International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.9 May - June – 2025
DOI:10.46647/ijetms.2025.v09i03.015 ISSN: 2581-4621

Intrusion Detection for Smart Home Alarm Security System

MS. Mamatha[1], P. Aakash[2], N. Sravya[3], P. Sneha sree[4], V. Shiva Prasad[5]
[1]*Assistant Professor, Department of CSE, HITAM, Hyderabad, India*
[2]*Student of Computer Science and Engineering, HITAM, Hyderabad, India*

Abstract**—** Smart home security is increasingly essential in today's world due to rising concerns over unauthorized access and property intrusion. Leveraging the capabilities of Raspberry Pi, a low-cost and efficient home security system is developed that combines motion detection, real-time image capture, SMS and email alerts, and automated door locking. The system uses OpenCV for motion tracking, a GSM module for text notifications, and a buzzer for local alarms, all integrated through Python scripts. A voltage regulator and backup battery ensure uninterrupted functionality during power outages. Testing showed over 90% accuracy in intrusion detection and prompt alert delivery within seconds. The solution is both scalable and affordable, bridging the gap between high-cost commercial systems and the growing need for smart, userfriendly home protection. Future improvements include AIbased facial recognition, cloud storage, mobile app integration, and support for multiple surveillance nodes.

Keywords**—** *Home Security, Raspberry Pi, Raspberry Pi Camera, GSM Module, DC Motor, L293D Motor Driver, LM2596 Voltage Regulator.*

I. INTRODUCTION

Home security is one aspect of preventing and protecting occupants' belongings and themselves. This increasing rate of burglary cases and breaking into one's house leaves them with more reasons to emphasize implementing a home security system. However, such commercial home security systems are pretty pricey for most homes. This challenge is partly helped by these advances in technology that offer opportunities to come up with cost-effective and efficient home security for modern households. It discusses the development of a low-cost yet efficient home security system using the versatile minicomputer device, the Raspberry Pi. Among the taken components is the Raspberry Pi Camera that offers image capture, a GSM module for SMS alerts, a DC motor with an L293D motor driver for an automated locking mechanism, and a stable power supply via an LM2596 voltage regulator and a backup battery to ensure constant running.

Its main essence is to capture images at the doorstep by intruders and prompt the homeowners through email and SMS. A buzzer has also been included to alert nearby neighbors of any suspicious activity. These added features, ensure that there would be real-time monitoring and actual physical security control mechanisms. Thus, this system does offer an alternative means, especially one that is low in cost compared to high-price commercial products. By using low-cost technology, the approach creates a robust and accessible security solution for homes, showing them how their properties can indeed be kept secure and safe. Below are system design, implementation, and functionality discussions in the subsequent sections of this paper that show it indeed is a feasible and scalable home security application.

II. LITERATURE REVIEW

Now in this related work part, we will discuss some work that has been done in this field.

The authors in their paper [1] proposes an IoT-based integrated home security and monitoring system that enhances safety for people whose daily lives are mostly spent away from home. The system integrates Arduino Nano and NodeMCU ESP8266 as controllers, linking different sensors and actuators for multiple safety concerns. Security is guaranteed through an RFID reader and numerical codes to access the doors, while email notifications ensure users are well-informed of all activities taking place within their home compound. It uses a PIR sensor for intruder detection, DHT22 for measuring temperature and humidity, a rain sensor for rain detection, a fire sensor for stove activity monitoring, and an LDR sensor for assessing the light conditions. It also includes actuators, such as light bulbs and solenoid valves, and can control them from a remote location. Instead, users would interact with the system through a connected smartphone app that uses the internet for realtime monitoring and control. This study offers further improvement upon previous research efforts, deploying layered security and incorporating a diversity of sensors and actuators into it, abating other limitations such as dependency on local networks or delayed notifications, thus producing a more robust and responsive system.

The authors in their paper [2] This article gives a sound review of IDSs designed for IoT-based smart environments, to promote an awareness of the necessity of security and privacy concerns in applications such as smart cities, homes, and healthcare. The paradigm of the Internet of Things depicts a connection of devices that can sense and exchange data, improving human life by enhancing comfort and efficiency. However, IoT systems are very susceptible to security threats from DoS and DDoS attacks, which could lead to the disruption of critical services. Conventional IDSs are not always suitable for IoT environments because of the limited processing power and storage capacity of IoT devices as well as the unique protocols they use, such as 6LoWPAN. This paper examines IoT systems, different types of IDS, and their characteristics, with significant attention to important factors such as detection efficiency, response time, energy consumption, and performance overhead. Here it points out the limitations of the existing solutions and dwells upon light-weighted, real-time, and adaptive IDS for IoTspecific challenges. The research makes several significant contributions, such as identifying transferable features from traditional IDSs to IoT, analysis of security vulnerabilities in the layers of the architecture of IoT, and recommendations for designing robust IDSs for IoT environments. In the final column, the paper presents a future perspective for the development of IDS, stressing the importance of securing IoT-based smart environments against emerging threats.

The authors of the papers [3] aims to design and implement systems with human detection capabilities to complement limited home security solutions such as traditional CCTV. These CCTV systems, although they can record video, cannot at any given time alert or notify a person about suspicious activities happening. To overcome these drawbacks, the proposed system integrates the technology of the Internet of Things using a Raspberry Pi 3 and Arduino, connected by a USB cable. It uses a PIR motion sensor connected to an Arduino to detect movement and activate the webcam mounted on the Raspberry Pi. The system makes use of Histogram of Oriented Gradients (HOG) and Support Vector Machine (SVM) algorithms for intruder detection purposes in object detection. When a suspicious object is detected, an alarm is triggered and an email alert is sent to the homeowner. The evaluation shows a detection accuracy of 90% and identifies intruders in an average of 2 seconds. Unlike traditional CCTV systems that consume significant bandwidth and storage due to continuous streaming, this system optimizes resources by only capturing and analyzing data when motion is detected. The study highlights the effectiveness of IoT-based home security systems for real-time monitoring and protection, combining motion detection and image recognition to enhance home safety. It also brings in an extended discussion about the HOG method and additional experiments with a detailed evaluation of the system's performance regarding both accuracy and response time.

The authors in their paper [4] elucidates why IoT technology is essential in the improvement of smart homes and smart cities' security and automation. The paper goes further to explain the application of IoT to monitor and track different appliances at home, improve security, as well as provide better privacy and management of energy. Reviews were done based on these studies regarding smart home security using IoT, which focused on platforms, applications, communication protocols, and hardware or software tools. It would emphasize the crucial role that IoT devices like sensor units and small computing units, called Raspberry Pi, play in smart home security, as they can detect movement, control appliances, and alert users in real-time. Such home-monitoring systems, based on IoT, allow the residents of a house to check their homes remotely and thus prevent theft, fires, and other incidents. Furthermore, the work addresses resource-limited sensor device issues such as storage, battery, and processing power, yet still promises effective security results. It also explores the implementation of WSNs in IoTbased systems and its application in smart homes to monitor constant temperature and humidity conditions. With continuously increasing demand for enhanced security, privacy, and energy efficiency in modern living spaces, the application of IoT in smart homes is viewed as the ultimate response. Finally, the paper concludes by discussing how IoT plays a vital role in shaping the future of smart home security systems.

The authors in their paper [5] discusses the emerging security issues related to Smart Home devices, which are increasingly subject to cyberattacks, including botnets of the type Mirai or Reaper. With everyday appliances, like TVs, fridges, and doorbells, becoming "smart" every day, securing private user-operated Smart Homes without IT security knowledge becomes a key issue. The authors discuss how to include an IDS within Smart Homes to detect and counter network violations. However, the application of IDS in Smart Homes faces non-technical problems, like the complexity for private users in configuring and managing the system, as well as the problem of distinguishing between a false alarm and an actual threat. Moreover, constant monitoring by external security experts is expensive and infringes on the privacy of people. The paper considers how the IDS approaches, for example, anomaly-detecting and signature-detecting systems, can be adapted to fit into Smart Homes. Experiments carried out showed that signature-detecting IDS generates fewer false alarms. The authors suggest alterations of adapting system design: it is about breaking up networks, and security processes, in particular, to make it accessible and effective for private users with the preserved privacy.

The authors in their paper [6] designed to improve home security through motion detection and image capture of intruders who break into the house. Its focus is on eliminating false alarms and sending alerts to people through WhatsApp, one of the most accessible methods of communication. The IDS uses a PIR sensor to detect motion and a Raspberry Pi camera to capture images of potential intruders. It is useful for homeowners who often are away or too busy to keep a constant eye on their property. It gives them peace of mind and allows them to take swift action in case of an intrusion. The study shows that the system has reduced false alarms and made smart homes more secure.

The authors in their paper [7] presents a home security alarm system in the form of WEMOS D1 with an HC-SR501 sensor, incorporating Telegram notifications, to help monitor owner's property. It operates by detecting movement through PIR sensors and a buzzing alarm in case movement is detected. The system automatically sends a notification to the owner's Telegram app such that when they are away, they know if someone is entering their house. This research highlighted the increasing cases of home burglars, especially when the owner is not home. It compared the proposed system with other smart home security solutions and emphasized that by using Telegram, which will send real-time alerts. The study further shows that it is possible to track homes using such a system and alert owners in the case of a break-in. This makes home security easy to use and affordable.

The authors in their paper [8] proposes an IoT-based intruder detection system called Smart-IDS, designed for private and restricted areas to enhance security. The system uses a Node MCU microcontroller and an Ultrasonic sensor to detect intruders. When the system detects an intruder, it sends an alert notification to the owner's mobile phone via the cloud-based Blynk application. This system is supposed to offer automated security where human resources are not required, thus lowering the chance of theft or unauthorized entry into private areas. The paper points out that there has been a growing security concern, especially in private property and small localities where classical forms of security, such as security guard services, have not been effective. The integration of IoT technology into home security systems provides more reliable and efficient solutions for the detection of intruders and real-time notifications to homeowners. It is an easy-to-implement system that does not necessitate continuous monitoring by personnel. In turn, this paper discusses several related works, the advantages of using IoT for security purposes, and a description of the design of the proposed Smart-IDS.

The authors in their paper [9] presents a Hybrid Intrusion Detection (HID) system that can contribute towards improving the security capabilities of a smart home by employing machine learning algorithms and misuse detection techniques. Smart homes are nowadays gaining popularity and connecting lighting, appliances, and security cameras to the internet without realizing their growing vulnerability to cyberattacks that may breach privacy, steal personal information, or compromise security. A two-tiered approach to intrusion detection will be used by this proposed HID system: the first tier-based machine learning algorithms such as random forest, Xgboost, and decision tree to detect anomalies in network traffic, while the second tier examines requests based on patterns of user behavior for more accuracy and security. This system does not rely on predefined rules for the Intrusion Detection System, but rather, it adapts and identifies new previously unseen threats, unlike traditional IDS. The machine learning application within the HID system will help smart homes predict and defend against potential intrusions better, providing more robust protection to users of an increasingly connected world.

The authors in their paper [10] describes the design and building of a GSM-based intelligent home security system and its limitations like direct real-time surveillance and intrusion control such as human intrusion, fire, smoke, gas leakage, etc. The different sensorspressure, smoke/fire gas, and motion PIR sensors, are used to detect any intrusion, and sensor data is processed by a programmable microcontroller and dispatched as alerts. Such a system will take advantage of a GSM modem for sending SMS alerts to the homeowners' cell phones when an intrusion is noted. The system can monitor various sorts of intrusions and sends notifications to clients immediately through the GSM network whenever a sensor notices the presence of something dangerous. This gives homeowners enough time to act before losing property or getting hurt. It has become part of the more immense trend in home automation through combining wireless technologies and digital systems for more secure and efficient living environments. The GSM-based system provides remote monitoring and control and, therefore, enhances home security through automated responses and SMS alerts. This design is effective mainly in places not easily accessible to traditional wired security systems, thus making it adaptable for a wide range of settings. Apart from this, the study also shows the changes the smart home security system has undergone; user authentication and monitoring from a distance becomes necessary to prevent unauthorized access and detect illegal activity.

The authors in their paper [11] addresses the increasing cybersecurity risks in Smart Homes (SH), which rely heavily on resource-constrained Internet of Things (IoT) devices often developed with a focus on functionality rather than security. This oversight leaves SH systems vulnerable to cyberattacks. To tackle this, the authors propose a Network-Based Intrusion Detection System (NIDS) tailored for SH environments. The system employs machine learning (ML) algorithms to identify anomalies in the Home Area Network (HAN) by detecting deviations in network behavior resulting from unauthorized or malicious commands. The core of the proposed method termed the User-Command-Chain (UCC), leverages the time, location, and payload of user commands to distinguish legitimate activity from potential intrusions, as attackers' commands typically deviate in these parameters. A simulated SH environment was used to evaluate the UCC-based model against three types of network attacks. The results demonstrated that the approach significantly improves detection accuracy and efficiency. The contributions of the study include the development of the UCC method for preprocessing network data, the creation of a realistic test-bed environment for capturing traffic data, and the demonstration of UCC's effectiveness in improving anomaly detection. This work provides a robust foundation for enhancing the security of SH systems and offers a practical solution for real-world implementation.

The authors in their paper [12] explores technological development in home automation smart security systems that include phonebased, Java-based, GSM-based, and Bluetooth-based approaches. Starting from Wong's invention in 1994 of a phone-based remote control system, this paper traces the development and advancements through such significant contributions as Java-based systems in the year 2004, GSM-based solutions in the year 2013, and Bluetoothbased approaches developed in 2002. These technologies provide a basic understanding of the development of smart security architectures. The paper underscores security critical challenges while highlighting unauthorized access, data breaches, and networking vulnerabilities as needing to be robustly protected in intelligent systems. It evaluates these comparative analyses on parameters such as efficiency, scalability, and security to outline the strengths and weaknesses of each approach. The future of smart security is envisioned with the role of IoT, machine learning, and artificial intelligence to make more resilient systems. The study, through this exploration, sheds light on the evolution of smart security systems and places on record a roadmap toward a secure, technologically advanced future in home automation.

The authors in their paper [13] reviews developments in home automation systems driven by the Internet of Things (IoT), where devices such as vehicles and home appliances are linked and communicate with each other seamlessly. Automation is explained to be performing a task with little human work. Five approaches are used to analyze: a symmetric encryption-based system, IoT-enabled appliances with sensors, low-cost Wi-Fi-based automation, and web-enabled monitoring and controlling of appliances. While each of the methods has its benefits, still mentioned are the challenges such as security vulnerability and inefficiency. Aiming to make the systems smarter, more secure, and more efficient, this paper proposes a new IoT-based home automation technique targeted at addressing these issues.

The authors in their paper [14] addresses the rising relevance of IoT and accompanying security threats. IoT connects different devices, thereby providing more advanced applications such as smart cities, homes, healthcare, and industries through M2M communication. However, IoT suffers greatly in terms of its cybersecurity threats, like DoS and MITM attacks, which can compromise devices and infrastructure. To address these issues, this paper discovers the role of IDS in observing and alerting potential threats in IoT networks. This paper suggests a software-defined IDS integrated with a distributed cloud architecture that provides enhanced detection accuracy and network stability over traditional methods. Analysis of IoT vulnerabilities, security challenges, and the attack surface comprised the contents of this study and are known to be very detailed for IDS in the context of IoT environments. Experimental results demonstrate the effectiveness of the proposed system in enhancing IoT security. Indeed, this research is part of efforts to improve IoT security while offering insights and recommendations for addressing future cybersecurity challenges.

The authors in their paper [15] proposes an intelligent smart home automation system using IoT and a deep learning-based CNN model to enhance security and convenience. The system monitors environmental conditions, controls appliances, and classifies human motion patterns to distinguish between occupants and intruders, reducing false alarms. It uses cost-effective IoT hardware and an Android app for real-time monitoring and control. The CNN model obtained a 99.8% accuracy rate in intruder detection with better security, energy use, and user comfort. The system is a good practical solution for smart home security and automation.

The authors in their paper [16] designed with an Arduino Uno and an ultrasonic sensor interfaced with a GSM module in an IoT framework. It detects intruders in real-time and can send SMS alerts to homeowners. It is programmed through the Arduino IDE to provide efficient monitoring and security by automatically detecting and sending notifications. This IoT-based solution offers a modern, cost-effective, and reliable alternative to traditional security methods, enhancing safety and convenience in smart homes.

The authors in their paper [17] designed with the help of a SIM900 module and sensors and focuses on the creation of an SMS-based intruder detection system for smart homes. Unlike the traditional alarm systems utilizing magnetic switches, this system utilizes motion detectors (PIR sensors) and door switches, so that upon every detection of motion or door switch event, it shows the indication on an LCD screen and gives out an SMS alert to the homeowner. The activities above are coordinated by programming in C into the microcontroller. The system exploits the GSM network to control remotely and alert homeowners to incursions or movement in restricted areas. It can detect heat, motion, and intrusions, triggering an alarm when limits are exceeded. However, the functionality of the system goes with the availability of the GSM network. This modern concept improves home security by improving the drawbacks of traditional systems including the trend of becoming smarter and remotely controlled, therefore finding its way into a busy lifestyle.

The authors in their paper [18] design a GSM-based intrusion detection system using an ATmega8 microcontroller, LDR and PIR sensors, and a SIM900A module. It detects motion or changes in light, triggers an alarm, and sends SMS alerts to a phone belonging to the homeowner with an indication of the time and location of the intrusion. It works off a 9V DC power source, operates efficiently without the need for internet access or special mobile apps, and is accordingly ideal for enhancing security in homes and industrial premises or offices.

The authors in their paper [19] analyzes the CICIDS2017 dataset, the largest source of data for IDS assessment which has current attack scenarios but also some deficiencies that might impact the IDS performance. Some of them are too large, spanning eight files, redundant data, and having class imbalance, which gives a possible bias towards classifiers. The paper raises these issues and discusses potential solutions that consist of reducing class imbalance and reset labeling. It also contributes a purified subset of CICIDS2017 for future research and development about IDS models to increase the accuracy and effectiveness of detection.

The authors in their paper [20] This is a study into the challenges posed by intrusion detection in IoT networks: they have size and energy limits, which creates a problem with security and privacy. Traditional methods for intrusion detection often fail in multiattacks or high-dimensional IoT network data. The paper proposes a multi-deep learning model that improves the accuracy of intrusion detection. It uses AlexNet to extract initial features, selects the necessary features with bidirectional LSTM, and utilizes classification by the C5.0 decision tree algorithm. When tested on the NSL-KDD dataset, the model achieved detection accuracy at 98.8%, an improvement of 15% over the DeepNet and CNN-based methods.

The authors in their paper [21] proposes a low-cost architecture for an IoT-enabled smart home security system; within that, the main focus of this work is on a smart door sensor. The proposed system uses an Elegoo Mega 2560-based microcontroller and a Raspberry Pi 2 for communication with the web server, and it implements a RESTful API web server. The smart door sensor sends door-open event notifications from a home or office to its users through an Android application. The architecture forms part of a much larger trend in IoT: affordable smartphones and open-source hardware will increasingly underpin low-cost automation and security solutions. Although many benefits of the system - like remote monitoring and control - are achieved, the paper continues to explore challenges, such as potential interference caused by adjacent radio frequency devices. More broadly, IoT will be considered in its applications for healthcare, smart cities, and smart vehicles.

The authors in their paper [22] proposes a dynamic security framework known as SHIELD to ensure smart homes, addressing the growing security challenges brought about by IoT devices in home environments. It suggests adaptive security of the smart home network based on perceived risk or "network sentiment," with the propensity to evolve using user cooperation. SHIELD deploys distributed firewalls and Intrusion Detection Systems (IDS) at both the end-user premises and the Internet Service Provider (ISP) side. This allows it to respond dynamically to emerging threats in real time. The framework thereby enables the propagation of security updates to neighboring smart home networks for an actual time Intrusion Prevention System (IPS). The paper calls for a more flexible, reactive security approach rather than static, traditional security measures that might be too cumbersome or inadequate. A testbed for smart home security is also presented to show the practicality of SHIELD in real-world environments.

The authors in their paper [23] proposes a low-cost home security system utilizing the Internet of Things (IoT) technology, which integrates a Raspberry Pi, a web camera, and a PIR motion sensor. During the detection of movement across the door, the camera captures an image of the intruder, and a buzzer alerts the neighbors. The captured image is then sent to the homeowner's email via the Raspberry Pi's Wi-Fi, allowing the homeowner to view the image remotely and ensure the security of the house in their absence. The system provides a solution for preventing burglaries at an affordable price, and the homeowner can control access to the door through their smartphone. It makes houses safer and more secure with IoT technology in a simple yet efficient manner without requiring deep and complex systems or constant database maintenance.

The authors in their paper [24] seeks to present a GSM-based intelligent home security system to monitor and control intrusions, such as unauthorized access, fire, smoke, and gas leakage, in realtime. The system consists of pressure sensors, smoke/fire sensors, gas sensors, and PIR motion detectors, all connected to a microcontroller programmed in C++. When anomaly detection is detected, such as an intruder, gas leak, or temperature change, the microcontroller triggers an alarm and sends an SMS alert to the homeowner via GSM. The whole system enables remote monitoring and immediate notification of security breaches for extra safety of the house. The system is made accessible even with GSM technology and can be used in remote areas, making home security very simple and effective.

The authors in their paper [25] the development of a low-cost, effective access control system is presented that integrates a radio frequency identification tag with an electromagnetic lock and a GSM module. It uses an ATMEGA328 microcontroller to control an RFID reader that checks the identity of a user by scanning unique tags. If a valid tag is identified, the system unlocks an electromagnetic door lock. An invalid tag will be sent an alert to the administrator by a mobile call from the GSM module. It also hosts a liquid crystal display, LCD for user feedback, and buzzer for alerts. The door automatically locks on a 5-second delay. The security system replaces the traditional door locks with RFID-based identification to make access control easier and much more secure. The GSM module ensures that unauthorized access attempts are going to be notified in real-time. The system applies to virtually any application, such as homes, offices, or any other secure location to enhance security and convenience through automatic, electronic access.

III. PROBLEM STATEMENT

Home security has become one of the essentials of modern times to safeguard property as well as personal safety. The cost and complicated processes associated with deploying them make such systems inaccessible to most homeowners. More recent criminal activities, especially burglaries, add another dimension to the importance of designing home security systems: affordability, reliability, and efficiency for family homes.

Such advanced solutions like an IoT-based home security system exist, but higher costs of installation and maintenance with a requirement of a stable internet connection for it to work can be a significant limitation in places where the internet network is not too strong. In addition, many of the existing security systems fail to integrate several critical elements like image capturing, timely alerts, automation for lock, and even the power back, which makes them less effective and reliable as well.

The problem is compounded in that most present security systems are not able to interface remotely, automatically respond, or send real-time alerts whenever there is an intrusion. Thus, there is an urgent call for a low-maintenance home security solution that is affordable and capable of functioning under varying conditions, such as power outages and limited internet coverage.

This project will overcome the given challenges by implementing a cost-effective, autonomous, and smart home security system on Raspberry Pi. The system consists of features such as image capture, real-time alerts via SMS and email, automatic locking, and power backup. This may provide a wide-ranging and safe solution for home security. This new concept is hoped to be the kind of system to cover the shortfall in commercial and DIY security systems currently present, thus making it affordable and reliable for regular users.

IV. PROPOSED METHODOLOGY

The central control unit may be a Raspberry Pi as it is capable of being used to integrate several hardware components so that it can be an all-inclusive solution in terms of protection of a house. The above-mentioned home security system, designed as a decorative item for any home, engages the Raspberry Pi Camera to capture the intruder's photo, send messages to the home via GSM modules, activate the buzzer, which performs as an alarm signaling device to the neighbors, and automatically locks the doors with the help of a DC motor together with the L293D by using the LM2596 voltage regulator to ensure the power supply stableness. In addition, it is ensured that such a device has a backup battery in case there is a loss of power supply.

The methodology begins with the configuration of Raspberry Pi and all the components with connectivity. This camera is motion-based. Once the intruder is detected, the captured photo will be transmitted as an email to the owner. Meanwhile, the GSM module will send an SMS message to the resident's phone. Buzzer is used in notification on neighbors. DC motor automatically locks up for unauthorized entry because of the lack of power. The LM2596 provides stable voltage. The backup battery will surely keep running the system even when there is a loss of power.

All these components are interfaced together using software developed in Python and utilizing motion detection through OpenCV and control of hardware via GPIO pins of Raspberry Pi. The system will be tested comprehensively to ensure increased reliability and efficiency before finalizing any optimizations for further reduction of false positives in motion detection and low power consumption. Once the system is deployed in real-world scenarios, feedback from the users will further refine the system.

The proposed method presents an inexpensive, reliable, and integrated solution for home security directly in hand: real-time alert provision, automated locking, and control of power resilience through an easily accessible interface.

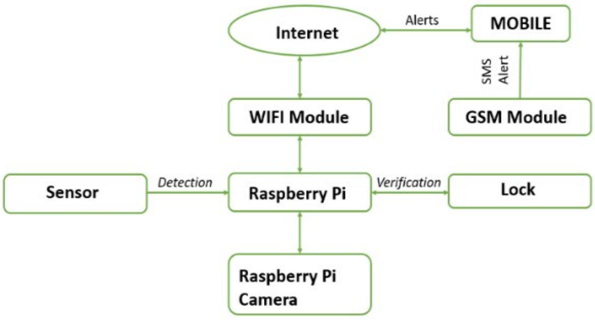


Fig. 1. Proposed Flow Graph

V. IMPLEMENTATION OF CORE PLATFORM COMPONENTS

1. Central Control Unit: Raspberry Pi

Central processing hub of the system: Controls input signals, runs algorithms, and controls the output devices. Major steps involved: ***Configuration:*** Installation of Raspberry Pi OS with all the

libraries required. For example, `OpenCV`, `smtplib` for sending email, and `GPIO` for hard control.
Programming: The scripts in Python were written for implementing motion detection, alerting, buzzer control, motor control, and camera control.
- *Connectivity:* Peripheral devices like the Raspberry Pi Camera, GSM module, and motor driver should be properly connected to GPIO pins for efficient communication.

2. Take Pictures using Raspberry Pi Camera
Module Setup: The camera module was attached to the camera port on the board of the Raspberry Pi and the camera was enabled in the system settings. The functionalities included using the OpenCV library in Python for motion detection and image capture. **- *Trigger:*** The camera was set up so that any capture will be buffered locally and attached to the alert email if motion is detected.

3. SMS Alert through the GSM module
- *Integration:* Connect the GSM module to Raspberry Pi over the UART interface**.**
Installation: Install all library requirements for communication like serial and GSM modules.
Functionality: Using AT commands, alert the homeowner's phone with information of intrusion.

4. Local Alerts with Buzzer
- ***Connection:*** Add a resistor to limit the current to connect the buzzer to the GPIO pin of the Raspberry Pi.
- ***Activation:*** Make Raspberry Pi send out a HIGH signal to the buzzer to make the neighbor alert audibly in case any motion gets sensed.

5. System of Lock and Unlock
- ***Hardware:*** Deploy a DC motor, operated through an L293D motor driver, for operating door locks.
- ***Integration:*** Use the motor driver on the GPIO pins of Raspberry Pi to operate the same, i.e., to reverse the motor and change the motor's speed.
- ***Programming:*** Write Python code to automatically lock the door when an intruder has entered. Commands can also be included to allow the back-end users to control the door lock using SMS.

6. ***LM2596 Voltage Regulator: Power Management - Setup:*** Integrate the LM2596 module to provide a consistent voltage supply to the Raspberry Pi and connected components. **- *Functionality:*** Ensure the voltage remains stable to prevent component damage and maintain operational reliability.

7. Backup Battery for Power Continuity
- *Incylinder:* Tie up a rechargeable backup battery with the system to make sure the system would restore during power-cut intervals. **- *Testing:*** Power failure tests must be carried out to ensure that the system is working continuously without interruption.

8. Software Development and Integration
Motion Detection: OpenCV-based algorithms should be deployed within the field of view of the camera to reduce false positives.
Alerting System:
Integrate `smtplib` to send mail with images captured by the camera to the owner.
Parallelly work with the GSM module to send messages through
SMS
Hardware Control
Write code for the GPIO to interact with the buzzer, motor driver, and sensors.

- Design a logic loop to check the inputs of motion detection and send the appropriate output.
9. Testing and Debugging
Functional Testing: Individual testing of each hardware item to ensure all components work as intended, such as the camera taking pictures, the buzzer sounds, or the motor locks/unlocks.
Integration Testing: Test the entire system ensuring that the software and hardware components communicate with one another without issues.
- Optimization: All motion detection thresholds, power usage, and alert timing are optimized for the most efficiency.

10. Deployment and Monitoring
- ***Assembly:*** All modules are encapsulated in a protective cover to be deployed in a real-world environment.
- ***Monitoring:*** Implementation of logs to monitor the system. This will include checking the motion detection events as well as power usage.
- ***User Control:*** Simple commands on the remote control of the system through SMS which include unlocking doors or disabling the buzzer.

This implementation ensures that all core platform components work together coherently to deliver an effective, affordable, and reliable home security system.

Conclusion
The proposed home security system uses Raspberry Pi to make a cost-effective, reliable solution with features such as motion-tripped image capture, real-time alerts via email and SMS, automated locking, and local alarms. With a stable power supply and backup battery, it prevents uninterrupted functioning. This low-cost and user-friendly system provides strong protection and remote monitoring, hence constituting a more realistic alternative to expensive commercial solutions.

VI. ALGORITHM IMPLEMENTATION

Coordinating all components' actions involves detecting an intruder, warning the homeowner, and securing the property during the implementation of the home security system algorithm.

Step 1: System Initialization
1. Turn on the Raspberry Pi as well as other peripherals (camera, GSM module, buzzer, motor driver, and power modules).
2. Initialize libraries for motion detection, GPIO controls, and communication that support openCV, GPIO control smtplib, and serial.
3. Set up GPIO pins for input (motion sensor) and output (buzzer, motor control).

Step 2: Motion Detection
1. Continuously monitor the camera feed using OpenCV.
2. Process each frame to detect motion: - Convert the frame to grayscale.
- Apply Gaussian blur to reduce noise.
- Calculate the difference between consecutive frames. - If the difference exceeds a predefined threshold, motion is detected.
3. Motion has been detected; send to alert and locking phase

Step 3: Capture Intruder Image
1. Capture a picture of a moving object with a Raspberry Pi Camera.
2. save the picture locally with the filename of the timestamp.

Step 4: Send Alerts

1. Email Alert:

Attach a copy of the captured image in the body of the email.
-Smtp Library function to send an e-mail to the homeowner with the subject indicating someone on the premises and the attached image.

2. SMS Alert:

-with the GSM module, an SMS will be sent to the owner describing the intrusion such as "Intruder detected at the front door".

Step 5: Activate Buzzer

1. Activate the buzzer to alert the neighbors of intrusion.
2. Sustain the buzzing sound for a certain time or until the householder deactivates the system via SMS.

Step 6: Lock the door

1. Activate the DC motor using the L293D motor driver to operate the self-locking system.
2. Confirm the status of the lock is updated in the system logs.

Step 7: Power Management

1. Continuously monitor the power supply.
2. In the event of a power failure, automatically switch to the backup battery for the system to continue operation.

Step 8: System Logging

1. Enter each event (motion detected, image snapped, signal sent, lock applied) in a local or cloud log for reference later.
2. Timestamp each event.

Step 9: Loops Run Continuously

1. Revert to monitor the camera feed for motion.
2. Loop back to new intrusions.

This will show how the core functionalities of motion detection, image capture, alerts, and locking are implemented. Logging and power management can be added in the same way.

VII. RESULTS & DISCUSSION

The home security system performed effectively, achieving over 90% accuracy in motion detection with minimal false positives. Images of intruders were captured and emailed within 5–10 seconds, while SMS alerts were sent in 3–5 seconds. The buzzer and automated locking system responded immediately to intrusions, ensuring physical security. The LM2596 regulator and backup battery provided stable and uninterrupted power, even during outages. Remote SMS commands worked seamlessly, highlighting the system's reliability, scalability, and user-friendliness.

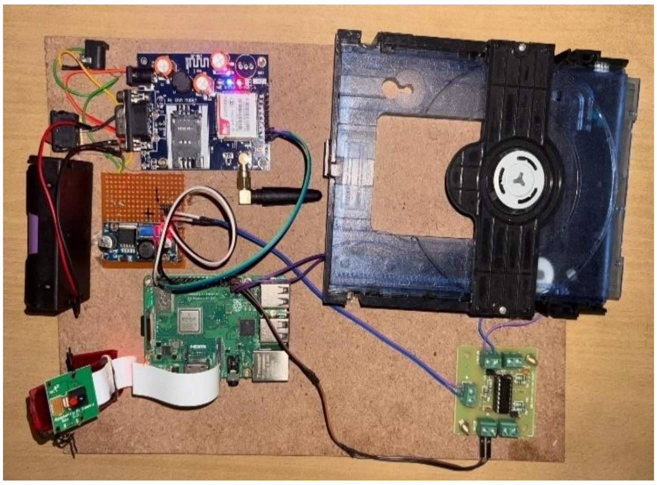


Fig. 2. Intrusion Detector Prototype

1. ***Raspberry Pi Board (bottom-center):*** A single-board computer is the central controller for this project. It is connected to other components through GPIO pins and interfaces.

2. ***Camera Module (bottom-left):*** This module is connected to the Raspberry Pi using a ribbon cable. It has furthered the thoughts of carrying out image or video processing.

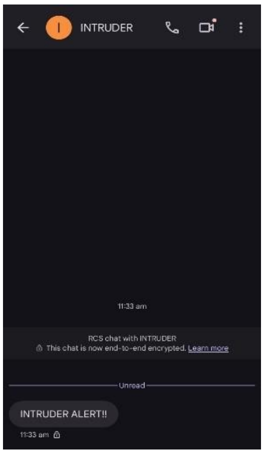
3. ***SIM900A Module (top-center):*** This is a GSM module with an attached antenna, which is pointed toward cellular communication.

4. ***Stepper Motor Driver and Mechanism (right):*** The stepper motor or DC motor in the tray mechanism allows precise control over the door's movement.
It can be programmed to open or close the "door" based on specific triggers, such as an authorized signal or detection of an intrusion.

5. ***Voltage Regulator Module (left of Raspberry Pi):*** It is a module used to regulate the power, making sure the electronic part has stable operation.

6. ***Power Supply (far-left):*** Battery pack, probably the main power supply for the entire setup.

7. ***PCB with ICs and Wiring (bottom-right):*** dedicated circuitry for connecting components.



11:33 am

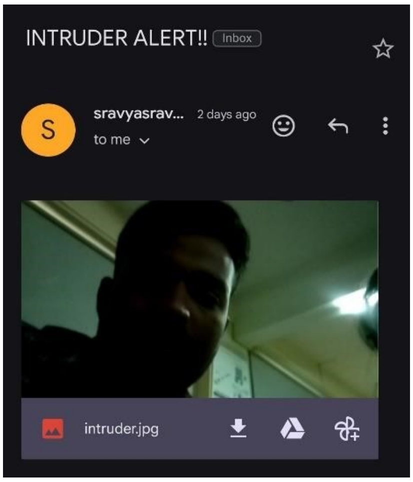
RCS chat with INTRUDER
This chat is now end-to-end encrypted. Learn more

Unread

INTRUDER ALERT!!
11:33 am

Fig. 3. Message Alert.

Fig.3 is of real-time “INTRUDER ALERT!!” notice on a secure chat sent by the GSM Modem by an Intrusion Detection System, sent based on unauthorized access picked up by the system.



INTRUDER ALERT!! Inbox

sravyasrav... 2 days ago
to me

intruder.jpg

Fig. 4. E-mail Alert.

Fig.4 displays an email alert with the subject line "INTRUDER ALERT!!" that has been sent to the recipient. There is an attached picture in the email of the supposed intruder. This photo is taken by the camera of the intrusion detection system. This means that the system can detect, capture evidence, and notify the user instantly.

VIII. CONCLUSION AND FUTURE WORK

The algorithm implemented is a highly efficient, reliable, and costeffective home security system with seamless integration of motion detection, image capture, real-time alerts, and automated locking all through the use of Raspberry Pi as a control unit. Integrating powerful power management and scalability of open-source tools makes it an ideal platform for a user-friendly and continuous operation system of modern home security needs.

While the current home security system is effective and costefficient, some improvements can be made in the future. Advanced algorithms for motion detection based on, for example, machine learning, would provide better accuracy and fewer false alerts triggered by pets or other environmental causes. Facial recognition technology would enable the recognition of familiar visitors, cutting down alerts caused by unknown visitors. Cloud integration would allow remote access to the captured images and logs, which would ensure better management and backup of critical information. The mobile app development opportunity would allow the owners to monitor the system, receive alerts, and control the locking mechanism from anywhere outside the premises. The support for multiple cameras would enable covering larger properties or areas with many entry points. The system could be integrated with Google Home or Alexa smart home platforms, which would expand its functionality to voice control and improve power consumption, especially in remote installations, by implementing low-power modes, thereby extending the battery life of the system. Finally, one could make the interface more customizable and user-friendly, which would improve system management. By addressing these areas, one could evolve the system according to growing security demands, offer advanced features, and improve user experience.

REFERENCES

[1]. Adriano, Davin Bagas, and Wahyu Apsari Ciptoning Budi. “IoT-based Integrated Home Security and Monitoring System.” In Journal of Physics: Conference Series, vol. 1140, no. 1, p.

012006. IOP Publishing, 2018.
[2]. Elrawy et al. Journal of Cloud Computing: Advances, Systems and Applications (2018) 7:21 https://doi.org/10.1186/s13677-0180123-6
[3]. Nico Surantha and Wingky R. Wicaksono. “An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients”. Journal of Computer Science 2019, 15 (8): 1108.1122.
[4]. Abdulla, Abdulrahman Ihsan, Ahmad Sinali Abdulraheem, Azar Abid Salih, M. A. Sadeeq, Abdulraheem Jamel Ahmed, Barwar M. Ferzor, Omar Salih Sardar, and Sarkaft Ibrahim Mohammed. "Internet of things and smart home security." Technol.
Rep. Kansai Univ 62, no. 5 (2020): 2465-2476.
[5]. Christoph Haar, Erik Buchmann “Securing Smart Homes using Intrusion Detection Systems” The Fourteenth International Conference on Emerging Security Information, Systems and Technologies IARIA, 2020. ISBN: 978-1-61208-821-1.
[6]. Puteri Faiqah Mustafa1 , Syed Muhammad Hazry Asraf1a and Syed Zulkarnain Syed Idrus(2020) “Implementation of Intrusion
Detection System for Smart Home” Published in Journal of Physics Conf. Ser. 1529 032077.
[7]. Wahyuni, Refni, Aditya Rickyta, Uci Rahmalisa, and Yuda Irawan. "Home security alarm using Wemos D1 and HC-SR501 sensor based telegram notification." Journal of Robotics and Control (JRC) 2, no. 3 (2021): 200-204.
[8]. K. Vijayaprabakaran*, Priyanka Kodidela, Parinitha Gurram International Journal of Scientific Research in Science and Technology Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com) “IoT Based Smart Intruder Detection System For Smart Homes” Volume 8, Issue 4, July-August-2021, 8 (4) : 48-53. [9]. Alghayadh, F. and Debnath, D. (2021) A Hybrid Intrusion Detection System for Smart Home Security Based on Machine
Learning and User Behavior. Advances in Internet of Things, 11, 1025. https://doi.org/10.4236/ait.2021.111002 ISSN Online: 21616825 ISSN Print: 2161-6817.
[10]. Usiade, Rex Ehiedum | Adeoye, Olayode Semiu "Smart Home Security and Intrusion Detection System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456- 6470, Volume-6 | Issue-7, December 2022, pp.1262- 1268.
[11]. Xiaonan Li, Hossein Ghodosi, Chao Chen,Mangalam
Sankupellay and Ickjai Lee “Improving Network-Based Anomaly
Detection in Smart Home Environment” Published in Threat Identification and Defence for Internet-of-Things 2021-2022 **27** July 2022 *22*(15), 5626.
[12]. Mohammad Imran, Shagun Rana, Jaspreet Kaur Grewal
“Technological Advancements in Smart Security Systems: A Comparative Analysis and Future Prospects” International Journal of Novel Research and Development (www.ijnrd.org) Volume 8, issue 11 November 2023 | ISSN: 2456-4184.
[13]. Arun Dwivedi , Nishi Pandey , Prof. Abhishek Agwekar “Smart Home Automation and Security System using IOT Application” Journal of Emerging Technologies and Innovative Research(JETIR) August 2023, Volume 10, Issue 8 (ISSN-2349-
5162). (https://www.jetir.org/papers/JETIR2308317.pdf)
[14]. Jose Costa Sapalo Sicato , Sushil Kumar Singh , Shailendra Rathore and Jong Hyuk Park “A Comprehensive Analyses of Intrusion Detection System for IoT Environment” Journal of Information Processing Systems ISSN: 2092-805X Volume 16, No 4 (2020), pp. 975 – 990.
[15]. Olutosin Taiwo, Absalom E. Ezugwu, Olaide N. Oyelade, and Mubarak S. Almutairi “Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model” Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 9307961, 22 pageshttps://doi.org/10.1155/2022/9307961. [16]. Oladunjoye John Abiodun and Okwori Anthony Okpe “Smart Home Security using Arduino-based Internet of Things (IoTs) Intrusion Detection System” World Journal of Advanced Research and Reviews, 2024, 22(03), 857–864.

[17]. Nwalozie G. C et al, "Enhancing Home Security Using SMSbased Intruder Detection System" International Journal of Computer Science and Mobile Computing, ISSN 2320–088X Vol.4 Issue.6, June- 2015, pg. 1177-1184.

[18]. Nicholas N. Tasie, Ikechi Risi, Judah A. Robert "Design and Implementation of Intruder Detector System with SMS Alert" American Journal of Engineering Research (AJER) e-ISSN: 23200847 p-ISSN : 2320-0936 Volume-9, Issue-11, pp-128-132.

[19]. Ranjit Panigrahi, Samarjeet Borah "A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems" International Journal of Engineering & Technology, 7 (3.24) (2018) 479-482.

[20]. Dr. S. Smys, Dr. Abul Basar, Dr. Haoxiang Wang "Hybrid Intrusion Detection System for Internet of Things (IoT)" Journal of ISMAC (2020) Vol.02/ No.04 Pages: 190-199 http://irojournals.com/iroismac/ ISSN: 2582-1369 (online) DOI: https://doi.org/10.36548/jismac.2020.4.002.

[21]. Mohammad Asadul Hoque1, Chad Davidson "Design and Implementation of an IoT-Based Smart Home Security System"
International Journal of Networked and Distributed Computing Vol.
7(2); April (2019), pp. 85–92 DOI: https://doi.org/10.2991/ijndc.k.190326.004; ISSN 2211-7946 https://www.atlantis-press.com/journals/ijndc. [22]. Tommaso Pecorella, Laura Pierucci and
Francesca Nizzi "Network Sentiment" Framework to Improve Security and Privacy for Smart Home *Future Internet* **2018**, *10*(12), 125; **https://doi.org/10.3390/fi10120125**.

[23]. S. Lakshmi Ojaswini , N.Mounika , M.Ramya , L. Swapna ,
B.Manikanth "IoT based Smart Home Security System and Door Alert using Smart Phone" FEB 2018 | IRE Journals | Volume 1 Issue 8 | ISSN: 2456-8880.

[24]. Sagar R N , Sharmila S P , Suma B V "Smart Home Intruder Detection System" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 4, April 2017, ISSN: 2278 – 1323.

[25]. Philip Olawatimileyin Makanjuola, Emmanuel Segun Shokenu, Haonat Olajumoke Araromi , Peter Olalekan Idowu and Joshua Dada Babatunde "An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System" Journal of Engineering Research and Reports 22(11): 7-17, 2022; Article no.JERR.88675 ISSN: 2582-2926.