IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Smart Home Automation System

[1]Shrutika Dolas, [2]Arpita Salve, [3]Sayee Waskar, [4]Atnurkar .A.B
[1]Student, [2]Student, [3]Student, [4]Assistant Prof.
[1]DBATU University,
[2]DBATU University,
[3]DBATU University,
[4]Shivaji university

Abstract:-

Smart home automation systems have become a central focus of modern intelligent infrastructure, driven by rapid advancements in Internet of Things (IoT) technologies, embedded systems, and wireless communication. This paper presents a comprehensive smart home automation framework designed to integrate heterogeneous sensors, actuators, and connected appliances into a unified, scalable ecosystem. The proposed system utilizes low-power IoT nodes, cloud connectivity, and edge-based data processing to automate core household operations, including lighting control, environmental monitoring, intrusion detection, and energy management. A multi-layer architecture—comprising perception, network, and application layers—ensures efficient data flow, interoperability, and secure communication among devices..

Introduction:-

A **Smart Home Automation System** is an advanced technological solution designed to enhance the comfort, security, convenience, and energy efficiency of residential environments. By integrating various electronic devices, sensors, and appliances with centralized control mechanisms, the system enables users to monitor and manage their home remotely or automatically. Modern smart homes use technologies such as the **Internet of Things (IoT)**, **wireless communication**, **cloud computing**, and **artificial intelligence** to create an intelligent living space that responds to user preferences and environmental changes.

Literature Review:-

1. Overview and scope

Research on smart home automation has matured from isolated device control projects to multi-layered ecosystems that combine IoT hardware, edge/cloud platforms, AI, and user-facing apps. Reviews show the field spans several research streams: architectures and communication, energy management, security & privacy, user acceptance, and intelligent automation (ML/AI). The literature emphasizes that smart homes are now studied both as standalone systems and as components of wider smart-city infrastructures.

2. Architectures and communication technologies

Early work focused on device-level implementations (Arduino/Raspberry Pi prototypes, Zigbee/Z-Wave). Recent surveys classify common architectural layers as: device/sensor layer, gateway/edge layer, network/communication layer, and application/cloud services. Research compares protocols (Wi-Fi, Bluetooth Low Energy, Zigbee, Z-Wave, Thread, MQTT/CoAP) in terms of latency, power use, and scalability — and repeatedly notes tradeoffs between ease of deployment (Wi-Fi) and energy/mesh benefits (Zigbee/Thread). Interoperability and vendor lock-in remain recurring practical problems in the literature.

3. Energy management and sustainability

Energy management (SHEMS) is one of the most active subareas: researchers propose load-scheduling, demand-response, local renewable integration, and predictive algorithms to reduce consumption and cost. Systematic reviews show a shift from rule-based controllers to data-driven approaches (forecasting household consumption, appliance-level disaggregation) and increasing interest in real-time control tied to dynamic pricing and PV/battery systems. However, many studies either use small datasets or simulate household behaviour, so field validations are still limited.

4. Security, privacy, and trust

Security/privacy is the most cited challenge across surveys. Threats identified include device vulnerabilities, weak authentication, insecure cloud services, and side-channel information leakage from sensors. Researchers classify mitigation techniques (encryption, mutual authentication, secure boot, intrusion detection) but note limited adoption in low-cost consumer devices. User trust and regulatory pressure are rising: recent policy moves and labeling proposals aim to improve baseline cybersecurity for consumer IoT devices. The literature argues that technical fixes must be paired with design for privacy and clearer data-practices to rebuild user confidence.

5. User acceptance, usability, and social factors

Acceptance studies use technology acceptance models and surveys to show adoption depends on perceived usefulness, ease of use, cost, privacy concerns, and perceived control. Specific populations (older adults, people with disabilities) are studied for assisted-living benefits, but social barriers (trust, digital literacy) and economic barriers persist. User studies often stress need for transparent controls, explainability of automated decisions, and simple recovery actions when automation fails.

6. Intelligent automation and AI

Recent work integrates machine learning for activity recognition, anomaly detection, and personalized automation rules. Approaches include supervised learning for device classification, unsupervised/semi-supervised methods for anomaly intrusion detection, and reinforcement learning for adaptive control (thermostats, HVAC scheduling). Key challenges: scarcity of labelled in-home datasets, concept drift as household behaviour changes, and explainability/verification of learned policies in safety-critical contexts.

7. Standards, regulation, and market trends

Researchers note emergent regulatory responses and labeling initiatives aimed at baseline security and transparency for consumer devices. Such efforts (e.g., national cybersecurity labels and voluntary trust marks) are expected to influence manufacturer practices and consumer choices — a trend also reported in policy and industry analyses. These non-technical levers are highlighted as necessary complements to engineering solutions.

Objectives

- Develop a standalone Home Automation System (HAS) to automate and integrate household appliances into a network, ensuring centralized control.
- Create a wireless control application with speech and switch mode capabilities for convenient and seamless control of home appliances.
- Implement a feature within the application to monitor the condition and status of household appliances, contributing to ongoing improvement of the Home Automation System.
- Establish secure communication lines using Node MCU and secure Wi-Fi protocols (SSL over TCP and SSH) to prevent unauthorized access and ensure the security of the HAS.
- Ensure the HAS is compatible with any Wi-Ficapable device, allowing for flexible and secure control of home appliances from various platforms such as PCs, iOS, Android, etc

Scope of the Project The objective is to develop a functional prototype enabling wireless remote control for a network of household appliances. The software is designed for Android devices, incorporating features such as voice command control, switch mode control, and the ability to directly view device status within the application. The versatility of this software extends its application to various contexts. The prototype's scope encompasses the management of electrical equipment, making it suitable for installation in malls, small companies, and residences. It facilitates remote access to appliances over both intranet and internet connections, offering control in diverse environments. This system employs technology to create a Home Automation System (HAS), allowing us to utilize our everyday electronics from a distinct perspective

Literature Survey

[1] The project seeks to accomplish automation through the popular mobile operating system Node MCU, specifically the Android Operating system.

This allows for the control of electrical and home appliances using Android mobile phones, providing the convenience of remotely managing appliances even when outside the house, eliminating concerns about accidentally leaving them on. Implementing a Home Automation System (HAS) tailored for the elderly and disabled can significantly enhance the quality of life for individuals who might otherwise depend on caregivers or institutional care.

[2] The consumption of energy in electronic devices, particularly in Air Conditioners (ACs), is considerable. The primary goal of the intelligent AC control system is to reduce electricity wastage. Our system achieves this by implementing control over the AC temperature, which is influenced by people's traffic patterns, utilizing a GSM module.

[3] The suggested design employs the EmonCMS platform for the aggregation and visualization of monitored data, as well as for remotely controlling home appliances and devices. The process involves collecting, processing, and uploading or downloading data to and from the cloud server.

[4] The application of wireless technologies in the smart home is addressed by highlighting the advantages and limitations of existing approaches to tackle diverse and concurrent issues associated with the distributed control of household systems. Special attention is devoted to addressing the user localization problem, aiming to minimize the intrusiveness of monitoring systems. The review and discussion encompass wireless architectures, presenting them as flexible and seamless tools that contribute to achieving a change in thinking towards a fully automatic and autonomous environment.

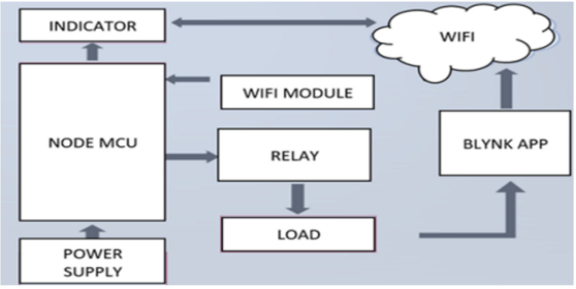
[5] Introducing the uIDCoAP architecture, our innovative framework is specifically crafted to accommodate IoT services on everyday embedded systems, such as conventional consumer appliances. The software framework, tailored for embedded appliance nodes, aims to simplify the process for producers by delivering a user-friendly, standardized, and intuitive Application Programming Language (APL). With this concept in mind, our framework not only includes a low-level communication API but also offers functionalities to construct RESTful services, enhancing the overall accessibility and usability of embedded systems in the IoT domain.

[6] This study introduces an approach to establish a cost-effective Wireless Fidelity (Wi-Fi) based Home Automation System (HAS), embodying the concept of smart device internetworking. The primary aim of the Wi-Fi-based Wireless Sensor Network (WSN) is to oversee and regulate various aspects of a smart home, encompassing electrical, safety, and environmental parameters. The study delves into a machine intelligence system based on vision, specifically focusing on a temperature and humidity sensor, capable of discerning the operational status of common home devices. Through the proposed technique for detecting appliance conditions, a distinctive home automation system is developed. Leveraging IP addressing techniques within the Internet of Things framework facilitates remote network accessibility for the suite of home devices. The project utilizes two boards: an Intel Galileo Gen 2 and a Raspberry Pi, with wireless networking enabling communication between these boards and user devices. The Home Automation System comprises sections such as gas leak detection, fire alarm, burglar alarm, rain sensor, load and voltage control switching, and current sensing. To meet the core requirement of monitoring and controlling equipment, a smartphone application is employed.

[7] The research outlines a machine intelligence system leveraging vision to discern the operational status (on or off) of common household devices. This innovative approach results in the development of a distinctive home automation system. The utilization of IP addressing techniques within the Internet of Things framework facilitates remote accessibility of the suite of home devices over a network. For this project's implementation, two boards are employed: An Intel Galileo Gen 2 and a Raspberry Pi. Communication between these boards and user devices is facilitated through wireless networking, enhancing the efficiency and connectivity of the system.

Methods and Materials

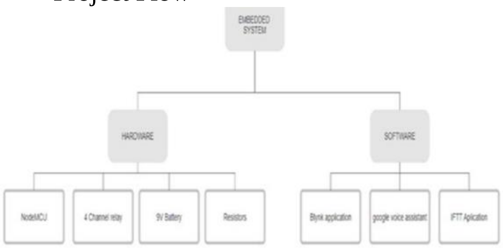
Block Diagram



Working

The central controlling unit in the system is the Node MCU microcontroller. Users issue commands for appliance operation through a mobile application. The BLYNK application, utilizing a Wi-Fi connection, establishes a wireless network and interprets user commands through voice or switch mode. These commands are then transmitted as signals to the Node MCU unit. To enable Wi-Fi communication and command reception over a wireless network, the Node MCU incorporates a WiFi module within its architecture. Upon receiving the signal, the Node MCU utilizes a relay to toggle the appliance on or off. The appliances, relay, and Node MCU are physically interconnected, forming a prototype for a wireless remote switching system for home appliances. This model employs Wi-Fi for wireless control, providing an indoor range of up to 45m. Commands to switch appliances on and off can be issued via radio buttons on the smartphone application. Additionally, a feature has been developed to enable voice commands for remote appliance control using a smartphone. Any device with Wi-Fi capabilities can be employed to control the prototype. Security is ensured through secure connections, utilizing SSL over TCP and SSH. The design is straightforward, facilitating integration into various appliances and scalability. The application on the smartphone displays the status of each appliance, providing a convenient overview of the system.

Project Flow



Four Channel Relay Module: The module includes four individual relays physically connected between the Node MCU and household appliances. These relays receive signals Figure 2 from GPIO pins of the Node MCU, allowing the connection or disconnection of home appliances from the power supply. They function as the switching devices within the system. Node MCU: Serving as the microcontroller unit in the prototype, the Node MCU is equipped with an integrated Wi-Fi module (ESP8266 0.9). This module enables the wireless remote switching of home appliances. Blynk Application: Tailored for the Internet of Things (IoT), the Blynk application assumes a pivotal role in the prototype. It possesses the capability to remotely control hardware, showcase sensor data, store and visualize data, etc. Its primary role in this context is to interpret user commands and transmit them to the hardware over a wireless network.

Google Assistant: Functioning as a system software on Android phones, Google Assistant interprets voice commands issued by users to turn appliances on or off. It serves as the voice-controlled interface within the system. IFTTT Application: IFTTT as an intermediary application in the system. It becomes relevant when the voice commands interpreted by Google Assistant are not directly understandable by the Blynk application. IFTTT interprets commands from Google Assistant and sends on/off signals to the Blynk application via the Blynk server, facilitating smooth communication among various components in the system.

Components Required

1. Node MCU
2. Channel relay
3. Battery 9V
4. Resistor 2.2kohm
5. LED
6. USB Cable
7. Blank PCB KS100
8. Male pin, Female pin, and Jumper Wires

Embedded System Setup

Hardware Assembly The hardware assembly primarily involves linking the supply, ground pins, and digital pins of the NodeMCU to the four relays on the relay module. The essential setup of this prototype is straightforward. Connect any desired device for control to the remaining four relays. While assembling the hardware, it's crucial to keep track of which digital pin corresponds to each relay. This alignment follows the settings in the Blynk application. Configure the radio buttons on the Blynk application to toggle a specific Node MCU digital pin and ensure that the physical relay connections match this configuration. Figure 3 For instance, if D3 is assigned to operate with the radio button on the Blynk application corresponding to relay 1, physically connect relay 1 to Node MCU D.

Software Setup – Blynk Interfacing

- Install the Blynk application.
- The project is established, given a name, and has Node MCU hardware and Wi-Fi connection type selected.
- Blynk will now send an authentication token to the email address provided. Figure 4 The Blynk server's hardware will be recognized by this authentication token.
- Since the prototype makes use of a 4-channel relay module, the side bar's four buttons are added to the screen.
- After that, each of the four buttons can be personalized by giving them names and choosing the corresponding digital pin.
- The Blynk application has now finished setting up.

Results and Discussion

Advantages

- Effortless installation without legal complications
- Theft deterrence through wireless operation, eliminating physical wire vulnerabilities.
- Extended control range of 150 feet indoors for comprehensive home automation
- Robust security ensured through a connection established over a secure network.
- Versatile integration into diverse setups, enabling easy addition or removal of appliances as needed.

Disadvantages

- Android devices with API versions lower than 16 necessitate internet access to convert voice to sentence or string.
- External voices may impact our results when utilizing voice mode.
- There's a likelihood that the speech command

Future Scope Given the current circumstances, there is an opportunity to create a solution that works across different platforms, including Windows and iOS. Expanding the automation to cover all household devices removes the limitation of operating only a set number of gadgets. The prototype can incorporate various sensors, such as a PIR for motion detection and security alerts, a DHT11 sensor for monitoring ambient temperature and humidity, adjusting the fan or air conditioner accordingly, and an LDR for sensing daylight and controlling the lamp. By extending the project's reach beyond homes and small offices, it can cater to a wide array of locations.

Reference

[1]. S. Dey, A. Roy and S. Das, "Home automation using Internet of Thing", 2016 IEEE 7th Annual Ubiquitous Computing Electronics & Mobile Communication Conference
(UEMCON), 2016.

[2]. Rekha Gole, Komal Sangale and Rishil Ramesh, "Smart Air Conditioning Control System: A Literature Review", International Journal of Information and Computer Science, 2019.

[3]. Majid Al Kuwari, Ramadan Abdulrahman et al., "Smart-Home Automation using IOT-based Sensing and Monitoring Platform", IEEE 12th International Conference on Compatibility Power Electronics and Power Engineering, 2018.

[4]. Federico Viani, Fabrizio Robol and Polo Alessandro, "Wireless Architectures for Heterogeneous Sensing in Smart Home Applications: Concepts and Real Implementation",

Proceedings of the IEEE, vol. 101, no. 11, Nov. 2013.

[5]. Takeshi Yashiro, Shinsuke Kobayashi, Noboru Koshizuka et al., “An Internet of Things (IOT) Architecture for Embedded Appliances”, IEEE Region 10 Humanitarian Technology Conference, 2013.

6]. Vaishnavi S. Gunge and Pratibha S. Yalagi, "Smart Home Automation: A Literature Review", National Seminar on Recent Trends in Data Mining-RTDM, 2016.

[7]. Ali Mohammed Al-Kuwari, Cesar OrtegaSanchez, Atif Sharif and Vidyasagar Potdar, "User-Friendly Smart Home Infrastructure: Bee House", IEEE 5th International Conference on Digital Ecosystems and Technologies, May31-June3 2011.