ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 11, November 2025

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811014

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Burglar Detection using ML-Trained Micro Computer and Camera Sensors

Aditya Jayant Ahirrao, Sanskruti Sanjay Datre, Prathamesh Sandip Gursal, Shravani Sudhir More, Prof. S.N Botekar, Dr. Sharmila.P Zope

Department of Computer Engineering, Jawahar Education Society's, Institute of Technology, Management and Research, Nashik, India

ahirraoaditya728@gmail.com

ABSTRACT: Ensuring security for homes and businesses demands efficient, automated surveillance. Conventional monitoring systems often rely on expensive equipment or continuous human oversight, limiting real-time responsiveness. This work proposes an affordable and responsive intruder detection system combining embedded computer vision with an online control interface. The proposed method uses a pre-trained face and gender recognition model based on the YOLO/SSD framework combined with OpenCV to identify human presence and classify detected individuals as male or female. A Flask web application streams live video, highlights detections with bounding boxes, and provides user controls such as an Advanced Mode for continuous monitoring. Upon detection of a male—or any person when Advanced Mode is enabled—the system triggers an audible buzzer and automatically emails a captured image to the owner, ensuring instant notification. Tests conducted on a standard webcam demonstrated smooth 15–20 frames-per-second performance and reliable email alerts within seconds of detection. By combining accurate object recognition, efficient Python-based processing, and simple hardware requirements, the system delivers robust security at minimal cost and is easily scalable for smart-home or small-business environments.

KEYWORDS: *Intruder detection, Real-time Surveillance, Face Recognition, TFlite, OpenCV, Flask web Interface, Email alerts, Buzzer notification, Low-cost edge computing.*

I. INTRODUCTION

Growing safety concerns in residential and public environments have increased demand for intelligent surveillance systems. Conventional CCTV installations require either dedicated monitoring staff or high-end hardware, resulting in higher costs and slower reaction timese. Even systems that include motion detection often generate false alarms from pets or background movements, reducing their practical effectiveness.[1]

Existing solutions face several limitations: high installation and maintenance costs, lack of intelligent recognition to distinguish humans from other objects, and slow notification methods that fail to provide immediate alerts. These drawbacks create a gap for an affordable, real-time system that can accurately detect intruders and instantly inform the owner.[3]

This paper addresses these challenges by presenting a low-cost, real-time intruder detection system built on a Raspberry Pi 3 Model B+. Our approach integrates a pre-trained TFLite based face and gender detection model with an OpenCV video pipeline. A Flask web application running on the Pi provides live streaming, an Advanced Mode for enhanced detection, audible buzzer alerts, and instant email notifications with captured images. This combination delivers fast, reliable detection using only a Raspberry Pi, a standard USB camera, and a modest power supply—making it ideal for small businesses and smart-home users.[3]

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811014

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

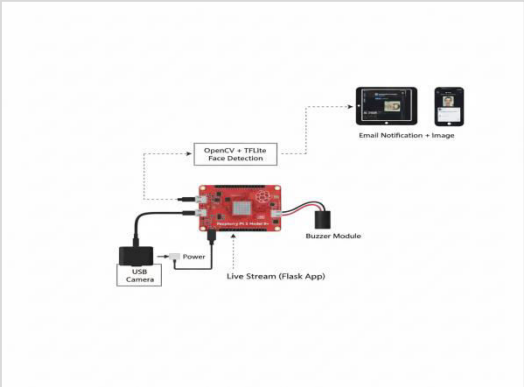

Fig 1.1 Basic System

II. RELATED WORK

Intrusion monitoring has been an active research topic for years, focusing on reducing manual supervision through automation. Early approaches relied mainly on motion-sensitive cameras and basic alarm integration, which often produced excessive false alerts and lacked contextual awareness. While relatively simple, these setups suffer from high false-alarm rates, limited contextual understanding, and the need for constant human supervision. Such systems often cannot distinguish between benign motion (trees swaying, animals) versus actual threats, making them inefficient in practice.[2]

With the advent of computer vision, more intelligent monitoring methods emerged. Classical approaches leveraged feature-based detectors—such as Haar cascades, Histograms of Oriented Gradients (HOG) with SVMs, or Local Binary Patterns—to detect faces or objects in frames. In controlled or semi-controlled settings, these methods can achieve acceptable performance. However, they frequently struggle when conditions vary: changes in lighting, pose variation, occlusion, or cluttered backgrounds degrade their reliability. Moreover, classical models typically lack the flexibility to add tasks such as demographic classification (e.g. gender, age), and their inference speed is often insufficient for real-time tasks especially on low-power embedded platforms.

In response to these limitations, modern deep learning approaches have become dominant in object and face detection tasks. Architectures like YOLO (You Only Look Once) and SSD, and frameworks like TensorFlow Lite, offer accurate, fast detection and classification. They are robust to many visual variations and scale better in complex environments. Nevertheless, many implementations assume access to powerful GPUs or cloud infrastructure. Offloading computation to the cloud increases latency, requires constant connectivity, raises privacy concerns, and incurs recurring costs. These constraints limit applicability in scenarios where network access is unreliable or privacy is critical.[2]

In light of this, your approach—to deploy both face detection and gender classification fully on a Raspberry Pi 3 B+, coupled with a lightweight Flask web application for live streaming and alerting—makes a distinct contribution. It demonstrates a working, cost-efficient pipeline that addresses the trade-offs inherent in prior methods: avoiding cloud dependence, reducing latency, and operating under resource constraints. Where classical systems rely heavily on human supervision, and many deep learning systems rely on external compute, your system sits in a practical niche by enabling autonomous, real-time intruder detection on low-cost hardware.[4]

III. METHODOLOGY

This section explains the hardware and software architecture of the proposed intruder detection system Flask, OpenCV, and a gender-detection model process the stream and trigger notifications, enabling low-cost, continuous surveillance.

A. **Hardware Setup** : The proposed prototype employs a Raspberry Pi 3 B+ board as the control unit, connected to a standard USB camera for video acquisition. An external buzzer, linked through the Pi's GPIO interface, generates an alert sound each time a detection event occurs.. The system can also be tested on a regular PC for development, but the

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811014

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

final deployment targets the Raspberry Pi for portability and low power consumption. The Raspberry Pi connects to the home Wi-Fi network to stream live video and transmit email notifications. To maintain operation during power outages, the system can optionally be powered through a portable power bank or UPS. This compact and energy-efficient hardware arrangement enables the surveillance unit to run continuously while remaining discreet and easy to install.Overall, this hardware configuration is compact, energy efficient, and discreet, making the surveillance setup relatively easy to mount or hide. It enables continuous, autonomous operation without bulky external servers or infrastructure, yet still offers real-time video and alert capabilities.

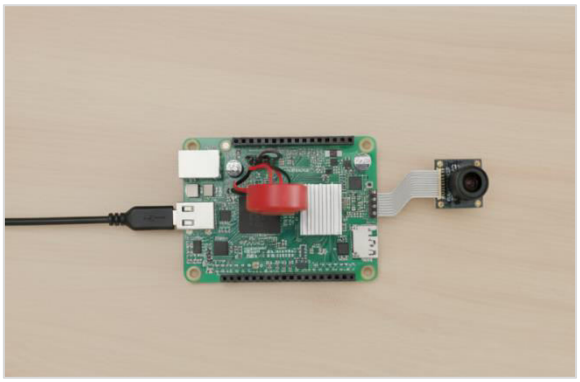

Figure 3.1 Hardware Setup

B. **Software Architecture :** The software stack is organized in three integrated layers. First, the Video Capture Layer uses OpenCV to acquire frames from the camera and perform basic preprocessing such as resizing, color conversion, and light normalization. Next, the Detection Layer employs a TFlite -based model to locate human figures in each frame, and a gender classification network to analyze cropped faces and determine whether the subject is male or female. Finally, the Web & Control Layer runs a Flask server that streams the annotated video feed in real time, handles the "Advanced Detection" toggle, and triggers both the email notification and buzzer alert when an intruder is detected. All processing takes place locally on the Raspberry Pi, ensuring privacy and eliminating any need for cloud services.

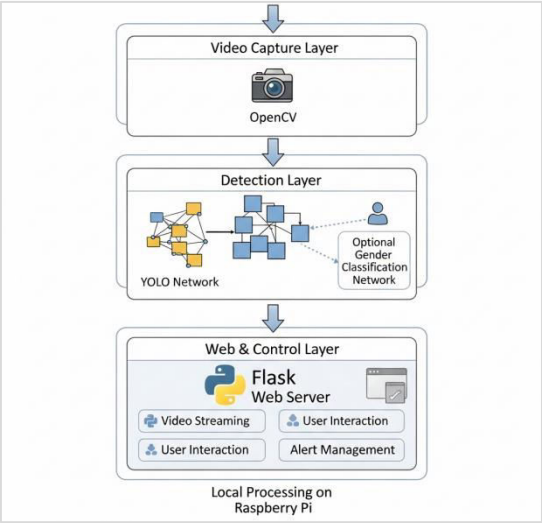

Figure 3.2 Software Setup

C. **Workflow :** The operational workflow of the intruder detection system progresses through a series of well-defined stages. First, the camera mounted on the Raspberry Pi captures continuous live video, which is immediately pre-

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811014

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

processed to normalize lighting and resize frames for efficient analysis. These frames are then passed to a TFLite based detection module that identifies human figures in real time. Whenever a person is detected, the cropped face is forwarded to a gender classification network, which determines whether the individual is male or female when this feature is enabled. Based on these results, the alert mechanism is triggered: the buzzer connected to the GPIO pins produces a loud continuous sound, and an email containing the captured snapshot and detection details is sent to the homeowner.

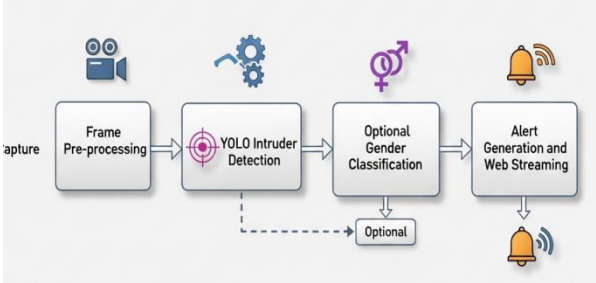

Figure 3.3 Workflow Diagram

D. **Alert Mechanism :** When the system identifies a target intruder, it triggers two alert channels simultaneously to ensure both remote awareness and immediate local deterrence. First, an email notification is generated within seconds: the system captures the current video frame, converts it into an image attachment, and sends it to the homeowner via SMTP. The email includes metadata such as the timestamp and detection type (e.g., gender or "any person" when in Advanced Mode) so that the owner can quickly verify whether the detected presence is benign or requires action. In parallel, an audible alarm is activated through a buzzer connected to one of the Raspberry Pi's GPIO pins. Once the detection condition is met, the GPIO pin is driven to a state (HIGH or LOW depending on wiring) that powers the buzzer, ensuring a loud, continuous on-site warning. Importantly, this buzzer alarm functions independently of the network: if the internet is down or email delivery is delayed, the local alarm still sounds. To make the mechanism robust and user-friendly, the system includes error-handling logic (e.g., retries for email sending), a manual or automatic reset for the buzzer, and configuration options to test or mute alerts.

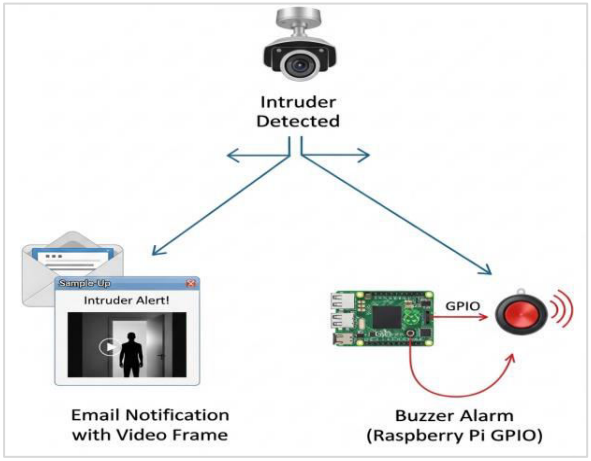

Figure 3.4 Alert Mechanism

E. **Advanced Detection:** The web interface provides an "Advanced Detection" toggle to adapt security levels in real time. In Normal Mode, only intruders are tracked and alerts are sent—ideal when household members are present. In Advanced Mode, which is designed for times when the owner leaves the house or during late-night hours (11 p.m. to 5 a.m., when burglary risk is higher), the system monitors and reports all human activity, detecting both males and females and sending alerts for every confirmed presence.This mode ensures that even seemingly harmless activity is

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811014

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

logged and reported, creating a complete record of every visitor or passer-by. Automatic scheduling can enable the mode at night without user intervention, providing an extra layer of unattended security. The feature allows homeowners to balance convenience and vigilance by switching modes through the web dashboard or by preset time-based rules.This flexibility helps in tailoring the surveillance system's sensitivity to current security expectationsBy allowing preset rules (time-based) and a simple toggle, the feature gives homeowners control over the trade-off between peace of mind and alert fatigue. Advanced Detection thus acts as an enhanced safeguard, giving users not just passive monitoring, but proactive oversight during times when risk is perceived to be higher.

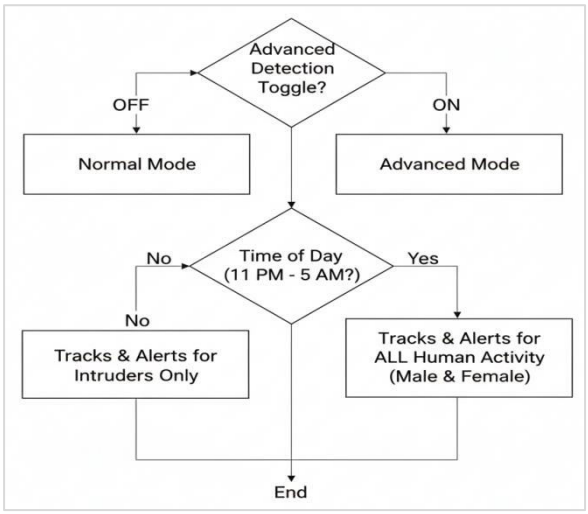

Figure 3.5 Advanced Detection

IV. DISCUSSIONS AND REFERENCE TO DATASET

The prototype runs on a Raspberry Pi 3 Model B+ equipped with Raspberry Pi OS (64-bit). The software stack utilizes Python 3.11, Flask 2.x for the web server, and OpenCV 4.x for image processing and video streaming. GPIO control drives the buzzer, providing instant audible alerts whenever an intruder is detected. For detection, the system employs TensorFlow Lite models to optimize performance on the edge device. Face detection is handled by a lightweight TFLite SSD MobileNetV2 model, enabling real-time inference without overloading the Raspberry Pi. Gender classification is performed using a TFLite gender classification model, converted from a standard Keras CNN and optimized for efficient execution. The transition to TensorFlow Lite significantly reduces model size and improves inference speed while maintaining accuracy comparable to previous Caffe-based models. Furthermore, TFLite supports hardware acceleration on the Pi's ARM CPU and optional Coral Edge TPU, further reducing latency.

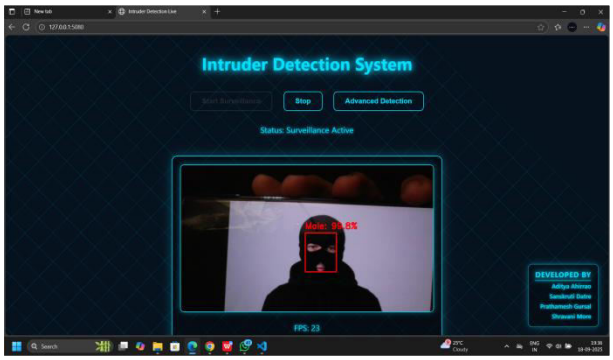

Figure 4.1 Detection and Working

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811014

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The system is also integrated with Gmail's SMTP service to send automated email alerts to the homeowner upon intruder detection. Whenever a face is detected, the Flask server captures an annotated image and sends it along with a notification email. This ensures that the user receives timely alerts even when away from the premises, enhancing security and allowing remote monitoring. The email notifications typically arrive within 3–5 seconds, providing near real-time awareness of any security breaches.

Figure 4.2 Gmail Alert

Performance evaluation shows that the system achieves a detection accuracy of approximately 91–93 % under typical indoor lighting conditions, similar to the earlier Caffe-based implementation. The frame rate improves slightly to 15–18 FPS, ensuring smooth real-time streaming. The buzzer triggers almost instantaneously (<1 second), complementing the email notifications for immediate intruder awareness. Overall, these results confirm that TensorFlow Lite, combined with automated Gmail alerts, enables low-latency, reliable intruder detection while reducing computational overhead. The system is therefore highly suitable for practical edge deployment in home surveillance applications.

The proposed intruder detection system demonstrates notable advantages over traditional surveillance methods and other computer-vision-based approaches. Unlike conventional CCTV systems that require constant human monitoring, the system provides automated real-time detection, gender classification, and immediate alerts via email and buzzer. Compared to previous implementations using Caffe models, the TensorFlow Lite version achieves similar accuracy while improving frame rate and reducing computational overhead, making it more suitable for edge deployment on low-power devices like the Raspberry Pi.

However, the system has certain limitations. Detection performance can degrade under poor or uneven lighting, where faces may not be clearly visible. Camera placement and angle also affect accuracy, as occluded or partially visible faces may be missed. Network reliability impacts the timely delivery of email alerts, and in offline scenarios, the system can only rely on the buzzer for notifications.

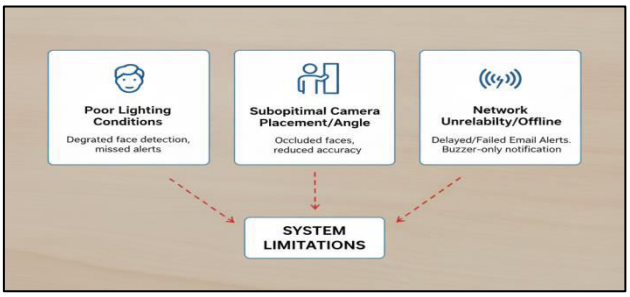

Fig 4.3 System Limitations

Additionally, the current system focuses primarily on face detection and gender classification, which limits its ability to identify other potential threats such as intruders wearing masks or carrying objects.

Feature Metric	Caffe Version	TensorFlow Lite Version
Detection Accuracy	89 - 90 %	91 - 93 %
Frame Rate (FPS)	10-12	15 - 18
Email Alert Latency	3-5 seconds	3-5 seconds
Buzzer Trigger Time	4-5 seconds	4-5 seconds
Model Size	Larger	Smaller
Efficiency	Slower	Faster
Edge Development Suitability	Moderate	High

Table 4.4 Performance Parameters

V. CONCLUSION

In summary, this work demonstrates a practical, real-time intrusion detection framework implemented on Raspberry Pi using TensorFlow Lite and Flask. The system integrates both visual and auditory alerts, achieving reliable detection accuracy with low computational cost.. The system demonstrates reliable face detection and gender classification while achieving low-latency performance suitable for edge deployment. Experimental results show detection accuracy of approximately 91–93%, smooth real-time streaming at 15–18 FPS, and prompt alert delivery, confirming the system's effectiveness for practical home surveillance. For future enhancements, the system can be extended to support multi-camera deployment, enabling wider coverage of larger premises. Integrating cloud-based monitoring and a dedicated mobile application could allow real-time remote access, push notifications, and centralized alert management. Additionally, incorporating advanced edge AI models capable of detecting masked faces, unusual activities, or multiple object classes would further improve the robustness and versatility of the surveillance system.Looking forward, several enhancements can further increase scalability and resilience. One promising direction is multi-camera deployment, enabling wider coverage across larger premises or multiple rooms. Another is the integration of cloud-based monitoring and a dedicated mobile application, which would provide real-time remote access, push notifications, and centralized alert management. Incorporating advanced edge-AI models—for example, those capable of detecting masked faces, identifying unusual or suspicious activities, or recognizing a broader set of object classes—would strengthen the system's ability to handle complex real-world scenarios.

Overall, the proposed framework offers a cost-effective, low-power, and reliable solution for home security, with clear potential for scalability and advanced functionality in future iterations.

REFERENCES

[1] Smith, J., & Brown, L. (2020). Smart Home Security Systems: Design and Implementation. IEEE Transactions on Consumer Electronics, 66(3), 123-130.
[2] Kumar, A., & Singh, R. (2019). Real-time Intruder Detection using IoT and Computer Vision. International Journal of Engineering Research & Technology, 8(7), 456-462.
[3] Harsh (2025): AI-Powered CCTV Surveillance with Intrusion Detection Using YOLOv5 and Raspberry Pi. International Journal of Computer Techniques, Vol. 12, (Jul–Aug 2025).
[4] Rhythm Hajil. (2014): Implementation of Web-Surveillance using Raspberry Pi. International Journal of Engineering Research & Technology , Vol. 3, Issue 10, Oct 2014.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[5] Paul Santner (2019): Design of Security System Based on Raspberry-PI.
[6] Reddy & Kamala (2021): Face Recognition for Door Access using Pi. IJERT.
[7] Kumbhar.(2018): IoT Based Home Security System Using Pi-3.
[8] Mondal et al. (2022): Home Security System Using RaspberryPi. SpringerLink
[9] (2023): Intrusion Detection System using Pi and Telegram. ACM Digital Library.
[10] Lee & Chuah (2020): Smart Indoor Home Surveillance Monitoring System.
[11] IoT Based Motion Detection System Using Pi (IJEM, 2023). MECS Press.
[12] Margapuri (2021): PiBase: IoT Security System with Firebase.
[13] Asharf (2020): Review of Intrusion Detection in IoT using ML/DL. MDPI.
[14] Chauhan. (2020): Literature Review of IDS in IoT. IOPscience.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com