Smart Burglar Alarm System for Real-Time Intrusion Detection and Alerting

[1]DARSHAN S, [2]MALATESH S H, [3]LAKSHMI NARAYANA REDDY JV, [4]LIKITH GOWDA, [5]DHANUSH G

[1,3,4,5]Students, [2]Professor and HOD,
[1]Dept of CSE,
[1]M S Engineering College, Bangalore, India

Abstract- Security and surveillance systems have become increasingly important due to the rising incidents of burglary, fire hazards, and violent activities in residential, commercial, and institutional environments. Traditional security systems mainly rely on basic alarm mechanisms, manual monitoring, or passive surveillance, which lack intelligence, real-time decision-making, and remote alerting capabilities. These limitations often result in delayed responses and increased dependence on human supervision. To address these challenges, this paper presents a smart burglar alarm system that integrates embedded systems, sensor-based detection, computer vision principles, and Internet of Things (IoT) communication for real-time intrusion detection and alerting.

The proposed system is designed using a Raspberry Pi as the central processing unit, which continuously monitors multiple inputs from a door sensor and a flame sensor to detect unauthorized entry and fire hazards. In addition to sensor-based detection, a camera module is incorporated to enable visual threat analysis. The system supports image classification to identify potentially dangerous scenarios such as weapon presence or fighting activities. By combining physical sensor data with visual information, the system enhances threat detection accuracy and reduces the likelihood of false alarms compared to conventional single-layer security systems.

Upon detecting any abnormal or dangerous condition, the system automatically triggers local alerts using a buzzer and LED to warn nearby occupants. Simultaneously, real-time notifications along with relevant images are sent to the authorized user through Telegram, enabling remote monitoring and immediate awareness regardless of location. The system is implemented using Python and employs multithreading to ensure continuous sensor monitoring while allowing parallel execution of image processing and graphical user interface (GUI) operations. This design ensures low response time, uninterrupted operation, and efficient handling of multiple security events.

Experimental evaluation demonstrates that the proposed system effectively detects intrusions, fire hazards, and image-based threats with minimal delay. Testing results confirm reliable alarm activation, accurate image classification based on predefined categories, and prompt delivery of Telegram alerts. The integration of sensor-based detection and visual verification improves system reliability and provides contextual information to users, enhancing situational awareness and enabling faster decision-making during emergency situations.

In conclusion, this work presents a cost-effective, scalable, and intelligent burglar alarm system suitable for real-world deployment. By integrating IoT communication, embedded computing, and basic computer vision techniques, the proposed system offers automated monitoring, real-time alerting, and reduced dependence on continuous human surveillance. The modular architecture allows future enhancements such as AI-based threat recognition, cloud data storage, and mobile application integration, making the system a strong foundation for next-generation smart security solutions.

.***Keywords-*** Smart Security, IoT, Burglar Alarm System, Raspberry Pi, Computer Vision, Telegram Alerts

INTRODUCTION

Security has become a critical concern in modern society due to the increasing frequency of burglary, fire hazards, and violent incidents in residential, commercial, and institutional environments. Conventional security systems such as mechanical locks, basic alarm units, and closed-circuit television (CCTV) cameras provide limited protection because they often rely on manual monitoring and lack intelligent decision-making capabilities. These systems are typically reactive rather than proactive, resulting in delayed responses and increased dependence on human intervention, which can compromise safety and reliability.

Recent advancements in embedded systems, Internet of Things (IoT), and computer vision technologies have enabled the development of smart security solutions capable of autonomous monitoring and real-time alerting. IoT-based systems allow devices to communicate over the internet, providing remote access and instant notifications, while embedded platforms such as Raspberry Pi offer sufficient processing power to integrate sensors and cameras. Additionally, computer vision techniques enhance security by enabling visual interpretation of suspicious activities, making it possible to detect not only intrusions but also dangerous scenarios such as weapon presence or physical violence.

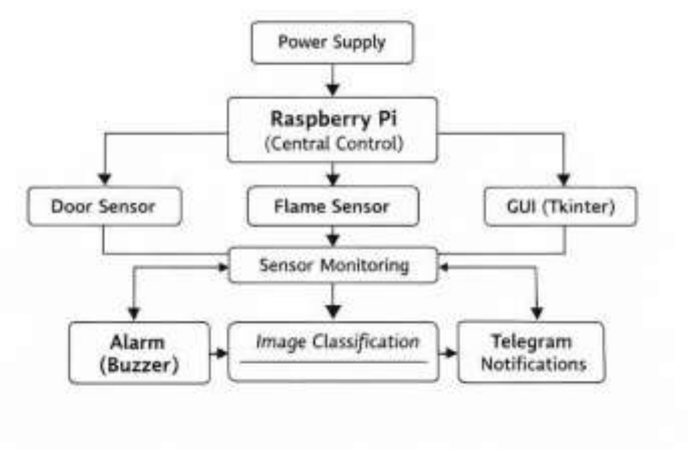
This paper presents a smart burglar alarm system that integrates sensor-based detection, basic computer vision techniques, and IoT-based communication to provide real-time intrusion detection and alerting. The proposed system uses a Raspberry Pi as the central controller to monitor door and flame sensors and analyze visual data captured through a camera module. When a potential threat is detected, the system automatically triggers local alarms and sends real-time notifications with visual evidence to the user via Telegram. The objective of this work is to develop a cost-effective, reliable, and scalable security solution that reduces false alarms, minimizes human supervision, and enhances overall safety

RELATED WORK

Early burglar alarm systems primarily relied on mechanical switches, magnetic contacts, and audible alarms to detect unauthorized access. While these systems were simple and cost-effective, they lacked intelligence, automation, and remote notification capabilities. Later developments introduced sensor-based security systems using Passive Infrared (PIR) sensors, door sensors, and flame or smoke detectors to improve detection accuracy. However, most of these systems provided only local alerts, requiring human presence for effective monitoring. GSM-based security systems improved this limitation by enabling SMS alerts, but they involved additional hardware costs, limited multimedia support, and dependency on cellular networks, making them less flexible for modern applications.

Recent research has focused on IoT-based and Raspberry Pi–based security systems due to their enhanced processing capabilities, internet connectivity, and support for cameras. Several studies have demonstrated the use of computer vision techniques for detecting suspicious activities such as weapon presence, violence, or abnormal behavior. IoT communication platforms such as Telegram, MQTT, and cloud-based services have been widely adopted for real-time alerts due to their low cost and fast message delivery. However, many existing solutions either focus solely on sensor-based detection or rely heavily on computationally expensive vision models. The proposed system addresses these limitations by combining multi-sensor detection with basic image classification and IoT-based alerts in a single, cost-effective framework, thereby improving reliability, reducing false alarms, and enabling real-time remote monitoring.

SYSTEM ARCHITECTURE



The proposed Smart Burglar Alarm System is designed with a centralized architecture in which a Raspberry Pi acts as the main processing and control unit. It interfaces with multiple input devices, including a door sensor and a flame sensor, to continuously monitor unauthorized entry and fire hazards. A camera module is also integrated to provide visual input for image-based threat analysis, enabling the detection of suspicious activities such as weapon presence or fighting scenarios. All input devices are connected to the Raspberry Pi through GPIO and USB interfaces, ensuring real-time data acquisition and centralized control.

The processing and decision-making logic are implemented using Python on the Raspberry Pi, where sensor monitoring operates continuously alongside image classification and user interface modules through parallel execution. When a threat is detected, the system activates local alert mechanisms such as a buzzer and LED to warn nearby occupants. Simultaneously, real-time notifications along with relevant images are sent to the authorized user via Telegram using an IoT-based communication interface. This architecture ensures fast response, remote monitoring, reduced false alarms, and scalability for future enhancements such as AI-based threat detection and cloud integration

METHODOLOGY

` The Smart Burglar Alarm System is implemented using a Raspberry Pi as the central control unit to enable real-time monitoring and automated alerting. Initially, the Raspberry Pi configures all hardware components, including the door sensor, flame sensor, buzzer, LED, and camera module. The system then enters a continuous monitoring mode, where sensor inputs are read through GPIO pins to detect unauthorized entry and fire hazards. A dedicated monitoring thread ensures uninterrupted detection and quick response to abnormal conditions.

In parallel, image-based threat analysis is supported through a camera and a Python-based graphical user interface. Selected images are processed using basic image classification logic to identify weapon presence, fighting scenarios, or normal activity. When a threat is detected through sensors or image analysis, the system activates local alerts using the buzzer and LED and simultaneously sends real-time notifications with relevant images to the user via Telegram. Multithreading enables parallel execution of monitoring, image processing, and user interaction, ensuring low latency, reliability, and scalability.

HARDWARE AND SOFTWARE REQUIREMENTS

Hardware Components: Raspberry Pi as the central controller, door (magnetic) sensor for intrusion detection, flame sensor for fire hazard detection, USB/Pi camera for visual threat analysis, buzzer for audible alerts, LED indicator for visual alerts, 5V power supply, and jumper wires/breadboard for connections.

Software Tools: Raspberry Pi OS, Python (3.x), RPi.GPIO for GPIO control, OpenCV (cv2) and PIL (Pillow) for image processing, Tkinter for graphical user interface development, Telebot (pyTelegramBotAPI) for Telegram-based notifications, and the threading module for parallel execution.

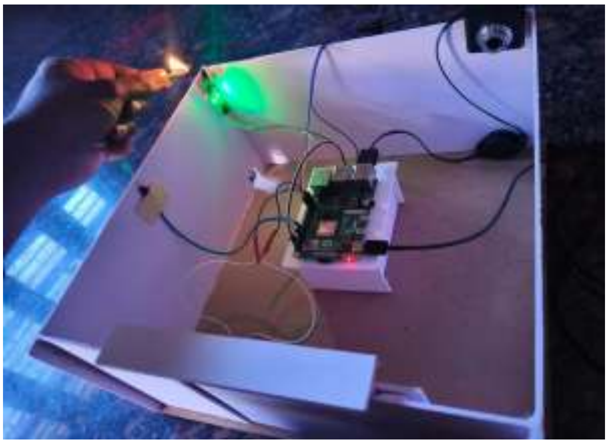
.

RESULTS AND DISCUSSION

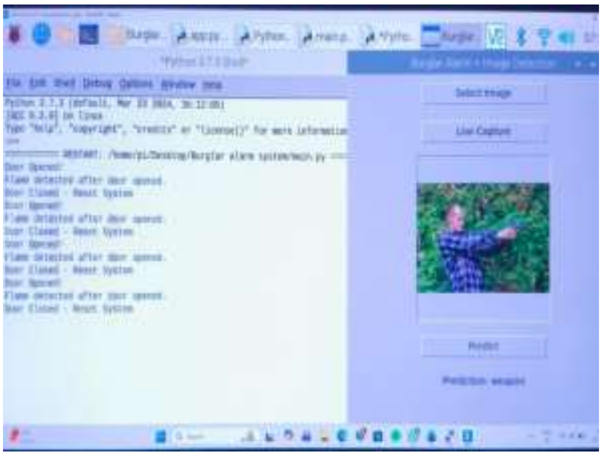
The proposed Smart Burglar Alarm System was tested under various real-world scenarios to evaluate its functionality, reliability, and responsiveness. The system successfully detected unauthorized door openings using the magnetic door sensor and fire hazards using the flame sensor. In all test cases, the Raspberry Pi processed sensor inputs in real time and triggered the buzzer and LED immediately upon threat detection. Telegram notifications were delivered instantly to the user, confirming the effectiveness of the IoT-based alerting mechanism. The response time between detection and alert generation was minimal, demonstrating the system's suitability for real-time security applications.

Image-based threat detection was evaluated by selecting images representing weapon presence, fighting scenarios, and normal activities through the graphical user interface. The system correctly classified images based on predefined categories and triggered alarms and Telegram alerts for weapon and fighting images, while no alarm was generated for normal images. This additional visual verification layer improved reliability by reducing false alarms that typically occur in sensor-only systems. The use of multithreading ensured that sensor monitoring continued uninterrupted while image processing and GUI operations were performed simultaneously.

Overall, the results indicate that the integration of sensor-based detection, image analysis, and IoT communication provides a robust and efficient security solution. The system demonstrated stable operation, accurate threat detection, and effective remote monitoring. While the current image classification approach is basic, the results validate the system architecture and methodology, and they highlight strong potential for future improvements using advanced AI-based models and cloud integration

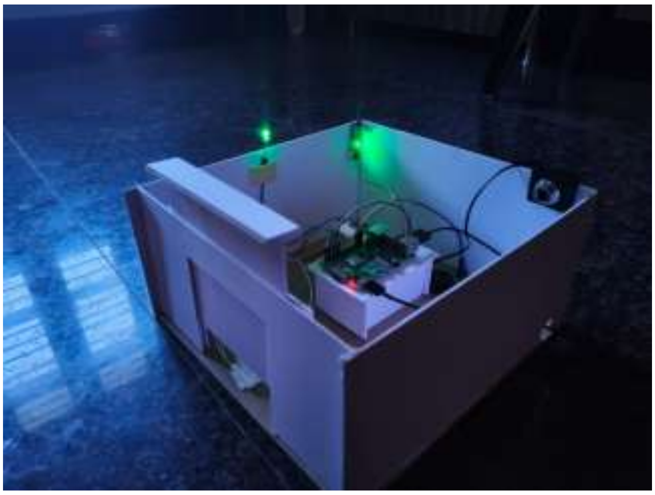


1. Flame Sensor Test



2. Image Classification Test – Weapon Image

3. Image Classification Test – Fighting Image



4. Door Sensor test

CONCLUSION AND FUTURE SCOPE

This paper presented a Smart Burglar Alarm System for real-time intrusion detection and alerting by integrating embedded systems, sensor-based monitoring, basic computer vision techniques, and IoT-based communication. The system successfully detects unauthorized entry and fire hazards using door and flame sensors, while visual threat analysis adds an additional layer of security by identifying weapon presence and fighting scenarios. The use of a Raspberry Pi as the central controller, along with Python-based software and multithreading, ensures real-time responsiveness, reliable operation, and efficient handling of multiple tasks simultaneously. Experimental results demonstrate accurate threat detection, immediate local alerts, and timely remote notifications through Telegram. The proposed system is cost-effective, scalable, and reduces dependence on continuous human surveillance, making it suitable for residential, commercial, and institutional security applications

The proposed system provides a strong foundation for further enhancement and expansion. Future work can focus on integrating advanced machine learning or deep learning models, such as convolutional neural networks, to improve image-based threat detection accuracy and reduce false positives. Additional sensors, including motion, gas, vibration, or smoke sensors, can be incorporated to enable multi-layered security and safety monitoring. Cloud integration can be implemented for data storage, event logging, and analytics, allowing long-term monitoring and trend analysis. The system can also be extended with a dedicated mobile application for improved user interaction, remote control, and real-time visualization. Furthermore, integration with automated response mechanisms such as smart locks, sprinklers, or emergency lighting can transform the system into a fully autonomous smart security solution..

REFERENCES

1. Raspberry Pi User Guide – Eben Upton, Gareth Halfacree, 4th Edition, Wiley, 2016.
   - Reference for Raspberry Pi hardware setup, GPIO pin usage, and interfacing with sensors.
2. Python Programming for Raspberry Pi – Richard Blum, 2nd Edition, Pearson, 2015.
   - Provided guidance on Python programming, multithreading, and hardware interfacing.
3. Learning OpenCV 3: Computer Vision in C++ with the OpenCV Library – Adrian Kaehler, Gary Bradski, 3rd Edition, O'Reilly Media, 2016.
   - Used for understanding image processing and handling images in Python with OpenCV.
4. S. P. Kaur, "IoT Based Smart Security System Using Raspberry Pi," International Journal of Engineering Research & Technology, vol. 8, no. 4, 2019.
   - Reference for IoT-based monitoring and integration of Raspberry Pi with sensors.
5. A. Sharma, R. Kumar, "Real-Time Security System Using Image Processing and IoT," International Journal of Advanced Research in Computer Science, vol. 10, 2019.
   - Guided the implementation of image-based threat detection and real-time alerts.
6. Raspberry Pi Documentation: https://www.raspberrypi.org/documentation/
   - For GPIO setup, Python libraries, and sensor interfacing tutorials.
7. PyTelegramBotAPI Documentation: https://github.com/eternnoir/pyTelegramBotAPI
   - Reference for integrating Telegram messaging into the Python application.
8. Tkinter Python Documentation: https://docs.python.org/3/library/tkinter.html
   - For GUI design, widgets, and event handling.
9. OpenCV Python Documentation: https://opencv.org/
   - For image reading, encoding, and processing in Python.
10. PIL/Pillow Documentation: https://pillow.readthedocs.io/en/stable/
11. "Raspberry Pi Security System Using Python," Electronics Hub, https://www.electronicshub.org/raspberry-pi-security-system/
    - Practical tutorial for setting up sensors, alarms, and Python code integration.
12. "IoT Based Smart Home Security System Using Raspberry Pi," Circuit Digest, https://circuitdigest.com/microcontroller-projects/iot-smart-home-security-system
    - Guidance for connecting sensors and implementing real-time alerts.
13. Python 3.x – https://www.python.org/
    - Programming language used for the entire software implementation.
14. RPi.GPIO Library – https://pypi.org/project/RPi.GPIO/
    - Python library for Raspberry Pi GPIO pin control.
15. Threading Module – Python Standard Library https://docs.python.org/3/library/threading.html
    - Used to enable parallel sensor monitoring and GUI operations.
16. Telegram API – https://core.telegram.org/bots/api