7A) is an open standard for two-way, sub-Ghz, medium-range wireless communications, adapted for sensor-actuator applications using private networks. The D7A comes from ISO 18000-7 for active RFID and operates in sub-GHz ISM bands. The protocol specification is free to use without any patent or license requirement. [2]

- Radio Frequency Identification (RFID)

As the name Radio Frequency Identification suggests, it is a technique that uniquely identifies objects using radio waves. An RFID system has a label, an antenna, and a reader. Using the antenna, the reader sends a signal to the label to get the unique data, and the label responds with its unique data. The label can be attached to objects, this allows them to be uniquely identified and be part of the IoT network, in this way they can communicate on the network. There are two types of RF tags in the label system, the active label and the passive label. [4]

- ZigBee

ZigBee is a technology that has been created to be able to improve the operation and use of wireless sensor networks (WSN). ZigBee Alliance has been in charge of developing this technology, designed in 1998, standardized in 2003 and revised in 2006. This technology works at frequencies of 868 MHz, 902-928 MHz and 2.4 GHz, has a low cost, is reliable and scalable. It has a low data transmission speed, which can be used within a range of up to 200 meters and can even use 128-bit AES encryption. ZigBee is developed on the IEEE 802.15.4 standard that obtained approval in 2003. The protocol allows devices to communicate in a variety of network topologies with low power consumption, which helps to increase the autonomy of equipment using the technology. This protocol is used in areas such as industrial automation, home automation, smart metering and metering, etc. [3]

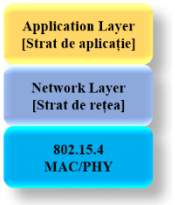


Figure 4 – ZigBee Protocol Stack

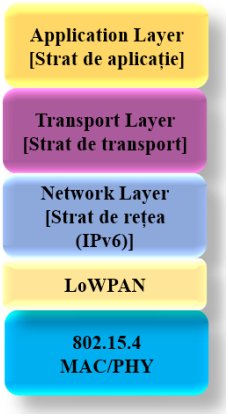


Figure 5 – 6LoWPAN Protocol Stack

- 6LoWPAN

6LoWPAN is the first and most commonly used standard in IoT communication protocols because it is a standard IP-based interconnection protocol. It can be connected directly to another IP network without intermediate entities such as translation gateways or proxy. This standard was created by the Internet Engineering Task Force (IETF), a standard Internet protocol (IP) communication over low-power

IEEE802.15.4 wireless networks that use IPv6. This is aimed at accepting addresses (IPv6) of different lengths. It is also a low cost, a low energy consumption with bandwidth. 6loWPAN supports different types of topologies, such as mesh and star topology. 6loWPAN proposes an adaptation layer between the MAC and network level (IPv6) to manage the interoperability between IEEE 802.15.4 and IPv6. The most competitive alternative to 6LoWPAN is ZigBee, as seen in Figure 4 . Both use the same IEEE 802.15.4 protocol at the physical level.

## 4. Designing a smart factory using IoT and Wi-Fi technologies

IoT and Wireless Sensor Network (WSN) technologies can be used to deploy a smart home over Wi-Fi. Through IoT, all home devices can be connected to the Internet via Wi-Fi, so they can be monitored remotely. Sensor and device grouping technology in WSN technology detects and collects data from different parts of the smart factory, and this information is sent to a central location. In this section of the article, a simulation is designed using the software "Cisco Packet Tracer 8.0" that simulates various devices and sensors to implement security and control functions of a smart factory. Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. [6] The proposed system can control and monitor various devices and devices using a "Smartphone" or a personal computer. Cisco Packet Tracer offers a variety of smart devices and objects that can be configured and programmed. The personal wireless gateway router has been used to connect all devices and components over the Wi-Fi network using the IEEE 802.11 standard. The devices were registered on the network by assigning an IP address. On the router, encryption protocols can be configured to protect the wireless connection such as Wired Equivalent Privacy (WEP), Wi-Fi Protect Access – Pre-Shared-Key (WPA – PSK), WPA2, as we can see in Figure.6.

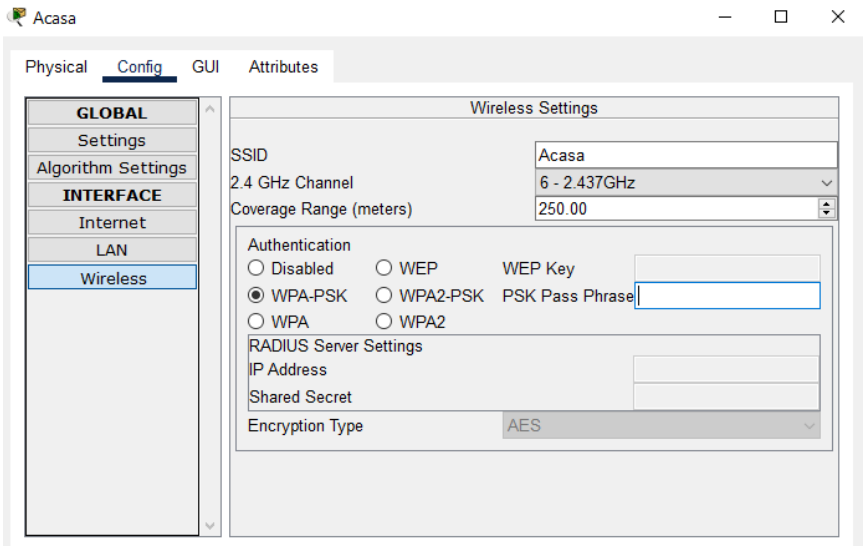


Figure 6 – Home router configuration page.

Figure 7 shows the components and the sensor. The router is connected to the devices via wireless and wired network connection. Different devices can be controlled and monitored, connecting them to the same wireless network. A laptop, an alarm, 2 cameras, a fan, a gas sensor, 5 doors and an RFID reader are connected to the gateway router.

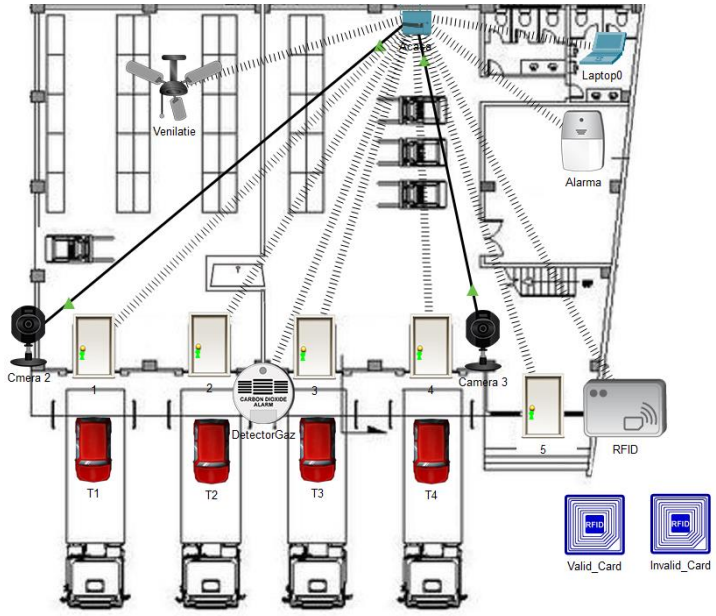


Figure 7 – "Smart" components connected to the home gateway

## 5. Conclusions

In this paper, the concept of the "Internet of Things (IoT) was generally presented, which contains architectures, existing technologies, their usefulness, as well as the main challenges of the IoT field. A simulation of the security of a smart factory was conducted in the Cisco Packet Tracer program to understand IoT concepts and how they work. In terms of future development directions, I want to address the technological and social issues that prohibit RFID technology from enabling IoT and meeting ubiquitous computing expectations. With the EPC standard, an adaptive and scalable security scheme will be created that offers new cryptographic suites, while wanting to implement certain security policies. I consider a technical security solution that can present a promising solution for RFID-based IoT applications.

## 6. Bibliography

[1] Marwa Chamekh and Mohamed Hamdi and Sadok El Asmi and Tai-Hoon Kim (2018) "Security of RFID Based Internet of Things Applications: Requirements and Open Issues", IEEE Publishing House, Conference name "2018 15th International Multi-Conference on Systems, Signals & Devices (SSD)", Oraş Yasmine Hammamet, Tunisia, Date 19-22 March 2018, ISBN 978-1-5386-5305-0. URL:https://ieeexplore-ieee-org.am.e-nformation.ro/document/8570558/figures#figures

[2] https://www.dash7-alliance.org/

[3] https://en.wikipedia.org/wiki/Zigbee#Zigbee_Alliance

[4] Muhammad Junaid,Munam Ali Shah,Imran Abbas Satti "A survey of internet of things,enabling technologies and protocols", *2017 23rd International Conference on Automation and Computing (ICAC)* , 26 October 2016, ISBN: 978-0-7017-0260-1 at URL:https://ieeexplore.ieee.org/document/8082058; I PUT IT AT 5

[5] Eleonora Borgia, Danielo G. Gomes, Brent Lagesse, Rodger Lea, Daniele Puccinelli, "Editorial Special Issue on Internet of Things: Research challenges and Solutions", Computer Communications, Volumes 89–90, 1 September 2016;

[6] Kriti Chopra, Kunal Gupta, Annu Lambora "Future Internet: The Internet of Things- A Literature Review", 10 October 2019, ISBN: 978-1-7281-0211-5;