IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Smart Home-Control and Monitoring system using Smart Phone

TARUN KUMAR SINGH, YASH RAJPUT, SHIVAM RAWAT, SUNNY SURI, ADITEE MATTOO
Student B.Tech (Information Technology), NIET, Greater Noida
Student B.Tech (Information Technology), NIET, Greater Noida
Student B.Tech (Information Technology), NIET, Greater Noida
Student B.Tech (Information Technology), NIET, Greater Noida
Department of Information Technology, NIET, Greater Noida

Abstract. This paper presents a low cost and flexible home control and monitoring system using an embedded micro-web server, with IP connectivity for accessing and controlling devices and appliances remotely using Android based Smart phone app. The proposed system does not require a dedicated server PC with respect to similar systems and offers a novel communication protocol to monitor and control the home environment with more than just the switching functionality.

Keywords: Internet of things, smart home, remote controlled, home automation, Android smartphone, Arduino

1 Introduction

The Internet of Things (IoTs) can be described as connecting everyday objects like smart-phones, Internet TVs, sensors and actuators to the Internet where the devices are intelligently linked together enabling new forms of communication between things and people, and between things themselves [1]. Now anyone, from anytime and anywhere can have connectivity for anything and it is expected that these connections will extend and create an entirely advanced dynamic network of IoTs. IoTs technology can also be applied to create a new concept and wide development space for smart homes to provide intelligence, comfort and to improve the quality of life.
In this paper, we extend our previous work [2] and present a low cost and flexible home control and monitoring system using an embedded micro-web server, with IP connectivity for accessing and controlling devices and appliances remotely using Android based Smart phone app. The proposed system does not require a dedicated server PC with respect to similar systems and offers a novel communication protocol to monitor and control the home environment with more than just the switching functionality. We have utilized RESTful based Web services as an interoperable application layer that can be directly integrated into other application domains like e-health care services, utility, distribution, or even vehicular area networks (VAN).

2. Classic smart home overview

Smart home is the residential extension of building automation and involves the control and automation of all its embedded technology. It defines a residence that has appliances, lighting, heating, air conditioning, TVs, computers, entertainment systems, big home appliances such as washers/dryers and refrigerators/freezers, security and camera systems capable of communicating with each other and being controlled remotely by a time schedule, phone, mobile or internet. These systems consist of switches and sensors connected to a central hub controlled by the home resident using wall-mounted terminal or mobile unit connected to internet cloud services.

Smart home provides, security, energy efficiency, low operating costs and convenience. Installation of smart products provide convenience and savings of time, money and energy. Such systems are adaptive and adjustable to meet the ongoing changing needs of the home residents. In most cases its infrastructure is flexible enough to integrate with a wide range of devices from different providers and standards.

The basic architecture enables measuring home conditions, process instrumented data, utilizing microcontroller-enabled sensors for measuring home conditions and actuators for monitoring home embedded devices.

The popularity and penetration of the smart home concept is growing in a good pace, as it became part of the modernization and reduction of cost trends. This is achieved by embedding the capability to maintain a centralized event log, execute machine learning processes to provide main cost elements, saving recommendations and other useful reports.

3. Smart home services

Home automation or smart homes (also known as domotic) can be described as introduction of technology within the home environment to provide convenience, comfort, security and energy efficiency to its occupants [3]. With the introduction of the Internet of Things, the research and implementation of home automation are getting more popular [4]. Various wireless technologies that can support some form of remote data transfer, sensing and control such as Bluetooth, Wi-Fi, RFID, and cellular networks have been utilized to embed various levels of intelligence in the home [5]. The studies in [2, 6] have presented Bluetooth based home automation systems using Android Smart phones without the Internet controllability. The devices are physically connected to a Bluetooth sub-controller which is then accessed and controlled by the Smart phone using built-in Bluetooth connectivity. Researchers have also attempted to provide network interoperability and remote access to control devices and appliances at home using home gateways. [7] proposed mobile IP based architecture and its potential applications in Smart homes security and automation without any actual deployment and testing. Lately few researchers have also presented use of Web services, simple object access protocol (SOAP) and representational state transfer (REST) as an interoperable application layer to remotely access home automation systems. [8] introduced a smart home management scheme over the Ethernet network based on XML SOAP standards. The drawback of using SOAP based Web a service is that it is complex and adds overhead to the client and server when parsing the message, resulting in slower operation and higher bandwidth.

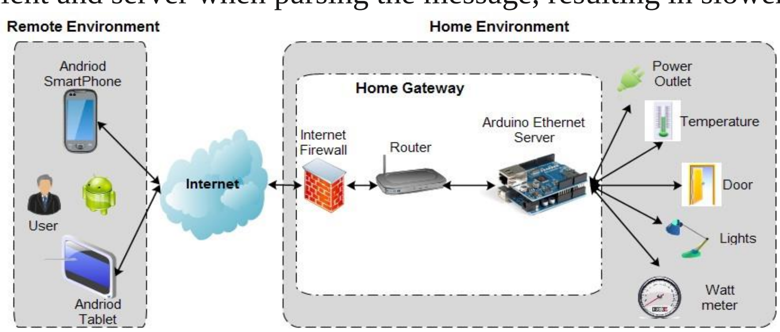

Figure 1. Overview of Conceptual structure.

3. Internet of things [IoT] overview

The internet of things (IoT) paradigm refers to devices connected to the internet. Devices are objects such as sensors and actuators, equipped with a telecommunication interface, a processing unit, limited storage and software applications. It enables the integration of objects into the internet, establishing the interaction between people and devices among devices. The key technology of IoT includes radio frequency identification (RFID), sensor technology and intelligence technology. RFID is the foundation and networking core of the construction of IoT. Its processing and communication capabilities along with unique algorithms allows the integration of a variety of elements to operate as an integrated unit but at the same time allow easy addition and removal of components with minimum impact, making IoT robust but flexible to absorb changes in the environment and user preferences. To minimize bandwidth usage, it is using JSON, a lightweight version of XML, for inter components and external messaging.

4. System Implementation

Software of the proposed home automation system is divided into two parts: server application software and microcontroller firmware. The server application software is a library implementation of a micro Web-server running on Arduino Uno using the Ethernet shield. To successfully communicate between remote user and the Home Gateway, configuration stage and sensor/actuator control stage layers have been implemented on the Arduino. Fig. 2 shows the flowchart of connection establishment between the Arduino and the Internet.

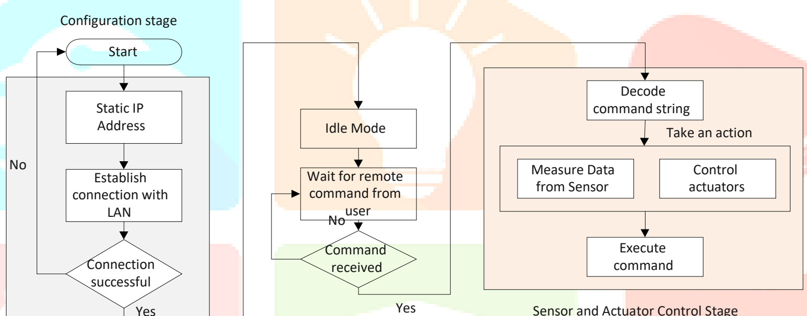

Fig. 2. Home Gateway flow chart for the connection establishment with the Internet

4.2 Smartphone application and features

The Smart phone app for home control and monitoring applications provides the following functionalities to the user: 1) Remote connection to the Home Gateway. 2) Device control. 3) Device Monitoring. 4) Managing schedule. Fig. 3 shows the graphical user interface for controlling and managing the home environment using Smart phone

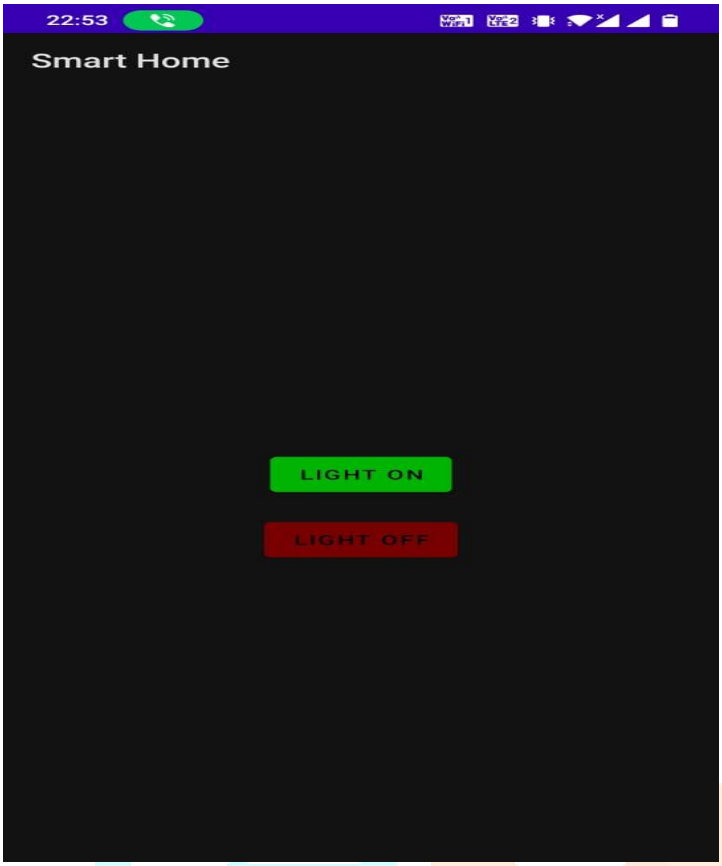

Fig. 3. Graphical user Interface of app.

5.1 Event processing languages

Event processing is concerned with real-time capturing and managing predefined events. It starts from managing the receptors of events right from the event occurrence, even identification, data collection, process association and activation of the response action. To allow rapid and flexible event handling, an event processing language is used, which allows fast configuration of the resources required to handle the expected sequence of activities per event type. It is composed of two modules, ESP and CEP. ESP efficiently handles the event, analyzes it and selects the appropriate occurrence. CEP handles aggregated events. Event languages describe complex event-types applied over the event log.

5.2 Rediscovering workflow from events

In some cases, rules relate to discrepancies in a sequence of events in a workflow. In such cases, it is mandatory to precisely understand the workflow and its associated events. To overcome this, we propose a reverse engineering process to automatically rediscover the workflows from the events log collected over time, assuming these events are ordered, and each event refers to one task being executed for a single case. The rediscovering process can be used to validate workflow sequences by measuring the discrepancies between prescriptive models and actual process executions. The rediscovery process consists of the following three steps:

(1) construction of the dependency/frequency table. (2) Induction of dependency/ frequency graphs. (3) Generating WF-nets from D/F-graphs.

6. Advanced smart home

In this section, we focus on the integration of smart home, IoT to define a new computing paradigm. We can find in the literature section [11–14] surveys and research work on smart home, IoT and cloud computing separately, emphasizing their unique properties, features, technologies, and drawbacks. However, our approach is the opposite. We are looking at the synergy among these three concepts and searching for ways to integrate them into a new comprehensive paradigm, utilizing its common underlying concepts as well as its unique attributes, to allow the execution of new processes, which could not be processed otherwise.

devices connected to a local area network [LAN]. This enables the communication among the devices and outside of it. Connected to the LAN is a server and its database. The server controls the devices, logs its activities, provides reports, answers queries and executes the appropriate commands. For more comprehensive or common tasks, the smart home server, transfers data to the cloud and remotely activate tasks in it using APIs, application programming interface processes. In addition, IoT home appliances are connected to the internet and to the LAN, and so expands smart home to include IoT. The connection to the internet allows the end user, resident, to communicate with the smart home to get current information and remotely activate tasks.

To demonstrate the benefits of the advanced smart home, we use RSA, a robust asymmetric cryptography algorithm, which generates a public and private key and encrypts/decrypts messages. Using the public key, everyone can encrypt a message, but only these who hold the private key can decrypt the sent message. Generating the keys and encrypting/decrypting messages, involves extensive calculations, which require considerable memory space and processing power. Therefore, it is usually processed on powerful computers built to cope with the required resources. However, due to its limited resources, running RSA in an IoT device is almost impossible, and so, it opens a security gap in the Internet, where attackers may easily utilize. To cope with it, we combine the power of the local smart home processors to compute some RSA calculations and forward more complicated computing tasks to be processed in the cloud. The results will then be transferred back to the IoT sensor to be compiled and assembled together, to generate the RSA encryption/decryption code, and so close the mentioned IoT security gap. This example demonstrates the data flow among the advanced smart home components. Where, each component performs its own stack of operations to generate its unique output. However, in case of complicated and long tasks it will split the task to sub tasks to be executed by more powerful components. Referring to the RSA example, the IoT device initiates the need to generate an encryption key and so, sends a request message to the RSA application, running in the smart home computer. The smart home computer then asks the “prime numbers generation” application running on cloud, to provide p and q prime numbers. Once p and q are accepted, the encryption code is generated. In a later stage, an IoT device issues a request to the smart home computer to encrypt a message, using the recent generated RSA encryption key. The encrypted message is then transferred back to the IoT device for further execution. A similar scenario may be in the opposite direction, when an IoT device gets a message it may request the smart home to decrypt it.

To summarize, the RSA scenarios depict the utilization of the strength of the cloud computing power, the smart home secured computing capabilities and at the end the limited power of the IoT device. It proves that without this automatic cooperation, RSA would not be able to be executed at the IoT level.

A more practical example is where several detached appliances, such as an oven, a slow cooker and a pan on the gas stove top, are active in fulfilling the resident request. The resident is getting an urgent phone call and leaves home immediately, without shutting off the active appliances. In case the relevant IoTs have been tuned to automatically shut down based on a predefined rule, it will be taken care at the IoT level. Otherwise, the smart home realizes the resident has left home [the home door has been opened and then locked, the garage has been opened, the resident’s car left, the main gate was opened and then closed, no one was at home] and will shut down all active devices classified as risk in case of absence. It will send an appropriate message to the mailing list defined for such an occasion.

7. Practical aspects and implementation considerations for IoT and smart home

Smart home has three components: hardware, software and communication protocols. It has a wide variety of applications for the digital consumer. Some of the areas of home automation led IoT enabled connectivity, such as: lighting control, gardening, safety and security, air quality, water-quality monitoring, voice assistants, switches, locks, energy and water meters.

Advanced smart home components include: IoT sensors, gateways, protocols, firmware, cloud computing, databases, middleware and gateways. IoT cloud can be divided into a platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). demonstrates the main components of the proposed advanced smart home and the connection and data flow among its components.

The smart home application updates the home database in the cloud to allow remote people access it and get the latest status of the home. A typical IoT platform contains: device security and authentication, message brokers and message queuing, device administration, protocols, data collection, visualization, analysis capabilities, integration with other web services, scalability, APIs for real-time information flow and open source libraries. IoT sensors for home automation are known by their sensing capabilities, such as: temperature, lux, water level, air composition, surveillance video cameras, voice/sound, pressure, humidity, accelerometers, infrared, vibrations and ultrasonic. Some of the most commonly used smart home sensors are temperature sensors, most are digital sensors, but some are analog and can be extremely accurate. Lux sensors measure the luminosity. Water level ultrasonic sensors.

Float level sensors offer a more precise measurement capability to IoT developers. Air composition sensors are used by developers to measure specific components in the air: CO monitoring, hydrogen gas levels measuring, nitrogen oxide measure, hazardous gas levels. Most of them have a heating time, which means that it requires a certain time before presenting accurate values. It relies on detecting gas

components on a surface only after the surface is heated enough, values start to show up. Video cameras for surveillance and analytics. A range of cameras, with a high-speed connection. Using Raspberry Pi processor is recommended as its camera module is very efficient due to its flex connector, connected directly to the board.

Sound detectors are widely used for monitoring purposes, detecting sounds and acting accordingly. Some can even detect ultra-low levels of noise, and fine tune among various noise levels.

Humidity sensors sense the humidity levels in the air for smart homes. Its accuracy and precision depend on the sensor design and placement. Certain sensors like the DHT22, built for rapid prototyping, will always perform poorly when compared to high-quality sensors like HIH6100. For open spaces, the distribution around the sensor is expected to be uniform requiring fewer corrective actions for the right calibration.

Smart home communication protocols: bluetooth, Wi-Fi, or GSM. Bluetooth smart or low energy wireless protocols with mesh capabilities and data encryption algorithms. Zigbee is mesh networked, low power radio frequency-based protocol for IoT. X10 protocol that utilizes powerline wiring for signaling and control. Insteon, wireless and wireline communication. Z-wave specializes in secured home automation. UPB, uses existing power lines. Thread, a royalty-free protocol for smart home automation. ANT, an ultra-low-power protocol for building lowpowered sensors with a mesh distribution capability. The preferred protocols are bluetooth low energy, Z-wave, Zigbee, and thread. Considerations for incorporating a gateway may include: cloud connectivity, supported protocols, customization complexity and prototyping support. Home control is composed of the following: state machine, event bus, service log and timer.

Modularity: enables the bundle concept, runtime dynamics, software components can be managed at runtime, service orientation, manage dependencies among bundles, life cycle layer: controls the life cycle of the bundles, service layers: defines a dynamic model of communication between various modules, actual services: this is the application layer. Security layer: optional, leverages Java 2 security architecture and manages permissions from different modules.

OpenHAB is a framework, combining home automation and IoT gateway for smart homes. Its features: rules engine, logging mechanism and UI abstraction. Automation rules that focus on time, mood, or ambiance, easy configuration, common supported hardware:

Domoticz architecture: very few people know about the architecture of Domoticz, making it extremely difficult to build applications on it without taking unnecessary risks in building the product itself. For example, the entire design of general architecture feels a little weird when you look at the concept of a sensor to control to an actuator. Building advanced applications with Domoticz can be done using OO based languages.

Deployment of blockchain into home networks can easily be done with Raspberry Pi. A blockchain secured layer between devices and gateways can be implemented without a massive revamp of the existing code base. Blockchain is a technology that will play a role in the future to reassure them with revolutionary and new business models like dynamic renting for Airbnb.

8. Smart home and IoT examples

We can find in the literature and practical reports, many implementations of various integrations among part of the main three building blocks, smart home, IoT and cloud computing. For example, refer to [12–14]. In this section we outline three implementations, which clearly demonstrate the need and the benefits of interconnecting or integrating all three components, as illustrated in Each component is numbered, 1–6. In the left side, we describe for each implementation, the sequence of messages/commands among components, from left to right and from bottom up. Take for example the third implementation, a control task constantly runing at the home server (2) discovers the fact that all residents left home and automatically, initiates actuators to shut down all IoT appliances (3), then it issues messages to the relevant users/residents, updating them about the situation and the applied actions it took (6).

The use of (i) in the implementations explanation, corresponds to the circled numbers in **Figure 5**.

8.1 Discovery of water leaks and its prevention

First step is deploying water sensors under every reasonable potential leak source and an automated master water valve sensor for the whole house, which now means the house is considered as an IoT.

In case the water sensor detects a leak of water (3), it sends an event to the hub (2), which triggers the “turn valve off” application. The home control application then sends a “turn off” command to all IoT (3) appliances defined as sensitive to water stopping and then sends the “turn off” command to the main water valve (1). An update message is sent via the messaging system to these appearing in the notification list (6). This setup helps defending against scenarios where the source of the water is from the house plumbing. The underlying configuration assumes an integration via messages and commands between the smart home and the IoT control system. It demonstrates the dependency and the resulting benefits of combining smart home and IoT.

8.2 Incident management to control home appliances

Consider the scenario where you leave home while some of the appliances are still on. In case your absence is long enough, some of the appliances may over heat and are about to blowout. To avoid such situations, we connect all IoT appliances’ sensors to the home application (2), so that when all leave home it will automatically adjust all the appliances’ sensors accordingly (3), to avoid damages. Note that the indication of an empty home is generated by the Smart Home application, while the “on” indication of the appliance, is generated by IoT. Hence, this scenario is possible due to the integration between smart home and IoT systems.

9. Conclusions and summary

In this paper, a novel architecture for low cost and flexible home control and monitoring system using Android based Smart phone is proposed and implemented. Any Android based Smart phone with built in support for Wi-Fi can be used to access and control the devices at home. When a Wi-Fi connection is not available, mobile cellular networks such as 3G or 4G can be used to access the system.

We describe the advantages and benefits of each standalone component and its possible complements, which may be achieved by integrating it with the other components providing new benefits raised from the whole compound system. Since these components are still at its development stage, the integration among them may change and provide a robust paradigm that generates a new generation of infrastructure and applications.

As we follow-up on the progress of each component and its corresponding impact on the integrated compound, we will constantly consider additional components to be added, resulting

References

1. Kortuem, G., Kawsar, F., Fitton., D., Sundramoorthy, V.: Smart objects as building blocks for the internet of things. Internet Computing, IEEE, vol. 14, no.1, 44--51 (2010)
2. Piyare, R., Tazil, M.: Bluetooth based home automation system using cell phone. Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on, pp. 192195.(2011)
3. Wikipedia. Home automation, http://en.wikipedia.org/wiki/Home_automation
4. Liu, Y.: Study on smart home system based on Internet of things technology. In Informatics and Management Science IV. vol. 207, W. Du, Ed., ed: Springer London, 73--81 (2013)
5. Al-Qutayri, M.A., Jeedella, J.S.: Integrated Wireless Technologies for Smart Homes Applications. In Smart Home Systems, M. A. Al-Qutayri, Ed., ed: InTech (2010)
6. Yan, M., Shi, H.: SMART LIVING USING BLUETOOTH-BASED ANDROID
7. SMARTPHONE. International Journal of Wireless & Mobile Networks (IJWMN), vol. 5, no.5, pp. 65--72 (2013)
8. Park, B.: Mobile IP-based architecture for smart homes. International Journal of Smart Home, vol. 6, no.1, 29--36 (2012)
9. Perumal, T., Sulaiman, M.H., Sharif, K.Y., Leong, C.Y.: Development of an embedded smart home management scheme. International Journal of Smart Home, vol. 7, no.2, 15--26 (2013)