International Journal of Latest Research in Humanities and Social Science (IJLRHSS)
Volume 06 - Issue 12, 2023
www.ijlrhss.com || PP. 153-160

Smart Home Security: A Security System Built on the Internet of Things – IoT

Kelson Carvalho Santos[1,2], Wesley da Silva Guimarães[2],
João Carlos Gonçalves[2]

[1]*Computing Department, Federal Institute of Piaui (IFPI),*
Av. Pedro Freitas, 1020, Sao Pedro, Teresina, 64018-000, PI, Brazil.
[2]*Faculty of Computring (FACOM), Federal University of Uberlandia (UFU),*
Av Joao Naves de Avila, 2121, Santa Monica, Uberlandia, 38408-100, MG, Brazil.

Abstract: The Internet of Things (IoT) encompasses new concepts and technologies that enable the realization of a connected real-life environment where "intelligent things" interact without human intervention. This technology finds applications in various sectors, including health, agriculture, industry, and urban lighting. This study focuses on implementing IoT in residential security by developing an integrated hardware and software system. The primary purpose of this system is to enable users to monitor their residences remotely, whether from short or long distances, using a mobile device. The proposed application is designed to be a cost-effective residential security solution. It operates by issuing smartphone alerts when any movement is detected within the sensor coverage area, allowing real-time monitoring of the residence's interior through images. The tests conducted have demonstrated that the developed application successfully fulfills the objectives outlined in this study. It serves as an additional resource in the evolving field of IoT, which, despite being in its early stages, needs more practical applications that implement the concepts discussed in the literature.

Keywords: Cybersecurity, Internet of Things, IoT, Smart Home.

1. Introduction

In recent years, the proliferation of Internet connections has led to the emergence of various concepts within the virtual ecosystem. A notable aspect is the connectivity of "things," such as houses, cars, refrigerators, and watches, among others, to the network, enabling them to exchange data. This phenomenon is encapsulated in the Internet of Things (IoT) [1].]

The Internet of Things has had far-reaching impacts across multiple sectors. It has introduced possibilities for enhanced productivity and better data capture for strategic decision-making in the industry. The medicine allows real-time patient monitoring from any location, revolutionizing disease treatments by expanding diagnostic capabilities beyond signs observed by professionals and symptoms reported by patients. IoT holds significant potential in education, agriculture, public lighting, urban mobility, and other domains [2] [3].

Aligned with the IoT concept, homes are transformed into intelligent entities (Smart Homes) capable of autonomously performing diverse actions, promoting increased comfort and safety for residents. These environments are equipped with temperature, light, fire sensors, and various devices that exchange data to operate intelligently [4].

The rising home invasions highlight the need for technologies to ensure greater security, whether residents are present or not. Incidents of this nature can lead to material damage and jeopardize lives. Thus, there is a fundamental need to develop technologies to augment home security, given that existing resources fall short of guaranteeing security in these environments.

In this context, this work introduces an integrated hardware and software system to enable users to monitor their homes in real-time from any location. Unlike current residential security solutions, our proposed application stands out for its cost-effectiveness and adherence to the Internet of Things concept. Additionally, this work aims to contribute to expanding resources in the Internet of Things universe, particularly in the realm of Smart Homes.

2. Related Work

A considerable body of work has delved into various aspects of home automation, with a notable increase following the advent of prototyping boards that streamline project development. This section highlights relevant works related to the presented proposal.

In [5], a Smart Wireless Home security system was devised to dispatch alerts to the homeowner through the installed device via the Internet in case of an intrusion, optionally triggering an alarm. What distinguishes

this proposal is the system's ability to forward alerts to the user's phone from any distance, irrespective of internet connectivity. [6] introduces an IoT system for monitoring and controlling home appliances via the Internet. The home automation system utilizes a smartphone as the user interface, establishing communication with home appliances through an Internet gateway using a low-power communication protocol such as Zigbee, with a Raspberry Pi serving as the server. Notably, the system includes a feature to monitor fireplace smoke levels, issuing alerts in case of a presumed fire.

The architecture presented in [7] focuses on a smart door sensor that notifies the user of events when a door is opened in a home or office environment facilitated by a smartphone application. This proposed architecture involves an Arduino-compatible Elegoo Mega 2560 microcontroller board (MCU) and a Raspberry Pi board, communicating with a web server implementing a RESTful API.

[11] proposes a perspective on the development of new resources as a means to establish an Internet of Things environment. The research outlines the phases of IoT development, incorporating RFID, smart sensors, communication technologies, and internet protocols, with Machine-to-Machine (M2M) technology identified as the initial step toward achieving a connected environment. The study provides a comprehensive view of IoT technologies, encompassing technical details and diverse applications contributing to new technologies for decision-making and various scenarios, emphasizing the pivotal role of IoT in the current landscape.

In [12], the authors detail implementing a home security system with human detection capabilities. The application aims to transcend simple monitoring by incorporating a presence sensor (PIR). When movement is detected, the camera activates, capturing an image subjected to Gradient Histogram (HoG) and Support Vector Machine (SVM) analysis to identify the captured element. If Machine Learning (ML) techniques recognize patterns indicative of a human being, an alert is sent to the homeowner's mobile device. The authors report an achieved accuracy rate of 89%.

These cited works demonstrate the practicality of the developed applications, contributing significantly to home and resident safety and advancing technologies for Smart Homes and the broader Internet of Things.

3. Material and Methods

This work progressed through the following five steps, as illustrated in Figure 1.

Firstly, we conducted a requirements survey outlining the scope and methodology, accompanied by a comprehensive literature review. The second stage involved specifying the necessary resources and components, detailing the tools and materials acquired for constructing the system presented in this study. The third stage marked the actual development of the residential security solution.

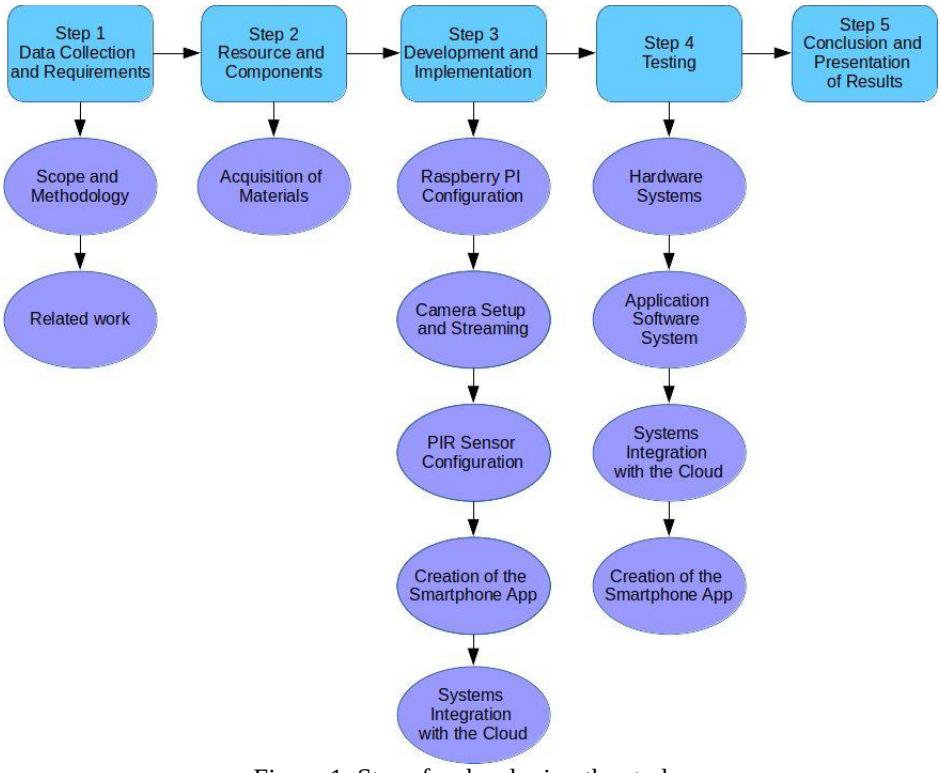


Figure 1: Steps for developing the study.

Moving on to the fourth stage, we performed comprehensive tests to assess the entire system's functionality and analyze each component's behavior. In the fifth and final stage, we present the conclusions and results outlined in this text.

The development and implementation discussed in the third step of the figure above are elaborated in two modules: one focusing on the hardware implemented in the home and the other on the application software installed on the user's smartphone. This is illustrated by the architecture depicted in Figure 2.

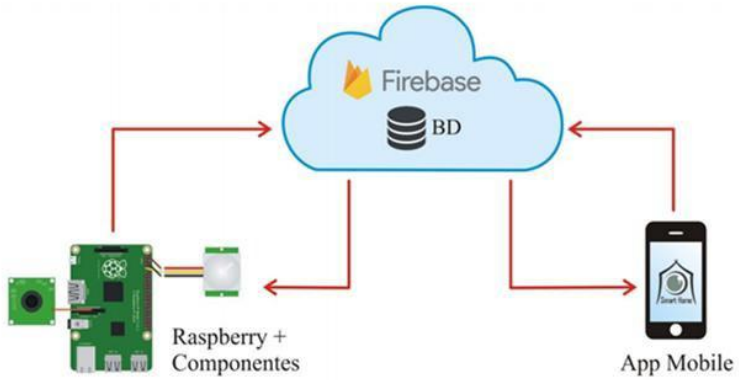


Figure 2: Modular architecture for experiments.

3.1 Hardware

The implemented integrated hardware system demonstrated a relatively low cost compared to traditional residential security systems. It is crucial to note that these cost estimates may vary, influenced by several factors, mainly as specific components are not domestically produced in Brazil and necessitate importation from other countries.

The single-board computer chosen for this project was the Raspberry Pi 3 Model B+. This device plays a pivotal role in receiving events from the motion sensor and images from the camera, subsequently transmitting this data to a cloud database. The Raspberry Pi, utilizing embedded software, also checks the database to determine if the user, via the smartphone application, has activated the motion sensor. Upon detecting movement, the sensor dispatches an alert to the board when enabled. Upon receipt of the alert, the board activates the camera, captures images, and forwards the records to the cloud database, which then triggers an alert on the user's mobile device.

Data communication within the integrated hardware system was achieved through the Python 3 programming language, facilitating the system's autonomous operation. User interaction is limited to activating the sensor for image recording and alert generation, with data transmission utilizing JSON (JavaScript Object Notation).

Figure 3 illustrates the interconnected hardware during the implementation and testing phase.

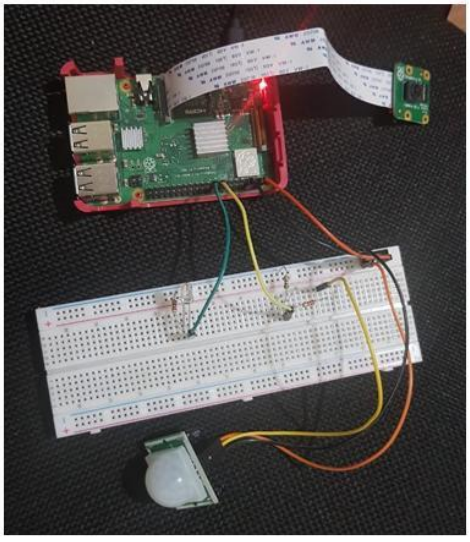


Figure 3: Hardware module.

3.2 Software

This module includes the Smart Home application, developed for the Android Operating System (OS) from version 4.0 onwards. For creation, we used the IDE (Integrated Development Environment) Android Studio with the use of XML (Extensible Markup Language) [8] and Java programming language [9]. ADT (Android Development Tools) plugins in Android Studio were used during simulation tests

The application performs queries and sends data to the Firebase platform [10]. Firebase receives information from the integrated hardware system. It sends it to the application using JSON, where the data is interpreted and visualized on the smartphone that serves as the user interface.

To detail how the application works, the requirements for good user interaction are below.

In Figure 4, we can see the login and main menu screens. The login screen is the beginning of the system that allows access to the enabled user. After being logged in, the user sees the main menu, where four options are available: access to camera images, the motion sensor, alerts, and project credit information. From the main menu, it is also possible to close the application.

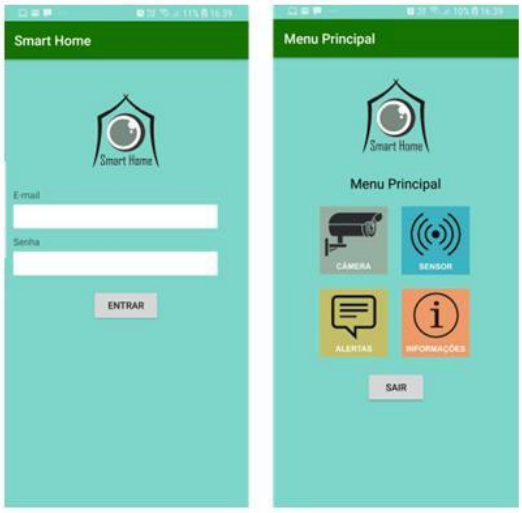


Figure 4: Software interface.

In Figure 5, we will find the camera and motion sensor options. The camera option allows access to images. It is possible to activate or deactivate the transmission of images in real-time. In the sensor option, activating or deactivating it is also possible. This option, when activated, detects the presence, and synchronously, the camera captures the images and sends them as an alert to the application installed on the user's smartphone. When deactivated, the sensor does not detect the presence, so the camera is not enabled, and alerts are not issued.

Alerts are automatically generated upon detecting movement. The integrated hardware system transmits data to the cloud, which is then relayed to the user's application. Figure 6 illustrates a code segment for managing alerts within the user's application software.

The data exchange between the integrated hardware system within the home and the application installed on the user's smartphone occurs via the Internet. This facilitates the seamless transmission of information, whether over short or long distances, aligning with the principles of the Internet of Things concept.

The integrated hardware system is Internet-enabled, allowing camera images and motion sensor alert signals to be conveyed to a cloud database (Firebase). Subsequently, this data is redirected to the user's application. Conversely, the reverse connection follows a similar process: the user initiates a request through their smartphone, which is transmitted to the integrated hardware system. The request is processed, and the corresponding response is returned to the user.

The results section presents the data collected and analyzed during the tests. The primary objective is to validate the effectiveness of the integrated monitoring system, featuring a camera and motion sensor controlled through a smartphone application.

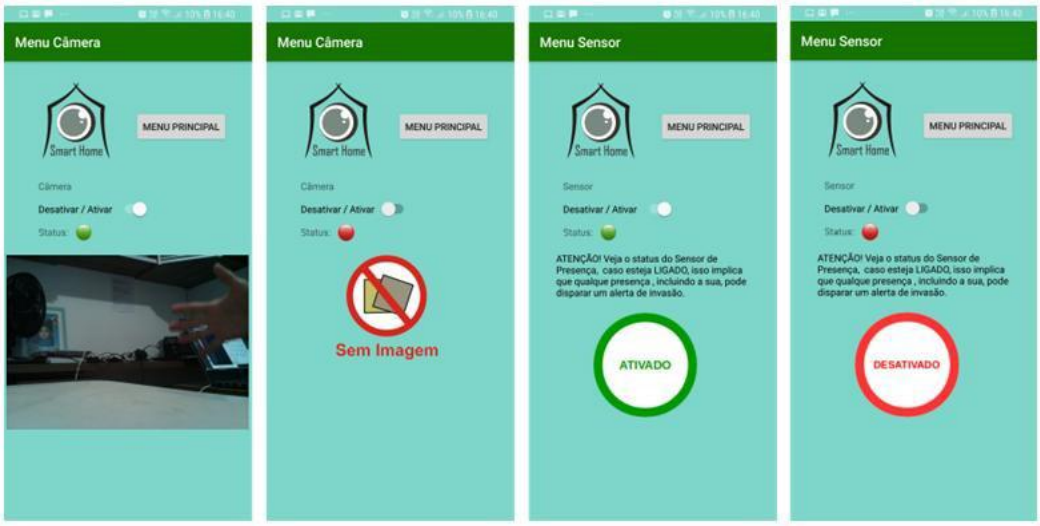


Figure 5: Interfaces with camera and sensor options.

```java
package com.kelson.smarthome;
import android.app.NotificationManager;
import android.app.PendingIntent;
import android.content.Context;
import android.content.Intent;
import android.media.RingtoneManager;
import android.net.Uri;
import android.util.Log;
import androidx.annotation.NonNull;
import androidx.core.app.NotificationCompat;
import com.google.firebase.messaging.FirebaseMessagingService;
import com.google.firebase.messaging.RemoteMessage;
public class MyFirebaseMessagingService extends FirebaseMessagingService {
    public static final String TAG = "ALERTAS";
    @Override
    public void onMessageReceived(@NonNull RemoteMessage remoteMessage) {
        super.onMessageReceived(remoteMessage);
        String from = remoteMessage.getFrom();
        Log.d(TAG, "Alerta recebido de:" + from);
        if (remoteMessage.getNotification() != null){
            Log.d(TAG, "Alerta:" + remoteMessage.getNotification().getBody());
            mostrarAlerta(remoteMessage.getNotification().getTitle(), remoteMessage.getNotification().getBody());
        }
        if (remoteMessage.getData().size() > 0){
            Log.d(TAG, "Dados: " + remoteMessage.getData());
        }
    }
    private void mostrarAlerta(String title, String body){
        Intent intent = new Intent(this, Mensagem.class);
        intent.setFlags(Intent.FLAG_ACTIVITY_CLEAR_TOP);
        PendingIntent pendingIntent = PendingIntent.getActivity(this, 0, intent, PendingIntent.FLAG_ONE_SHOT);
        Uri soundUri = RingtoneManager.getDefaultUri(RingtoneManager.TYPE_NOTIFICATION);
        NotificationCompat.Builder notificationBuilder = new   NotificationCompat.Builder(this)
                .setSmallIcon(R.drawable.on)
                .setContentTitle(title)
                .setContentText(body)
                .setAutoCancel(true)
                .setSound(soundUri)
                .setContentIntent(pendingIntent);
        NotificationManager notificationManager = (NotificationManager) getSystemService(Context.NOTIFICATION_SERVICE);
        notificationManager.notify(0, notificationBuilder.build());
    }
```

Figure 6: Code to receive alerts.

4. Results and Discussion

The system's hardware and software modules were constructed according to the planned specifications, and subsequent tests were conducted to ensure compliance with the specified requirements.

Initially, unit tests were performed on the hardware components. In Figure 7, the assembled hardware is depicted, highlighting the presence of the camera, the presence sensor, the Raspberry board, and other essential elements for the proper functioning of the application.

The ensemble of hardware described above is governed by routines executed on the Raspberry board, which is responsible for establishing connections with the cloud database. The system operates according to the anticipated requirements: the camera activates when the presence sensor detects a specific event, triggering the sensor through the application installed on the user's smartphone.

Figure 8 provides an overview of the test results conducted with the motion sensor and camera, showcasing real-time transmission of the environmental image. A snippet of the code implemented in the integrated hardware system is shown in Figure 9.

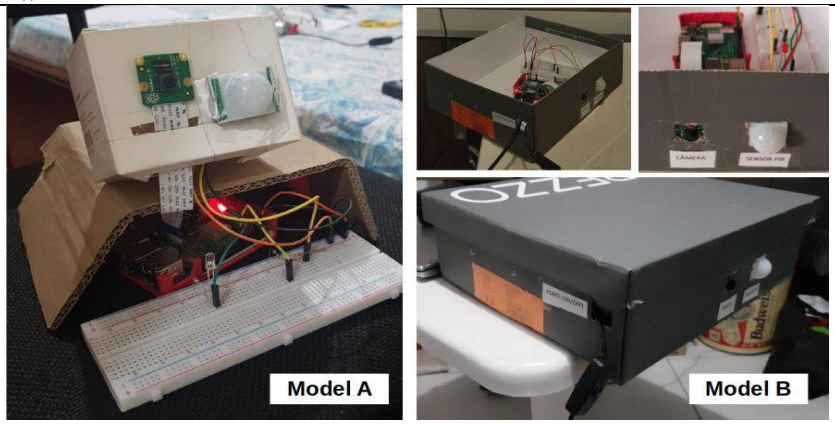
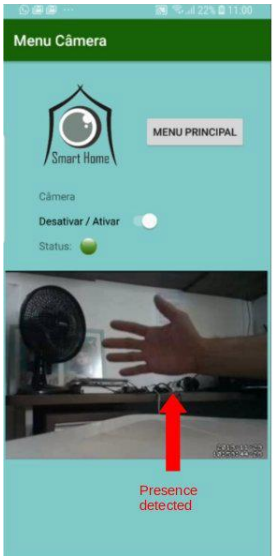
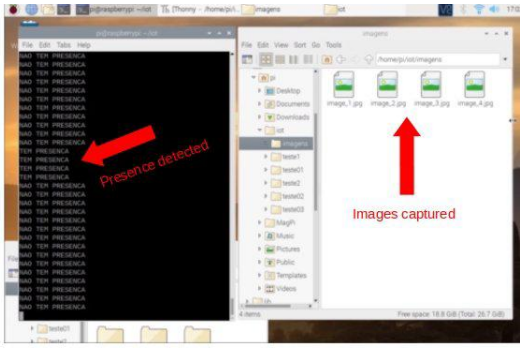


Figure 7: Hardware module prototype





Camera capturing images when presence is detected (sensor activated).

Figure 8: Presence detection images captured.

```python
from picamera import PiCamera
from time import sleep
from datetime import datetime

import RPi.GPIO as gpio
import time

gpio.setwarnings(False)
gpio.setmode(gpio.BCM)
gpio.setup(23, gpio.IN)
gpio.setup(24, gpio.OUT)

P=PiCamera()
P.resolution= (1024,768)
P.start_preview()
i = 0

while True:

    if gpio.input(23) == gpio.HIGH:
        print("TEM PRESENCA")
        gpio.output(24, gpio.HIGH)
        time.sleep(0.5)
        i = i + 1
        P.capture('/home/pi/Pictures/image_%s.jpg' % i )
    else:

        print("NAO TEM PRESENCA")
        gpio.output(24, gpio.LOW)
        time.sleep(0.01)
```

Figure 9: Code for presence detection and image capture.

In tests conducted with the camera, issues were identified during the transmission of the video stream. These complications were addressed through multiple attempts to identify an optimal frame rate to prevent any image quality loss. The configuration plugin utilized by the Raspberry board's operating system enables the definition of a transmission rate of up to 100 frames per second. This rate should be determined based on the camera's capabilities and the bandwidth the service provider provides.

The distance between the transmission system, embedded hardware and software, the cloud server, and the mobile device can negatively impact system performance. Poor quality mobile connections can particularly hinder the video transmission experience, especially when a high frame rate is established.

The PIR HC-SR501 presence sensor model, capable of detecting movements within a radius of up to 7 meters, was incorporated into the project. This sensor underwent several tests until reasonably accurate identification was achieved.

The sensor is powered by 5V, where the data pin emits a "High" signal indicating movement and a "Low" signal indicating no movement. The main challenge encountered during testing was synchronization with the camera. On the sensor, when the output is activated by detected movement, it remains at "High" for a short period (adjustable using the "time" option of the potentiometer), even when there is no longer any movement.

Adjustments were made during testing to the waiting time duration and sensitivity to stabilize the PIR using the potentiometer. Sensor stabilization can vary between 5 and 200 seconds. Consequently, adjustments were necessary to align the sensor with the camera better, ensuring improved synchronization between the devices.

A remaining issue in the project is the frequency of alerts sent in a short timeframe. The system currently has a high frequency of motion detection and alert notifications. Refining the system to establish an appropriate interval for sending alerts is imperative. For instance, the system could be configured to wait at least 10 seconds before issuing the following alert.

Following the tests, it was determined that the developed system is effective, efficiently notifying the user of a potential intrusion in the monitored location. However, further studies are needed to address the identified problems and enhance the system's performance.

5. Conclusion and Future Works

The developed application has the potential to contribute to security solutions for Smart Homes, focusing on monitoring cameras and motion sensors. The project's implementation cost is relatively low compared to traditional alarm services, which often involve additional charges for provided services.

The primary motivation behind this work was to present a practical resource based on IoT (Internet of Things). As the literature describes, this effort demonstrates that many smart devices can be effectively produced and commercialized.

In future work, we plan to conduct additional studies to address challenges encountered during the system construction. The ultimate goal is to propose a comprehensive residential security solution, encompassing monitoring for doors, windows, lights, and other Smart Home components. Besides, we aim to perform new experiments with the current system, exploring the integration of audible alarms to enhance the alert system.

References

[1]. Ashton, K. (2009). That ‘Internet of Things’ Thing. RFID journal, 22(7), 97-114.
[2]. Atzori, L., Iera, A., Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, 56, 122-140. doi: 10.1016/j.adhoc.2016.12.004
[3]. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660. doi: 10.1016/j.future.2013.01.010
[4]. Robles, R. J., Kim, T. H., Cook, D., Das, S. (2010). A review on security in smart home development. International Journal of Advanced Science and Technology, 15, 13-22.
[5]. Kodali, R. K., Jain, V., Bose, S., Boppana, L. IoT based smart security and home automation system. In 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, 1286-1289. doi: 10.1109/CCAA.2016.7813916.
[6]. Pavithra, D., Balakrishnan, R. IoT based Monitoring and Control System for Home Automation. In 2015 Global Conference on Communication Technologies (GCCT), Thuckalay, India, 2015, 169-173. doi: 10.1109/GCCT.2015.7342646

[7]. Davidson, C., Rezwana, T., Hoque, M. A. Smart Home Security Application Enabled by IoT: Using Arduino, Raspberry Pi, NodeJS, and MongoDB. In 2018 Smart Grid and Internet of Things (SGIoT), Niagara Falls, ON, Canada, 2018, 46-56. doi: 10.1007/978-3-030-05928-6_5
[8]. Android Studio. <https://developer.android.com/> accessed on 16 dec 2023
[9]. Oracle Java. <https://www.oracle.com/java/> accessed on 16 dec 2023.
[10]. Firebase. <https://firebase.google.com/> accessed on 16 dec 2023.
[11]. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys tutorials, 17(4), 2347-2376. doi: 10.1109/COMST.2015.2444095
[12]. Surantha, N., Wicaksono, W. R. (2018). Design of smart home security system using object recognition and PIR sensor. Procedia Computer Science, 135, 465-472. doi: 10.1016/j.procs.2018.08.198

Warning:

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views or official policies of the Faculty of Computring (FACOM) of the Federal University of Uberlandia (UFU), and of the Computing Department of the Federal Institute of Piaui (IFPI).

Authors' profile:

He is a PhD student in Computer Science at the Faculty of Computing (FACOM) at the Federal University of Uberlândia (UFU). He has a master's in Applied Computing in Educational Informatics (2013) from the State University of Ceará (UECE). Besides, she has a specialization in Computer Networks (2009) and a bachelor's degree in Computing (2004) from the State University of Piauí (UESPI). He is an Effective Professor at the Informatics and Communication Center at the Federal Institute of Piauí (IFPI), with experience in Technologies for Education, Computer Networks, and Information Security. His research in the doctoral program focuses on Anomaly-Based Intrusion Detection Systems, with an emphasis on generalization methods for intrusion detection in machine learning models.

He graduated in Systems Analysis and Development degree from the Northern University of Parana, a specialization in Windows Network Administration from the University of Araraquara, and a Master's degree in Computer Science from the Federal University of Uberlandia. He has been employed as a teacher at Senac Minas since 2001. His expertise lies in the field of Computer Networks, with a focus on Corporate Email Servers for the Internet and Systems Analysis and Development. Additionally, he possesses advanced skills in Excel and has teaching experience at Senac during the mentioned period. He serves as a speaker on computer networks at educational centers and universities. Besides, he is an authorized professor at the Cisco Academy Senac Minas, where he conducts preparatory courses for the CCNA and CCENT exams. It is actively engaged in research within the Postgraduate Program in Computer Science at FACOM - Faculty of Computing at the Federal University of Uberlândia. His research revolves around the “Definition of standards for the reduction of false positives in detecting spam in electronic mail services.”

He graduated in Systems Analysis and Development from the Federal Institute of Triangulo Mineiro in 2016. He works as a full-stack web developer at Sankhya Gestão de Negócios. He has experience in Computer Science, including diverse topics such as computer science teaching, web systems development, Internet of Things (IoT), machine learning, computer maintenance, and applied computing.