

IoT Based Smart and Secure Home System

Abhinav Kumar¹, Gaurav Kumar²

¹Department of Computer Science and Engineering Galgotias College of Engineering and Technology
Greater Noida, India mailtoabhinavsinha@gmail.com

²Department of Computer Science and Engineering Galgotias College of Engineering and Technology
Greater Noida, India gauravvarshney221@gmail.com

Abstract

This electronic device is an Application of Internet of Things that will enhance the capability of any common electronic device to a remotely accessible device by plugging the required device to this panel and also will provide security to the home. Smart and Secure Home System will consist of both user and home side modules. At the user side the smartphone/tablet (Android, Windows or i-OS based) or web browser on any computer will act as a transmitting device, which will control the switching and intensity of home appliances, i.e., a small bulb to AC and Refrigerators. While the module installed at home will act as a receiver. There is a special functionality in this whole system which justifies it to be called a Secure Home System. There will be a presence sensor installed in every single room which will sense the presence of anyone, if sense mode is switched ON, and immediately notify the user about this event. The doors of the home will also be connected to the electronic panel installed at home which can be controlled by the user at the user end. The whole electronic panel installed at home will have two set of technologies installed in it to get connected and come over Internet, i.e., WiFi and GSM based connection. In the case the user is not able to access internet at certain time, then he/she can control the devices through SMS also, this feature is made possible by having GSM module present on the panel at home.

Key Words: IoT, Cloud Computing, Smart Home, Secure Home, Smartphone, Server

I. INTRODUCTION

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro services and the internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements [1]. Smart and Secure Home will work on these fundamentals of IoT. Every home appliance will have a unique Identity which will be used to identify that particular device on network. This means that private as well as public IP addresses are needed to configure.

Secure Home is the added feature which totally automate the security system of a home or office. This is made possible by adding the doors to the same network and implementing presence sensors in the rooms/halls.

II. USEABILITY AND SCALABILITY

The user interface is well designed that a normal smartphone user can easily use all of its features. The GUI application provides user with easy identification of their home appliances and doors connected to the panel. Such application is to be developed for all major Operating Systems so that users of a large scale can use the system.

A. Android Application on Google Play Store

It will be very easy for android smartphone user to get the application on their android

application market place named Google Play Store. This application will be absolutely free to download and install in their Android smartphones. The application will be developed for almost all the current running versions of android. The application will have simple user interface. All they need is to just login and access their home appliances and doors.

B. IOS Application on Apple App Store

For the iOS users, the application will be freely available on App Store. The interface will be almost same while the application will be available for all current running versions of iOS.

C. Windows Phone Application on Windows Store

Windows have its own Store for applications, this app will easily be available for Windows Phone users for free. Windows Operating System is well known for its user interface and this app will be very user friendly.

D. Web Site which can be Accessed from Any Web Browser

The use of this system is not only limited to smartphones or tablets but whole application will also be available online which can be accessed from anywhere and from any device having a web browser and an internet connection. The user interface for web application will be simple to use and attractive.

E. Voice Control Capability

The mobile applications will have the option of voice as an input, in addition to instruct the app with the finger touch user can also control the appliances with their voice by saying the commands. For this feature to be available we will use Google Voice services to determine the command and convert it to required data [3].

III. LITERATURE SURVEY

As per our survey currently there exist no such system with all of these functionalities. Various systems only provide GSM connection to the panel, while various does not provide the

feature of intensity control or Secure Home System. This Smart and Secure Home system is the combination of various features. Also the reach of this device will surely be wide, as users of different community can use it.

Mobile devices and dynamic services affect a dynamically changing environment, which can result in very difficult interaction. In addition, how to provide services efficiently and appropriately is always an important issue for a smart home. To solve the problems caused by traditional architectures, to deal with the dynamic environment, and to provide appropriate services, we propose a service-oriented architecture (SOA) for smart-home environments, based on Open Services Gateway Initiative (OSGi) and mobile-agent (MA) technology. This architecture is a peer-to-peer (P2P) model based on multiple OSGi platforms, in which service-oriented mechanisms are used for system components to interact with one another [2].

IV. IMPLEMENTATION

This system is far different from any other remote access technologies. This system can be used with any appliance by just plugging that device into the panel. For doors we need a special kind of door locking system which can be controlled via electronic signals.

Internet is used as the medium of connection between the user at some other place and the appliance at home.

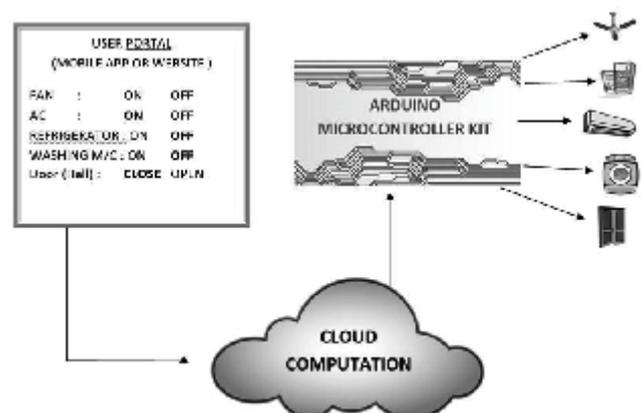


Figure 1. A general architecture of system.

The panel at home has the internet connection via WLAN or GSM Data Communication technologies. Now once the appliances are connected to this panel and since the panel is connected over internet it can be easily accessed and data can be shared between the user and the panel. Once the panel receives data, the received data will be converted to digital signal which can be done by programming at panel side. This signal then can be used by the appliances or doors for switching.

The system can be divided in three sides to understand its implementation.

A. Home Side

At the home side there are home appliances and the panel installed on the wall generally. The home appliances are connected to the panel itself to get all of them to network. All the home appliances have their own unique Identity which will be used by the panel to identify each of them.

The panel will comprise of Hardware and Software components. C.P.U., Physical memory (RAM), WLAN module as well as GSM module need to be embedded in the panel. All these components (even more) are embedded in Arduino (Genuino) kits which will be used as Hardware.

While it requires a functioning WLAN drivers it needs an Operating System. This module is specifically a mini computer with very limited capabilities. Linux OS will be embedded in the panel to get working WLAN drivers. These are the software requirements for the same.

This whole network of Home appliances will work just like a private network inside an organization.

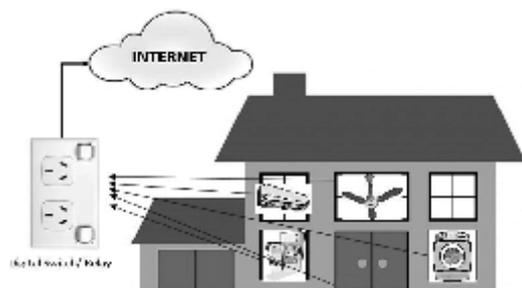


Figure 2. Home environment showing the home side.

B. User Side

At the user side there will be a Graphical Interface which allows them to login t their account and access the registered appliances in their account. These registered appliances will be those which were registered at the time of installation of the system. The interface will be smartphone application for the respective OS of the smartphone. Web application can also be used by accessing it through any web browser at any computer by the user. All a user need is to login with their credentials and continue to control their appliances and doors.

C. Medium Layer (the Virtual Side)

To make the above mentioned two sides there is a requirement of a medium. This medium is provided as aServer which will be used as a central point to transmit data from one side to another. This Server related mechanism is basically the Cloud Computing. We will use Amazon Web Services (AWS) as the Cloud service to serve the application and web site to access the database. For communicating data between both sides, it is needed to share same database among both the sides. As Amazon Web Services is an IaaS (Infrastructure as a Service) provider, it will take care of the infrastructure and several tools will be used for several apps as per the requirements. It is the responsibility of this layer to make the movement of data in between both the sides.

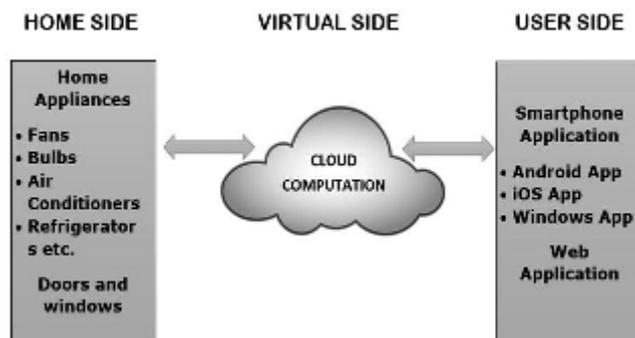


Figure 3. Block diagram showing multiple sides of system.

I. SIMULATION AND TEST

For simulation of the above discussed mechanism

we have created a home environment connecting few of the home appliances with the simulated electronic panel and hosted a beta version of the web application on local host. The simulation went on in several phases [4]:

A. Modelling

All the components were mounted in a bread board with proper connections following the required precautions. As this was a generative test, we don't prescribe the exact behavior of our test performed, but rather what it could perform. The panel and the web application both were connected through Internet in local host.

B. Test Generation

From the non- deterministic model, a well-defined set of planned actions is generated. The capability and the robustness of the system was tested and the actions such as the sessions creation and synchronization check were taken.

C. Simulation Invocation

Generated set of actions were executed. During each planned action a part of the system is interacted. We divided the system in parts (different sides- Home side, User side etc.) and observed the functioning of the simulation for each part.

D. Validation

Finally, at some point in time later, the action log of this simulation could be queried and aggregated to detect any failures or abnormalities. Being a separate process from running the test themselves, it also becomes possible to add new validations and “backfill” failures from previous points in time.

From the above simulation of the system we observed that the system was working fine and during the testing it was found that more relays will be needed for more number of appliances. This clearly shows that number of relays required in the panel (and hence the size of the panel) is directly proportional to the number of Home Appliances to be connected.

VI. CONCLUSION

This paper gives basic idea of getting all the home appliances on Internet and shows the basic idea of using data communication to control electrical and electronic signals. This paper also merges the idea of Smart Home to Secure Home by using the same sort of setup and hence is making use of IoT.

This System uses platforms such as Arduino as hardware and Linux as Operating System in the Home side, both of which are FOOR (Free Open Source Resources). So the cost of implementation is very less overall. The system provides a great scalability as the user of most of the communities will get benefitted with this. This kind of system is of a great use in the upcoming days with the advancements in the technologies such as Internet of Things (IoT).

ACKNOWLEDGMENT

We gratefully acknowledges the contribution of each other in analyzing and writing this particular paper. We appreciate each other's knowledge and the understanding in between us.

Furthermore, we would like to thank Mr. Ajeet Bhartee, our lecturer and guide who let us get informed about the recent researches and technologies.

We feel highly privileged to thank Prof. Dr. Bhawna Mallick, Head of Department, Department of Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida, India for her appreciation and motivation. It could never be possible to write this paper without her continuous support and motivation.

REFERENCES

- [1] Margaret Rouse, Ivy Wigmore, Definition Internet of Things (IoT), July. 2016.[Online]. Available: <http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>
- [2] Sung-Jung Hsiao, Kuang-Yow Lian, Wen-Tsai Sung, “Employing cross- platform smart home control system with IoT technology based” - International Symposium on Computer,

Consumer and Control, 2016.

- [3] Rohit Kumar, Tapan Kumar “Voice Controlled Wheel Chair”, unpublished.
- [4] Ryan Neufeld, What is simulation testing?, Aug. 2015. [Online]. Available: <http://homegrown.io/articles/what-is-simulation-testing>.