IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Development of a Secure IoT-Based Home Automation System

Miss. Priya Dhule
P.G. Student Computer Engineering Department
Gokhale Education Society's,
R. H. Sapat College of Engineering, Management studies and Research, Nashik,
Savitribaiphule Pune University, Pune

Abstract: *Advances in technology such as internet-of-things (IoT) and its wide-ranging applications have made it necessary to have smart homes. The ease with which home appliances can be remotely monitored and controlled improves the standard of living, as automatic processes are used to replace manual efforts to perform some basic functions in the home. The busy schedules of individuals have heightened the pressing need for intelligent homes. Household owners tend to pay more for electricity consumption even though they were not physically present at home, but their devices were either intentionally or ignorantly left ON when not in use. Elderly people and physically challenged individuals find it hard to execute fundamental tasks manually, such as switching ON/OFF lights, fan, TV set, and other home appliances. In this work, a smart home that can remotely automate the operation of home appliances and smartly make decisions without human interference is proposed. In addition, this paper presents a smart home system that has an interactive graphical user interface on an android device to allow the user to choose whether to remotely control and monitor the home from their android device or to enable automatic control using sensors that are interfaced with a home-based PIC microcontroller. The temperature sensor, the light sensor, the passive infrared sensor (PIR) and the Wi-Fi module, which enable internet connection between the microcontroller and the Android application, are all interfaced with the PIC microcontroller at the receiving end, while at the transmitting end, the graphical user interface application on the android device sends commands to the microcontroller to which the sensors and loads are interfaced. The proposed system will be very helpful in energy conservation, while ease of remotely operating home appliances is also provided to both physically challenged and healthy individuals..*

Keywords: Internet-of-things, microcontroller, sensors, smart home

I. INTRODUCTION

The theory of home automation has been around since 1970"s.As much as IoT helping in automating tasks, the benefits of IoT can be extended for build up the current safety standards. The modern homes are automated through the internet and the home appliances are controlled. For an example with smart locking control, you can remotely secure equipped doors and windows from anywhere in the world whether you're in bed, at work or on vacation. Integrated Automation: your smart security system can be more than just alarms, cameras, sensors and locks. The home automation segments also includes smart lighting, smart TVs other appliances. wearable's (smart watch, fitness brands, smart headphones, smart clothing) are expected to witness the growth in the future generation. today in India, nearly 22.5per cent of the consumers were familiar with the concepts of IoT, with maximum awareness seen in the 36- 55age group. A smart home focuses on the automation and control of environmental services such as day lighting, heating, ventilation and air conditioning systems, monitoring and control, security and safety, and energy savings. The alerts and the status of the IoT system can be accessed by the user from anywhere even where Internet connectivity may not be readily available (since it is not necessary for the mobile phone to be connected to internet only board is required to have an access to

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Wi-Fi). Home security made a drastic changes in the past few decades and continue to advance much more in the coming years.

The IoT application domains are very important and will increase over time, as they offer powerful means to help and support the special needs of the elderly and people with disabilities , enabling users to monitor and control the environment. A smart home focuses on the automation and control of environmental services such as day lighting, heating, ventilation and air conditioning systems. The main purpose of this project is to monitor temperature, liquid petroleum gas (LPG) leakage and fire detection.

the authors name can be used along with the reference number in the running text. The order of reference in the running text should match with the list of references at the end of the paper.

II. LITERATURE RIVIEW

A ZigBee based home automation system In the ZigBee based home automation system, it consists of a coordinator, router and some other devices for connectivity. The Wifi network configured in the home is a standard four port switch modem router which act as a gateway between the local Wifi network in the home and internet and any device in the range of the wifi network can access the home gateway. But as the ZigBee compatible devices are less and not advanced ZigBee based home automation systems are less prioritized as compared to other controllers now a days in internet of things

GSM based home automation system The GSM is the best option for home controlling from a distant place where the internet is not accessible or not efficient. In the GSM based system the communication is established between the user and the home through the SMS (Short Message Service). A GSM modem is used for this. The communication between the automation server and the GSM modem is done through the attention (AT) commands and sending and receiving of SMS messages are through PDU(Protocol Description Unit) because all GSM modules may not supports text mode. Anyway the GSM based system is the better option in the absence of internet however it is limited compared to the internet services.

Security in internet of things enabled home automation The security is the major look up in case of every system. The internet of things has got many ways in its security resolving. A paper formulated a reconfigurable DTLS (Datagram Transport Layer Security) cryptography engines for the end to end security in IoT applications and also SSL encryption etc are also many ways of securing the internet of things connected devices.

III. METHODOLOGY

he methodology for developing a secure IoT-based home automation system involves several stages, ranging from system design and development to security implementation and testing. Below is the step-by-step approach to achieve this project:

1. System Design and Requirement Analysis

- Objective: Define the scope and functionality of the IoT-based home automation system.
- Requirements: Identify the appliances to be controlled (e.g., lights, fans, security systems) and the communication protocols (e.g., Wi-Fi, Zigbee, Bluetooth).
- Security Features: Design security requirements such as encrypted data transfer, secure authentication, and multi-factor authentication to protect user privacy and prevent unauthorized access.

2. Selection of IoT Devices and Platforms

Hardware Components:

- Microcontroller: Select an IoT platform (e.g., Raspberry Pi, Arduino) to act as the central controller.
- Sensors and Actuators: Choose sensors (e.g., temperature, motion) and actuators (e.g., relays, smart plugs) for monitoring and controlling appliances.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

- Communication Modules: Integrate wireless communication technologies such as Wi-Fi (ESP8266/ESP32), Zigbee (Xbee), or Bluetooth (HC-05/HC-06) for deviceconnectivity.
- Software Platform: Choose an appropriate development platform (e.g., Arduino IDE, Node-RED, or Raspberry Pi with Python) for programming the devices.

3. System Architecture Design

- Centralized Control System: Design a centralized controller (either cloud-based or local server) that connects to all IoT devices. This system should allow users to control devices remotely.
- User Interface: Develop a mobile application (Android/iOS) or a web-based interface for the users to interact with the system. The interface should be intuitive and allow users to control devices, monitor status, and view energy consumption.
- Data Flow: Ensure that data between devices and user interfaces is securely transmitted.

4. Security Implementation

Data Encryption: Use strong encryption techniques (e.g., AES, RSA) to secure communication between devices, the controller, and the user interface.

Authentication Mechanisms:

- Implement secure user login using multi-factor authentication (MFA) to protect access to the home automation system.
- Use OAuth or token-based authentication for secure communication between the mobile/web application and the server.

Secure Communication Protocols: Implement secure communication protocols like TLS/SSL for data transmission to ensure the confidentiality and integrity of data.

Access Control: Set up role-based access control to ensure different levels of access for users (e.g., admin, user).

5. System Integration

- Device Setup: Integrate sensors, actuators, and microcontrollers into the system. This includes wiring the sensors and actuators to the controller and ensuring proper communication between devices.
- Backend Integration: Develop the backend system (e.g., Node.js, Python Flask) to manage device data, user interactions, and security features.

6. Energy Management and Optimization

- Energy Monitoring: Implement a real-time energy monitoring system that provides users with the current status of their devices and energy consumption. This helps in identifying energy usage patterns and optimizing electricity usage.
- Automated Scheduling: Allow users to create schedules for devices (e.g., automatically turning lights off after a certain time or adjusting temperature settings based on time of day).

7. User Interface Development

- Mobile Application: Develop a mobile app using tools like React Native, Flutter, or native Android/iOS frameworks for remote control of the appliances.
- Web Interface: If applicable, create a web dashboard using frameworks like Angular, React, or Vue.js, to provide users with an additional interface for controlling and monitoring the devices.
- Real-Time Feedback: Implement real-time updates and status reporting to show appliance states (on/off), energy usage, and security alerts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

8. Testing and Validation

- Functional Testing: Test all functionalities to ensure devices respond correctly to commands, and the user interface is intuitive and responsive.
- Security Testing: Conduct penetration testing, vulnerability scanning, and security audits to identify and fix any security flaws.
- Load and Performance Testing: Ensure the system can handle multiple devices and user requests without performance degradation.

9. Deployment and Final Evaluation

- Deployment: Deploy the system to a test environment or real-world scenario to verify its performance under practical conditions.
- User Feedback: Collect feedback from end-users on usability, system reliability, and any security concerns.
- Optimization: Based on feedback, refine the system for better performance, security, and energy efficiency.

10. Documentation and Reporting

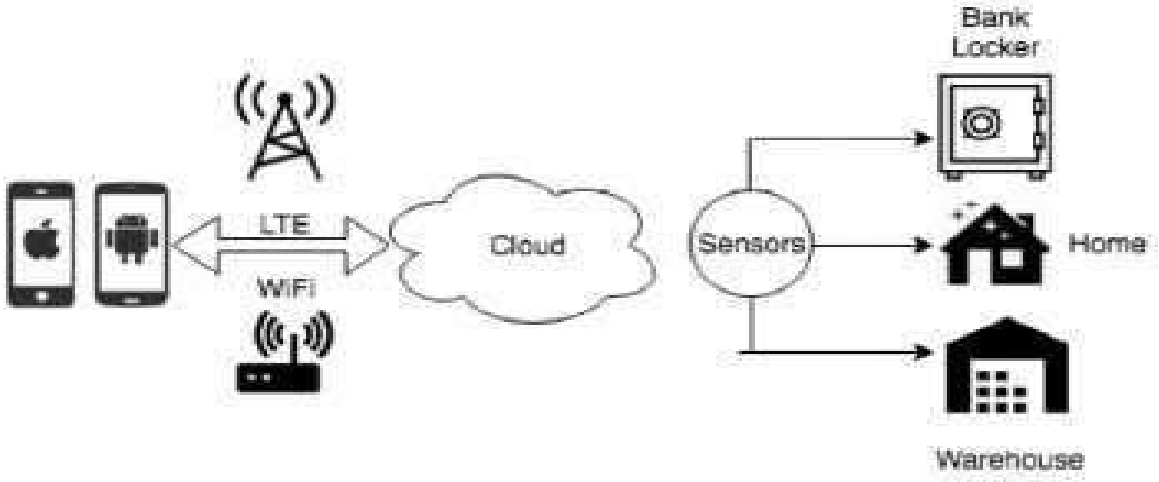
User Manual: Provide documentation for end-users to understand how to install, configure, and use the home automation system.

System Documentation: Include detailed technical documentation on the system architecture, security features, device setup, and softwar

Tools and Technologies Used:

Hardware: Raspberry Pi/Arduino, ESP8266/ESP32, Sensors (motion, temperature), Actuators (smart plugs, relays), Zigbee/Bluetooth modules.

Software: Python, Node.js, Android Studio (for mobile app), HTML/CSS/JavaScript (for web)



IV. CONCLUSION

The home automation system has been experimentally proved to work satisfactorily by connecting sample appliances to it and the appliances were successfully controlled from a wireless mobile device .Home security is rapidly growing field and there are news and improved burglar alarms popping up every day. People can control their electrical devices through set up controlling actions through mobile. Finally we come to a conclusion that before making the decision of installing home security system we must gather complete knowledge about the security system

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

REFERENCES

[1].https://www.researchgate.net/publication/31255942 [2]._IoT_based_smart_security_and_home_automationstem
[3].https://smartify.in/knowledgebase/iot-based-homeautomation-system/ [4].https://www.slideshare.net/shohin/iot-homeautomation-using-arduino-cayenne[5].https://www.scribd.com/document/383625534/IoTBased-Smart-Security-and-Home-Automation-System
[6].https://www.semanticscholar.org/paper/IoT-basedsmart-security-and-home-automation-system-KodaliJain/381344084f632fd0006bbd0b560a65e674f18f34 https://en.wikipedia.org/wiki/Electronic_componen