WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

EMBEDDED AI SOLUTION FOR INTELLIGENT HOME SECURITY MONITORING

Neeraj M Khavatagoppa[1], Nandita M Mathad[2], Poornima Bykaud[3]

[1]*S G Balekundri Institute of Technology*, Karnataka, India neerajmk03@gmail.com
[2]*S G Balekundri Institute of Technology*, Karnataka, India mathadnanditamallikarju n@gmail.com
[3]*S G Balekundri Institute of Technology*, Karnataka, India byakudpoornima@gmail.com

A B S T R A C T :

Embedded AI Solutions for Intelligent Home Security Monitoring" is a holistic solution that aims to transform home security by adopting cutting-edge embedded artificial intelligence and edge computing technologies. The solution centers around real-time data processing for quicker decision-making, providing strong privacy and increased security. It boasts of AI-powered video analysis, facial recognition, and motion detection to effectively detect unwanted activity, differentiate between residents and intruders, and minimize false alarms. The system offers real-time alerts, live video streams, and actionable information to homeowners via mobile applications while integrating effortlessly with smart home devices such as automated locks, lighting, and alarms for an integrated security solution. state-of-the-art system aimed to secure homes by using embedded artificial intelligence and edge computing for immediate processing and decision-making of data. The system uses AI-based video analytics, motion detection, and face recognition to detect unauthorized activities, reduce false alarms, and provide strong monitoring. Efficiently designed to run on low-power embedded devices, the system delivers trusted performance in any environment, even in resource-limited situations, and processes information locally to preserve privacy and avoid security breaches. Automating and streamlining security tasks, cost-effective and easy-to-use this solution equips homeowners with smart, real-time monitoring and control, improving safety, convenience, and peace of mind while establishing a new standard for home security innovation.

Keywords— Embedded AI, Edge Computing, Facial Recognition, Motion Detection, Real-time Monitoring, Smart Home Integration, Enhanced Security, Instant Alerts, Low-power Platforms, Privacy Protection

Introduction

Home security has always been a top issue, fueling the need for sophisticated systems that provide security, reliability, and user convenience. As technology advanced, embedded systems and artificial intelligence (AI) brought revolutionary solutions for intelligent security monitoring into view. Such solutions take advantage of bringing together various components to improve safety, simplify monitoring, and automate responses. The incorporation of devices like Raspberry Pi, solenoid locks, relays, fans, PWM drivers, temperature sensors, camera modules, and motion sensors has allowed systems to be developed with real-time threat detection and prevention capabilities. Conventional security solutions, usually restricted to static monitoring and manual controls, are unable to cope with dynamic threats, are slow to respond, and require heavy human intervention. In-built AI-powered solutions mitigate these challenges through the integration of real-time data processing, automation, and sophisticated analytics. Not only does this enhance home security, but it also enhances operational. efficiency and guarantee user convenience. The system utilizes connected devices to track important parameters, detect abnormalities, and issue real-time alerts. For instance, camera modules and motion sensors recognize unauthorized presence, temperature sensors guarantee security by maintaining environmental monitoring, and solenoid locks improve access control.

The combination of these elements forms an integrated system that focuses on security, efficiency, and data privacy. With embedded AI combined with hardware elements, local data processing is facilitated for quick response while communication is secure. By rethinking conventional security procedures, the solutions are a new leap in home security technology to provide a secure and smart environment to live in. The transformation of monitoring homes with intelligent security systems is a new milestone in fulfilling contemporary security requirements. By integrating AI-powered analytics with embedded systems, such solutions provide unmatched safety, efficiency, and responsiveness. Alongside hardware integration and smart analytics, the effectiveness of an embedded AI-based home security system also depends on software frameworks and communication protocols. Successful implementation demands real-time operating systems (RTOS), light machine learning models optimized for embedded systems (e.g., TensorFlow Lite or OpenVINO), and secure communication protocols like MQTT, HTTPS, or Zigbee. These software components maintain the system responsive, secure, and scalable. In addition, with the emergence of IoT ecosystems, these types of systems are now able to interoperate with voice assistants like Amazon Alexa or Google Assistant for voice-activated control and status reporting. Future developments could be predictive threat analytics, cloud-edge hybrid models, and self-healing security systems, in which the system itself is capable of detecting faults, changing its behavior, and providing continuous security. Such continuous development guarantees that smart home security systems are not just suited to the existing requirements but also future-proof to tackle new challenges.

Literature Survey

[1] Sharma. P and Verma. R Submitted a "Machine Learning- Based Smart Home Security System" in the International Journal of Advanced Research in Computer Science in 2023. The paper presented a machine learning-based security system for smart homes based on motion sensors, camera modules, and temperature sensors. The system utilized a Raspberry Pi for processing, supporting functionalities such as anomaly detection and remote alerts. The use of pre-trained AI models lowered false alarms considerably while increasing detection accuracy. Drawbacks, however, were the reliance on consistent internet connectivity as well as the difficulty of connecting older home devices.

[2] Chen H, and Wu L. Suggested "Home Security System Using AI and IoT Integration" in the Journal of Innovative Technologies in Smart Environments in 2023. IoT devices like temperature and motion sensors were integrated with AI functions for making decisions automatically. A master Raspberry Pi received data from connected devices and handled real-time notifications. The system was capable of identifying and taking action on exceptions such as intrusions and unusual temperature fluctuations. Still, there were issues of data security and the expense involved in implementing advanced sensors mentioned as areas for improvement.

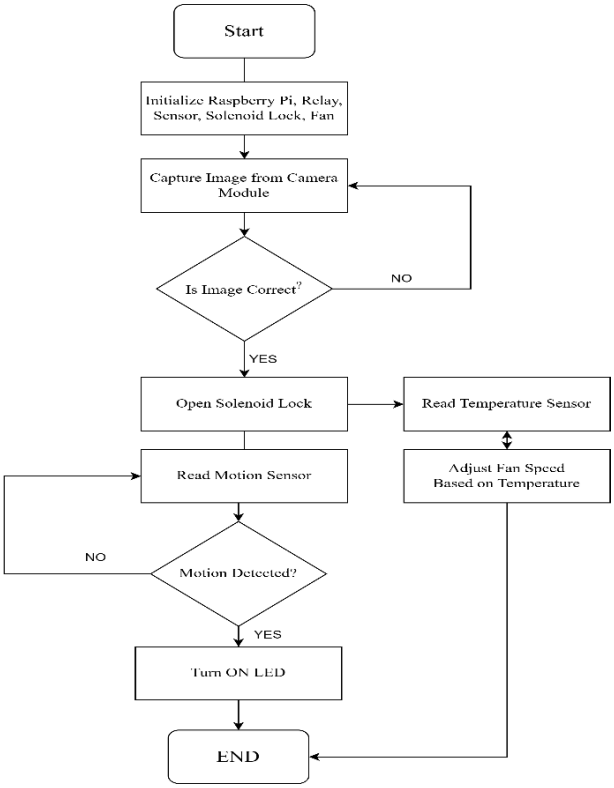

Fig4.1: Block Diagram

[3] Singh A., and Kaur M. Suggested a "Hybrid AI and IoT- Based Home Security Monitoring System" in the International Journal of Artificial Intelligence Applications in 2023. The study introduced a hybrid security solution with embedded AI for threat assessment and IoT for sensor connectivity. The system applied a camera module for video monitoring, motion sensors for activity detection, and temperature sensors for tracking environmental temperatures. Automated response capabilities, including alarm triggering and door locking, were important aspects. Scalability and the cost of initial deployment continued to be major issues.

METHODOLOGY

"Embedded AI Solutions for Intelligent Home Security Monitoring" is the organized integration of embedded systems, artificial intelligence, and IoT-based communication to design a responsive and intelligent home security solution. The system revolves around the Raspberry Pi 4 Model B, which is used as the main processing unit based on its excellent computation powers and broad GPIO support. Major input devices are the DHT11 temperature and humidity sensor, PIR movement sensor for movement detection, and a Pi Camera module for picture taking and face recognition. Output devices like a solenoid lock ensure safe access control, and a relay module, exhaust fan, and LEDs enable environmental control and visual notification. The software development was done with Python in the Thonny IDE to enable effective interfacing with the hardware modules and the execution of AI-based decision-making algorithms. The system is based on the principle of local processing of data to provide real-time response and improved privacy, with the provision for remote access and monitoring through IoT networking. This approach provides for a comprehensive solution to intelligent security and automation for smart homes of today.

BLOCK DIAGRAM

The flowchart depicts a Raspberry Pi-intelligent automation system with security and environmental control combined. It starts with the initialization of all the components such as the camera, solenoid lock, temperature sensor, motion sensor, fan, and relay module. The camera takes a picture, which is checked against specified parameters. If checked, the solenoid lock is switched on to provide access. The system subsequently reads the ambient temperature and adjusts the fan speed in response through PWM control to provide comfort. At the same time, motion is sensed and an LED activated as a visual warning. Where there is no motion or the image fails to be confirmed, the system loops back or does nothing. After all operations have been performed, the system goes back to standby mode to continuously monitor and maintain effortless operation. This combined processsincreases home security, enhances energy efficiency, and auto-regulates the environment

SYSTEM MODEL

The prototype uses a Raspberry Pi 4 Model B as the main processing unit, controlling and managing all the connected devices. Sensors and actuators are connected to the Raspberry Pi through GPIO pins and are attached on top of a breadboard for easy prototyping. An image sensor module (via the CSI interface) is employed for capturing images and facial recognition, a critical component of the access control system.A fan for cooling or exhaust is built into the system and most probably controlled by PWM through temperature input from a sensor such as the DHT11. The relay module (with a red LED indicator that is visible) is utilized to turn high-power devices such as the fan or solenoid lock on or off based on system logic. There are several jumper wires that provide communication between components and Raspberry Pi using digital and analog pins. The breadboard comes in handy for arranging and linking sensors like the DHT11, PIR motion sensor, and transistors or MOSFETs, if any, for control.The wholesetup exhibits real-time automation: upon power-up, the system sets up all the devices, reads sensor inputs, processes images and captures, and performs automated tasks such as unlocking the solenoid, setting fan speed, or energizing an LED upon movement.

This model enables real-time edge computing through the processing of sensor inputs and camera feeds at the local level, providing immediate response and better data privacy without always being connected to the cloud. It also enables

IoT-based remote access such that homeowners can monitor and control devices using a web or mobile app interface.

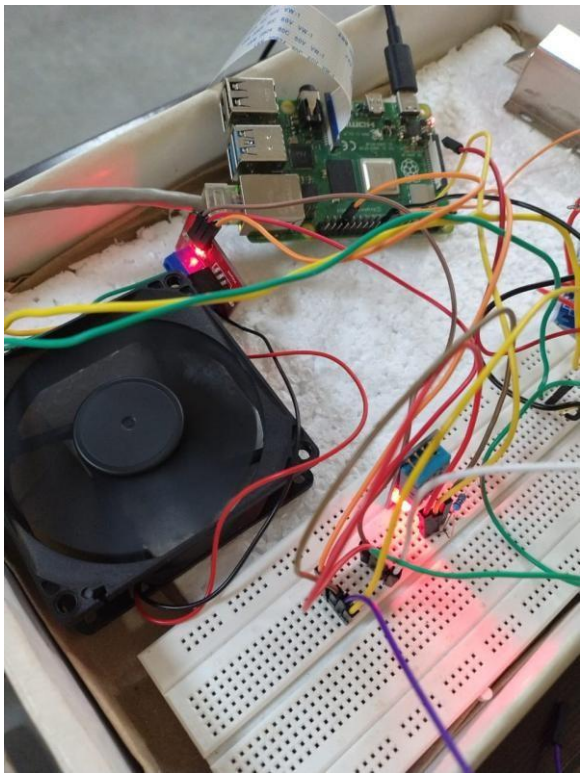

Fig 5.1: System model

CONCLUSION AND FUTURE SCOPE

There can be great enhancement of the system in the future by incorporating multi-modal sensor fusion. This is done by integrating information from different sensors like infrared, ultrasonic, vibration, and audio sensors to enhance the accuracy and reliability of threat detection. Utilizing multiple types of sensors, the system can minimize false alarms and have a clearer understanding of the surroundings, which results in enhanced situational awareness.Another exciting technology is the application of edge AI with federated learning. This method enables numerous devices to collectively enhance their AI models by exchanging only the parameters learned rather than raw data, thus ensuring user privacy. Federated learning has the

potential to provide permanent threat detection algorithm enhancement on dispersed devices without compromising sensitive data.detection of a genuine threat can deliver on-the-spot assistance. Such incorporation might involve capabilities such as automatic calling, live video streaming, or location information sending to emergency services, enabling swift and coordinated response to incidents.Lastly, the use of blockchain technology for data security and integrity is another future prospect. Blockchain can produce tamper-proof security event logs, providing transparency and protection from unauthorized changes. This can build greater trust in the system and enhance its reliability, especially in sensitive security applications.Overall, these enhancements, along with continued advancements in AI, embedded systems, and IoT, will make home security solutions more intelligent, adaptive, and seamlessly integrated into smart home ecosystems, providing users with enhanced protection and convenience.

REFERENCES

[1] Sharma. P and Verma. R Designed a "Machine Learning- Based Smart Home Security System" for the International Journal of Advanced Research in Computer Science in 2023.

[2] Chen H, and Wu L. Designed "Home Security System Using AI and IoT Integration" for the Journal of Innovative Technologies in Smart Environments in 2023.

[3] Kumar N, and Reddy P. Suggested an "Embedded AI System for Smart Access Control" in the International Journal of Embedded Solutions in 2023.

[4] Singh A., and Kaur M. Suggested a "Hybrid AI and IoT- Based Home Security Monitoring System" in the International Journal of Artificial Intelligence Application.