International Journal of Scientific and Management Research
Volume 08 Issue 05 (May) 2025
ISSN: 2581-6888
Page: 13-19

# Design and Implementation of an Intelligent Microcontroller-Based Home Security System

**Munoda Mafuratidze**
Master of Engineering in Electrical Power Engineering, The University of Zambia, **Zambia**
**DOI -** http://doi.org/10.37502/IJSMR.2025.8502

## Abstract

This research presents design and implementation of an intelligent microcontroller- based home security system aimed at enhancing residential safety through real-time, multi- layered protection and user-friendly management. Leveragig PIC 16F877A microcontroller and an HC-06 Bluetooth module, this system enables wireless communication with a dedicated Android application for remote monitoring, arming, disarming and emergency notifications. The system integrates infrared motion sensors, magnetic contacts, and automated response protocols to detect unauthorised entry, activating a series of responses including alarms, image capture and SMS alerts. Unlike traditional systems which are often limited to basic alarm triggers, this design captures images of intruders, stores evidence and sends images directly to the home owner's smartphone. The system was developed with MickroC software and MIT Application Inventor, this system combines hardware versatility with software flexibility, creating a scalable, cost-effective solution suitable for modern home security needs.

**Keywords:** Microcontroller, Security, Intrusion, Detection, Image Capture, Automation, Smartphone Control, Bluetooth.

## 1. Introduction

### 1.1 Background of Study

Home security systems have evolved from simple alarm-based systems to sophisticated multifunction systems aimed at deterring and preventing unauthorised access. Traditional systems often reliant on a detector-to-alarm combination, lack the intelligence to distinguish between legitimate threats and non-threatening movements [1] [2]. Advanced monitoring systems with moving cameras also encounter limitations such as failing to differentiate between intruders and household pets or triggering false alarms due to environmental factors. The PIC 16F877A microcontroller [3] offers a versatile foundation for integrating sensors, communication modules and peripheral devices for real-time detection, monitoring and automated responses [12].

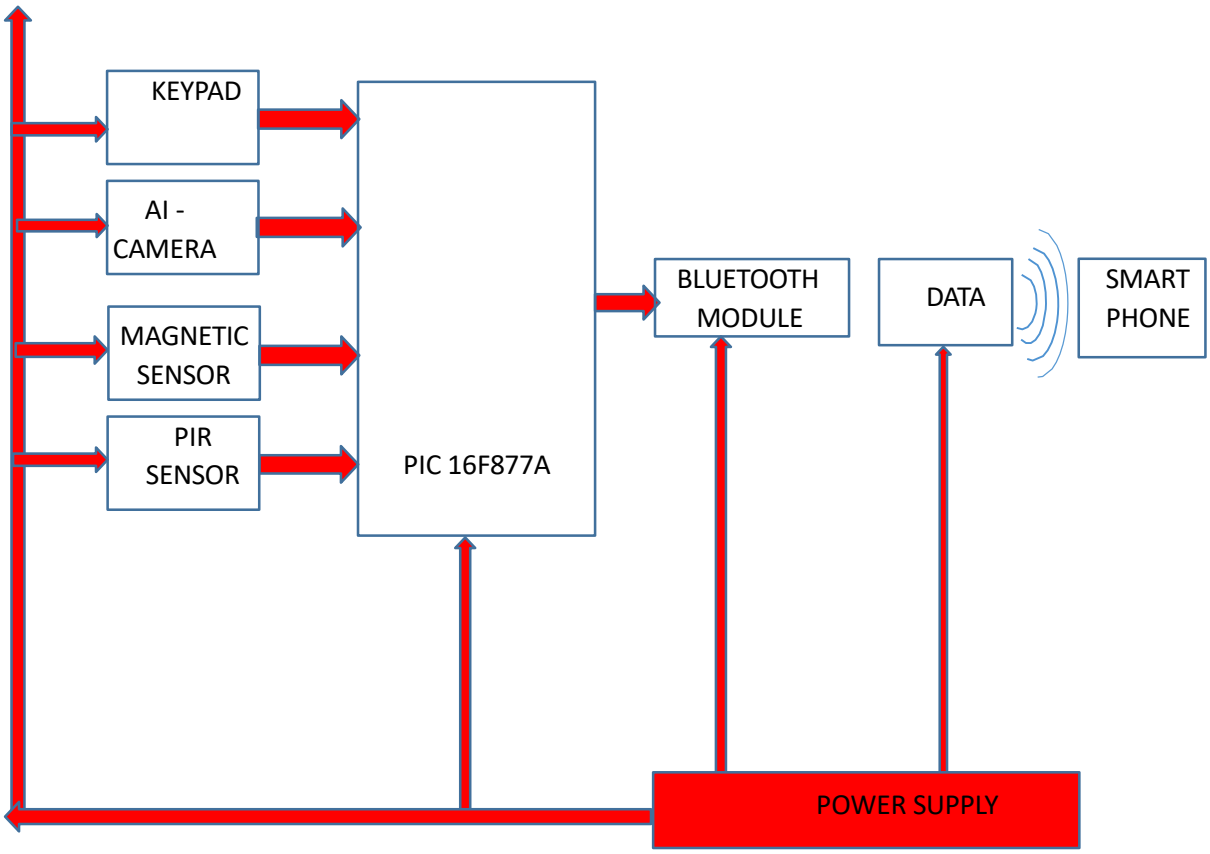
This research aims to bridge the gap by designing a robust, intelligent home security system that offers a higher level of customisation, accuracy and ease of use. Most existing home security systems either alert home owners after an incident have occurred or provide limited functionality, often failing to meet modern security needs [5]. High-end systems are often prohibitively expensive and many accessible systems are prone to false alarms or can be easily bypassed [4] [6]. This research addresses these challenges by developing a microcontroller-

based home security system that combines affordability with advanced features such as image capture, SMS alerts and smartphone integration.

### 1.2 Objectives

i. To provide remote system management via an Android application, allowing users to arm, disarm and customise security settings.
ii. To enable smartphone-activated image capture and live streaming for real-time surveillance.
iii. To ensure low-power operation with backup battery support for uninterrupted functionality.

## 2. Methodology System Architecture

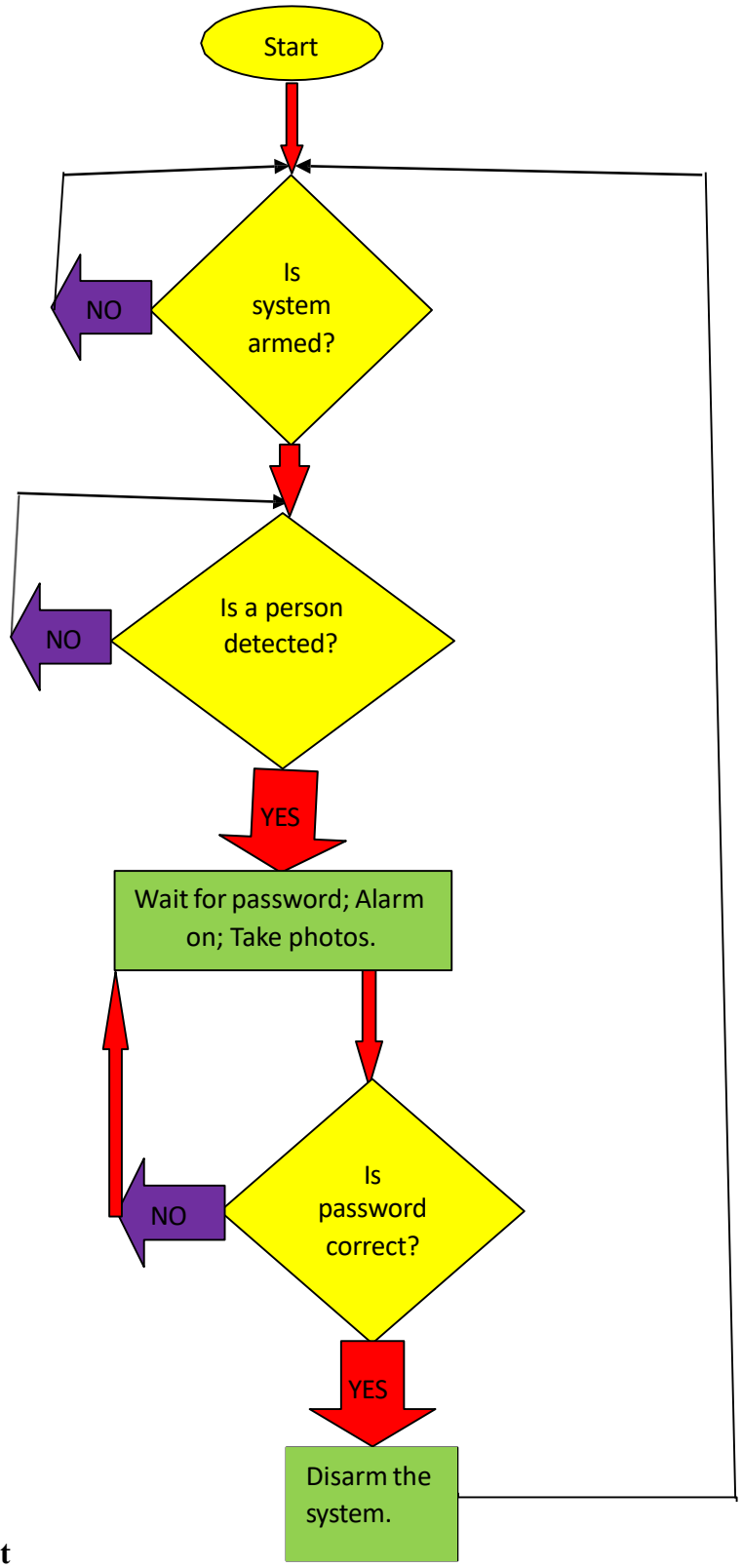



***Block diagram for home security system.***

The home security system architecture comprises of the following interconnected modules:

1. PIC 16F877A microcontroller: Manages sensor input, alarms and communication with the Android application.
2. Bluetooth Module (HC-06): Enables wireless communication between the microcontroller and smartphone within a range of up to 100 meters.
3. Sensors:
   - AI-Cameras and PIR Sensors: Detect motion and provide real-time alerts.
   - Magnetic Contacts: Installed on doors and windows to detect unauthorised entry.

4. Smartphone Application: Developed using MIT App Inventor enabling user interaction with the system including arming/disarming, image capture and alert notifications.
5. Power Supply and Backup: Automatically switches to battery backup in case of power failure, ensuring continuous functionality.




**The flow chart**

***Flow chart for the home security system.***

**System Implementation**

The system allows the users to enter a password via a keypad to arm or disarm the system. Once armed, the system continuously monitors sensor inputs. When an intrusion is detected, the microcontroller triggers alarms, activates the camera and initiates data transmission. Unauthorised activity prompts the system to capture and send images to the home owner's smartphone via SMS, sound alarms and provides the option to activate live streaming for real time verification. The Android application allows users to monitor activity, customise alert settings and update passwords for enhanced security.

The home security system employed Passive Infrared (PIR) sensors at main entry points to detect body heat and motion. When movement has been detected, these sensors signal the microcontroller which then initiates response protocols. Magnetic contacts on doors and windows detect breaches or disruptions, triggering alerts, alarms and defensive actions. The microcontroller programmed in MikroC, processes input signals, controls devices like (alarms and cameras) and interfaces with a Bluetooth module. The Android application built using MIT App Inventor connects to the microcontroller enabling users to configure security settings, view alerts, receive images and access live camera feeds.

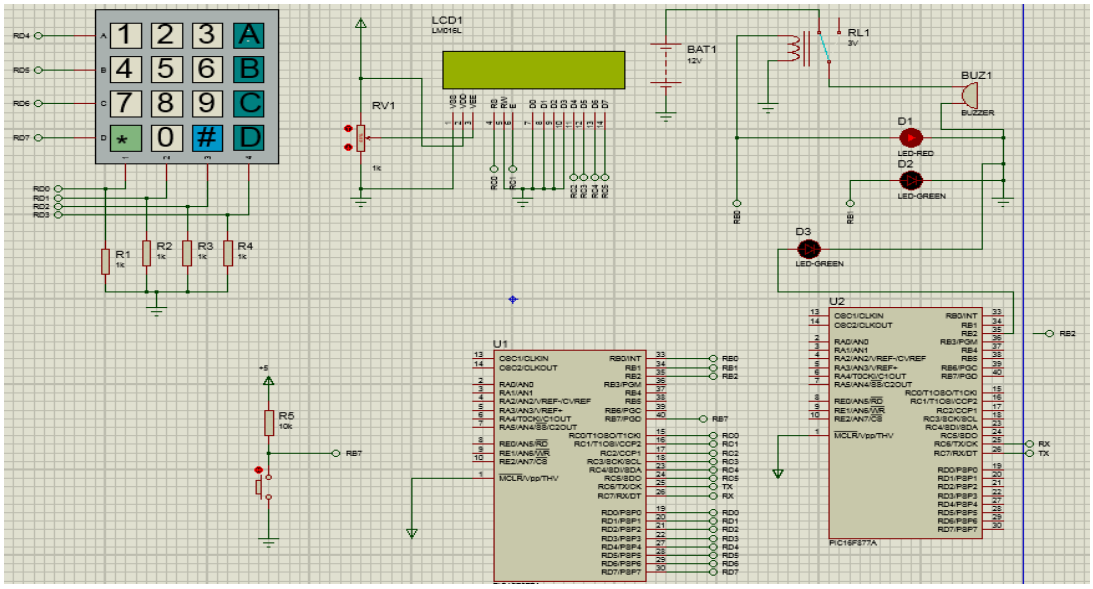
A relay circuit manages seamless transitions to battery backup so as to maintain power during outages, ensuring continuous operation. Automated phone functions such as image capture, sms alerts and live stream options are managed by AutomateIt Pro and Trigger apps which are activated by sensor signals. MikroC code defines the system's logic for sensor activation, alarms, image capture and data transmission. Circuit design was simulated using Proteus 8.3, followed by breadboard testing to confirm reliability under various conditions.

**Code**

The snap code demonstrates how to use library function for handling of the MCU's internal EEPROM module for microcontroller PIC 16F877A and how to use timers and their interrupts.

```
void code_read(){       //read data from EEPROM
        Delay_ms(20);
        master[0] = EEPROM_Read(0x00);       // Read data from address 0 Delay_ms(20);
        master[1] = EEPROM_Read(0x01);       // Read data from address 1
```

## 3. Results




***Home Security Schematic***

**Table below shows system responses to user actions.**

| **Condition** | **System Action** |
|---|---|
| System is powered | LCD displays prompts for password entry |
| Default password set | User prompted to create a desired password. |
| PIR sensor activated | Alarm triggers, SMS alert is sent, camera captures image, and video stream activated |

This intelligent microcontroller-based home security system demonstrated high accuracy, efficiency, and ease of use, with successful integration of various components for a comprehensive security solution. Testing indicated minimal false alerts, with the system reliably differentiating between legitimate threats and non-threatening motions

## 4. Conclusion

This research successfully achieved the design and implementation of an intelligent home security system using the PIC16F877A microcontroller, enhancing security by enabling real-time intrusion detection, alarm activation and evidence capture. Smartphone integration for remote monitoring adds valuable layer of accessibility allowing users to manage and respond to security events conveniently. This research demonstrates a scalable, cost-effective solution adaptable to various residential security needs, illustrating the practical potential of affordable, user centred security systems. This research illustrates how a balanced approach combining technological sophistication with ease of use can deliver high value security for modern homes. By prioritising advanced intrusion detection, robust system management and user accessibility, the system sets a precedent for future intelligent security solutions addressing the growing demand for seamless, reliable home protection.

**Recommendation**

The research suggested potential improvements such as integrating Wi-Fi for extended range, adding more sensors or using AI for motion detection accuracy. Enhanced AI integration security precision is recommended because AI can improve the accuracy of motion detection through advanced image and sound processing distinguishing between genuine threats and false alarms. AI driven cameras and sensors, for example, analyse movement patterns, alerting users only when suspicious activity is detected. These improvements should be increasingly common as AI is further integrated with IoT to enhance the smart home's situational awareness and adaptability to changing environments. 5G and Wi-Fi 6 for connectivity is also important because expanding on Wi-Fi or cellular connectivity can enable faster and more reliable connections between devices and allow for real-time monitoring and alerts [9]. This connectivity ensures that users can receive immediate updates or access video streams without latency especially as more IoT devices require substantial bandwidth to operate effectively. The risk of cyber threats grows with more IoT devices connected to networks. Blockchain [8] for data security technology is emerging as a secure method for verifying data integrity in IoT ecosystems, creating tamper-resistant records and ensuring privacy in data exchanges between devices [8]. Future smart home systems are expected to integrate energy efficient devices and sustainable practices managed intelligently by AI for sustainability and energy management

**References**

1) T. Rizal, U. Munirul, Bustami, M. Syibbran and J. B. Muhammad, "Home Surveillence System Based on Internet of Things and Thermal Sensors," in Malikussaleh International Conference on Multidisciplinary studies, Aceh, 2022.
2) Sharmin, S. A. Rehana, U. M. Sohid and H. A. Syed, "Smart Security Surveillance Using IoT," in IEEE International Conference on Inventive Systems and Control, 2017.
3) Usaide, R. Ehiedum and O. Semiu, "Bluetooth-Based Wireless Home Security System with Intruder Alert Mechanism," International Journal of Trend in Scientific Research and Development, vol. 6, no. 7, 2022.
4) G. N. Balaji, K. Saravanan, R. Poorani, T. V. Priya and R. R. Raj, "Advanced Security System Using Pic through Bluetooth," International Journal of Trend in Scientific Research and Development, vol. 1, no. 5, 2017.
5) E. Waleed, "AI-Driven Security in Smart Homes: Challenges and Opportunities," Journal of Intelligent Systems and Internet of Things (IJSIoT), vol. 08, no. 02, pp. 54-62, 2023.
6) S. Ahmed and M. J. Iqbal, "MickroC for PIC Microcontroller Programming: A Practical Guide," Embedded Systems Research Journal, vol.6, no.2, pp. 55-63, 2021.
7) U. Bhaskar and B. K. Ramesh, "Microcontroller-Based Home Security System with Remote Monitoring," International Journal of Advanced Research in Computer Science and Electronics Engineering,, pp. 11-19, 2022.
8) S. H. Gopalan, A. Manikandan, G. Sujatha and N. P. Dharani, "Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks," International Journal of Networked and Distributed Computing, vol. 12, pp. 237-249, 2024.
9) S. K. Vimal, P. Ramesh, J. M. Senthil and M. R. Rafi, "Adoption of IoT in 5G and Wi-Fi Technology Towards Smart Cities," SSRG International Journal of Computer Science and Engineering, vol. 8, no. 10, pp. 1-4, 2021.

10) "Microcontrollers (MCUs)," Microchip Technology Inc, 2023. [Online]. Available: https://www.microchip.com, [Accessed 11 11 2024].
11) J. K. Mohamed, "Security of The Embedded and IoT Sesytems: Threats and Attacks, and Countermeasures," International Journal of Creative Research Thoughts, vol. 9, no. 8, 2021.
12) J. Park, M. Tehranipoor, Y. Bai and D. Forte, "Real-time instruction-level verification of remote IoT/CPS devices via side channels," Discover Internet of Things, 2022.
13) M. Dahiya, "Short Range Wireless Network: Bluetooth," International Journal of Advanced Research in Computer Science, vol. 8, no. 3, 2017.