SMART ENERGY HOME AUTOMATION SYSTEM USING IOT WITH TELEGRAM BOT

MS.S. Harini# ,G. Akash*,A. Madhan Raj*,V. PeriyaSamy*,R. Gowri Shankar*.

Assistant professor , *Student
#* Adithya Institute of Technology
Coimbatore, India.

Abstract- The Internet of Things (IoT) has generated excitement for a few years now, with start-ups and established businesses placing bets on the industry's growth. Along with the business solutions, IoT has been very vital in connecting things to the internet. There by achieving a communication among the connected devices. The Internet of things (IoT) is getting more traction in recent years. One of the usage scenarios of IoT is smart home. Smart home basically provides home automation for installed devices at home such as thermostat, lighting, air conditioning, etc and allows devices connected to the Internet to be controlled remotely by user. They still lack of important usage of IoT i.e. providing energy efficiency, energy monitoring, dealing with security, and managing privacy. This paper proposes a smart home system with microcontroller as the backend that not only serves as home automation and merely a switch replacement, but to also record and report important things to the owner of the house e.g., when someone trespasses the house (security perimeter), fire alert, gas leakage monitoring and to report the calculation of how much money has been spent in consuming the electrical appliances. The communication between user and the system is done using Telegram Bot.

Keywords – Home Automation, Relay, ESP 32, Telegram bot, Internet of Things (IOT), Smart Phone, Load, Power consumption, Alert System.

I.INTRODUCTION

A "thing" is an object equipped with sensors that gather data which will be transferred over a network and actuators that allow things to act (for example, to switch on or off the light, to open or close a door, to increase or decrease engine rotation speed and more). This concept includes fridges, street lamps, buildings, vehicles, production machinery, rehabilitation equipment and everything else imaginable. Sensors are not in all cases physically attached to the things: sensors may need to monitor, for example, what happens in the closest environment to a thing.To ensure sufficient functioning of IoT devices, it's far not enough to install them and let things go their way. There are

some procedures required to manage the performance of connected devices (facilitate the interaction between devices, ensure secure data transmission and more).Device identification to establish the identity of the device to be sure that it's a genuine device with trusted software transmitting reliable data. Configuration and control to tune devices according to the purposes of an IoT system. Some parameters need to be written once a device is installed (for example, unique device ID). Other settings might need updates (for example, the time between sending messages with data). Monitoring and diagnostics to ensure smooth and secure performance of every device in a network and reduce the risk of breakdowns. Software updates and maintenance to add functionality, fix bugs, address security vulnerabilities.

prevent such problems, it makes sense to log and analyse the commands sent by control applications to things, monitor the actions of users and store all these data in the cloud. With such an approach, it's possible to address security breaches at the earlies stages and take measures to reduce their influence on an IoT system (for example, block certain commands coming from control applications). Also, it's possible to identify the patterns of suspicious behaviour, store these samples and compare them with the logs generated by an IoT systems to prevent potential penetrations and minimize their impact on an IoT system.

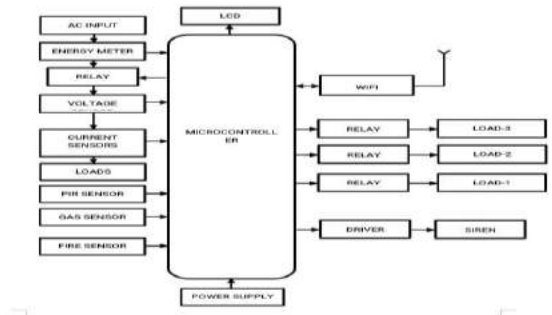

Figure 1. block diagram of our proposed system

II. HOME AUTOMATION SYSTEM

Alongside with device management, it's important to provide control over the users having access to an IoT system. User management involves identifying users, their roles, access levels and ownership in a system.It includes such options as adding and removing users, managing user settings, controlling access of various users to certain information, as well as the permission to perform certain operations within a system, controlling and recording user activities and more.

Security is one of the top concerns in the internet of things. Connected things produce huge volumes of data, which need to be securely transmitted and protected from cyber-criminals. Another side is that the things connected to the Internet can be entry points for villains. What is more, cyber-criminals can get the access to the "brain" of the whole IoT system and take control of it.

Control applications send automatic commands and alerts to actuators, for example notifications Windows of a smart home can receive an automatic command to open or close depending on the forecasts taken from the weather service.When sensors show that the soil is dry, watering systems get an automatic command to water plants.To help monitor the state of industrial equipment, and in case of a pre-failure situation, an IoT system generates

and sends automatic to field engineers. The commands sent by control apps to actuators can be also additionally stored in a big data warehouse.This may help investigate problematic cases (for example, a control app sends commands, but they are not performed by actuators – then connectivity, gateways and actuators need to be checked).

On the other side, storing commands from control apps may contribute to security, as an IoT system can identify that some commands are too strange or come in too big amounts which may evidence security breaches (as well as other problems which need investigation and corrective measures).

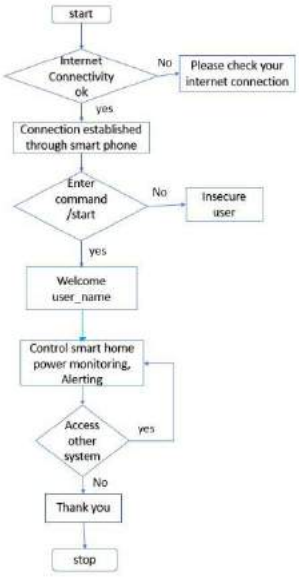

Figure 2 flow diagram of smart home energy efficient home automation using telegram bot

III. SYSTEM DESIGN AND IMPLEMENTATION

In smart home automation it helps the user by various method. In this our

Control applications can be either rule-based or machine-learning based. In the first case, control apps work according to the rules stated by specialists. In the second case, control apps are using models which are regularly updated (once in a we, once in a month depending on the specifics of an IoT system) with the historical data stored in a big data warehouse.

Although control apps ensure better automation of an IoT system, there should be always an option for users to influence the behaviour of such applications (for example, in cases of emergency or when it turns out that an IoT system is badly tuned to perform certain actions).

proposed system we use telegram bot as communication between user and the system.

we divide the system into 3 blocks

- monitoring power consumption,
- alerting system,
- load controlling**.**

Monitoring power consumption means it calculate daily consumption of voltage, current and display in both telegram and LCD.

Monitoring system:

In our proposed system monitor the daily power consumption by using voltage and current sensors. Voltage and Current sensors used to senses the voltage and current passed through the supply. And daily power consumption can be notifies through the user by using Telegram Bot.

Load controlling system:

Controlling the loads by using the relay. The relay is connected to the ESP32 controller. If any load will be on that message notify to the user and user can control the load by using IoT.

Alerting system:

If any fault occurred in our home the sensors detect the fault and notifies to the user by using Telegram application. And user can control the home appliances by using the telegram and activate the siren without no delay and also turn-off the whole system.

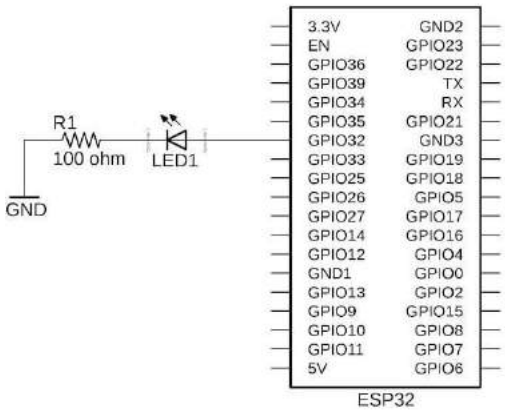

Figure3.ESP32 microcontroller pin diagram

IV.HARDWARE REQUIREMENTS:

- ESP32,
- PIR SENSOR,
- GAS SENSOR,
- FIRE SENSOR,
- VOLTAGE SENSOR,
- CURRENT SENSOR,
- WIFI MODULE,
- ENERGY METER,
- LCD,
- POWER SUPPLY.

V.SOFTWARE REQUIREMENTS:

- ARDUINO IDE**,**
- TELEGRAM.

In our proposed system we use ESP 32 microcontroller for control the whole system.

Also the sleep current of the ESP32 chip is less than 5 μA, making it suitable for battery powered and wearable electronics applications-sensitive pins, alongside a built-in Hall Effect and temperature.

The ESP32 is way advanced compared to the ESP-12e. Among several features, the ESP32 packs a CPU core, a faster Wi-Fi, more GPIOs (especially increased Analog pins that we all desired), supports Bluetooth. 4.2 and Bluetooth low energy. The board also comes with touch**.**

Power Requirement As the operating voltage range of ESP32 is 5V, the board comes with a LDO voltage regulator to keep the voltage steady at 3.3V.

It can reliably supply up to 600mA, which should be more than enough when ESP32 pulls as much as 250mA during RF transmissions.

The output of the regulator is also broken out to one of the sides of the board and labelled as 3V3.This pin can be used to supply power to external components. Power to the ESP32 development board is supplied via the on-board Micro B USB connector.

if you have a regulated 5V voltage source, the VIN pin can be used to directly supply the ESP32 and its peripherals.

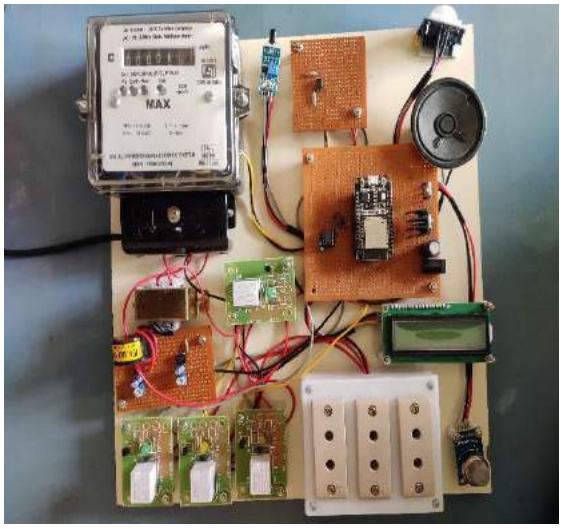

Figure 5 prototype kit of our proposed system.

VI.CONCLUSION AND FUTURE WORK:

In this paper, we conclude in our proposed system we introduce a new system for smart Energy Efficient home automation by using IoT and Telegram application. In our system real time power consumption monitoring and smart alerting system is being integrated. If any fault occurred in our home the sensors detect the fault and notify to the user without no delay by using telegram application. In Our system provide reliable and flexible way to implement home automation system. using the IoT

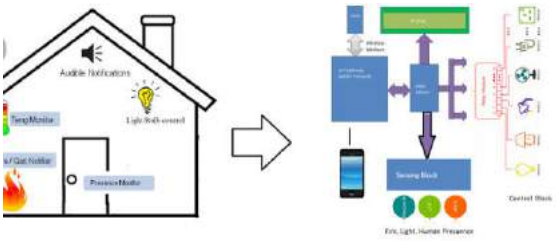

Figure 4 architecture of smart home automationAlternatively,

connectivity, we can monitor and access our smart home easily from anywhere, which will definitely will prove to be energy efficient. It act has a helping hand for the old age and differently abled person.

VII.REFERENCES

1. Q. F. Hassan," Introduction to the Internet of Things," in Internet of Things A to Z: Technologies and Applications, IEEE, 2018.
2. Q. Wang and Y. G. Wang, "Research on Power Internet of Things Architecture for Smart Grid Demand," 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, 2018, pp. 1-9.8.
3. Y. Hsieh, "Internet of Things Pillow Detecting Sleeping Quality," 2018 1st International Cognitive Cities Conference (IC3), Okinawa, 2018, pp. 266-267.
4. X. Li, P. Wan, H. Zhang, M. Li and Y. Jiang, "The Application Research of Internet of Things to Oil Pipeline Leak Detection," 2018 15th International Computer Conference on Wavelet Active Media Technology and Information

Processing (ICCWAMTIP), Chengdu, China, 2018, pp. 211-214.

5. Y. Kung, S. Liou, G. Qiu, B. Zu, Z. Wang and G. Jong," Home monitoring system based internet of things," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 325-327.
6. Y. Upadhyay, A. Borole and D. Dileepan, "MQTT based secured home automation system," Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-4.
7. O. Binderies, C. Berger and V. Malmsten Lundgren," The Best Rated Human Machine Interface Design for Autonomous Vehicles in the 2016 Grand Cooperative Driving Challenge," in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 4, pp. 1302-1307, April 2018.
8. P.Kunkun and L. Xian gong, "Reliability Evaluation of Coal Mine Internet of Things," 2014 International Conference on Identification. Information and Knowledge in the Internet of Things, Beijing, 2014, pp. 301-302.