International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 4378 - 4387

Self-Harvested Energy Implementation for Smart Hub using Raspberry Pi

T. V. Gandhi[1], S.K. Jagtap[2], A.S. Pandit[3], N. S.Gitte[4], P. D.Kalekar[5]
Department of E&TC, SKNCOE, SPPU, Pune.
[1]truptigandhi99@gmail.com
[2]skjagtap.skncoe@sinhgad.edu
[3]anuradha.pandit_skncoe@sinhgad.edu
[4]nikitagitte546@gmail.com
[5]prajaktakalekard32@gmail.com

Abstract

Smart homes are the components of developing smart cities. In recent years, countries around the world are taking efforts in promoting smart cities. Smart homes are the stimulating technological advancement which will make people's lives more convenient. The development of smart homes involves access control of the building's electricity, energy harvesting and storage for the active electronic devices and circuitries and wireless communication for smart switches and smart sockets. In order to design a smart home system, a practical design and implementation of security (access control system) for a building's power supply which adds a locking feature such that only authorized personnel are capable of altering the facility state of the smart sockets and switches in a building is needed and also a model of energy harvesting and storage system for the active electronic components of the circuitries and wireless communication for smart switches and sockets. The access control involves main four stages (a control unit, a comparator unit, a memory unit and thus the switching unit).The access control system provides a means of access control by having a security keypad that switches ON or OFF the building's electricity, provided the user knows security pin code. System also harvests and stores energy for all the active electronic devices employing a photovoltaic system with an ultra capacitor energy buffer. The designed secured smart home utilized smart power and switches and message queuing telemetry transport for straightforward controlling energy usage. The experimental results show an improvement in security as well as in energy management building.

Keywords— *Self-Energy Harvesting, Raspberry pi, Node MCU, Electricity, Wireless Technology.*

I. INTRODUCTION

The smart home and available smart devices become increasingly popular, most people do tend to require more comfort and home automation devices to upgrade their living spaces to enjoy a high-tech life, hence, leading to the demand to equip the houses with different a kind of sensors and actuators for optimal security and ease of appliances control. Many countries use communication-based controlling and monitoring architecture to save power and have detectors and recorders to record power. Communication through wired interfacing and interconnection is very entangled and critical to install whereas this system wireless interface is used because it is easy to install and advanced than the previous one. Various hardware techniques are used for power controlling and monitoring. The system implements security (access control system) for a building's power supply. Also, harvest and store energy for all the active electronic devices using a photovoltaic system with wireless communication for smart switches and sockets.

II. LITERATURE REVIEW

ISSN: 2233-7853 IJFGCN

Ms. D. Barge, A. R. Surve focused on various approaches which found to be helpful for energy conservation. Also, energy harvesting system implementation using new technologies like IoT, ANN can be explored here [1].

M. A. Sabrin, A. P. Mathew, gives an IoT network system for connected health and safety applications for the industrial outdoor workstation where the arrangement was able to monitor both physiological and environmental data forming a network from wearable sensors attached to workers' body and provide priceless information to the system operator and workers for safety and health monitoring [2].

T. A. Khoa and H. Hai, focuses on information security, big data, mobile networks, cloud computing, and the Internet of Things. Security efficiency can be enhanced by using a Secure Hash Algorithm 256 (SHA-256), which is an authentication mechanism that, with the help of the user, can authenticate each interaction of a given device with a WebServer by using an encrypted username, password, and token. This framework could be used for an automated burglar alarm system, guest attendance monitoring, and light switches, all of which are easily integrated with any smart city base[3].

A. Trigui and M. Ali, presented Wireless Power and Data Transfer (WPDT) system which is also capable of operating under a wide range of data rates. It allows a maximum data rate of 3.33 Mb/s for which maximum power delivery is 6.1 mW at 1 cm coils separation distance. The system recovers more power when it reaches 55 mW at 100 kb/s. Due to the system genericity, an operator gets an option to select the best compromise between power and data rates following the application or current need, without reconfiguring the receiver. There's one more advantage of this modulation technique which is the simple implementation and the ultra-low power consumption of the CWM demodulator despite its high-speed demodulation[4].

Y. Yang, presented a low-power farm environment detection system based on LoRa wireless technology. Which use various sensors in the laboratory to complete the detection of soil and model environmental parameters, and implement lighting control and irrigation control, cooling control and man-machine control. The designed system sleep current is very low equal to 0.3 μ A, the average working current, has the advantages of long transmission distance and low power consumption. After verifying the feasibility of the technology through an experimental model, the system was applied to a specific greenhouse and data collection and analysis were completed [5].

Thirumurugachandar and Sankari system explains that there is no need of energy from conventional source of energy and there is zero percent of pollution in this type of power generation. There is no need for any kind of power from mains and it is important to the areas, all tracks where footsteps are used to generate non-conventional energy such as electricity. The main motto of this was to face the energy crisis which is the main issue in the world [6].

J. Yadav and L. Patidar, presented a system that describes the process of making an efficient piezoelectric harvester. A piezoelectric energy harvester was has been simulated successfully and the results in the form of waveforms were obtained on the scope block of the simulation circuit. It shows clear from the results that to get smooth rectified output. The expected result is obtained from the circuit model developed in MATLAB [7].

C. Jia and X. Zhang plans reduces the data storage, time, and space of each sensor and optimizes the control of the IBEMS.The research results provide a reference for setting up a safe and reliable IBEMS based on spatial distribution and it helps to promote blockchain technology in other scenarios of the UPIoT [8].

ISSN: 2233-7853 IJFGCN

L. Yang and H. Deng, presented a privacy protection scheme which is based on information hiding, scheme guarantees the sensitive data transmitted securely. At First, the smart home Real-time sensor data are classified into two parts, sensitive data and non-sensitive data through machine learning, the process can be controlled according to the user's preferences. Secondly, the sensitive data can be transmitted securely by ordinary channels using the method of combination encryption with information hiding [9].

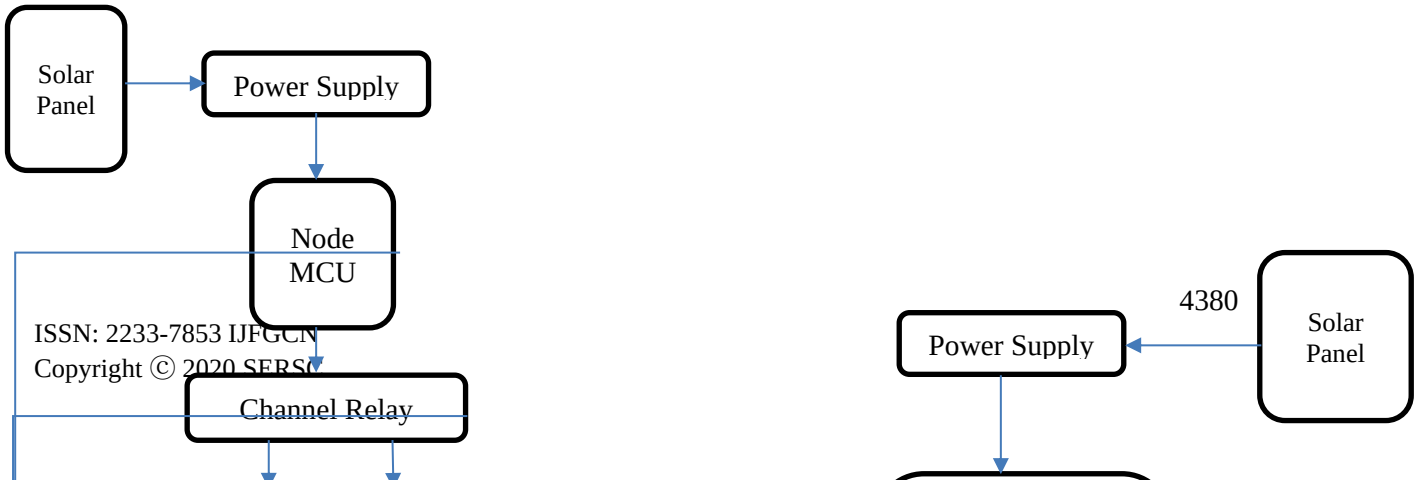
A. M. zungeru and B. diarra,contributioned two types of design of smart home systems. 1) A practical design and implementation of security for a building's power supply which adds a locking feature such that only authorized personnel is capable of altering the power state of the smart sockets and smart switches in a building.2)A model of energy harvesting and storage system for the active electronic components of the circuitries and wireless communication for smart switches and sockets [10].

D. S. Kale, D. L. Bhombe and Dhiraj P. Tulaskar,system presented an Implementation of Soil Energy Harvesting System For Real-Time Monitoring Of Agriculture used to build the yield of plants by observing and controlling ecological conditions (parameter) and along these lines giving important data to the farmers [11].

R. Bhamral and S. Mahajan, overview of the key issues related to the development of IOT technologies and services and wireless energy harvesting unit. Number of research challenges has been identified, which are expected to become major research trends in coming next years. The most relevant application fields have been presented, and several use cases identified [12].

III. SYSTEM METHODOLOGY

The system is designed such that smart sockets wirelessly provide necessary data to a central Controller, to reduce energy consumption in a smart building. The main building blocks are a smart hub, smart socket, smart switch, smart switchboard, energy harvesting system, and access control. Access control is the first form of buildings power supply security. It connects power from the smart meter to the rest of a building through a smart switchboard. By entering the correct pin code using an inbuilt keypad on Access control, only authorized users can turn on or off the power into the entire building. The proposed system has two power sources; one is the energy harvesting system, and the other is the main power line from a power grid into a building. At the core, the proposed system is the smart hub. The smart hub provides centralized control of the whole building's electricity, creates the internal Wi-Fi network access point for the system, and also bridges the internal network to cellular networks by the use of a GSM modem. Through the smart hub, an authorized user can remotely and locally monitor and control the power states of smart switches, smart sockets, and smart switchboards in a building and hence monitor and control the state
of appliances connected to a building’s power supply.



ISSN: 2233-7853 IJFGCN

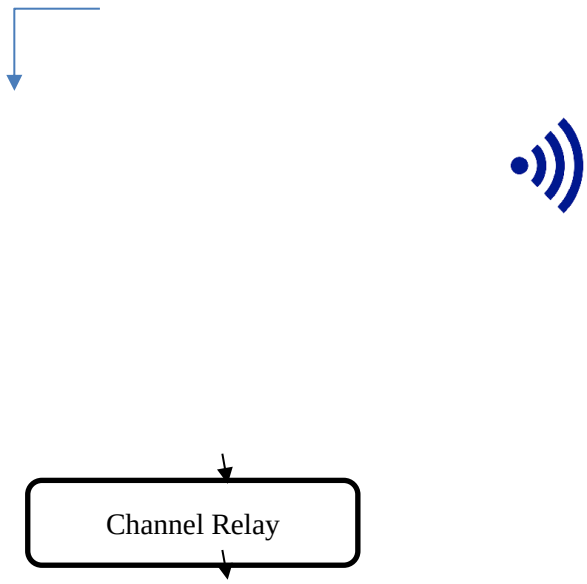


Fig.1 Block diagram of the system.

Smart switches, smart sockets, and smart switchboards are the actuators of the system. They are responsible for the physical control of AC power into appliances in a building, and they do so based on the commands wirelessly communicated from the smart hub or based on a user's physical interaction with the switches present on them.

To connect a house's main distribution box and control (switch on/off) by use of relays the main house electrical routes (house lights, house sockets). Have two methods of user input. It is via internal keypad or wirelessly through SMS. Have two methods of relaying information to the user. That is via internal display monitor or wirelessly through SMS. Capable of locking and unlocking ability to switch the power state of the main house relay switches with a key code. Wirelessly collect data from smart sensors. Wirelessly collect the data and control (switch on/off) the smart switches and smart sockets. Wirelessly lock and unlock ability to switch the power state of the smart switches and smart sockets. For the realization of the WSN based Smart Home System, the smart hub houses a Raspberry Pi microprocessor and a USB dongle modem of which are connected to set up a communication link for transferring data around the system. The GSM micro-controller sets up a link between Smart Hub and the user's cell phone. The Raspberry Pi acts as both the Smart Hubs control center, and Wi-Fi between the Smart Hub and the Smart Sockets or Smart Switches.

The smart home switch acts as a remote switch that can be turned on or off either by commands wirelessly sent from the smart hub or physically by a user. To switch the circuit, it controls on or off based on commands from the smart hub or the action of a user manually pressing on the in built switch to change between the two power states (ON/OFF). Send state of the switch (ON/OFF) to the smart home hub. Lock the state of switch (on/off) so that it cannot be manually turned on/off when commanded by the smart hub. The smart home socket acts as a remote socket that can be turned on or off either by commands wirelessly sent from the smart hub or physically by a user. To switch the circuit, it controls on or off based on commands from a smart hub or action of a user manually pressing on the

ISSN: 2233-7853 IJFGCN

inbuilt switch to change between two power states (On/Off). Send the state of its switch (on/off) to a smart hub. Lock the state of its switch (on/off) so that it cannot be manually turn on/off if commanded by the smart hub.

IV. EXPERIMENTATION

This section describes the design process of the wireless sensor network (WSN) based smart home system. The proposed system has a node called “smart home hub (smart hub)” to function as the core sink node of the WSN based smart home, and three other nodes. Through the smart hub, a user can interact with appliances connected to the smart sockets and switches. The electrical connections between the raspberry pi to the keypad and LCD screens are made, using female sockets at the Raspberry Pi and male pins at the breadboard side. The USB dongle modem is connected directly to the Raspberry Pi USB port. User input interactions with the smart home hub are done through the keypad and output from the smart home hub is through the character LCD screens. From this state, an authorized user can remotely change the facility or lock states of the smart home switches. If another user were to press the switch on an unlocked switch, the change of power state would be reflected on the information displayed on the LCD screen. However, if a user press on a locked smart home switch, the input from the user will be ignored, and the power state of the switch will not change nor will the information displayed on the LCD screens.

ISSN: 2233-7853 IJFGCN

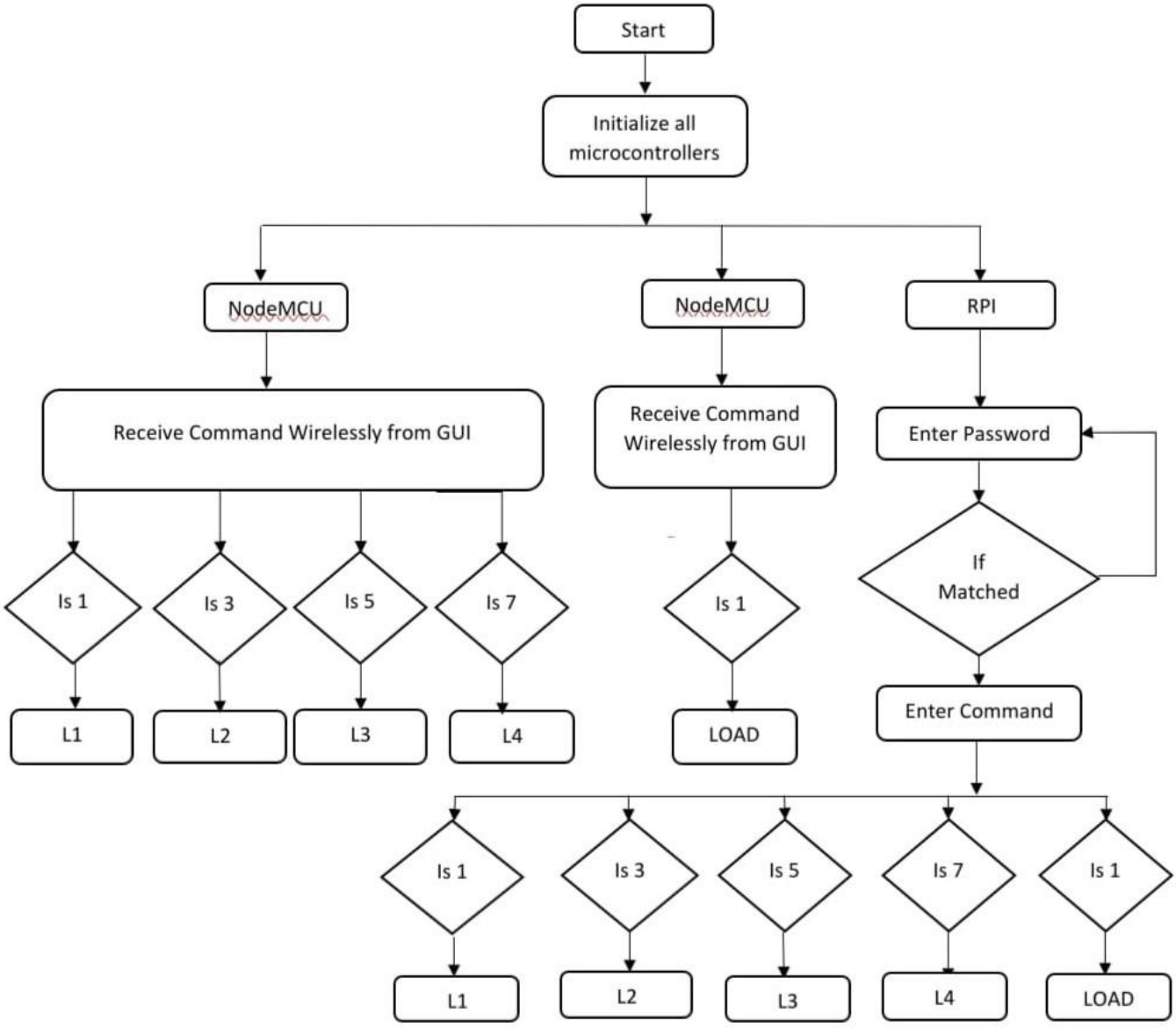


Fig2. Flow chart of the system.

The main components of the system are raspberry pi and node MCU, for wireless communication. Raspberry pi is connected to keypad, LCD and GSM. So to access the commands to the load, one has to enter the password in keypad which is viewed on LCD. If the password is correct, then the command is taken and accordingly load works for two different node MCU's and their load respectively. Now, for respective load to work according to the command, they are assigned some values. For load L1, when you press 1 it gets ON and when you press 2 it gets off accordingly. For load L2, when you press 3 it gets ON and when you press 4 it gets off . For load L3, when you press 5 it gets ON and when you press 6 it gets off. For load L4, when you press 7 it gets ON and when you press 8 it gets off. These were the values for load of the first node MCU which has four loads connected to it. Now, to the second node MCU only one load is connected and it gets ON when you press 1 and OFF when you press 2. Two node MCU's have their own different IP address and so are the values for their load differentiated.

V. RESULTS AND DISCUSSION

ISSN: 2233-7853 IJFGCN

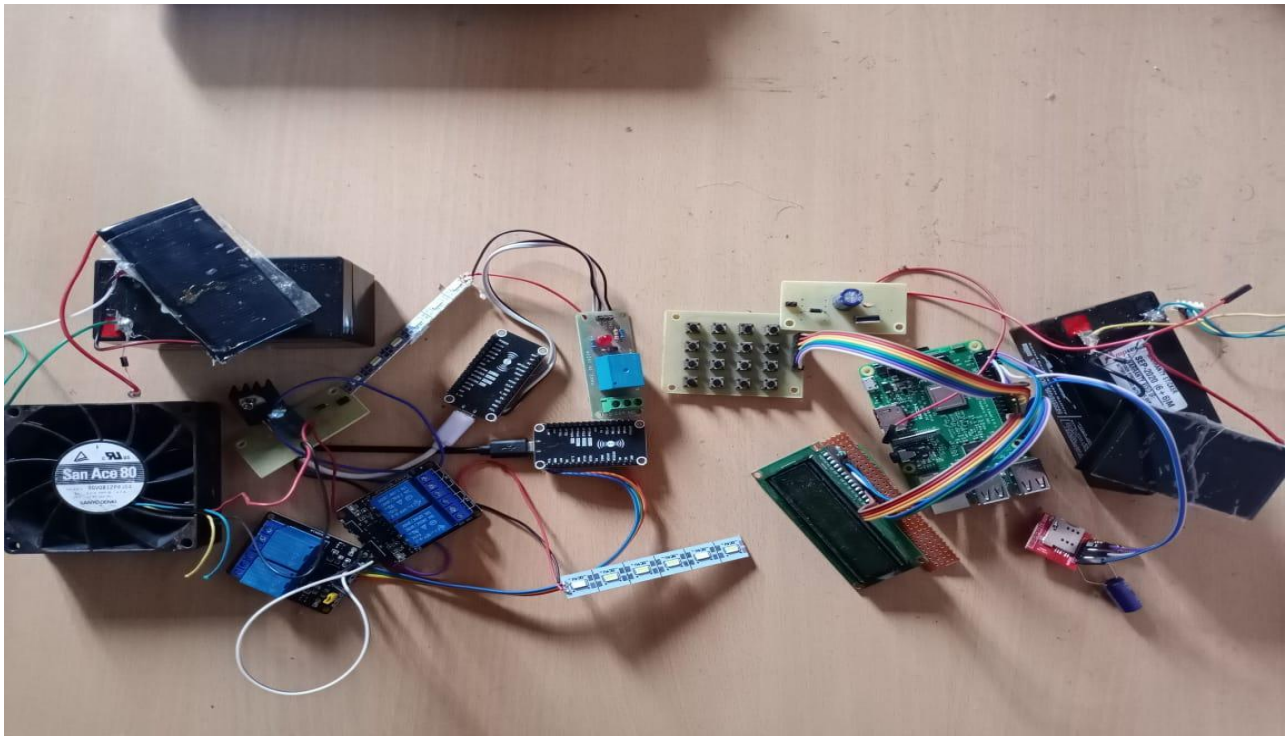


Fig. 3 Experimental setup of the system

Procedure 1: System-Locked

Description: When the system is locked, a pin code request is displayed on the Smart Hub LCD screen as shown in Fig.4. A user must enter the correct pin code using the inbuilt keypad into the system. Entering of a wrong password by a user leads to an error message to be displayed on the smart hub LCD screen. The smart hub LCD screen then displays a new pin code request for a user to retry. A correctly entered pin code leads to the display of enter command as shown in Fig.5.

Fig.4 Enter password

Fig.5 Enter command

Procedure 2: System Unlocked

When the command is enter the system processes the message and sends commands to the affected smart sockets/switch. This is accomplished by selecting an available smart switch or smart socket by entering the number associated with the device. Having selected the device, the Target-Device-Edit function is called. Example: If '1'is press on keypad light will switch on as shown Fig.6 and so on. If

ISSN: 2233-7853 IJFGCN

the user is satisfied with the changes made and does not desire to make further changes, they can press on the keypad and go back to the system locked state.

Procedure 3: Target-Device-Edit

Description: This is the function called upon by the System-Unlocked function when a user wants to change a Smart home socket or Smart home switch device (Smart Devices) Power-State or Lock-State. The function performs this by displaying a blinking cursor over the state (power state or lock-state) that is being modified. Interacting with the keypad, allows a user to toggle a blinking cursor between the two states (power-state or lock-state), toggle the value of the states (on/off or unlocked/locked) and return to the System-Unlocked function.

Fig.6 Load on

Function 4: Smart home Socket/Switch-Main-Loop
Description: This is a function that is used by the smart home sockets or switches when they receive an MQTT data packet command from the smart hub or when a user has pressed the local switch on the socket or switch. When a command is received, it is processed to check whether it affects its power state or the lock state of the device. If the command is to change the lock state, it then deactivates any commands from the local switch until the switch is unlocked. If the command is to change the power state, it toggles the current power state of the switch or socket. Apart from a command from the smart hub, if it receives a command from the local switch, it is first checked whether the switch is locked or not. If the switch is locked, the pulses from the switch are ignored, but if it is not locked, it toggles the power state of the switch or socket and then updates the Smart Home Hub of the change in the state.

Advantages and Applications:

1. Independent of main power supply for electricity.
2. Smart grids tell us the consumption of an energy meter at any time, so users are better informed of their real consumption.
3. Use of renewable energy resources.
4. Solar water heating, Solar heating of buildings, Solar distillation, Solar pumping, Solar electric power generation, etc.

VI. CONCLUSION

The system presents the design and implementation of a secured smart home switching system based on wireless communication and self-energy harvesting. The system introduces main access control of the building's electricity, energy harvesting, and storage for the active electronic components of the circuitries and wireless communication for smart switches and sockets. In energy harvesting, readily available energy from environment is converted to usable electrical energy that provides a viable solution for continuous powering of various loads. Also harvests and stores energy for all the active

ISSN: 2233-7853 IJFGCN

electronic devices using a photovoltaic system with an ultra-capacitor energy buffer and shows improved energy management in a building. The security of the entire smart home system including the smart control of home appliances is guaranteed.

REFERENCES

[1] Ms. D. Barge, A. R. Surve, "*A Review on Energy Conservation System with IoT Oriented Technique*",International Research Journal of Engineering and Technology (IRJET), 2020.

[2] M. A. Sabrin, A. P. Mathew, "*Literature Review of Design and Implementation of a Wearable Sensor Network System for IoT-Connected Safety and Health Applications*",International Research Journal of Engineering and Technology (IRJET) ,2020

[3] T. A. Khoa and H. Hai, "*Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study*", Hindawi Wireless and communication , Research Article , 2020

[4] A. Trigui and M. Ali, "*Generic Wireless Power Transfer and Data Communication System Based on a Novel Modulation Technique*", IEEE Transaction on Circuits and System,2020

[5] Y. Yang , " *Design and Application of Intelligent Agriculture Service System With LoRa-based on Wireless Sensor Network*" , International Conference on computer Engineering and Application , 2020

[6] Thirumurugachandar and Sankari,"*Efficient Energy Harvesting And Reusing System*", International Research Journal of Engineering and Technology (IRJET), 2020

[7] J. Yadav and L. Patidar, "*Energy Harvesting From Piezoelectric Materials*", International Research Journal of Engineering and Technology (IRJET), 2020

[8] C. Jia and X. Zhang, "Design of *a dynamic key management plan for intelligent building energy management system based on wireless sensor network and Blockchain Technology*", School of Intelligent Manufacturing, Jiangsu Vocational Institute of Architectural Technology, 2020

[9] L. Yang and H. Deng, "*Preference Preserved Privacy Protection Scheme for Smart Home Network System Based on Information Hiding*", IEEE Access, 2019

[10] A. M. zungeru and B. diarra , " *A Secured Smart Home Switching System based on Wireless Communications and Self-Energy Harvesting* ", IEEE , September 2019

[11] D. S. Kale, D. L. Bhombe and Dhiraj P. Tulaskar, "*Implementation of Soil Energy Harvesting System for Agriculture Parameters Monitoring and Controlling Using IOT: A Review*", International Research Journal of Engineering and Technology (IRJET) , 2017

[12] R. Bhamraland S. Mahajan , "*Reviewon internet of things based on wireless harvesting unit* ", International Research Journal of Engineering and Technology (IRJET),2017

ISSN: 2233-7853 IJFGCN

ISSN: 2233-7853 IJFGCN