iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50230

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Intruder Alert System

Soniya Komal V[1], Sayyida Kaunain[2], Sheefa Naaz[3], Indrakumar M[4], Irfan Mohammed[5]
[1]*Assistant Professor, Department of CSE, Rajiv Gandhi Institute of Technology, Visvesvaraya Technological University, Bangalore, India*
[2, 3, 4, 5]*UG Students, Department of CSE, Rajiv Gandhi Institute of Technology, Visvesvaraya Technological University, Bangalore, India*

Abstract: ***In this paper, we present an intruder alert system that detects and classifies potential intruders in a given environment using computer vision and machine learning. A network of cameras and a central processing unit run an object detection algorithm and a machine learning classifier in the system. This project was designed and built with an Arduino mega microcontroller, system connected to a GSM module with SIM (subscriber identification module) from a network provider (LDR) sensor which is used in this project is connected to a microcontroller unit, GSM module, and other electronic devices which thus detect any intruder in a classified area, activates the alarm system, and sends text message notifications to the house owner specifying the location and time of intrusion to the house owner's programmed phone number. The design worked in real-time in an area with good network coverage, as expected, according to preliminary testing. It has a wide range of applications in surveillance, particularly in industrial and home security, where internet connectivity is unavailable. The findings demonstrate that the system is capable of accurately identifying and categorizing possible intruders with low rates of false positives.***
Keywords: Machine learning, Object detection Algorithm, Microcontroller, GSM module, Surveillance

I. INTRODUCTION

Intruder alarm systems are an important tool for ensuring the safety and security of people and property. The concept of an integrated home security system is an important implementation to aid in the security of our family and home. When we examine various home automation systems over time, we can see that they have always attempted to provide home residents with dependable and secure methods of accessing their homes. On the other side, IoT is emerging today with a slew of apps in different sectors, including the security and surveillance industry. IoT technology may enhance home security by providing real-time monitoring, remote control, and security system automation. With the increasing availability of low-cost IoT devices, smart home security systems have become increasingly common and affordable to homeowners. Our system uses IoT devices like sensors, cameras, and smart locks to provide enhanced security features that traditional home security systems lack. This research aims to design and implement a low-cost intruder detector system with a connected mobile application using a similar approach but different control units and sensors.

Here are some of the objectives of the project:

1) Its goal is to detect if any unwanted strangers are following authorised personnel, effectively preventing intruders from circumventing the entrance security system.
2) To address the issue of inadequate home security by providing a direct method of improving it.
3) To use object detection to identify anyone standing outside the door.
4) To then notify the owner whether or not the person ringing the bell has authorised access.
5) Using a camera, provide visuals of who is at the door.
6) To send all of the aforementioned information to the user via a mobile application.
7) To give the user the ability to open the door if he or she recognises the person.

II. LITERATURE SURVEY

An intruder alert system is a device that detects unauthorised entry into a secure area and alerts the appropriate personnel. A literature review on intruder alert systems reveals that several studies have been conducted on the design, development, and implementation of these systems. The following is a synopsis of some of the research papers published in this field:

1) The design and implementation of a wireless intruder alert system using ZigBee technology were presented in 2017. A control unit, sensors, and a wireless communication network make up the system. The findings demonstrate the system's capacity to identify intrusions and notify the necessary personnel.

2) The performance of various types of intruder alert systems, such as acoustic sensors, infrared sensors, and motion sensors, is compared in one of the research paper that was published in the 2018 International Conference on Computing, Electronics, and Communications Engineering (iCCECE). According to the study, the motion sensor-based system was the most effective at detecting intruders.
3) The development of an intruder alert system using Arduino and a GSM module was described in a research paper in 2019. The International Journal of Electrical and Computer Engineering (IJECE) published it. A sensor module, a control unit, and a GSM module comprise the system. The results demonstrate that the system is capable of detecting intruders and sending SMS alerts to the appropriate personnel.
4) Intruder detection system employing computer vision and deep learning methods is proposed in another paper in 2020. A camera module and a deep learning algorithm make up the system. The outcomes demonstrate that the system is capable of real-time, accurate intruder detection.
5) The concept and implementation of an intruder alert system utilising a Raspberry Pi are presented in one of the recent papers in 2021. This was published in the Journal of Control, Automation, and Electrical Systems.

The system is made up of a Raspberry Pi, a control unit, and a sensor module. The findings demonstrate that the system is capable of identifying intruders and notifying the necessary individuals.

Overall, the literature review indicates that intruder alert systems are a popular subject for research, with the several approaches to developing and executing these systems. While the specific technologies and techniques implemented may differ, the end objective will be to develop an effective and dependable system for detecting and alerting personnel of unauthorised access into a protected area.

III.METHODOLOGY

There are several modules that's describe the overall working of the project. These sections provide detailed step-by-step explanations of the entire process from beginning to end.

A. Object detection

This module employs cameras and machine learning algorithms to recognise and track objects in a given environment. Object detection is a computer vision technique that involves recognising and addressing objects in an image or video using a bounding box. Several steps are involved in the process - Image pre-processing, Feature extraction, Object proposal generation, Object localization.

1) Image Pre-processing: To improve image quality and reduce noise, the input image is pre-processed. Resizing, normalisation, and filtering are examples of such operations.
2) Feature Extraction: The pre-processed image is then examined in order to extract relevant features that can aid in the identification of objects in the image. Texture, colour, shape, and edge information can all be included.
3) Object Proposal Generation: Identifying potential object locations in an image based on extracted features is what object proposal generation is all about. This step may entail creating a set of bounding boxes that encompass potential object locations.
4) This is the final step in which the object detection results are refined and false positives are removed. Non-maximum suppression, which removes overlapping bounding boxes and keeps only the one with the highest confidence score, is one example.

B. Arduino Board

The goals of this module include storing the code and sending signals to the Wi-Fi stage. The Arduino board also reads signals from the camera. The Arduino board is made up of a physical programmable circuit board (also known as a microcontroller) and a piece of software, or IDE (Integrated Development Environment). Arduino operates in a very straightforward manner. It accomplishes its mission through the use of three principal sections: Inputs, Programming and Outputs.

1) Sensors and switches are connected to the controller to provide data. These are known as inputs, and they can be anything from on/off signals to variable voltage* signals or communication from another controller.
2) Programming: The board is programmed to take in information and make decisions based on it.
3) Finally, an output is the signal that the Arduino sends to a component. The output, like the input, can be an on/off, variable voltage*, or communication signal.

C. Relay Module

An Arduino is also linked to a relay driver circuit, which controls the electromagnetic door lock. A relay is a type of electrical switch. It is made up of an input terminal for a single or multiple control signals and an operating contact terminal. The switch may have an unlimited number of contacts in various contact forms, such as make contacts, break contacts, or combinations of the two.
After receiving electric signals, the relay module circuit does so. A relay driver circuit is a circuit that can drive, or manage, a relay so that it can function appropriately in a circuit. The driven relay can then function as a switch in the circuit, opening and closing according to the needs of the circuit. Relays are electrically operated switches that open and close circuits in response to electrical signals received from outside sources. The "relays" embedded in electrical products function similarly; they receive an electrical signal and send it to other equipment by switching on and off.

D. Working of the electromagnetic door

The Electromagnetic door is linked to the Wi-Fi network and can be accessed using a smartphone app.
The electromagnetic door is controlled by the relay driver circuit. It is programmed to lock and unlock a door when it receives a prompt from a registered mobile device via an electronic keypad, biometric sensor, access card, Bluetooth, or Wi-Fi. As an electronic device, the smart lock requires a power supply in the form of a battery. As a result, your lock will have a small, hidden battery compartment.
The electronic components in a smart lock will allow it to connect to your home internet via Bluetooth, Wi-Fi, or ZWave. This is what allows you to unlock the lock remotely using an internet-connected smart device.
Smart locks, like all locks, use a lock and a key. However, the key in this case is digital rather than physical. The key could be a keypad code or a command sent from a smartphone app.

E. UART and WI-FI

To update the entire data set via Wi-Fi, we use a UART Transmitter-Receiver. The TCP/IP protocol is linked to the controller via the cloud. Wi-Fi modules are part of the IoT transmission layer. Traditional hardware devices with embedded WIFI modules can connect to the Internet directly via WIFI, which is an important part of realising wireless smart home, M2M, and other IoT applications. One of the most common device-to-device communication protocols is UART, which stands for universal asynchronous receiver-transmitter.
The ability of traditional hardware devices with embedded Wi-Fi modules to connect directly to the Internet via Wi-Fi is crucial for the development of wireless smart home, M2M, and other Internet of Things (IoT) applications. Wi-Fi has played a crucial part in bringing IoT innovation to market by providing ubiquitous connectivity to link a variety of "things" to one another, the internet, and the 18 billion Wi-Fi devices already in use worldwide.

IV. PROPOSED ARCHITECTURE

The below figure represents the system architecture of our project. The architecture consists of a camera module, finger-print sensor module, Arduino Uno board, a database, relay driver circuit, the internet module, a remote control unit and an electromagnetic door. The data from the sensors is continually processed by the microcontroller and an alert is sent to the mobile station if something is sensed or something reaches beyond the limit of proximity.

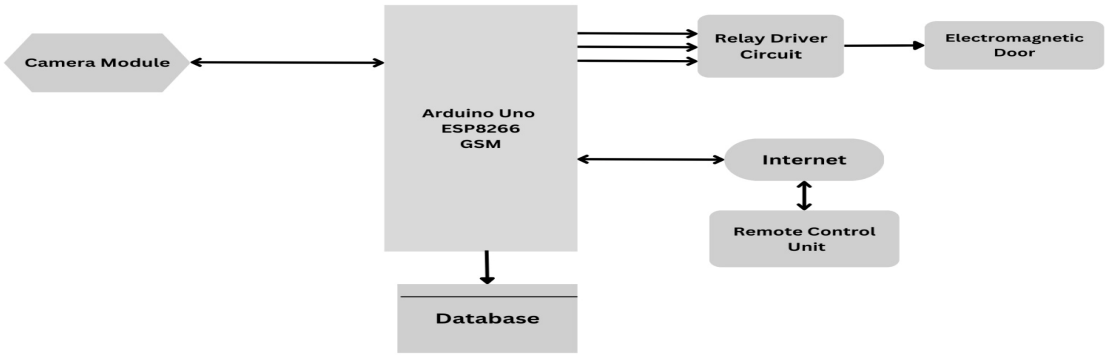


Fig. 1 System Architecture

The following elements are included in the architecture:

1) Sensors: These are the devices that detect intruders. Intruder alert systems employ a variety of sensors, including motion sensors, infrared sensors, acoustic sensors, and magnetic sensors.

2) Control Unit: This is the intruder alert system's central processing unit, which receives signals from sensors and processes them to determine whether or not an intruder is present. When an intruder is detected, the control unit is responsible for sending alerts to the appropriate personnel.

3) The communication network is used to deliver alerts from the control unit to the appropriate personnel. Depending on how the intruder alert system is implemented, this could be a wired or wireless network.

4) The power supply is used to provide power to the various components of the intruder alert system. Depending on the implementation, this could include batteries, power outlets, or solar panels.

5) A database is included to store the necessary details. These details can be accessed by the authenticated people if and when required.

6) Electromagnetic door: The door is connected to the smartphone application through Wi-Fi and can be controlled from there.

V. CONCLUSIONS

The paper describes a low-cost intruder alarm system that uses computer vision and machine learning to detect and categorizes possible invaders. A network of cameras and a central processing unit operate an object identification algorithm and a machine learning classifier in the system. When an intruder is detected in a classified area, the system activates the alarm system and sends information to the mobile application. The system employs Internet of Things (IoT) devices such as sensors, cameras, and smart locks to give increased protection features that standard home security systems lack. The research indicates that the system is capable of identifying and categorizing potential invaders with low false positive rates. Our work focuses primarily on the application elements of the various intruder systems, as well as the various technologies involved in making the intruder detection system practicable for real-world application. We reviewed the many systems that make use of low-cost components that have the potential to be industry standard. We encourage researchers to consider home automation as one of the most important parts of home security, as well as to create advanced sensing technologies to detect and secure homes from professional burglars. The most critical component in the proper deployment and production of automated home defense systems is security. A system like this will provide everyone in the house with a sense of protection while also putting their minds at ease.

REFERENCES

[1] G. Vakulya and G. Simon, ”Low power accelerometer based intrusion and tamper detector,” 2014 IEEE 11th International Multi-Conference on Systems, Signals Devices (SSD14), Barcelona, Spain, 2014

[2] S. S. Ravi, S. Usha, and R. Geetha, "A Review of Intrusion Detection Systems," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 639-646, 2014.

[3] R. Mohan, "Design and Implementation of a Low-Cost Home Security System," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 6, pp. 213-217, 2017.

[4] S. Saha and A. Saha, "An intelligent intrusion detection and alert system for smart homes," Journal of Ambient Intelligence and Humanized Computing, vol. 9, pp. 2277-2286, 2018.

[5] K. Ananthapadmanaban, P. Vinay Kumar Reddy, and M. K. N. Yenugu, "An Intruder Detection and Alert System using Raspberry Pi and PIR Sensor," IEEE International Conference on Smart Technologies for Smart Nation (SmartTechCon), 2019.

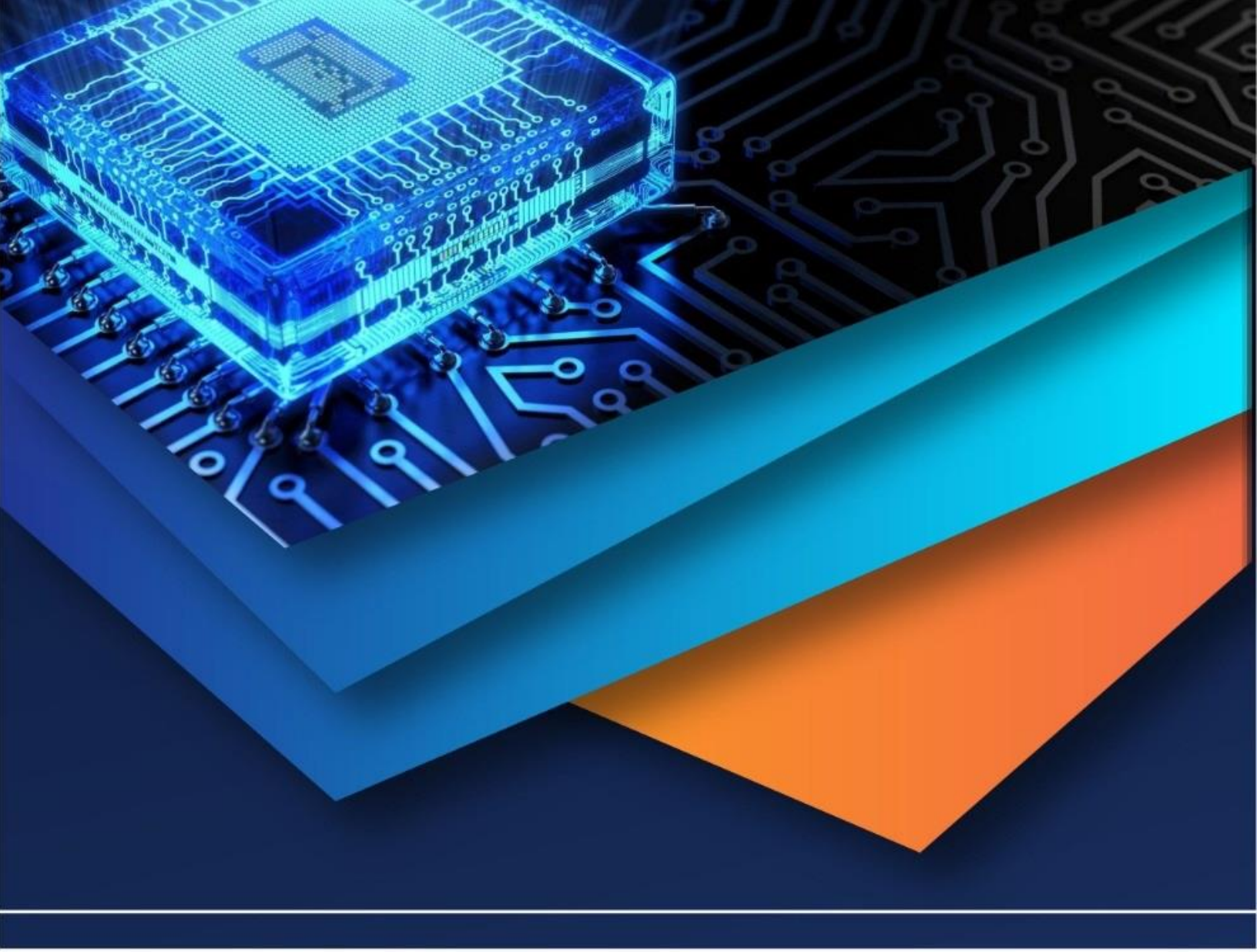
[6] Iyer Saikumar, Gaonkar Pranjal, Wadekar Shweta, Kohmaria Nayan and Upadhyay Prashant, IoT based Intruder Detection System Using GSM (April 8, 2020). Proceedings of the 3rd International Conference on Advances in Science Technology (ICAST) 2020, Available at SSRN

[7] M. A. M. Ali, A. H. Shah, and S. H. Ahmed, "Smart Home Intrusion Detection and Alert System using Machine Learning Techniques," IEEE International Conference on Control, Automation, Robotics and Vision (ICARCV), 2020.

[8] L. Liu, W. Ouyang, X. Wang, P. Fieguth, and J. Chen, ‘‘Deep learning for generic object detection: A survey,’’ Int. J. Comput. Vis., vol. 128, no. 2, pp. 261–318, Jan. 2020.

[9] Y. Wu, ‘‘Cloud-edge orchestration for the Internet of Things: Architecture and ai-powered data processing,’’ IEEE Internet Things J., early access, Aug. 7, 2021

[10] "Deep Learning Based Intruder Alert System for Smart Homes" Authors: S. R. Ali, S. A. Siddiqui, S. K. Singh, A. Sharma, and S. S. Islam,Published: 2022, IEEE Access, vol. 10, pp.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY