Smart Home Automation System
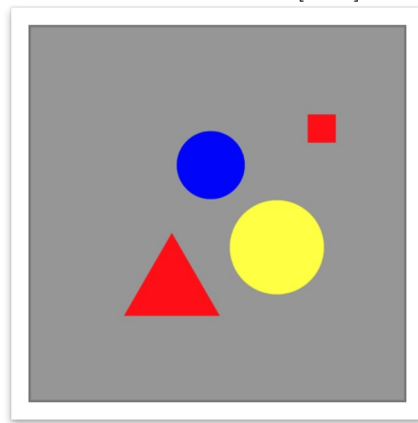
Research Paper Summary

RYAN ADEN GEORGE

21011101102

AI-DS B

OPEN ELECTIVE[IOT]

SHIV NADAR UNIVERSITY
CHENNAI

Computer Science and Engineering
Shiv Nadar University, Chennai
22 JANUARY 2023

Explanation

0.1 Summary

The key challenges in a smart home are intelligent decision making, secure identification, and authentication of the IoT devices, continuous connectivity, data security, and privacy issues. The existing systems are targeting one or two of these issues whereas a smart home automation system that is not only secure but also has intelligent decision making and analytical abilities is the need of time. In this paper, we present a novel idea of a smart home that uses a machine learning algorithm (Support Vector Machine) for intelligent decision making and also uses blockchain technology to ensure identification and authentication of the IoT devices. Emerging blockchain technology plays a vital role by providing a reliable, secure, and decentralized mechanism for identification and authentication of the IoT devices used in the proposed home automation system. Moreover, the SVM classifier is applied to classify the status of devices used in the proposed smart home automation system into one of the two categories, i.e., "ON" and "OFF." This system is based on Raspberry Pi, 5V relay circuit, and some sensors. A mobile application is developed using the Android platform. Raspberry Pi acting as the server maintains the database of each appliance. The HTTP web interface and apache server are used for communication among the Android app and Raspberry Pi. The proposed idea is tested in the lab and real life to validate its effectiveness and usefulness. It is also ensured that the hardware and technology used in the proposed idea are cheap, easily available, and replicable. The experimental results highlight its significance and validate the proof of the concept.

KEY SOLUTIONS FROM THE AUTHOR

To assure home automation continues in a normal fashion, it is necessary to check all important parameters that may complicate the system, one of which is no GUI environment for the users. Users cannot understand the working of the system due to the lack of a GUI environment. Secondly, there is no device restoration which is harmful to home appliances. Thirdly, there is no prediction of the electricity bill for the users, and all the previous home automation solutions are very expensive. So, we provide an effective solution to overcome all these problems by undertaking the following objectives. (i) The proposed solution is low cost because it did not use IP-based devices such as bulb and light. (ii) The proposed solution provides electricity bill prediction to the users. The proposed solution uses GSM technology which means a Global System for Mobile Communication (GSM) modem to control home appliances such as light, conditional system, and security system via Short Message Service (SMS) text messages. (iii) The proposed solution provides device restoration which means when you restore a computer or other electronic device, you return it to a pre-vious state. (iv) The proposed solution is a cloud-based solution which means it controls home appliances through the Internet. (v) The proposed solution provides Arduino and Raspberry implementation. For those who love to tinker with electronics, the Raspberry Pi and Arduino have become invaluable tools. They are both extremely popular options but are also very budget-friendly. Arduino is best used for real-time applications of hardware and software, and Raspberry Pi easily connects to the Internet. (vi) The proposed solution provides a prototype home design for the ease of the users. (vii) The proposed solution has an intelligent decision-making ability to classify the status of IoT devices used in the smart home automation system. (viii) The proposed solution ensures secure identification and authentication of users using blockchain technology.

Blockchain for Security of Smart Home

A key objective of the smart home automation system is to provide a trusted, secure identification and authentication of IoT devices. To ensure these objectives, we have used blockchain technology. Blockchain tech-

nology was introduced by Nakamoto in 2008 [35]. The main features of blockchain technology are security, anonymity, and decentralization [36]. These features can be fruitful to IoT by providing more security and reduced dependency on the central server. Moreover, blockchain technology also ensures tempered resistance data structure by utilizing data encryption and timestamp. In the proposed approach, the implementation of the blockchain module is accomplished in Java by defining the block's contents in a hash that is a unique identifier. Using each block, a block hash is computed, and a hash SHA-256 is, then, computed from it. On achieving a threshold, requests for connectivity are granted through managing blockchain, and then, a block is created. To validate the complete blockchain, a block of the chain is looped-over that verify a current block's hash to its corresponding previous block's hash.

BRIEF ALGORITHM

We have also designed an algorithm to explain the working of blockchain technology in the proposed approach given as follows. The whole process of blockchain implementation is also depicted in a flowchart shown in Figure 3 and Algorithm 1.

(1) At the first step, a block is created with the help of the block class (2) A hash is created using the SHA–256 algorithm on the successful creation of an already created block otherwise repeat step 1 (3) After the generation of hash, the next step is to store the blocks (4) At the last step, the validity of the blockchain will be accomplished. If the block is valid, then request for connectivity is granted (5) If the block is not valid, steps 1 to 4 are repeated