

IoT Smart Entrance using AI Thinker Card

D. Jaya Sai Pavani
B.E. Student

Department of ECE Sathyabama Institute
Of Science and Technology. Chennai, India

Dr. A. Aranganathan (M.TECH., Ph.D.)
Associate Professor

Sathyabama Institute of Science and
Technology, Chennai, India

Gandareddy Divyasree
B.E Student

Department of ECE Sathyabama Institute
of Science and Technology, Chennai, India

Abstract:- Today we live in a high tech age where crime is increasing day by day. With the increasing number of threats and invaders to society, everyone needs a high-tech security system that can keep their belongings safe. At the same time, we want to protect residential properties from all kinds of hazards. Attention is focused on using customer-side applications securely transfer information between layers of the IoT architecture. This document aims to provide a low-power, low-cost, and discreet IoT-based home security system that helps detect, identify, and authenticate the presence of strangers. The proposed solution uses a webcam as the image capture unit, a fingerprint reader for authentication, and a surprise such as Telegram Bot, which provides an API to build solutions compatible with the IoT infrastructure. The system uses a fingerprint reader to control the opening and closing of security locker doors. User ID must be verified using Fingerprint before entering the house. If the user is authorized, the door is opened otherwise the owner can check it through the camera and open the door if he want to allow that unauthorized party. The owner can open the door remotely

Keywords:- Home Security, Fingerprint module, Sim 800L, AI thinker ESP8266 Nodemcu.

I. INTRODUCTION

The concept of smart home is becoming very popular these days. A smart home can be thought of as an intelligent or automated home in which appliances can be automated There are different types of systems are existing now. They are all used for the security of the home and for home automation IOS-based home automation security system using General Packet Radio Service (GPRS) and controlled remotely. A security system is an essential part of every organization, bank and home. Its main purpose is to protect people and property from various risks such as crime and loss. The Internet of Things (IoT) is a physical network of devices, buildings, vehicles, and other items equipped with electronics, software, sensors, and network connections that enable objects or objects to collect and exchange data. The Internet of Things is expected to provide a high level of human-machine interaction. This project proposes a security system using IOT to prevent the primary objective of this project is to reduce human work. Automation has always been a prime factor for

security systems. Our aim in the project is to design and implement a security systemA system that offers controllability through a handheld mobile phone by means of IoT. The commands from a mobile phone are used to allow/deny access to the home. We propose IOT based theft detection project using controllers. In this proposed system. If an authorized person is entering the home, the person has to verify his user identity using fingerprint verification. If finger print matches the door will be open. When the user is not authorized, the image will be captured using the camera. The owner can view the image using the mobile application and he can deny/allow access. If the owner allows access, then the door will automatically open. Otherwise, it will be closed.

II. OBJECTIVE

The main purpose of the function is to improve the quality and convenience of life in the home. Increase security and use energy more efficiently. Build a powerful security firewall to protect your system from security threats. Reduce labor and increase use of the digital world to implement devices such as motion sensors, cameras, shutters, or thermostats for user-programmed processes. Monitor the status of activities happening around us. Protecting and centralizing control over our living environment.

III. EXISTING SYSTEM

There are different types of systems are existing now. They are all used for the security of the home and for home automation. IOS-based home automation security system using General Packet RadioService(GPRS)

A. Machine-to-machine Communication Based Smart Home Security System by NFC, Fingerprint, and PIR Sensor with Mobile Android Application

Here a multi-layer home security system (HSS) has been developed which maintains six levels of security and necessary control responses against unwanted burglars and intruders. As a part of this development, the first security level uses Near Field Communication (NFC) tag, the second level uses a secured password system and the third level uses finger print authentication. After that, a GSM module embedded with the proposed HSS sends the logged password to a remote server via M2M communication. The server encrypts the password and notices the homeowner via an android-based mobile application whether the person

is an authenticated person or not. In the final stage of security, if an intruder wants to enter the room by breaking the password without an NFC tag and finger print encryption a Passive Infrared (PIR) motion sensor will work and sounds a buzzer for alarm. Therefore, the automatic and embedded operation of the proposed HSS makes it more secure, reliable, and robust than other traditional systems.

B. Home automation security system using Short Messaging Service

The unauthorized access into the home is identified by monitoring the state of the home door using Light Emitting Diode (LED) and IR sensors. The proposed system also allows legitimate users to control home lights and set the 4-digit passkey using SMS. The LED and IR sensors used to identify intrusions could easily be spoofed by a sophisticated attacker. Informing the user about an intrusion via SMS is not a good practice, as the user may not be near to the phone to receive the alert on time.

C. Smart Eye

It uses real-time home automation and a monitoring system using GPRS. The proposed system alerts the user about an intrusion who in turn can view the home using a live camera. Each home is connected to the central server, the user sends control commands to the server which the home system reads from the central server and executes. When a device a thome changes state it sends the information to the central server, which the user can access. The central controller-based security system proposed by Dr. Isaac Ferando "Home Security System on Intelligent Network" failed to implement any modern security hardware or did not consider defense against sophisticated intrusion attempts. A central controller-based security system raises some serious privacy and security concerns considering the large-scale user data available at the central controller and increases the potential for large-scale surveillance. Moreover, central controller-based security systems are not feasible for single isolate homes.

IV. PROPOSED METHODOLOGY

The proposed methodology has camera, finger print module, and motor are connected to the controller sensors. After If an authorized person is entering the house, before that the person has to verify his user identity using finger print verification. If the finger print matches, the door will be open. When the user is not authorized, the image/video will be captured using the camera. The owner can view the image using the mobile application and he can deny/allow access.. if the owner allows access, then the door will automatically open, otherwise, it will close. The fire sensor will detect fire and produce an alarm. The IR sensor will be kept near the doors to sense human behavior. When the home is empty the owner will be ON theft mode. Advantages of Proposed System.

Nowadays, at every point in time, we need security systems for the protection of valuable data and even money. There are other methods of verifying authentication through password, RFID, and facial recognition but this method is the most efficient and reliable. Generally, passwords, Identification cards, and PIN Verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost. And also, the facial expressions may vary depending on other facts. The most secure system is fingerprint recognition because the fingerprint of none person never matches the other. these features make the project unique from the other existing systems.

Behavioral Model: The behavioral model consists of the following components: The RS232 interface is TTL level, the default baud rate is 57600 and can be changed. See communication protocol. Microcontrollers such as ARM, DSP and other single port serial devices, as well as 3.3V, 5V Microcontrollers can be directly connected. The computer needs to be connected to level translation, level translation notification, MAX232 circuits, etc.

- **Features of Perfect features:** Independent fingerprint registration, fingerprint registration, fingerprint comparison (1:1) and fingerprint search (1:N). Small size: Small size, no external DSP chip algorithm, built-in, easy to install, less error.
- **Ultra-Low power consumption:** The overall product has low power consumption, suitable for low power consumption needs. Anti-static index reached above 15KV. Application development is easy. Developers can provide control instructions and product development for self-fingerprinting applications without fingerprint expertise.

Adjustable security level: Suitable for different applications, the security level can be adjusted by the user. Finger touch sensing signal output, low rms value, standby current of sensor circuit is very low, less than 5uA.

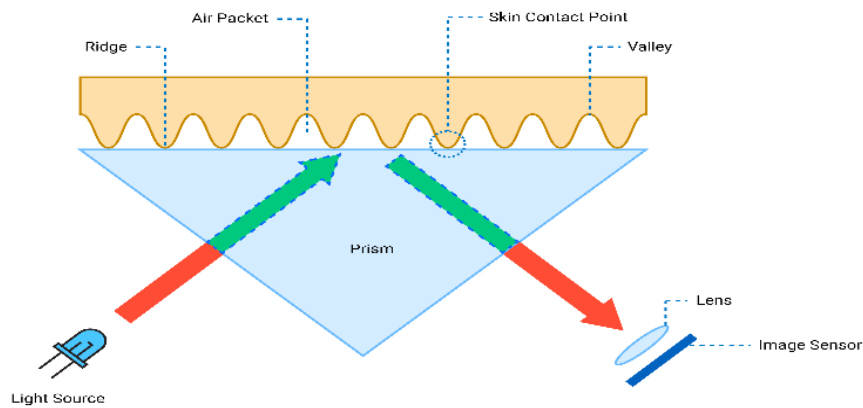


Fig. 1: Optical Fingerprint scanner Working Principle

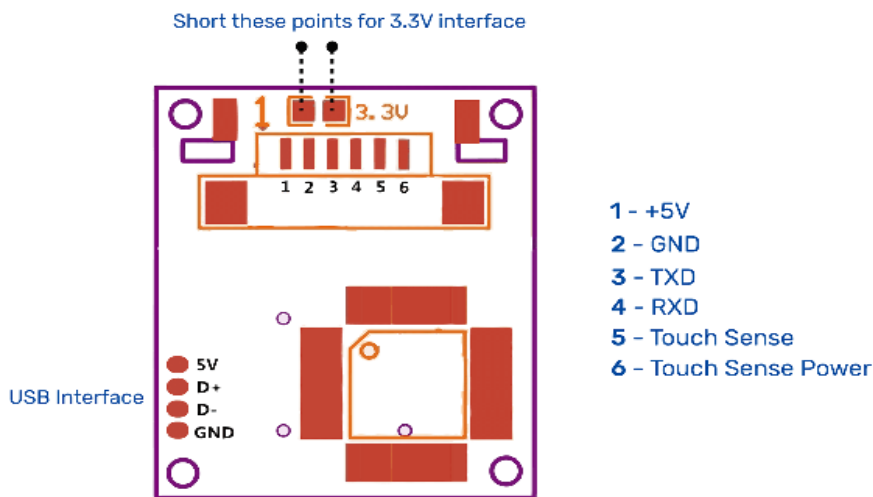


Fig. 2: R307 Fingerprint Scanner Pinout

The SIM800L GSM/GPRS module is a miniature GSM modem that can be integrated into various IoT projects. With this module you can do almost everything that a normal cell phone can do. B. Sending SMS Messages,

making phone calls, connecting to the Internet via GPRS, etc. This module supports quad-band GSM/GPRS networks, so it can work virtually anywhere in the world.



Fig. 3: SIM800L

- **AI THINKER ESP8266 NODEMCU:** Ai Thinker NodeMCU-ESP8266 is an open-source firmware and development kit that can be used to prototype or create IoT products. This includes the firmware running on his ESP8266 Wi-Fi SoC from Expressive Systems and hardware based on the ESP-12 module. The firmware uses the Lua scripting language. It is based on the Lua project and his expressive Non-OS SDK for ESP8266.

Function:

WIFI Module: ESP-12E

Processor:ESP8266

CP2102Chip

Built-InFlash:32Mbit

Antenna:Onboard Antenna

Peripheral **Interface:** UART/SPI/I2C/SDIO/GPIO/ADC/PWM

WIFI **Protocol:** IEEE802.11b/g/n

Frequency **Range:** 2.4G~2.5G(2400M~2483.5M)

WIFI**Mode:** Station/SoftAP/ SoftAP+Station

Power **Supply:** 5V

Logic **Level:** 3.3V

V. CONCLUSION

The home security system is a solution to problems like theft, crimes etc. The Controller is a great platform for building highly capable, embedded systems. This makes it possible for users to rest assured that their belongings are secure. For energy conservation by the use of a PIR sensor. So, this will save electricity. The end product will have a simplistic design making it easy for users to interact with. The project is aimed at developing the security of Homes against intruders.

VI. FUTURE SCOPE

The real-time tracking of the system works with the power consumption factor but still, this system has no indicator to indicate the value to charge physically present. We have proposed a system that can handle firewall problems but still, it has some security failures which need to be taken into account before the fabrication of this project. We used a third-party open-source software integration tool this system must be developed with standalone IDE control and processing unit to control the entire unit.

REFERENCES

- [1.] C. Shiyao, W. Ming, L. Chen, and R. Na, "The research and implement of the intelligent parking reservation management system based on ZigBee technology," in Proc. 6th Int. Conf. Meas. Technol. Mechatronics Autom. (ICMTMA), 2014, pp. 741-744.
- [2.] El Mouatezbillah Karbab, Djamel Djenouri, Sahar Boulkaboul, Antoine Bagula, CERIST Research Center, Algiers, Algeria University of the Western Cape, Cape town, South Africa, "Car Park Management with Networked Wireless Sensors and Active RFID", 978-1-4799-8802-0/15 ©2015 IEEE
- [3.] Faiz Ibrahim Shaikh, Pratik Nirnay Jadhav, Saideep Pradeep Bandarkar, Omkar Pradip Kulkarni, Nikhilkumar B. Shardoor "Smart Parking System Based on Embedded System and Sensor Network", International Journal of Computer Applications...
- [4.] Harmeet Singh, Chetan Anand, Vinay Kumar, Ankit Sharma, "Automated Parking System With Bluetooth Access", International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 3 Issue 5, May 2014, Page No. 5773- 5775
- [5.] Hilal Al-Kharusi, Ibrahim Al-Bahadly, "Intelligent Parking Management System Based on Image Processing", World Journal of Engineering and Technology, 2014, 2, 55-67.
- [6.] L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and R. Vergallo, "Integration of RFID and WSN technologies in a smart parking system," in Proc. 22nd Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM), 2014, pp. 104-110.
- [7.] Mr. Basavaraju S R "Automatic Smart Parking System using Internet of Things (IOT)", (International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015)
- [8.] M. M. Rashid, A. Musa, M. Aatur Rahman, and N. Farahana, A. Farahana, "Automatic Parking Management System and Parking Fee Collection Based on Number Plate Recognition.", International Journal of Machine Learning and Computing, Vol. 2, No. 2, April 2012, Published 2014.
- [9.] Thanh Nam Pham¹, Ming-Fong Tsai¹, Duc Binh Nguyen¹, ChyiRen Dow¹, And Der- Jiunn Deng² "A Cloud-Based Smart-Parking System Based on Internet-of-Things Technologies", IEEE Access, Received July 24, 2015, accepted August 16, 2015, date of publication September 9, 2015, date of current version September 23, 2015.
- [10.] X. Zhao, K. Zhao, and F. Hai, "An algorithm of parking planning for smart parking system," in Proc. 11th World Congr. Intell. Control Autom. (WCICA), 2014, pp. 4965-4969.