ISSN: 0123-3033 – ISSN-e: 2027-8284

INGENIERIA Y COMPETITIVIDAD
REVISTA CIENTÍFICA Y TECNOLÓGICA

Vol. 24 No. 1-2022 - DOI: 10.25100/iyc.24i1.11034

SYSTEMS ENGINEERING

Review of the use of IoT technologies and devices in physical security systems

INGENIERÍA DE SISTEMAS

Revisión del uso de tecnologías y dispositivos IoT en los sistemas de seguridad física

Mauricio Castaño-Gómez[1§], Ana M. López-Echeverry[1], Paula A. Villa-Sánchez[2]

[1]Universidad Tecnológica de Pereira, Facultad de Ingenierías, Grupo de investigación Nyquist, Pereira, Colombia

[2]División de proyectos, Casa de Software Prosof S.A.S, Pereira, Colombia

[§]*mauricio.castano@utp.edu.co, anamayi@utp.edu.co, paula2713@gmail.com*

Recibido: 20 de febrero de 2021 – **Aceptado**: 18 de junio de 2021

Abstract

Currently there has been an increase in insecurity and burglaries to homes, buildings, and various social places, which has led to search and implementation of mechanisms to protect people and these sites. In this way, houses with Physical Security Systems (PSS) are less affected by these events, and thanks to the technological advancement and the appearance of the Internet of Things (IoT), these systems has improved too much, being able to supply several needs with new functionalities, which are possible by new devices and technologies. In this sense, is desirable to resolve the question about what are the most used IoT devices and technologies in different PSS designs? Thus, the purpose of this article is to present the results of the literature review made, which sought to identify the common items used in modern IoT-bases PSSs, highlighting the advantages, disadvantages, and limitations of the implemented systems.

Keywords: *control access system, CCTV, Internet of Things, IoT, motion detection sensors, security, RFID.*

Resumen

En la actualidad ha habido un incremento en la inseguridad y robos a viviendas, edificios y diversos lugares sociales, lo que ha llevado a la búsqueda e implementación de mecanismos que permitan proteger a las personas y a estos sitios. De esta manera, las casas con Sistemas de Seguridad Física (SSF) son menos afectados por estos hechos, y gracias al

Como citar:
Castaño-Gómez M, López-Echeverry AM, Villa-Sánchez PA. Revisión del uso de tecnologías y dispositivos IoT en los sistemas de seguridad física. INGENIERÍA Y COMPETITIVIDAD. 2022;24(1):e30411034. https://doi.org/10.25100/iyc.v24i1.11034

avance tecnológico y la aparición del Internet de las Cosas (IoT) dichos sistemas han mejorado bastante, llegando a suplir varias necesidades con funcionalidades novedosas, que son posibles por los nuevos dispositivos y tecnologías. En este sentido, es deseable resolver el cuestionamiento sobre ¿cuáles son los dispositivos y tecnologías del IoT más comúnmente utilizados en diferentes diseños de SSF? Así pues, el propósito de este artículo es presentar los resultados de la revisión literaria hecha, en la que se buscó identificar los elementos comunes utilizados en los SSF modernos basados en IoT, destacando las ventajas, desventajas y limitaciones de los sistemas implementados.

Palabras clave: *CCTV, Internet de las Cosas, IoT, seguridad, sensores de detección de movimiento, sistema de control de acceso, RFID.*

1. Introduction

During the last few years, the growing concern in themes concerning security issues in all fields of life have increased, with the increment of different problems related to thefts to properties, houses, buildings, etc. [1,2], a situation that opens a panorama for the integration of current technology to guarantee the protection of both material goods and people's lives, and at the same time generates challenges for the construction of systems that can provide a solution.

Studies show that houses without security systems are more likely to be burglarized, with about 2.5 million thefts worldwide, of which 66% corresponds to dwellings [1]. Thus, despite that, the object or stolen value is only a small part, generates and grows a feeling of worry that can last years [3]. For these reasons, it is necessary to find a solution that contributes to mitigating crime [4]. It is remarkable now, that thanks to the Internet of Things (IoT) new characteristics and possibilities have been enabled for the Physical Security Systems (PSS).

The goal is to address the question of what are the most used IoT devices and technologies in different PSS designs? Therefore, the purpose of this article is to carry out a Systematic Literature Review (SLR) in conjunction with a systematic mapping [5,6], that allow identifying various systems that have been proposed and developed today, based on IoT devices and technologies, searching to highlight the advantages, disadvantages, and limitations that the authors have found, to finally present a base model that includes the most highlighted considerations.

1.1. General aspects of the Internet of Things

IoT as a growing paradigm is an ongoing mega-trend [4] in which the number of devices [7] have increased exponentially, being able to build a wide range of applications that seek to improve the work and facilitate the lifestyle by integrating new capabilities and systems automation [8].

Nowadays, the world is moving towards the concept of "Future Internet". The advent of the Internet of Things has led to a new wave of potential applications that could play an important role in daily life [9,10], changing and improving different aspects of it.

The Internet of Things allows the virtual and physical worlds to be brought together by various technical and social concepts, in addition, it is a paradigm that connects things, entities, or objects (like vehicles, buildings, systems, and people) in global network infrastructure, exchanging data of interest to complete several tasks (buildings security, traffic control, patient monitoring, among many others) [11–13].

In [14] is describe the principle and framework that suggests the use of IoT protocols for the machine-to-machine communication (M2M). That study proposes a multi-layer framework; sensing layer (sensors), network layer, and application layer. This provides the basis for the subsequent proposal of the IoT architecture, separated into 4 levels [15]. At the first level (sensing or perception)

are the devices that interact directly with the physical environment. At the second level (augmented or collection) are the devices that are responsible for receiving data from the sensors, and then send them to the next level for processing purposes. The last level is where the information is stored and made available to users for direct use [16].

The Internet of Things supports both pervasive and ubiquitous computing, with various devices (RFID Radio Frequency Identification tags, sensors, actuators, cell phones, etc.) being the core of the architecture [17].

In recent smart city applications, there is a large-scale deployment of cameras and other sensors that act as an eye of a sensory network that includes intelligent transportation, lighting, health, environment, and disaster management [18–22], demonstrating the great potential that IoT has.

1.2. Physical Security Systems

One of the fields that have seen the emergence of new systems is physical security. The new devices and elements created have made it possible to extend the capabilities of older Physical Security Systems (PSS), and nowadays have more robust applications that integrate a group of different components [23], as shown in Figure 1. New trends are increasingly seeking to create more proactive systems [24] that allow the ability to react to different situations.

Figure 1 shows the most common components that are integrated into a PSS, of which the following subsystems stand out: access control, motion/intrusion detection, surveillance or video monitoring (CCTV), alarms/notifications, lighting, and communication. These components can be grouped in systems such as; access control systems for the access control subsystem and a perimeter security system that groups the rest of the components excluding the communication subsystem, which is independent (it is in both groups).

Different traditional PSS present problems and limitations that expose vulnerabilities to possible thefts, loss of information, infiltration, and others, which demonstrates the need for constant updating. Examples of these systems are the traditional Closed-Circuit Television (CCTV) that consumes more energy and storage space, as they must record 24/7 and also need a lot of human intervention in the middle to can have the backup information in the cloud [25]. There are also smart cameras, current devices used in many IoT applications [26], in which security and privacy have become a concern due to their widespread deployment [25], which can more easily violate the basic security objectives for a smart camera [27,28].

On the other hand, considering traditional card-based Access Control Systems (ACS), these have many problems [29], related to the limited capabilities and old designs of readers, cards, protocols, and servers [30–34].

2. Methodology

The present research was divided into two phases: the first phase of Systematic Literature Review (SLR) and another of systematic mapping [5,6]. Initially, the first phase arose within the framework of the execution of an innovation and technological development project that is part of a call for proposals from the Ministry of Science, Technology, and Innovation (Minciencias). The project in question aims at building a physical security system for horizontal property based on IoT devices, a purpose for which a specific objective required the construction of a state of art in the particular subject of study.

On the other hand, seeking to contribute even more to the project and extend the initial phase carried out, a second phase was carried out in which the systematic review was extended to the

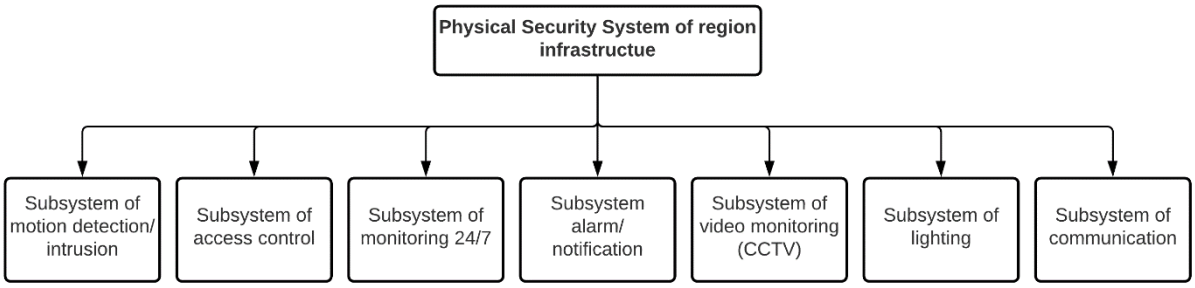

Figure 1. *Example of component structure of a PSS. Source: Adapted from* [23]

Table 1. *Main articles analized together with the given classification of subsystem in a PSS*

Article	Category
A Proposed System for Security in Campuses using IoT Platform: A Case Study of a Women's University [15]	Access control
AgentPi: An IoT Enabled Motion CCTV Surveillance System [24]	Perimeter security
An Automated Garage Door and Security Management System (A dual control system with VPN IoT & Biometric Database) [35]	Access control
Design and Implementation of an Automated Security System using Twilio Messaging Service [3]	Perimeter security
Intelligent Border Security Intrusion Detection using IoT and Embedded Systems [36]	Perimeter security
Internet of Things Based Intelligent Security using Android Application [2]	Access control
IoT and Wi-Fi Based Door Access Control System using Mobile Application [37]	Access control
IoT-Based Online Access Control System for Vehicles in Truck-Loading Fuels Terminals [29]	Access control
Low-Cost Energy Efficient Smart Security System with Information Stamping for IoT Networks [25]	Perimeter security
Smart City Management System using IoT with Deep Learning [38]	Perimeter security

Source: Own elaboration

main references cited in the works found in the previous phase, achieving with this a greater temporal coverage (the first phase was framed in only analyzing works after 2017). For these references, a systematic mapping of key terms was made, which allowed the identification of the different devices and technologies used in this type of systems, together with their advantages, disadvantages, and limitations.

In compliance with the specific objective already mentioned (on the construction of a state of the art), in the first phase, 10 articles were selected (see Table 1) to cover equally the different subsystems, which are classified in the categories of access control or perimeter security, and to which an in-depth analysis was made to give an idea of the key aspects, devices and IoT technologies that are included in modern physical security systems for horizontal property.

In Table 1, is detailed and explained all the process carried out for the development of the first phase in question.

2.1. Databases consulted

As a part of the development of this phase, access to the various databases provided by the Technological University of Pereira was available, in which, scientific research articles published in journals and conferences were searched. The main database consulted, from which most of the articles were obtained was IEEE Xplore, since it contained the largest number of results with proposed systems similar to the desired development of the project. Also, a single relevant result was obtained from Elsevier's Scopus database.

Additionally, for the second phase, other sources of information (online journals, databases, and repositories) were accessed, such as ResearchGate, Semantic Scholar, ScienceDirect, Google Scholar, Springer, Google Patents, Computer, IJARCSSE, and ACM.

2.2. Text strings used in the queries

For the different queries made in the first phase terms and keywords of the particular subject of study were used in various combinations, as shown below:

(IoT-Based OR IoT based OR Internet of Things OR IoT) AND (physical security) AND (system)

(CCTV OR surveillance) AND (intelligent OR smart) AND (system)

(IoT-Based OR IoT based OR Internet of Things OR IoT) AND (door OR entry) AND (control access)

(Intelligent OR smart) AND (security system)

2.3. Article selection criterions

Within this phase for each article, an initial review of the abstract, keywords, introduction, and conclusions was carried out to identify the relevance of the article and then move on to its detailed analysis. Among the selection criteria before the preliminary reading mentioned above are year preferably after 2018 and maximum 2017; the coincidence of keywords with other articles; in the abstract, a good structure is evidenced; in the introduction and conclusions an appropriate methodology, good bases, and references, as well as relevant results are appreciated.

2.4. Analysis of articles

For the 10 articles initially selected, we reviewed in detail the problem they solve, their methodology, approach, devices, and technologies used, their results, and, finally, their conclusions. In addition, in the review process, the main important references that are of interest for extension in the search and study of the second phase are extracted. These are then consulted and analyzed (in less detail), seeking to extract in brief the key items used for their solution together with the results.

It is noteworthy that from these 10 articles a total of 40 additional references were selected for consultation and analysis in the second phase.

3. Results

3.1. Physical Security Systems based on IoT

Being less frequent and at the same time, the most complete and costly systems are those used in border areas. In these areas, harsh geographical conditions make access and monitoring difficult. D. Alshukri et al. [36] implemented a system for intelligent security with intrusion detection capability using IoT and embedded systems, employing a set of sensors, actuators, and controllers. The overall control of the system for the various devices is performed using the controllers Raspberry Pi and an ESP8266. FLIR thermal cameras (Lepton) and a night camera

were deployed along with a motor, thus allowing 180° scanning. The night camera was accompanied by a spotlight and a laser gun that facilitate surveillance under various conditions. PIR, sound, and motion sensors were used for detection and subsequent activation of an alarm and an electric fence at the border. Finally, it should be noted that dual-channel wireless and wired network is used to ensure communication with the control center. This system has advantages in terms of ensuring surveillance and detection under various conditions such as darkness, fog, and rain, as well as scanning the entire area.

Other solutions for border security employ autonomous robots equipped with various types of sensors (PIR, ultrasonic, gas), cameras, and even laser weapons to open fire. Some of these are based on the Android system and are controlled by embedded systems. For communication and sending commands to these, the use of Bluetooth, wireless, and GSM technology is identified [39–44]. This type of solution has the advantage of requiring less human intervention (in this case from the soldiers at the border) for taking actions (since the robot-controlled from the command center can perform various actions such as firing), however, the disadvantages are that they are expensive systems besides that the entire system or security is centralized in the robot.

Now, for the most frequent perimeter security solutions, video surveillance systems such as CCTV are implemented, for which, it is proposed that only events of interest should be alerted [45], thus, in 2009 and 2011 [45,46], were proposed intelligent surveillance systems by motion detection to save on the great consumption of time required by normal video surveillance systems. Bahman A. Sassani et al. [24] propose a CCTV surveillance system (AgentPi) with motion and anomaly detection capabilities without the need for the use of physical sensors (achieved through the use of image subtraction algorithms), live video transmission for both local area network and remote networks, and also the activation of notifications by mobile means. For the construction of the system prototype, they considered: for processing a Raspberry Pi 2 version B and an evolutionary System on Chip (SoC), for the main storage a microSD card, a 5-megapixel Omnivision camera module, and an Android phone with the SMS server application for sending alerts. The software used is mainly open source, such as the Raspbian operating system, the Xvid Codec library, and the image processing algorithms OpenCV. The main advantages that can be found are the low cost and storage since the use of physical sensors is avoided, mainly open-source elements are used, and saving all the time is avoided. On the other hand, the main disadvantage is that the system remains on all the time, a situation that can generate cost overruns due to power consumption.

Prasad et al. [47] designed an intelligent monitoring and surveillance system using Raspberry Pi and PIR sensors. In their development they were able to effectively make the USB camera start recording when the PIR sensors detect motion, thus allowing to save in the amount of information to be stored. In addition, by using the system they can send information about how many people might be trying to break in.

In [25] a low energy consumption system was built, to look for economizing and save in the storage space. In their implementation they managed to make the cameras turn on only when motion is detected around them and to reduce the storage space, they developed a model (in Python language), which allows stamping in each frame of the video the date and time of the event, achieving integration of unstructured and structured data. Also, they propose an adjustment in a parameter in the system (it can be the time or space occupied) that allows establishing when to upload the information back up to the cloud. As a disadvantage in this implementation, it is found

that other security elements such as alarms/notifications are missing.

In [3] for the problem of lack of physical evidence [1] they propose a security system similar to the previous one, differing in the capture of images in burst to increase the probability of obtaining the image of the intruder, and in that they send an alert (SMS) and image to the e-mail using the Twilio messaging service [48], to the owner neighbors respectively. A similar system differentiated using GSM communication technology is also proposed in [49].

Another research proposes a system consisting of a panic button with an easily accessible location for users, which when is pressed sends a pre-recorded message along with the GPS location to the police. It is implemented using an ATmega16 microcontroller, a SIM900A GSM module, and 2 Android applications for interfacing with the hardware [50]. The advantages of this system are the sending of the message to the police, its simplicity, and economy, although its main and great disadvantage is the need to manually press the button in emergencies.

In [51] some prototypes for Intelligent Home Security Systems (IHSS) are described and they propose a fully automatic system with robots and Unmanned Aerial Vehicles (UAVs). The system had high performance; however, it turns out to be too expensive to be implemented in homes.

The oldest works observed, in 2010 [52] and 2002 [53] developed alarm security systems using technologies such as Bluetooth, GSM, Light Dependent Resistors, and Zigbee.

One of the recent research works proposed a smart home wireless security system, which sends an alert call to the user, thus, the user does not require any knowledge about a smartphone application. It is also possible to optionally activate the function to generate an alarm in case of intruder detection. For such implementation, they used the TICC-3200 Launchpad microcontroller, and for detection a PIR infrared sensor [54]. Their design choice is low cost and simple but has the disadvantage of not having added any functionality that allows the system to collect physical evidence or details of the intruder.

More recently, several research areas have been opting for the inclusion of Machine Learning and Deep Learning models that seek to extend new capabilities to systems. This fact for PSS is not an exception. Shubham Jain et al. [38] carried out a work in which they designed a smart city prototype that includes a component of intelligent streets with automatic lighting and equipped with an intelligent CCTV system that using a Convolutional Neural Network (CNN) model together with an image classifier manages to detect the presence of weapons and subsequently send an alert message to the authorities. For this implementation, PiCameras were used to capture images and locations at regular intervals. Regarding the training method used, the choice of the supervised learning [55] approach is evident, and in the image classifier (built with a pre-trained neural network [56]) to obtain better results augmentation and dropout processes are used. Their implementation presented a good result, reaching results on the test data set accuracy of 87%. This type of system is among the novelties, it opens a new trend and range of possibilities, although they still present certain limitations and difficulties for their implementation.

Next, moving from perimeter security systems to access control systems, there's also a set of proposals and applications that have been developed, which seek to solve various problems that have arisen over time.

Initially, on the way to the automation of door locking systems, work was done on detecting movement in front of the door and then moving on to the identification of persons. In this way

Britto et al. [57] proposed a Sixth Sense Door, introducing the concept of motion detection in front of the door.

According to the study conducted in [58] many security models for access control included a combination of RFID technology for authentication, an LCD for visualization, a motor for door movement, sensors to query the environment, an intercom module, and a control module.

In the patent of [59], a security system was presented for monitoring and automating a house with door locking using Raspberry Pi, with cameras, keyboard, and pi-lids, which is responsible for rescuing or obtaining the user's ID. Similar surveillance systems [2,60,61] that use facial recognition for entry, detect the person standing in front, and automatically if recognized the door opens, otherwise a notification about someone unknown is generated on the homeowner's cell phone. These use IR and PIR infrared sensors, Raspberry Pi 3B, Raspberry Pi camera modules, and DC motor. In general, good results are presented, but for low light (or other) conditions people were not recognized very efficiently.

Prarthana Jenifer et al. [35] recently in a study mentioned the need to protect access to industrial areas and private spaces within these areas. Therefore, to improve the secure and automatic access control of garage doors, they propose the design of a system with dual access, remote access to distant locations, and initial access with a physical authenticator. For the initial access solution, a fingerprint sensor with a biometric database is used, and for access to remote locations of the authenticator, a Virtual Private Network (VPN) with IoT is used, which through a web interface enables users to authenticate their credentials for entry to the desired area. For the implementation of the system, they used: a Raspberry Pi 3 in conjunction with the Python programming language, a fingerprint sensor with biometric database, a DC engine for opening and closing the doors, and, finally, they use a Virtual Network Computing (VNC) Viewer that allows graphical desktop sharing and connectivity of all system resources. The main disadvantage was that the fingerprint sensor used allows 100 copies to be stored, which for some cases may be too few. On the other hand, for access to the web interface, the person must have a smartphone, and although the use of these has increased a lot these days, it is possible that someone still does not have one, decides not to take it to work or is forbidden to do so.

An alternative system [62] integrates the Near Field Communication (NFC) reader of a smartphone, which acts as a module to open the entry point using a logic link control mechanism, and access permission is granted for code or password matching. The system allows three modes of operation; i) through the use of a single button, ii) through the entry of a password by the user and, iii) through a video guide that explains to the user how to obtain the ID and enter the password. This system is low cost; however, it is dependent on the smartphone.

Other systems based on GSM technology were proposed and implemented in [63–65]. These systems seek in different ways to detect the presence of a potential burglar or intruder, and subsequently, send alert notifications via SMS and activate a buzzer or alarm. Their implementations are based on a set of sensors such as infrared (PIR), touch, sound, and heat, and PIC 16F76 and Atmega 328 microcontrollers have been used for processing. In [63] a 5-digit code is used to unlock/lock the entry point. These systems present the limitation to collect evidence of what happens.

In 2014 Kale et al. [66], conducted a study comparing computer vision methods and algorithms that allow providing smarter security

features. They propose an intelligent home security system with an illumination-sensitive contextual model. In addition, they implement a facial recognition model for intruder detection and tracking. In their research they presented very good results, achieving not only intruder recognition, but they also obtained the ability of the system to ignore pets, animals, mosquitoes, etc., so as not to generate unnecessary alerts. This type of system proves to be effective and economical; it is only necessary an effort in the implementation and training for the algorithms to be used.

The door entry system proposed in [67] is composed of a switch, a camera, a solenoid and a speaker, all devices are integrated using a Raspberry Pi. When a person arrives at the entrance presses the switch, and immediately the camera captures the image of this for authentication by the person inside the house or office, the speaker is ready to listen to the other person. Once the user accepts the guest, the solenoid opens the door. This type of system is quite basic compared to others already exposed, but it stands out that its implementation is very simple, and, in addition, it turns out to be of low production cost.

In [68] a facial recognition was performed using IoT, the system upon recognizing a person opens the door and displays a greeting with the person's name, and in case of not recognizing the person, leaves the door closed. If the person not authorized to enter tries to do so, his image is sent as a security measure to an email. In its implementation, they used a standard USB camera, a Raspberry Pi, and a stepper motor. The system also works in real-time. They used the Labeled Faces in the Wild Database (LFW). In their work, they mention that they had good results, although emphasizing that new face recognition algorithms can be implemented to improve detection.

Several papers have used fingerprint door locking [69–71], noting that this method provides the highest security seen. These systems have used Arduino and wireless microcontrollers, webcam for surveillance, fingerprint sensor for door locking, PIR sensors for motion detection, GSM modem and, a buzzer and lights as warning methods.

As seen so far, there are several Android applications built that provide the necessary security, however, it is noted in [37] that the overall functioning is quite dependent on these applications. To solve this, the design of an access control system with two security methods is proposed. 1) Through a fingerprint, access to the application on the phone is secured, and in cases where it is lost or stolen, the user can change the method of access to the use of a password on a web page. 2) The system performs the matching verification of the IMEI number given in the user registration process. In the shown results of their work, a good performance is observed, moreover, it is a system that integrates several features and eliminates the dependence on an application. The disadvantage present in this system is the lack of a camera for surveillance, which also allows the capture of important information.

In [72], Kamelia et al. implemented a system based on Bluetooth, Android, and Arduino. A design was made to simulate an electronic key controlled by Bluetooth via the phone. Their design turns out to be simple and inexpensive due to the use of open-source technologies.

In 2016, with the work done by Kassem et al. [73], a smart door lock providing security via WiFi was proposed. This system is developed to improve the control of complexes with multiple apartments, and even when an owner has many keys (apartment, car, etc.). The system is embedded in the Local Area Network (LAN), the functionality of the system has been implemented by generating digital keys with the user's phone, which is used as the authentication method to

validate the legitimacy of the identity. To enhance security, several layers of security are included: 1) keys are continuously updated, 2) wired connection, 3) LAN security, and 4) phone encryption. An additional security method was added to be able to deactivate the keys of a stolen (or lost) cell phone. This multi-location, multi-door solution approach, not seen in previous studies, is innovative, secure, useful, and easy to implement. It is only noticeable that in their design they did not add functions for intrusion detection and subsequent alarm or notification production.

So far, is observed that the trend in research has been to improve the creation of new approaches and autonomous and intelligent systems for people access control, leaving aside vehicular access control. In [29] y [15], systems based on the use of RFID technology are proposed to implement methods of access for cargo trucks and access to a university campus.

For fueling stations or fuel terminals, a client-server system was implemented, in which each client (fueling station) has an RFID reader at the entrance. When a truck with an RFID tag approaches, its ID is obtained and sent to the server where it is compared in the database to see if it is registered, after which the vehicle is allowed to pass. The system showed very good results in terms of speed of communication, identification, and security.

Unlike the previous study where the entry and exit of trucks are always for those registered, in the situation presented in the university campuses it is found that there is a large flow of people belonging to the educational community (who visit the campus daily), and people who arrive at certain times (unregistered people). The system proposed in [15] was implemented in a case study conducted at the Women's University. Two ways of entry are proposed, but a first step registration must be performed, a procedure in which the license plate of the vehicle is entered and compared with those registered with the local entity in charge of vehicle control. Once the registration is completed, the vehicles can be entered, and here there are two ways; the first, for those belonging to the campus, work in the same way as the previous system. The second method of entry, available for vehicles or persons not belonging to the campus, consists in the completion of the registration, then employing IP cameras surveillance and monitoring of these vehicles is performed to provide greater security. This dual access method has proven to be very effective for vehicle access control.

The literature review of the different studies and documents revealed many systems that have been created in recent years, all of them with a varied use in IoT devices and technologies, which depends largely on the purpose, approach, and particular protection needs, for example, if a design is needed for access control or perimeter security. However, similarities have been found both at the general and particular level in the categories, of the elements (sensors, actuators, controllers) used. Thus, a compendium of the different types of IoT devices and technologies used in PSS is presented in Table 2 below.

3.2. Components for a complete IoT-based PSS solution

Based on the review of the various sources of the information shown and taking into account different conditions about the different devices and technologies (such as their advantages and disadvantages), as well as the ease and economy of implementation, a general component diagram (Figure 2) was made in UML notation, which integrates the two categories of subsystems, thus providing a complete IoT-based PSS solution.

The diagram shows the general components for the processing unit, storage, perimeter security

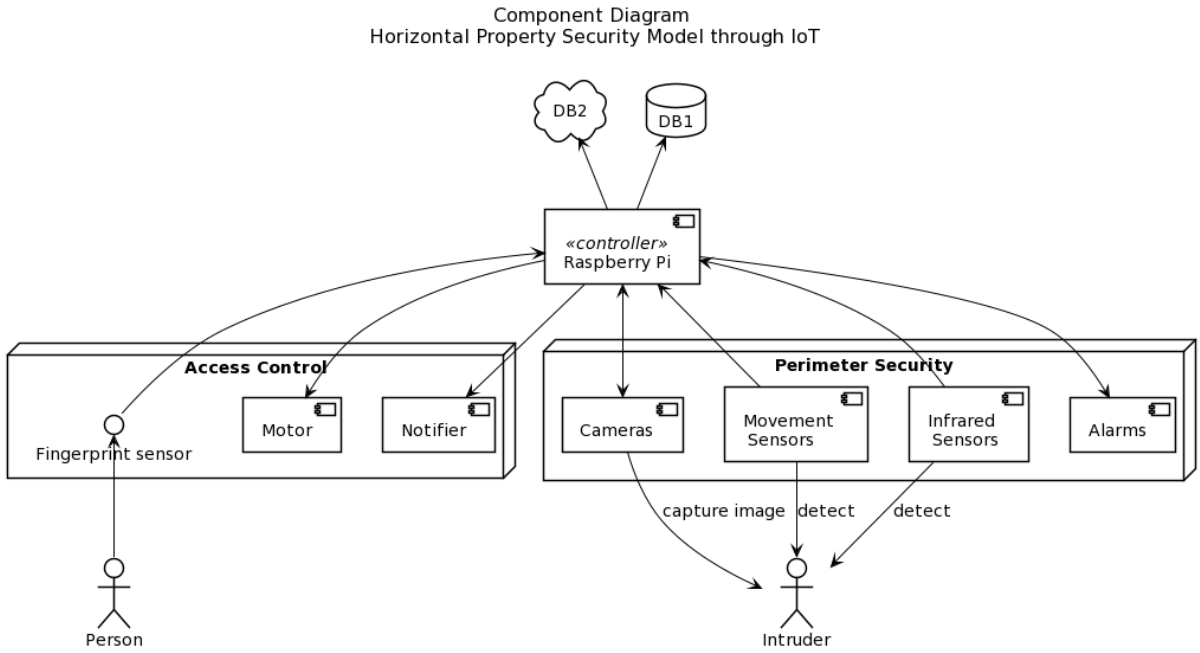

Figure 2. *General component diagram for a complete IoT-based PSS solution. Source: Own elaboration*

subsystem, and access control subsystem. The model presented is kept simple, seeking to be a basis or reference for the specific addition of more (or fewer) devices, based on the particular needs of a required solution. This is because the elements that can be included in a system for a home, residential complex, building, office, etc., vary due to adverse terrain conditions, budget, and other possible requirements.

In the controller component, a Raspberry Pi has been designated as the representation, since it is the most used among the different studies analyzed. However, it should be noted that different devices can go here, being only one or more to increase the overall processing capabilities.

The databases shown in the diagram make up the storage component of the system. There is both a local DB (Database) and one in the cloud, seeking that they can provide different services, such as visualization of the conditions or status of the protected site, notifications, possibility to change the access method, among others. On the other hand, as mentioned in one of the studies; IoT devices produce a large amount of data (Big Data) and, therefore, it is necessary to provide ways to manage them, thus, the DB in the cloud helps the information to maintain backup and in turn to the local DB is not filled, affecting the operation of the system.

It is important to note that the devices themselves can integrate databases, thus increasing the space. For example, one of the works cited mentions the inclusion of a fingerprint sensor with a biometric database.

In the node representing the perimeter security subsystem, the following components were included: cameras for image/video capture or to include recognition functions, sensors for motion detection and infrared for people detection, and an alarm component for specific situations. To make it an economical solution, the inclusion of an electric fence was discarded, and the alarm was provided as a warning mechanism.

For the access control system node, the following components are provided: a fingerprint sensor as an authentication method, an engine for opening

and closing the door, and an event notification component (such as sending e-mails or SMS). The use of fingerprint authentication is chosen because it is a method that proves to be very secure and efficient, unlike facial recognition which, despite extending new capabilities (such as differentiating between people and animals), is more difficult to achieve a high accuracy rate. It is also noteworthy that devices enabled for vehicular access control are not included.

4. Conclusions and future work

In this research it was possible to carry out a systematic review of the literature, gathering and analyzing 10 different articles that proposed new methods, approaches, and systems for the physical security of properties, such as houses, banks, offices, buildings, among others. And later, thanks to the references of these it was possible to execute in a second phase a systematic mapping with which it was possible to analyze 40 more studies, thus covering a wider time frame and breadth of PSS based on IoT.

A theoretical approach was made to the structure of the PSS, showing the different components that can be found, such as the surveillance subsystem, 24/7 monitoring subsystem (CCTV), alarm subsystem, notification subsystem, access control subsystem and communication subsystem. In addition, grouping the above into categories for a perimeter security subsystem, and an access control subsystem. For these two groups (the communication subsystem has not been investigated) it was possible to observe different proposals, showing the advances, preferences, and future trends in the field in question.

Finally, with the information gathered on the proposed systems together with their advantages and disadvantages, and other considerations, a table was constructed showing the compendium of devices and technologies most used for the design of these security solutions, explaining their different functions and advantages. In addition, a basic component diagram model was created, which represents the integration of the two groups of subsystems discussed, and which is intended to be useful and/or a basis for future implementations of other systems, since it allows visualizing important considerations related to the security needs to be covered, considering the possible devices, technologies, ease of implementation and cost for the desired solution.

On the other hand, it should be noted that the above-mentioned important considerations will be taken as future work, being a basis in the definition of the devices and technologies to be included in the development of a PSS for residential complexes, which will be implemented later within the execution of the innovation project that gives rise to this work.

Also, considering the wide use of video surveillance systems capable of capturing photos, and that IoT devices have low computational and storage capacity, it is proposed to search for and test methods or algorithms to improve the efficiency of data transmission within the IoT architecture of this type of systems.

5. Acknowledgments and funding statement

The present work was financed as part of the technological development project included in the call to proposals of Minciencias "851-2019 CONVOCATORIA LÍNEA DE FOMENTO A LA INNOVACIÓN Y DESARROLLO TECNOLÓGICO EN LAS EMPRESAS".

6. References

(1) alarms.org. Burglary Statistics: The Hard Numbers | National Council for Home Safety and Security [Internet]. 2019 [cited 2020 sep 9]. Available from:

https://www.alarms.org/burglary-statistics/.

(2) Girme GS, Patil SandipR. Internet of Things Based Intelligent Security using Android Application. In: 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT). Tirunelveli, India: IEEE; 2019 [cited 2020 sep 9]. p. 1101–5. https://doi.org/10.1109/ICSSIT46314.2019.8987847.

(3) Venkatesan S, Jawahar A, Varsha S, Roshne N. Design and implementation of an automated security system using Twilio messaging service. In: 2017 International Conference on Smart Cities, Automation Intelligent Computing Systems (ICON-SONICS). Yogyakarta; 2017. p. 59–63. https://doi.org/10.1109/ICON-SONICS.2017.8267822.

(4) Miettinen M, Marchal S, Hafeez I, Asokan N, Sadeghi A-R, Tarkoma S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). Atlanta, GA; 2017. p. 2177–84. https://doi.org/10.1109/ICDCS.2017.283.

(5) Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering. Keele University and Durham University Joint Report; 2007 jul [cited 2021 may 21]. Report No.: EBSE 2007-001. Available from: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

(6) Carrizo D, Moller C. Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático. Ingeniare Revista chilena de ingeniería. 2018;26(1):45-4. http://dx.doi.org/10.4067/S0718-33052018000500045.

(7) Madakam S, Ramaswamy R, Tripathi S. Internet of Things (IoT): A Literature Review. J Comput Commun. 2015; 3(5):164–73. http://dx.doi.org/10.4236/jcc.2015.35021.

(8) Fuentes Lanfor OG, Pérez Pérez JF. Implementación de un sistema de seguridad independiente y automatización de una residencia por medio del internet de las cosas. In: 2017 IEEE Central America and Panama Student Conference (CONESCAPAN). Panama City; 2017. p. 1–5. https://www.doi.org/10.1109/CONESCAPAN.2017.8277600.

(9) Greengard S. The Internet of Things. Cambridge, Massachusetts: The MIT Press; 2015. 232 p. (MIT Press Essential Knowledge series).

(10) Slama D, Puhlmann F, Morrish J, Bhatnagar RM. Enterprise IoT: Strategies and Best Practices for Connected Products and Services. 1ra ed. Beijing; Boston: O'Reilly Media; 2015. 492 p.

(11) Whitmore A, Agarwal A, Xu L. The Internet of Things—A survey of topics and trends. Inf Syst Front. 2015;17:261–74. https://doi.org/10.1007/s10796-014-9489-2.

(12) Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of Things for Smart Cities. IEEE Internet Things J. febrero de 2014;1(1):22–32.

https://doi.org/10.1109/JIOT.2014.2306328.

(13) Mattern F, Floerkemeier C. From the Internet of Computers to the Internet of Things. En: Sachs K, Petrov I, Guerrero P, editores. From Active Data Management to Event-Based Systems and More: Papers in Honor of Alejandro Buchmann on the Occasion of His 60th Birthday. Berlin, Heidelberg: Springer; 2010 [cited 2020 sep 11]. p. 242–59. (Lecture Notes in Computer Science). https://doi.org/10.1007/978-3-642-17226-7_15.

(14) Li T, Chen L. Internet of Things: Principle, Framework and Application. En: Zhang Y, editor. Future Wireless Networks and Information Systems. Berlin, Heidelberg: Springer; 2012. p. 477–82. (Lecture Notes in Electrical Engineering; vol. 144). https://doi.org/10.1007/978-3-642-27326-1_61.

(15) Singh V, Kharat V. A Proposed System for Security in Campuses using IoT Platform: A Case Study of A Women's University. En: 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). Mysore: IEEE; 2017. p. 305–10. https://www.doi.org/10.1109/CTCEEC.2017.8455076.

(16) El-Mougy A, Ibnkahla M, Hegazy L. Software-defined wireless network architectures for the Internet-of-Things. En: 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops). Clearwater Beach, FL; 2015. p. 804–11. https://www.doi.org/10.1109/LCNW.2015.7365931.

(17) Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Comput Netw [Internet]. 28 de octubre de 2010 [cited 2020 sep 11];54(15):2787–805. https://doi.org/10.1016/j.comnet.2010.05.010.

(18) Calabrese F, Colonna M, Lovisolo P, Parata D, Ratti C. Real-Time Urban Monitoring Using Cell Phones: A Case Study in Rome. IEEE Trans Intell Transp Syst. 2011;12(1):141–51. https://www.doi.org/10.1109/TITS.2010.2074196.

(19) Sevincer A, Bhattarai A, Bilgi M, Yuksel M, Pala N. LIGHTNETs: Smart LIGHTing and Mobile Optical Wireless NETworks — A Survey. IEEE Commun Surv Tutor. 2013;15(4):1620–41. https://www.doi.org/10.1109/SURV.2013.032713.00150.

(20) Khatoun R, Zeadally S. Smart cities: concepts, architectures, research opportunities. Commun ACM. 2016;59(8):46–57. https://doi.org/10.1145/2858789.

(21) Rashidi P, Cook DJ, Holder LB, Schmitter-Edgecombe M. Discovering Activities to Recognize and Track in a Smart Environment. IEEE Trans Knowl Data Eng. 2011;23(4):527–39. https://www.doi.org/10.1109/TKDE.2010.148.

(22) Habibzadeh M, Xiong W, Zheleva M, Stern EK, Nussbaum BH, Soyata T. Smart city sensing and communication sub-infrastructure. En: 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). Boston, MA; 2017. p. 1159–62.

https://www.doi.org/10.1109/MWSCAS.2017.8053134.

(23) Waleed A-KA, Kharchenko V, Uzun D, Solovyov O. IoT-based physical security systems: Structures and PSMECA analysis. En: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Bucharest; 2017. p. 870–3. https://www.doi.org/10.1109/IDAACS.2017.8095211.

(24) Sassani BA, David A, Li X, Mehdipour F. AgentPi: An IoT Enabled Motion CCTV Surveillance System. En: 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). Fukuoka, Japan; 2019. p. 454–8. https://www.doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00092.

(25) Kumar J, Ramesh PR. Low-Cost Energy Efficient Smart Security System with Information Stamping for IoT Networks. En: 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU). Bhimtal; 2018. p. 1–5. https://www.doi.org/10.1109/IoT-SIU.2018.8519875.

(26) Reisslein M, Rinner B, Roy-Chowdhury A. Smart Camera Networks [Guest editors' introduction]. Computer. 2014;47(5):23–5. https://www.doi.org/10.1109/MC.2014.134.

(27) Winkler T, Rinner B. Security and Privacy Protection in Visual Sensor Networks: A Survey. ACM Comput Surv. 2014;47(1):1-42. https://doi.org/10.1145/2545883.

(28) Fernandes E, Jung J, Prakash A. Security Analysis of Emerging Smart Home Applications. En: 2016 IEEE Symposium on Security and Privacy (SP). San Jose, CA; 2016. p. 636–54. https://www.doi.org/10.1109/SP.2016.44.

(29) Bahgat MM, Farag HH, Mokhtar B. IoT-Based Online Access Control System for Vehicles in Truck-Loading Fuels Terminals. En: 2018 30th International Conference on Microelectronics (ICM). Sousse, Tunisia: IEEE; 2018. p. 1–4. https://www.doi.org/10.1109/ICM.2018.8704087.

(30) Zurawski R, editor. Industrial Communication Technology Handbook. 2ª ed. CRC Press; 2014. 1564 p. (Industrial Information Technology).

(31) Reynders D, Mackay S, Wright E, Mackay S. Practical Industrial Data Communications: Best Practice Techniques. Elsevier; 2004 [cited 2020 sep 17]. 432 p. Available from: https://doi.org/10.1016/B978-0-7506-6395-3.X5000-1.

(32) Stallings W. Data and Computer Communications. 7ª ed. Upper Saddle River, N.J: Prentice Hall; 2003. 864 p.

(33) Khattab A, Jeddi Z, Amini E, Bayoumi M. RFID Security: A Lightweight Paradigm [Internet]. 1ª ed. Springer International Publishing; 2017 [cited 2020 sep 17] 171 p. (Analog Circuits and Signal Processing). Available from: https://doi.org/10.1007/978-3-319-47545-5.

(34) Chandra P, Bensky D, Bradley T, Hurley C, Rackley SA, CISM JRP, et al. Wireless Security: Know It All. Amsterdam; Boston: Newnes; 2008. 744 p.

(35) Prarthana RJ, Dhanzil AM, Mahesh NI, Raghul S. An Automated Garage Door and Security Management System (A dual control system with VPN IoT & Biometric Database). In: 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). Coimbatore: IEEE; 2018. p. 1468–72. https://www.doi.org/10.1109/ICECA.2018.8474630.

(36) ALshukri D, R VL, P SE, Krishnan P. Intelligent Border Security Intrusion Detection using IoT and Embedded systems. In: 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC). Muscat, Oman: IEEE; 2019. p. 1–3. https://www.doi.org/10.1109/ICBDSC.2019.8645587.

(37) Deepty RR, Alam A, Islam MdE. IoT and Wi-Fi Based Door Access Control System using Mobile Application. In: 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON). Dhaka, Bangladesh: IEEE; 2019. p. 21–4. https://www.doi.org/10.1109/RAAICON48939.2019.09.

(38) Jain S, Jatain A, Bhaskar S. Smart City Management System using IoT with Deep Learning. In: 2019 International Conference on Communication and Electronics Systems (ICCES). Coimbatore, India: IEEE; 2019. p. 1214–22. https://www.doi.org/10.1109/ICCES45898.2019.9002414.

(39) Alex AM, Jose ME, Rinsily KS, Bosco S, Shaji S. Android based intelligent robot for border security. Int Res J Eng Technol. 2017;4(4):2041–3. https://www.irjet.net/archives/V4/i4/IRJET-V4I4526.pdf.

(40) Kumar CN, Ramesh B, Shivakumar G, Manjunath JR. Android Based Autonomous Intelligent Robot for Border Security. Int J Innov Sci Eng Technol. 2014;1(5):544–8. http://ijiset.com/v1s5/IJISET_V1_I5_81.pdf.

(41) Prajakta S. J, Honrao SB. Advance Border Security Using Android Application. Int J Adv Res Innov Ideas Educ IJARIIE. 2016;2(3):3458–65. http://ijariie.com/AdminUploadPdf/Advance_Border_Security_Using_Android_Application_ijariie2615.pdf.

(42) Thilagavathy R, Murali J, Kamal P, Arunpandiyan P. Intelligent Unmanned Army Robot. Int J Adv Res Comput Eng Technol [Internet]. 2015;4(2):473–7. Available from: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-4-ISSUE-2-473-477.pdf.

(43) Sudhakar S, Kumar EP, Thiyagarajan S. Border Security and Multi Access Robot using Embedded System. Indian J Sci Technol [Internet]. 2016 [cited 2020 sep 25];9(16):1–5. https://www.doi.org/10.17485/ijst/2016/v9i16/92205.

(44) Jain K, Suluchana V. Design and Development of Smart Robot Car for Border Security. Int J Comput Appl. 2013;76(7):23–9. https://doi.org/10.5120/13260-0739.

(45) Fang L, Meng Z, Chen C, Hui Q. Smart Motion Detection Surveillance System. In: 2009 International Conference on Education Technology and Computer. Singapore: IEEE; 2009. p. 171–5. https://www.doi.org/10.1109/ICETC.2009.10.

(46) Khan AA, Iqbal M. A Motion Detection Based Surveillance System (MDSS). In: 2011 First International Conference on Informatics and Computational Intelligence. Bandung; 2011. p. 132–7. https://www.doi.org/10.1109/ICI.2011.31.

(47) Prasad S, Mahalakshmi P, Sunder AJC, Swathi R. Smart Surveillance Monitoring System Using Raspberry PI and PIR Sensor. Int J Comput Sci Inf Technol. 2014;5(6):7107–9. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.658.6805&rep=rep1&type=pdf.

(48) Twilio. What is Twilio and How Do Twilio APIs Work? [Internet]. (s.f). Available from: https://www.twilio.com/learn/twilio-101/what-is-twilio/.

(49) Bhatkule AV, Shinde UB, Zanwar SR. Home Based Security Control System using Raspberry Pi and GSM. Int J Innov Res Comput Commun Eng. 2016;4(9):16259–64. Available from: http://www.ijircce.com/upload/2016/september/83_9_Home.pdf.

(50) Choudhury B, Choudhury TS, Pramanik A, Arif W, Mehedi J. Design and implementation of an SMS based home security system. In: 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). Coimbatore: IEEE; 2015. p. 1–7. https://www.doi.org/10.1109/ICECCT.2015.7226115.

(51) Peng Z, Kato T, Takahashi H, Kinoshita T. Intelligent home security system using agent-based IoT devices. In: 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). Osaka: IEEE; 2015. p. 313–4. https://www.doi.org/10.1109/GCCE.2015.7398644.

(52) Huang H, Xiao S, Meng X, Xiong Y. A Remote Home Security System Based on Wireless Sensor Network and GSM Technology. In: 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. Wuhan, Hubei: IEEE; 2010. p. 535–8. https://doi.org/10.1109/NSWCTC.2010.132

(53) Sriskanthan N, Tan F, Karande A. Bluetooth based home automation system. Microprocess Microsyst. 2002; 26 (6):281–9. https://doi.org/10.1016/S0141-9331(02)00039-X.

(54) Kodali RK, Jain V, Bose S, Boppana L. IoT based smart security and home automation system. In: 2016 International Conference on Computing, Communication and Automation (ICCCA) [Internet]. Greater Noida, India: IEEE; 2016 [citado 25 de septiembre de 2020]. p. 1286–9. https://www.doi.org/10.1109/CCAA.2016.7813916.

(55) Oliver A, Odena A, Raffel CA, Cubuk ED, Goodfellow I. Realistic evaluation of deep semi-supervised learning algorithms. In: 32nd Conference on Neural Information Processing Systems (NeurIPS 2018) [Internet]. Monteréal, Canada; 2018. p.

3235–46. Disponible en: https://dl.acm.org/doi/pdf/10.5555/3327144.3327244.

(56) Shah M, Kapdi R. Object detection using deep neural networks. In: 2017 International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai: IEEE; 2017. p. 787–90. https://www.doi.org/10.1109/ICCONS.2017.8250570.

(57) Britto J, Chaudhari V, Mehta D, Kale A, Ramteke J. A Sixth Sense Door using Internet of Things. En: Smys S, Bestak R, Chen JI-Z, Kotuliak I, editores. International Conference on Computer Networks and Communication Technologies. Singapore: Springer; 2019. p. 545–55. (Lecture Notes on Data Engineering and Communications Technologies). https://doi.org/10.1007/978-981-10-8681-6_49.

(58) Chitnis S, Deshpande N, Shaligram A. An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. Wirel Sens Netw. 2016;8(4):61–8. http://dx.doi.org/10.4236/wsn.2016.84006.

(59) Lee A, Tyroler D, Chen H-J, Yuk H. Home automation system monitored by security system [Internet]. US9368009B2; 2016 [cited 2020 sep 25]. Disponible en: https://patents.google.com/patent/US9368009/en.

(60) Surantha N, Wicaksono WR. Design of Smart Home Security System using Object Recognition and PIR Sensor. Procedia Comput Sci [Internet]. 2018 [cited 2020 sep 25];135:465–72. https://doi.org/10.1016/j.procs.2018.08.198.

(61) Asnani H, Khan S, Nandeesh S. Securing an IoT based Home using Digital Image Processing and an Android Application. Int Res J Eng Technol [Internet]. 2018;5(8):410–5. Available from: https://www.irjet.net/archives/V5/i8/IRJET-V5I872.pdf.

(62) Hung C-H, Bai Y-W, Ren J-H. Design and implementation of a single button operation for a door lock control system based on a near field communication of a smartphone. In: 2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin). Berlin: IEEE; 2015. p. 260–1. https://www.doi.org/10.1109/ICCE-Berlin.2015.7391251.

(63) Ibrahim A, Paravath A, Aswin PK, Iqbal SM, Abdulla SU. GSM based digital door lock security system. In: 2015 International Conference on Power, Instrumentation, Control and Computing (PICC). Thrissur: IEEE; 2015. p. 1–6. https://www.doi.org/10.1109/PICC.2015.7455796.

(64) Khan SR, Al Mansur A, Kabir A, Jaman S, Chowdhury N. Design and implementation of low cost home security system using GSM network. Int J Sci Eng Res [Internet]. 2012;3(3):1–6. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.302.6908&rep=rep1&type=pdf.

(65) Ragade RR. Embedded home surveillance system with pyroelectric infrared sensor using GSM. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM).

Aurangabad: IEEE; 2017. p. 321–4. https://www.doi.org/10.1109/ICISIM.2017.8122192.

(66) Kale PV, Sharma DD. Intelligent Home Security System using illumination sensitive background model. Int J Adv Eng Ing Res Dev. 2014;1(5):1–11. https://doi.org/10.21090/ijaerd.0105105.

(67) Gupta RK, Balamurugan S, Nbsp KA and RM. IoT Based Door Entry System. Indian J Sci Technol. 6 de mayo de 2016;9(37):1–5. https://dx.doi.org/10.17485/ijst/2016/v9i37/102136.

(68) Kulkarni S, Bagul M, Dukare A, Gaikwad A. Face Recognition System Using IoT. Int J Adv Res Comput Eng Technol [Internet]. 2017;6(11):1720–3. Available from: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-6-ISSUE-11-1720-1723.pdf.

(69) Zaman HasanU, Tabassum TE, Islam T, Mohammad N. Low-cost multi-level home security system for developing countries. In: 2017 International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai: IEEE; 2017. p. 549–54. https://www.doi.org/10.1109/ICCONS.2017.8250522.

(70) Sarika CG, Bharathi Malakreddy A, Harinath HN. IoT-Based Smart Login Using Biometrics. En: Smys S, Bestak R, Chen JI-Z, Kotuliak I, editores. International Conference on Computer Networks and Communication Technologies. Singapore: Springer; 2019. p. 589–97. (Lecture Notes on Data Engineering and Communications Technologies). https://doi.org/10.1007/978-981-10-8681-6_54.

(71) Loong Pang K, Seng Teh H. Mobile-Based access control system with wireless access controller [Internet]. US 2019 318 559A1; 2019 [cited 2020 sep 25]. Available from: https://patentswarm.com/patents/US20190318559A1.

(72) Kamelia L, Noorhassan A, Sanjaya M, Mulyana WSE. Door Automation System Using Bluetooth-Based Android for Mobile Phone. ARPN J Eng Appl Sci [Internet]. 2014;9(10):1759–62. Available from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1045.7192&rep=rep1&type=pdf.

(73) Kassem A, Murr SE, Jamous G, Saad E, Geagea M. A smart lock system using Wi-Fi security. In: 2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA). Beirut: IEEE; 2016. p. 222–5. https://www.doi.org/10.1109/ACTEA.2016.7560143.