



Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compelecengFree
papers, 11
نایاب
مقالات
دانلود
Free
papers

A cloud based and Android supported scalable home automation system[☆]

Ilker Korkmaz ^{*}, Senem Kumova Metin, Alper Gurek, Caner Gur, Cagri Gurakin,
Mustafa Akdeniz

Izmir University of Economics, Faculty of Engineering and Computer Science, Sakarya Cd., No. 156, Balcova, Izmir, Turkey

ARTICLE INFO

Article history:

Received 15 May 2014

Received in revised form 28 November 2014

Accepted 28 November 2014

Available online xxxx

Keywords:

Home automation system

Cloud

Google Cloud Platform

Google Cloud Messaging

Android

ABSTRACT

In this paper, an Android based home automation system that allows multiple users to control the appliances by an Android application or through a web site is presented. The system has three hardware components: a local device to transfer signals to home appliances, a web server to store customer records and support services to the other components, and a mobile smart device running Android application. Distributed cloud platforms and Google services are used to support messaging between the components. The prototype implementation of the proposed system is evaluated based on the criteria considered after the requirement analysis for an adequate home automation system. The paper presents the outcomes of a survey carried out regarding the properties of home automation systems, and also the evaluation results of the experimental tests conducted with volunteers on running prototype.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

Home automation is the introduction of technology within home to enhance the quality of life of its occupants, through the provision of different services, such as tele-health, multimedia entertainment and energy conservation. In other words, home automation aims at the orchestration of digital devices for the convenience of users together with security and the capability to monitor multiple dwellings [1]. Traditional home automation systems involve the control of digital devices which provide functions such as heating, lighting and shading. Due to the rapid growth of information technology and modern entertainment systems in recent years, these primary functions are required to be enriched with additional services (i.e., music system volume reduction when the telephone rings [1]). In [2], the benefits of home automation systems (the smart house systems) are listed as safety, comfort, power saving and communications. In order to provide these benefits, some technical requirements must be also respected, such as low cost, plug and play, flexibility, ease of use and reliability [2]. In the study by Piyare and Tazil [3], the requirements are itemized in detail:

- The wireless home automation systems should be scalable to facilitate the integration of new devices.
- The system should provide a user-friendly interface on the host side, so that the devices can be easily setup, monitored and controlled. The system interface should also provide some diagnostics services to track potential problems.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Ziya Arnavut.

* Corresponding author. Tel.: +90 2324888258.

E-mail address: ilker.korkmaz@ieu.edu.tr (I. Korkmaz).

- The overall system should be fast enough to exploit the full potential of wireless technology.
- The system should be cost effective in order to justify its application in home automation.

In our study, a home automation system, which provides two alternative user friendly interfaces, an Android application and a web application, is presented. The system is built to serve multiple users, using up-to-date and emerging technologies, such as Google Cloud Platform, in order to support the communication between the main hardware components of the system.

One of our two main motivations for developing the proposed system is the increasing popularity of smart homes. Although ready to use home automation systems exist, nevertheless there is a need for a new system which considers networked smart homes, rather than the systems based on individual homes. Our second motivation is to decrease the cost of such pervasive systems by using free and open tools provided by emerging technologies. In addition, we prefer to use enabling infrastructures (i.e. cloud) to build Internet based connected home-networking. To support ease of use, it was decided to select an Android interface at the end point of each system.

We believe that an important feature of the system that would make it prominent in the field is its cloud based distributed architecture. The distributed infrastructure of the system is designed to be deployed and managed pervasively by an organization (either an owner company or the system builders). The local components of the homes connected in the system together with related system services could be managed by particular mobile users of those homes anywhere.

We propose that the key internal strength in our distributed networking based and Android supported home automation implementation is its optional and flexible structure. For example, the system has a profile infrastructure that gives different authorization rights to its different types of users. The system is open to new, optionally chosen devices. Moreover, the system is designed to offer different types of pricing services: i. free, ii. pay-per-usage on demand, iii. discounted cost for a number of different users, iv. fixed cost with full rights with any number of users.

This article extends the work in [4] and dissects the design, analysis and implementation of the proposed cloud based and Android supported home automation system.

In the following sections, the related works in the literature are first discussed and then the enabling technologies used in the proposed system are introduced. Following this, the details of the system architecture are given. After listing the analysis and evaluation criteria for an adequate home automation system, the paper describes the surveys and experiments conducted with volunteers on prototype implementation of the proposed system. A discussion of the proposed system regarding the outcomes of the experiments and the comments gathered from the volunteers is also given. Finally, the paper is summarized in Section 6.

2. Related work

There has been a significant amount of research and numerous approaches to the home automation systems. Although the idea of controlling home appliances via different methods is not new, there is a need to reconsider the management of smart homes. We believe that the proposed system contributes to the research in smart home automation by merging different advanced networking technologies with its Android-enabled and cloud-based structure.

The number of published works on home automation may indicate an evidence of trends in a certain field. To this end, we searched the terms “Smart Home/House” or “Home/House Automation” in three renowned scientific databases; Web of Science, Scopus and ScienceDirect. When dissecting the returned records, we observed that not every returned record focuses on the home automation concept. Nevertheless, the number of records returned can be considered evidence for the significance of this area and highlight its importance in the future. The number of records returned from the related queries in August 2014 is 2445 from Web of Science, 13,158 from Scopus, 2258 from ScienceDirect. These records include all available material in the databases (e.g., conference proceedings, book chapters, journal articles) covering all years.

Table 1 shows the percent of academic research including some technological terms (e.g., web, cloud, Android) and the concept “home automation”. In order to obtain the given values, the set of records that include the terms “Smart Home/House” or “Home/House Automation” is intersected with the set of the records of terms in each column. For example, 2445 records in Web of Science include the union of terms “Smart Home”, “Smart House”, “Home Automation” or “House

Table 1

The percent (%) of academic research including the technological terms; web, cloud, Android; and the concept “home automation”.

		Web	Cloud	Android	Web AND Cloud	Web AND Android	Cloud AND Android	Web AND Cloud AND Android
Smart home/house	Web of science	7.20	1.27	0.70	0.29	0.12	0.04	0.04
OR	ScienceDirect	43.98	11.12	4.38	7.71	3.41	1.73	1.59
Home/house automation	Scopus	23.43	4.18	2.61	1.88	0.90	0.47	0.24

Automation". When this set is refined with the term "web", the size of the new set is reduced to 176; in other words the intersected set that includes the home automation concept together with the term "web" is 176. The ratio of intersected set to the initial set is $176/2445 = 0.072$ (7.2%).

The first three columns of Table 1 show that, as expected, in home automation the web concept is dominant over the other relatively recent technologies, cloud and Android. The last column of the table presents the percent of the records that include web, cloud and Android search terms combined. Among these records, none were published before 2011 and many belong to 2014.

There are also some other home automation systems based on different technologies; such as Bluetooth, phone line; that are not mentioned in Table 1. Furthermore, some studies particularly focus either on the protocols/standards used in networking, or the hardware devices in the system, while others discuss the performance, security, energy awareness issues in home automation systems. Some of those related studies in literature are briefly summarized below.

There are a number of popular communication protocols/standards in home automation field, such as C-Bus, Universal Powerline Bus (UPB), X10, ZigBee, Z-Wave, that deal with the interaction of devices at home. As an example of works which focus on the communication between the devices at home, [5] may be given. In [5], following the discussion of the potential of ZigBee standards in home automation systems, a particular home automation system based on ZigBee and Wi-Fi network is presented and a virtual home is constructed. It is reported in the study that ZigBee technology has advantages, such as lowering the expense of the system and intrusiveness of the respective system installation compared to existing technologies. Since our aim in the study is to provide a distributed solution to the management of multiple home-automation systems and compare different technologies used in related work, the details of communication protocols/standards in the previous studies are not examined.

In [6], the Bluetooth based home automation system is presented. The system involves a primary controller and a set of Bluetooth sub-controllers in which each controller is physically connected to an individual home device. The sub-controllers are responsible for sending all messages to the primary controller. Although the system reduces physical wiring through the use of Bluetooth technology, it has the disadvantage of incurring an access delay due to the sharing of a single Bluetooth module between numerous devices.

One other Bluetooth-based system which uses cell phones is given in [3]. In the proposed system, home appliances are connected to a stand-alone Arduino BT board, with wireless communication between the cell phone and the Arduino BT board. The users of the system are required to acquire pairing passwords for the board and the cell phone to access home appliances in order to protect the system from unauthorized access.

In a Java based home automation system, developed in [7], an embedded board integrated into a server is physically connected to all home devices. Java technology used in the system provides built-in security. However, the use of a high end computer and the wired installation per home increases the expense of the system.

The system in [8] aims to reduce energy consumption, and is based on an embedded controller connected to the home web-server and the sensors/actuators at home. The users control home devices through the web site on the home web server. The user and control data are stored at home. Similar to the system in [7], the need to install a separate server per each home may be considered as a disadvantage of the system regarding the expense.

An innovative phone based remote control system is proposed in [9]. Unlike the numerous systems using the internet, communication is all performed over a fixed telephone line. The advantage is that it can be accessed via any telephone. However disadvantages include the lack of graphical user interface, the need to remember the user access code and the device codes.

Due to the limited resources and difficulties of expanding the scope of home automation applications, the cloud infrastructure is becoming extremely appropriate for home automation by enabling on demand access to shared pool of configurable computing devices and storages. The cloud infrastructure includes 3 service models: Software as a Service (it supplies customers with Web based applications, e.g., Google Cloud), Platform as a Service (it offers customers an application development and deployment platform as a service, e.g., Google App Engine) and Infrastructure as a Service (it offers various kinds of underlying computing and storage resources) [10]. Many researchers have carried out studies focusing on the use of cloud computing in home automation [10–13] to process and analyze the huge amounts of data generated by sensors deployed throughout smart homes.

Refs. [10,11] are the studies in which cloud based framework for smart home and a cloud based monitoring framework to implement the remote monitoring services of smart home are presented respectively. Ref. [12] involves the use of a networking cloud, Pachube, which is a real time data infrastructure that allows the management of data points from individuals, organizations and companies through the Internet. The home automation system developed in [12] employs the integration of multi-touch mobile devices, cloud networking, wireless communication, power-line communication to enable the remote control of lights and appliances within the home. The Arduino platform provides the communication between several components; Cocoa Touch and ObjectiveC are used in the implementation of the programs in the system.

Das et al. [13] proposed a home automation and security system in which motion detectors and video cameras are employed to detect the possible intrusion. A simple security system operates as follows: When the motion (intruder) is detected through sensors, video cameras are triggered to record and the system sends an alert to the user's mobile device. The system has two main components, the iOS application that executes on the mobile device (Apple's iOS devices) and server side scripts that run in a cloud.

Table 2

The properties and comparison of current home automation systems.

Properties		Degree of desirability	Proposed system	[5]	[6]	[8]	[13]
Networking technologies	Web application	3.40	+	+	–	+	–
	Mobile device application	3.73	+	–	–	–	+
	SMS (GSM service)	3.64	–	–	–	–	–
	Bluetooth	2.33	–	–	+	–	–
	Infrared	2.14	–	+	–	–	+
	Wi-Fi	3.64	–	+	–	–	–
Privacy issues	Storing user data in plain text	2.33	+	+	+	+	+
	Storing user data in encrypted text	3.87	–	–	–	–	–
	Storing device requests in plain text	2.86	+	+	+	+	+
	Storing device requests in encrypted text	3.47	–	–	–	–	–

A review of the literature highlights a number of commonly discussed properties of home automation systems. Additionally, the user preferences on these properties are measured by conducting a survey with a group of 20 volunteers. In the survey, the participants are asked to grade the degree of desirability for each property within the range [1,5] (from “not desirable” to “very desirable”). The properties are categorized in two groups; networking technologies and privacy issues; as shown in Table 2. In first group, 6 networking technologies are given. In the second group, privacy issues are graded. Participants indicate the degree to which they allow to store private user data (user rights, passwords) and/or the device requests (storing user behaviors via control messages) in plain or encrypted texts publicly.

The average degrees of desirability obtained are given, in the third column of Table 2, showing that Android is the most popular networking technology, whereas Infrared is the least. From the privacy related values in Table 2, the following two expressions can be stated: i. the participants prefer to share their data in an encrypted format. ii. the participants are much more concerned about their user data than their behavioral data.

The remaining part of Table 2 indicates whether the properties are available in a group of previously mentioned studies. The group consists of at least one sample from the studies where a different networking technology is used, and the studies where a running prototype exists. In Table 2, “+” denotes existence of the concerning property, “–” denotes the absence or the lack of information on the concerning property (not mentioned explicitly by the authors of the related study). The main objective of such a matching is to give a general overview of the systems based on predefined properties.

There are three remarkable outcomes of Table 2. First, the web application is the most commonly provided property by home automation systems mentioned. Second, systems do not offer the whole range of networking technologies; usually only one or two are supported. Though the security and privacy issues need much more attention, it was found that storing the data in an encrypted format is still not widely used in home automation systems, which is the third outcome.

In the survey, the users are also asked to grade the importance within the range [1,5] (1 for “not important”, 5 for “very important”) of multi-user services (e.g., adding and removing users, authorizing users for different devices) and dynamic device management (e.g., adding and removing devices). According to the survey results, the average grades were 3.2 for multi-user services and 4.13 for dynamic device management. Therefore, the participants are less interested in the multiuser support, and more interested in the capacity to add or remove devices.

In addition to aforementioned systems which offer different technologies in construction of home automation systems, in several other studies, different techniques are presented to improve different aspects of the smart home systems, such as the system performance, communication security, and energy consumption. For example, in [14] a data mining method is presented in which regularly occurring device usage patterns are discovered to improve the system performance. Ref. [15] introduces a distributed security platform for home automation, Trusted Domain, which is stated as being distinguishing by a unifying architecture based on IP and a unified security system. In [16], concerning energy aware smart homes, a smart home application is introduced that allows users to learn the energy profile of each home device and to identify the devices that consume most power by an Android application.

Although limited, the publicly available industrial research in the area of home automation systems, there exist several instances of projects developed in different countries by different companies [17,18].

3. Enabling technologies used in proposed system

Currently, the system designers have developed many different home automation systems using various types of technologies, of which some examples are discussed in Section 2. Our system design integrates trending software technologies in order to attract potential users of home automation systems.

We use the term “emerging” and “trending” to refer to any technologies/networks in the following three categories: i. the advanced technological hardware devices together with their softwares that are recently in-use by a high number of users (i.e., smart phones, tablet computers, Android OS, iPhone OS), ii. the software services that have much greater potential to be used by customers/users in different areas (i.e., cloud services, sensors-enabled network services, cloud tasks like storage and analysis of big data), iii. the networks and infrastructures that have the potential to be widely deployed and used by service

providers (i.e., distributed wireless and mobile networks, cloud networks, 5G, self-organizing networks like Long-Term Evolution (LTE)). Some other examples of emerging and trending technologies include wireless sensor and actuator networks, particularly body area sensor networks and cloud networks in health, Radio Frequency Identification (RFID) devices embedded within Internet of Things technologies. Emerging technologies in our viewpoint are the visible or invisible systems that mainly have the potential to be involved in many living spaces in the near future. For that reason, the security and privacy issues of these emerging technologies need much more care. We specifically deal with the context of home automation systems in this research and we qualify our project as an emerging technology product, since it involves the mobile and wireless smart devices running Android OS and its infrastructure is based on Google's cloud platform, together with Google's storage and messaging services.

In the proposed design, we mainly focus on the emerging cloud tasks. By integrating cloud services and Android devices with the ubiquitous behavior of customers, we aim to provide customers with the convenience of a home automation system that is seamlessly embedded in their life.

Regarding the software design of the system, our interest has been on designing a lightweight implementation using multiple open and free cloud services, together with open Android operating system features. Since Android running devices, e.g., smart phone, tablet devices or any hand-held devices, usually lack resources compared to laptops or personal computers, a lightweight application with simple interfaces to the end user would be a better design.

In order to reduce the complexity in hardware components of the proposed system, a single card, i.e., i.MX53, with adequate resources is selected as the core equipment. The remaining components of the hardware system in the house itself involve an Android running device on which the core card is embedded, and a few invisible cablings. All other hardware requirements (i.e., database server and application server) are freely available on the cloud. Thus, the management of the hardware devices deployed in-house is made easier, whereas the hardware devices in-cloud are managed automatically by the cloud providers. The rest of this section introduces emerging and enabling technologies used in the proposed system.

3.1. Cloud platform and cloud services

According to the definition by “United States National Institute of Standards and Technologies (NIST)”, cloud computing is a model which meets the demands of the shared pool of computing resources that are distributed and configurable [19]. Cloud computing enables the easy use of networks, servers, applications and services by software developers with minimum management efforts. The hardware and software resources of the cloud can be used based on a pay-per-usage business model [20].

Cloud platforms may be built as in three main types: public, private, and hybrid. A public cloud is open to everybody, and physically stores the data of users in any part of the cloud. In contrast, private clouds usually store the data of specific users in pre-determined private hardware. Hybrid versions integrate and use private cloud hardware with public cloud services; the user data may either be shared/stored in the public part, or be limited to the private part of the cloud.

A public cloud is considered in the proposed system since public clouds are usually free to users, as their set-up costs are covered by the provider. Some public clouds or some of their special services may also be offered on a pay-per-usage case. Our design uses a free and popular public cloud environment, Google Cloud Platform, in which there are many services including distributed application, database and messaging features. Those specific cloud services used in the proposed system are detailed as follows:

1. Google Cloud Platform [21] enables developers to build and deploy applications on Google's cloud infrastructure. It provides distributed storage and computing services.
2. Google App Engine [22] is a Platform-as-a-Service (PaaS) by Google. The cloud software developers can develop web applications on App Engine using its software development kit (SDK) freely.
3. Google Cloud Messaging (GCM) [23] for Android is a bi-directional service that enables messaging between application servers and Android devices. It allows the queueing and delivery of the messages of Android application with neither quota nor charge.
4. Google Cloud Datastore [24] is a data storage service. It is mainly a database with a distributed architecture and it differs from the traditional relational database in the way that it holds the non-relational data. The data objects stored in Google Cloud Datastore can be represented as entities.

Although the deployment and the maintenance of cloud technologies may be challenging tasks, and require great efforts, these issues are not considered in the proposed system because the authority to deploy, maintain and manage the cloud is its provider. In other words, the cloud computing part of the system is the responsibility of Google. Thus, the proposed system brings success with the use of Google services, ensuring the absence of maintenance problems.

3.2. Android operating system and Android services

In the proposed system, Android was chosen as an open operating system to be run on the two parts of the system: the end user's smart device, and the core embedded device deployed in-house. In addition, an open programming language, Java, was used to develop Android applications.

3.3. Java Server Pages (JSP)

The web page was developed using an open source web technology, JSP, to complete a whole open design.

Among those all technologies used in the proposed pervasive system, the main and the only practical requirement from the point of view of the user is Internet access. Simply put, the user needs to be on-line to use the cloud services.

4. System design, analysis and evaluation

This section presents the architecture of the proposed home automation system implemented through the project research period, and describes the approach and the systematic design of the project phases. First, related to the system architecture, the main components of the proposed system are described with diagrams depicting the communication infrastructures where those parts are in-use. Each part is briefly explained in different subsections. Second, a description in list form is given of the analysis and design criteria of the system, from the point of view of the system designers. Those criteria are taken into consideration at the implementation and system evaluation phases.

4.1. System architecture

The whole infrastructure design as a top-view communication diagram of the home automation system is given in Fig. 1.

In simple terms, the system involves the following three components: local hardware, web server, and mobile smart device. The local hardware includes the i.MX53 card and the local network devices to connect household appliances. The web server computer offers GCM service to connect the system with the local hardware and the mobile smart devices. Indeed, Google Cloud Platform is used to support bidirectional communication between local devices and the web server, and also between mobile devices and the web server. The web server also provides a web site for users (customers and administrators) to access the records stored in the database of the system. The final component is the smart device running Android operating system. The device, e.g. smart phone or tablet, has the Android application software installed, allowing customers contact and manage in-home devices via the server from any location. The Android application on the mobile smart device also provides its users with a user-friendly and non-complex graphical interface to easily control the automated machines at home.

The rest of this section dissects the three main components of the system regarding their tasks and functionalities.

4.1.1. Local hardware

Local hardware mainly consists of the i.MX53 card, given in Fig. 2, and its wireless or wired equipment connected to the appliances at home. One i.MX53 board integrated with a capacitive touch display screen is physically located at the target home to serve as the home's local central manager. i.MX53 device is able to send/forward bidirectional messages/signals between appliances and the server. The main resources of the i.MX53 hardware are its 1 GHz ARM cortex-A8 processor and its 1GB DDR3 main memory, which give it the capacity of a simple laptop computer.

i.MX53 card records the updated data to its session of which the identifier comes from the web server. The card regularly sends session data (home appliances data) to its serial port. The card is bootable from micro SD card. By configuring an

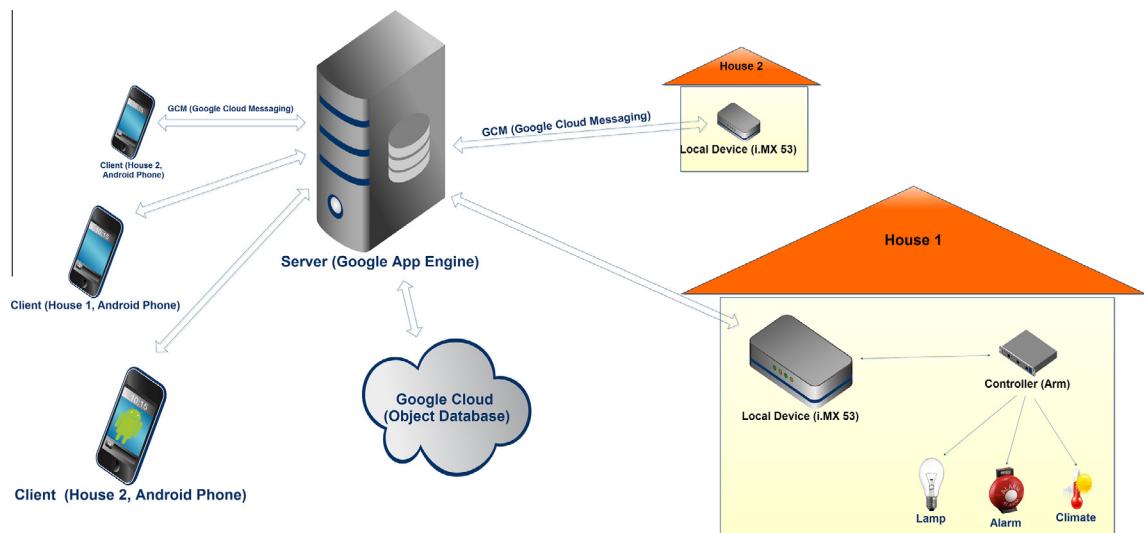


Fig. 1. Communication infrastructure of the proposed system.

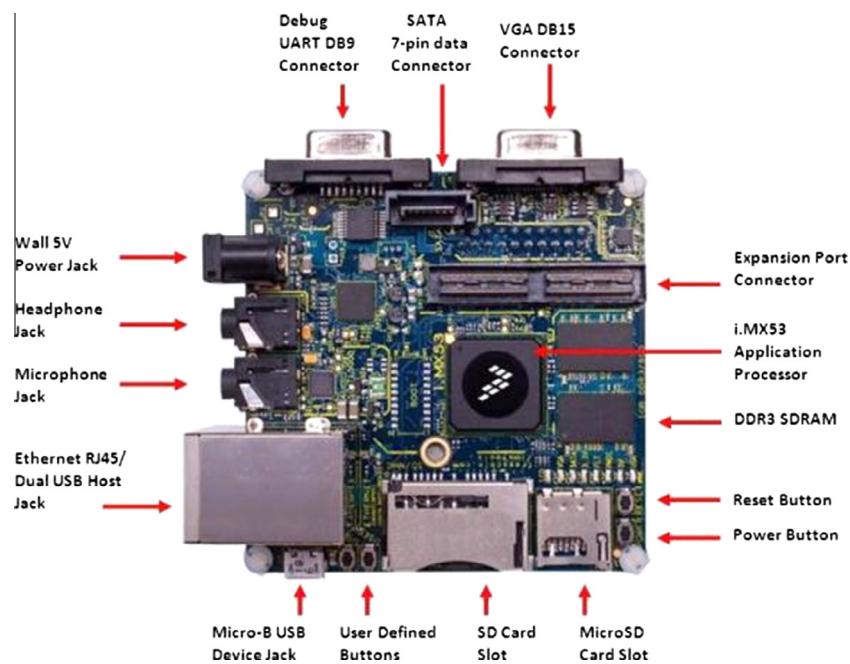


Fig. 2. i.MX53 embedded board.

Android operating system over an SD card connected to resource-powerful i.MX53 board, it is possible to integrate the system's Android application software into i.MX53. Thus, i.MX53 offers the same graphical user interface as the mobile smart device. The details about how the SD card is formatted and configured and how the local device driver is modified are beyond the scope of this paper.

After setting up the local hardware and equipments at related home, the authorized technician of the proposed home automation system enters the home id given by the administrator of the system and corresponding password onto the login page of the application on the local device. On the GCM server side, one-time registration is also necessary; a registration id is requested from GCM server and is recorded to the session manager of the application in the local device. The web server component will henceforth recognize the local device with that particular id. Hence, the registration id is tied to the corresponding app on a specific device and returned unique. To request a registration id, the application on a device needs only to send the sender id, which is actually the unique project number assigned by Google to the corresponding Google API project of the developer. However, Google has the right to access the device information before or during the registration process.

Fig. 3 shows the communication sequence diagram regarding the local component of the system. The arrow drawn from local hardware to the GCM server refers to the request for registration id. The corresponding registration id together with associated home id are returned to web server, as shown with the arrows between GCM server and system web server, which is also called cloud server, since it supports the cloud services. As the arrow from the web/cloud server to the local device shows, the updated states of the home automation system are sent back to local device from the web server, and recorded onto the local device's session using shared preferences. Then the local device sends the retrieved session data to its serial port where a controller is connected, as shown within the home image of **Fig. 3**. Although the controller device may be of any convenient kind, the proposed system uses an ARM controller to physically manage the home appliances. The prototype implementation of the proposed system uses an alarm triggered by smoke sensor, a lamp triggered by automatic switches controlled by the home automation system application, a curtain roller, and an air-conditioner representing the changes in home climate. Further physical appliances could be integrated to system on demand.

4.1.2. Web server

The web server stores the user records and serves the other components in the system. It manages the communication between the local device and mobile smart device, and the communication between local device and web site. Google Cloud Platform is used to support the bidirectional communication between home local device and web server, and also between the mobile device and web server. As the cloud platform, Google App Engine is installed within the web server. As a result, the terms "web server" and "cloud server" refer to the same server machine in this paper.

The communication between the server and local hardware, and the communication between the server and Android application are provided by GCM service. The GCM server used in this paper is not a built-in component of the system. Although depicted as one single machine in **Fig. 3**, the GCM server is actually just a representation of the distributed cloud

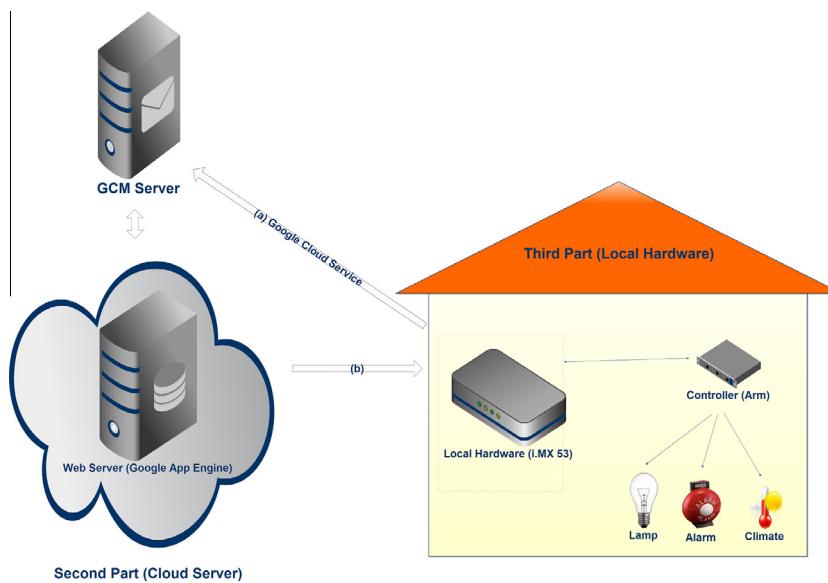


Fig. 3. Communication infrastructure for the local component.

platform provided by Google. The proposed system is connected to that cloud via Google App Engine available on the web server.

Google Cloud Messaging for Android is a service that enables developers to send/receive bidirectional data packets between servers and their Android applications on Android devices. The transferred packet could be a lightweight data message to trigger the Android application that there is a new message to be fetched from the server (i.e., a header or alarm data to point indirectly a huge-sized uploaded system data), or it could be an exact data message containing up to 4Kb of payload data to be used instantly in the system (i.e., direct system data to be used in Android application). The GCM service allows the queuing of messages and delivery to the target Android application.

The web server also hosts the system website. Database management of the stored data is done by the cloud as a distributed database using Google Cloud Datastore for this purpose on the web server. Database entities are created using Objective Database on Google Cloud.

The access to server data is managed through the website developed as a web page of JSP. The chosen development environments were the open distributed cloud platform by Google, open operating system Android and open programming language Java for the Android applications. Correspondingly, open source was the criterion chosen for the web page development. Another concern about the access method to web site is communication security. Access to the web page is provided through a secure connection using an https URL.

The communication sequence diagram regarding the web server (or cloud server) component of the system is shown in Fig. 4. The arrows in Fig. 4 represent the corresponding communication within the three main components of the system. Fig. 4 also infers that the web server is the global central manager of the proposed home automation system, which acts as a bridge between the other components.

Regarding the database, the main entities are as follows: devices with their states, users with their roles, homes with their appliances, and system specific data (i.e., the fixed/extraneous charges of fixed/extraneous services if applicable). Fig. 5 is the simplified entity-relationship diagram of the database at the design stage.

Requests, whether from the web page or the mobile device, to access user-related system/home data may be granted after an authentication mechanism using a pair of id and password. In default, there is no priority policy among the users of different homes or the platform used to access the data in cloud. The requests are granted according to the first-come-first-served rule in any part of the system. Nevertheless, there are two different types of users defined for any particular home: user as the owner of the home, and sub-users as the other users among the household. In Fig. 6, the use-case diagram for the user and the sub-users of the home automation system is depicted.

Briefly, in the proposed system, the sole user can select the services in the house to be integrated to the automation system, and authorizes the sub-users. Fig. 7 shows the interface in which the user authorizes two sub-user candidates for the house with ID 123.

Both the user and sub-users can manage the in-home appliances via the automation system; if two different types of users interact with the system during a specific same period, commands from the user role has priority over those from sub-user role; in this case, the user command only is granted to prevent a conflict within the same period of an actuation task.

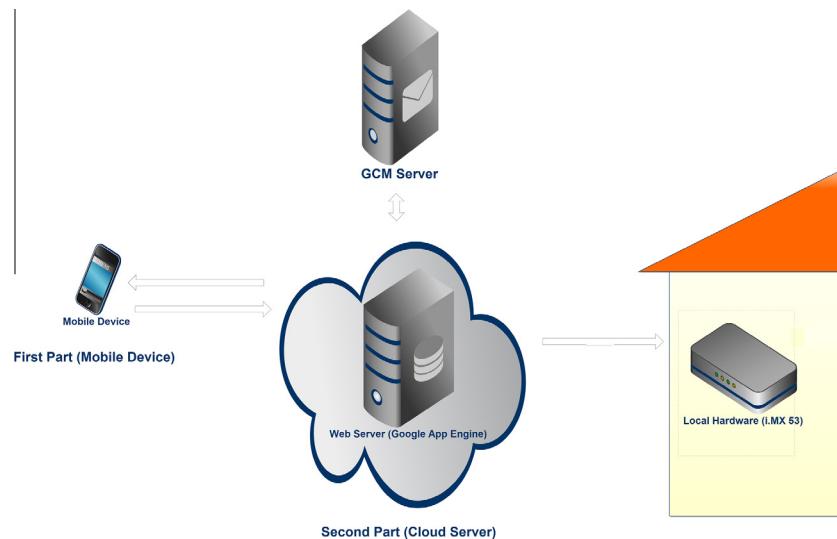


Fig. 4. Communication infrastructure for the web/cloud server.

Fig. 8 presents the web interface in which the user decides the devices to be controlled by the system. **Fig. 9** shows the web interface available to both the user and the sub-users of the home automation system, in which Lamp, Climate, Curtain and the Alarm are the controlled devices.

4.1.3. Mobile smart device

The mobile device, either a smart phone or a tablet, needs to run Android operating system since the user system involves an Android application. The mobile device application simply receives the users' requests, stores them in the session manager of the application by shared preferences, and transfers updated data to the web server using http POST method (https, that is secure http, is used to connect to web server using the web site in the system). The sessions are useful when it is necessary to store user data globally throughout the application. There are two approaches to data storage. The first is to store the data in a global structure variable in the program, and the second is to store the data in shared preferences. The problem with the first method is that the data will be lost once the user closes the application. Conversely, storing the data in shared preferences makes the data persistent even though the user closes the application.

Fig. 10 shows the communication sequence diagram regarding the mobile device. As shown with the initial arrow, arrow-1, in **Fig. 10**, the mobile device once requests the registration id from GCM server. When the id is returned from GCM server to web server, the web server recognizes the corresponding mobile device. After the user enters his/her authentication data pair into the login page of the Android application, the application transmits that data pair together with the registration id to the web server, as shown in arrow-2 of **Fig. 10**. If the user is granted access to the system, the web server returns the states of the home appliances to the mobile device, as shown in arrow-3 of **Fig. 10**. Arrow-4 in **Fig. 10** shows that when any state of the home appliance is changed by a user, the authentication data pair, registration id and updated states are resent to the web server using the POST method. The final arrow, arrow-5, in **Fig. 10** indicates that the web server sends the modified states of the appliances back to mobile device after forwarding them to the local device. The new states of the appliances will be recorded to mobile device's session using shared preferences of the application.

A sample sequence of Android application interfaces is given in **Fig. 11**. The interfaces of the system, both in server and mobile sides, are designed to be simple and user-friendly to increase the ease of use. The figure shows 3 screen shots of interfaces. The first (the leftmost interface) is the login interface of a registered user by email address (account) and the password (by logging in, the user will trigger the server to run the authorization system). The second shows the home system interface, which includes buttons to display the user account details, to send requests or to display the current status of an appliance. The last interface in **Fig. 11** presents the process occurring when the user presses the lamp button. The current state of the house lamp is shown on the screen, by changing light interval, the user can update the lighting level and after this information is saved, the updated data is sent to the web server.

4.2. System analysis and evaluation

In the initial phases of the whole project, within the analysis and design stages, the main criteria of an appropriate home automation system were discussed. In this section, the system designers present a list of measurement criteria to decide whether an office/home automation system is effective or not. Though these criteria may vary according to different

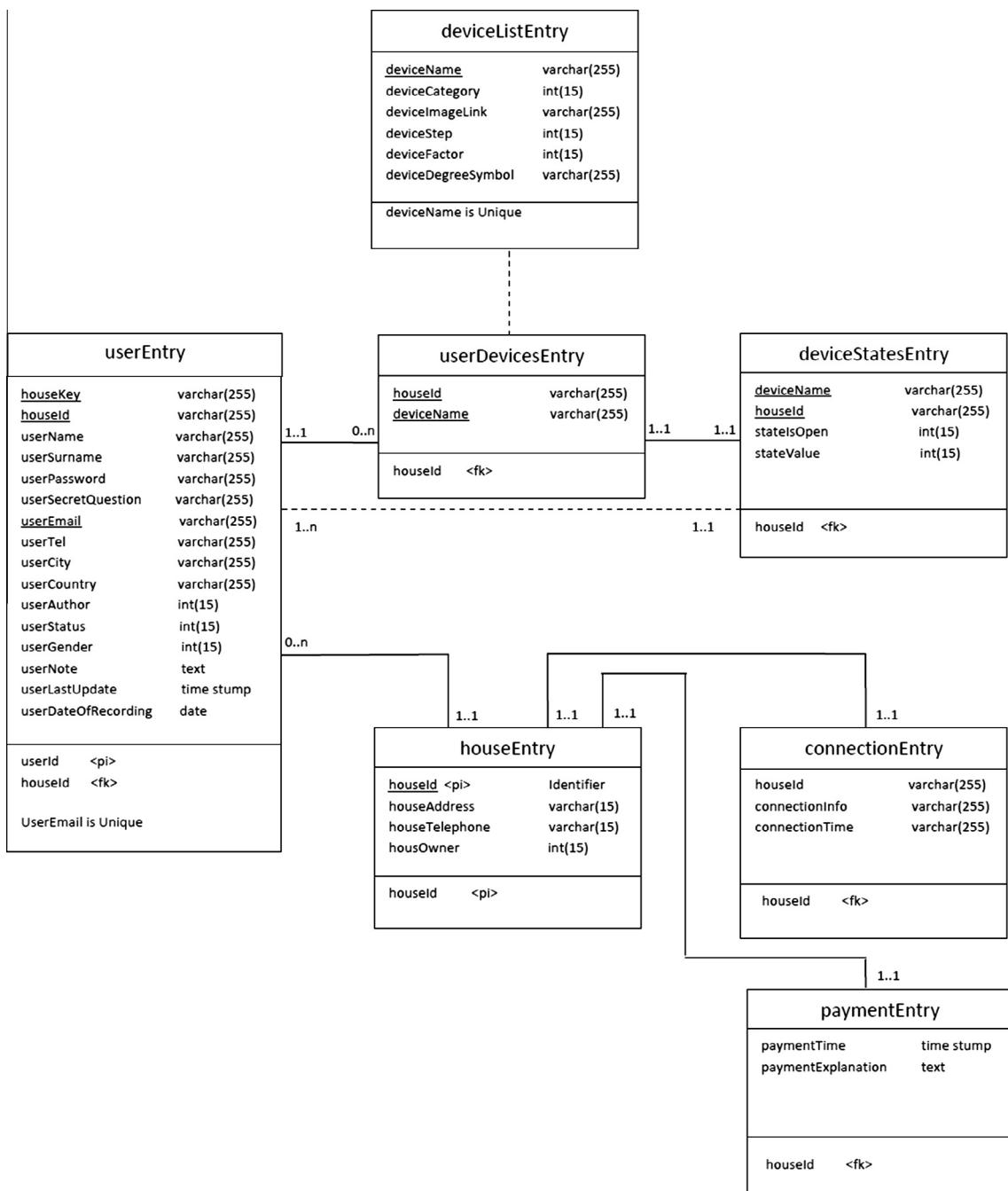


Fig. 5. The simplified entity-relationship diagram.

designers, this section firstly explains briefly how the analysis of the proposed home automation system has been conducted based on the listed determined criteria. Secondly, an evaluation of the proposed system regarding the criteria is given.

Within the analysis stage, the four main designers of the system, who are also authors of the paper, put themselves in the role of users of home automation systems and discussed what would be desired in such a system. Then all six co-authors of this paper discussed the functionalities of the system with respect to its software and hardware tasks. Based on the discussions among those six users, all considered properties or attributes for a convenient home automation system are taken into account, and then it was possible to draw up the final list of criteria that makes a home automation system adequate and qualified regarding the state-of-the-art technologies.

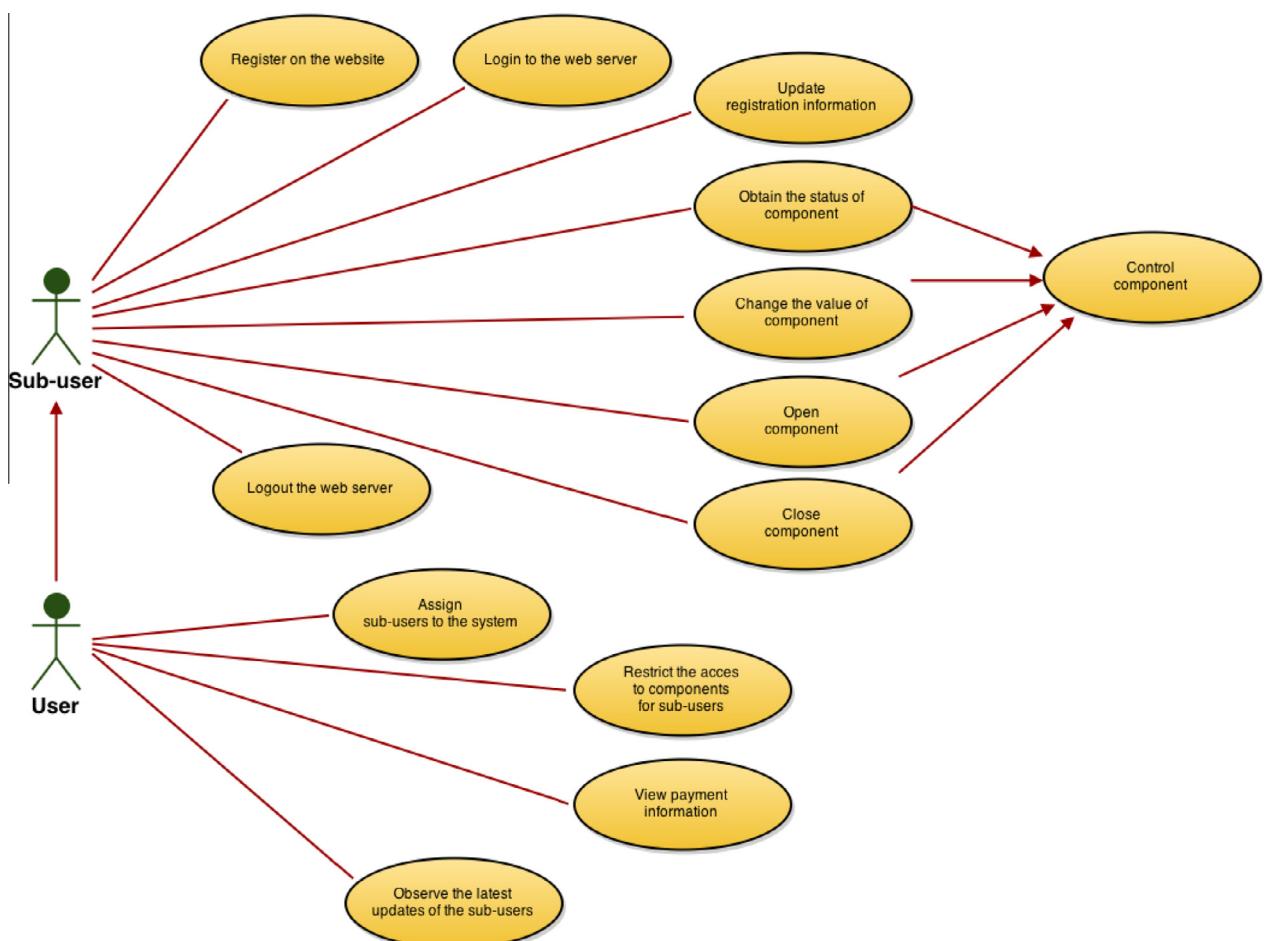


Fig. 6. The simplified web site use-case diagram of user and sub-users.

You can organize your family members if you are authorized.				
House Id	Name	Surname	Phone	Status ok?
123	Mustafa	Akdeniz	(0232 213 45 33)	<input checked="" type="checkbox"/>
123	Kemal	Ulubey	(0232 263 55 34)	<input checked="" type="checkbox"/>
123	Hasan	Aksam	(0232 420 58 40)	<input type="checkbox"/>

Save

Fig. 7. Authorization interface for the sub-users.

In order to quantify the level of importance of each criterion, an experimental survey was conducted with a group of 20 volunteer students from the software and computer engineering departments. 80% of those participants declared that they were very interested in emerging technologies and technological products, and 87% reported an interest in using a home automation system.

If you are authorized to select devices, this menu can help you.				
Device	Image Link	Category	Steps	My Device?
(1) Lamp		(Household)	(1)	<input type="checkbox"/>
(2) Climate		(Household)	(2)	<input type="checkbox"/>
(3) Alarm		(Household)	(100)	<input type="checkbox"/>
(4) Curtain		(Household)	(33)	<input type="checkbox"/>
<input type="button" value="Save"/>				

Fig. 8. The interface where the devices to be controlled by the system are selected by the user.



Fig. 9. The interface where the devices may be controlled by user or the sub-users.

In the survey, the participants were asked to assess the importance of each criterion within the range [1,5] (from “not important” to “very important”). The average of all grades for a criterion was used as its final assessment value, to be considered as the threshold regarding the performance. Later, a list of performance experiments with participants was conducted with the prototype of the system implemented for a single house, in order to evaluate the running system according to the given criteria.

In experimental setup, each participant played the role of a new user of the house in the system. The participants ran a group of single user and multi-user functionality tests under guidance. Each group of tests includes web application, Android application and web-Android interaction tests respectively.

In single user web application tests, each participant was requested to create a new account from the web page of the system, login to the system and manage the home remotely by modifying the states of devices. In Android application tests, the participants were mainly asked for using the system via their mobile smart phones. Before beginning the Android tests, the participants were directed to download and install the Android application package (.apk file) to their mobile Android phones. During this stage, the participants practiced controlling the home automation system with the accounts they created in the previous web test stage. In third stage of the single user experiments, the participants tested the interaction between the web and the Android applications via modifying the states of devices in one of the application, and checked that the states were modified in the other application.

In the multi-user experiments, the system was tested regarding the two different user roles, user and sub-user. Each participant played the role of both a user and a sub-user of the same house. Participants were asked to login to the web system as the user, and then create a sub-user for his/her home. According to the procedures of the system, the user must give

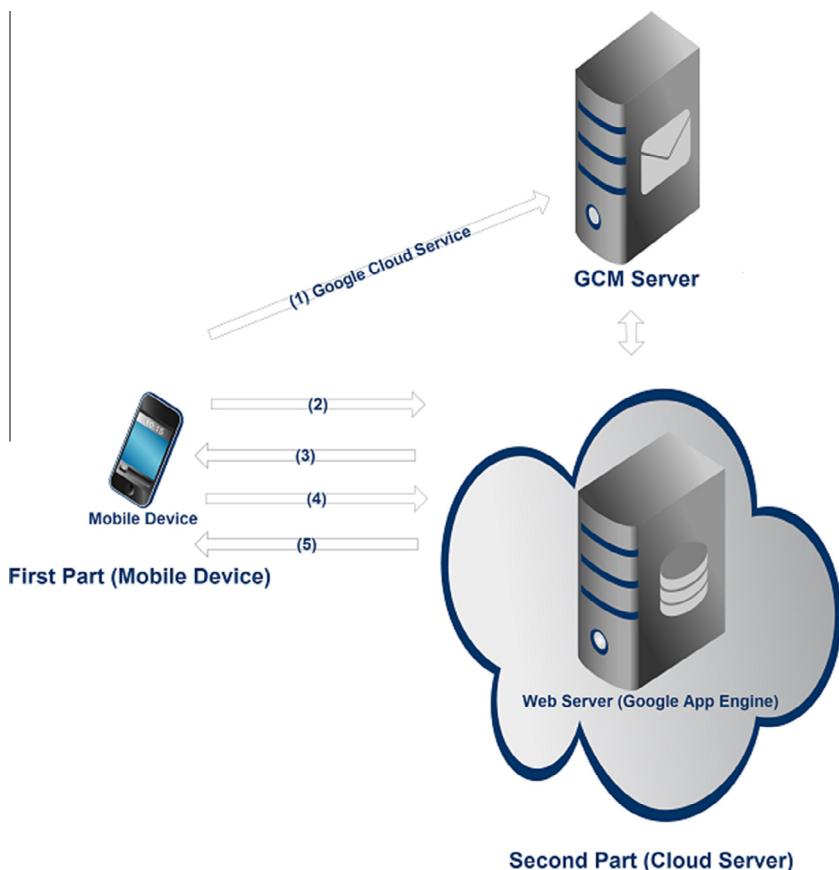


Fig. 10. Communication infrastructure for the mobile devices.



Fig. 11. A sample sequence of Android application interfaces.

control rights for each device to the sub-user. Following the authorization of the sub-user, the participant runs the similar group of three functionality tests performed in single user stage. Briefly multi-user experiments check whether the system is consistent with multi-users controlling the devices in the same house. The participant modifies the state of a device with one of the roles (user or sub-user), and then validates the change in state with the other role.

Moreover a stress test is performed to observe the response time delay in the system when multiple sub-users of the same house are regularly sending requests to the devices. In this experiment, 20 sub-user accounts are created for the same house, and each participant is assigned to one of the accounts. The participants are asked to use the system concurrently for a period of 10 min and note the observed response time of the system. The final response delay, which in this case is less than 1.5 s, is calculated by averaging those values.

To reach a final decision for our project regarding the mentioned list of criteria, the prior threshold values determined by the participants that refer to level of importance of the criteria (expectations) are compared with the experimental evaluation grades (results) of the running system. All evaluation results are summarized and classified as either adequate or inadequate for each criterion in the list in Table 3. In Table 3, the first column indicates the delivered list of criteria for an adequate home automation system, the second gives the expected threshold values (level of importance), the third presents the evaluation results. These results include the mean value for each criterion obtained by averaging the test scores of the running system, and the standard deviation value. Since the low standard deviation values indicate that the evaluation results of the participants do not spread out over a large range of values, the mean values in Table 3 are accepted to be reliable. The fourth column states the final decision for the corresponding criterion. If the average evaluation result, the mean value, for a criterion is greater than or equal to the expected threshold value, the system is considered as adequate with regard to the corresponding criterion, otherwise inadequate. The final column of Table 3 gives brief explanation and comments on our system with regard to the corresponding criterion.

There are three main outcomes of the evaluation stage:

1. The functionality tests were successfully performed on the system. The participants achieved control of all devices connected to the system.
2. It was observed that the participants were satisfied with the system according to all criteria except three: hardware safety, application data security, and emergency messaging. We believe that there were two reasons for the system failing the hardware safety and application data security criteria. The first is that the experiments were run on the prototype implementation in which the participants were unable to observe the devices in a real home. The second is that the cloud is such an abstract concept that the participants were not able to rely on the hardware and data security of a physically unknown web and database server. Although it is possible to plug and deploy an emergency messaging module into the proposed system, the prototype implementation is lack of such an emergency messaging component (e.g., distributed fire detection sensors, intruder detection mechanisms). For that reason, the result for the emergency messaging criterion is observed to be less than its threshold value.
3. The participants suggested some modifications/improvements on the web and mobile applications of the system. Some important suggestions are as follows: displaying the last user and the request, modifiable user interface (e.g., icons, background image), automatically shutting all system devices in case of emergency. The participants mentioned that there is a lack of iOS version for the mobile application. They also underlined their concerns on storing the private user data on a public server.

Table 3

List of criteria for an adequate home automation system (μ : average, σ : standard deviation).

Criterion	Threshold values	Results (μ/σ)	Decision	Explanation
Hardware safety	4.50	3.75/ 0.77	Inadequate	Web server and i.MX53 card need to be fixed in safe place
Application data security	4.36	4.25/ 0.62	Inadequate	Google distributed services provide data security. The authentication mechanism is used to log into the application
Power saving	4.21	4.50/ 0.50	Adequate	The user should select the related command for the appliances to be turned off
Energy awareness	3.85	4.50/ 0.59	Adequate	Lightweight application with few data communication is used. Only one web server is used to manage all homes (i.MX53 card is energy aware compared to a computer)
Cost	4.07	4.83/ 0.37	Adequate	Free cloud services with public cloud choice and only one server for all homes make the system cost-effective
Plug & play	3.43	4.42/ 0.67	Adequate	Android application and web site application are both ready to add/remove appliances. Networking between the new appliance and the local hardware is required
Scalability	4.15	4.33/ 0.58	Adequate	Number of homes, appliances, users may be increased with some extra configurations without changing the structures of server, local hardware, and Android application
Ease of use	4.29	4.67/ 0.47	Adequate	The same friendly GUI is used in both local hardware and mobile device
Reliability	4.21	4.33/ 0.58	Adequate	Google distributed services provide reliability
Response delay	3.62	4.33/ 0.47	Adequate	As GCM service is used as public and free, sometimes the messages are received by the mobile device with a reasonable delay (this issue may be handled by ordering a guaranteed bandwidth/service from Google with an extra charge)
Availability	4.21	4.67/ 0.47	Adequate	It is suggested to use the web server as a high quality one. Google's distributed platform provides availability
Ubiquity	4.71	4.77/ 0.55	Adequate	The application is mobile, the data is accessed from everywhere, the system is up any time
Emergency messaging	4.29	3.97/ 0.59	Inadequate	GCM and Android communicate. Application software needs to be modified regarding specific emergent events

5. Discussion and future work

While conducting the experiments to test the proposed implementation of the system with volunteer participants, we also noted their comments on the system. Those valuable comments, including their expectations about the services of the system and their suggestions to improve the system functionalities, are reported in Section 4.2. After discussing the feedbacks returned from the volunteer participants in the surveys, we decided on a few other minor functionalities to be offered within the system, either for some particular users or in general. One of these is validation of the user requests for device controls after a semantic consideration of the working values on the device. To give an example for a request to an air conditioner, assume that a user of a home automation system, who is intending to arrive home an hour later, wants to set the temperature to 25 °C using the Android application from outside the home. The system considers this request and decides to send or not to send the command simultaneously to the air conditioner device(s) by checking whether there is a difference between the temperature value of the command and the value in the home. Such semantic threshold values regarding the working conditions of the devices may be arranged in the system (e.g., setting the decision threshold for the air conditioner to 2degr range around the input value in command). The objective of such an approach is to decrease total home energy consumption, thus to offer a much more environmentally friendly home automation system. In response to the users, when the requested command is not forwarded to the device, a notification to their Android app could be sent indicating that the command is invalid. A possible alternative is to not respond to the user in any way, reducing extra battery/power consumption in message communication. To add such a semantic or rule-based decision mechanism to perform the actions associated with the input values will be a priority for future work for this system. So far, the application restrict the input data within an appropriate range regarding the nominal running values of the devices controlled (for example, the command for a usual home-type air conditioner used in Mediterranean countries could be granted on the condition that the temperature value requested lies in ≈ 18 to ≈ 30 in °C.)

Another functional improvement on the services provided would be to add an “in case of emergency” module. In case of a fire, the system shuts down the electricity automatically. This requires integrating a fire/smoke detection mechanism, involving a few extra sensors located in different rooms in the home, and a pilot relay on the main fuse to cut the electricity supply if the mechanism detects a fire. A common component of these emergent event detecting mechanisms is sending a message to notify the home owner about the case, which is inherently available as Android app notification in the proposed system. The prototype system currently involves smoke alarm that can be extended to an advanced fire alarm system; however, the implementation needs to be integrated to cover a relay. As another enhancement, an intruder detection system to detect any unauthorized entry attempts would require an identical mechanism involving motion sensors and/or video cameras placed at windows, doors and/or concealed locations in the home. The emergency module could also be extended to cover other cases, including disasters like floods and earthquakes. Such extensions would basically require additional hardware mechanisms deployed with the corresponding sensors. Android application of the system could easily be modified with plug and play feasibility, which allows the dynamic addition or removal of new items/modules/devices to or from Android and web applications by the users of the system, whereas the hardware integration of the new modules needs administrator approval.

Regarding the privacy issues concerning the people to be equipped with such an automation system for life, as mentioned in Section 4.2, the survey results show that there are potential concerns when people's private data is stored or logged in a system, and they would prefer to share their private data in a cipher rather than in a plain text format. With respect to this issue, the proposed system stores private user credentials required to manage the system, but neither stores the behavioral user data in device requests nor logs any history of commands in control messages. The user credentials are stored in a plain text form within the free database of public cloud system provided by Google Cloud Platform. Nevertheless, the communication protocol used for transmitting the data to web server of the system deployed in the cloud uses https connection. The https is generally identical to http, with the important exception that it uses an encrypted connection. At least one version of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols is used in https to provide confidentiality through their cryptographic encryption techniques. Although the user data is not stored in an encrypted manner in the web server in our proposed system, the web communication in the system is secure, due to the fact that an https request using SSL connection is required for an interaction between the user and the web server.

According to its privacy policy and license agreements, Google combines big data from its free public apps used globally. It is also well known that the big data concept is not only a significant asset, but also a commercial one, especially used in the advertising sector. In order to restrict Google from using the proposed system's data for any other purpose than storage without the permission of users, a particular contract with Google may be considered. However in this case, a fee may be charged for any of the proposed system's cloud tasks and services provided by Google.

Another alternative to prevent analyzing the user data in the system would be to use a private cloud architecture in the system. In this way, the privacy policy on user data may be declared by the home automation system builder. Although the proposed system would be identical in concept, such a modification employing a private cloud deployed by the system developers would require a complete revision on the system's infra-structural implementation.

Another alternative may be to send all user data to the web server in the cloud after encryption at the client application side. However, such a computational enhancement leads to extra cost in time and battery on the mobile smart device.

Instead, using https introduces a standardized security level to the proposed system, as recommended for an encrypted communication via internet.

A final important point is that Android application will log out the user who either quits or puts the application in the background. It would be optional for the user not to be logged out whenever the mobile application is put in the background, but this option was not available in the prototype version of the system. Putting into the foreground the application in the mobile smart device requires a new attempt to log into the system, which leads to the need for complete re-authentication.

As a future work suggested by the participants of the survey, the Android application could also be converted to iOS application version serving to the iPhone users. This needs neither a change in the concept design nor a modification in the cloud infrastructure of the system, but requires the re-implementation of the mobile app of the system with different APIs, and sending notifications to iOS device using Apple Push Notification service (APNs). However, we consider that paying a yearly fee to Apple to publish and distribute the iOS version of app is contrary to the free and open structure we have followed in development stage of the project.

6. Conclusion

The proposed cloud based home automation system involves three hardware components: a local device to transfer signals to home appliances, a web server to store customer records and support services to the other components, and a mobile smart device running an Android application. The functionalities of each different component of the system were dissected, and the communication infrastructures of the parts were explained. Distributed cloud platforms and services of Google were used to support messaging between the components. Such a design of service and data distribution through public and free Google platform makes the system cost-effective.

The prototype implementation of the proposed system was evaluated based on the criteria considered after the requirement analysis for an adequate home automation system. The prototype system was also tested and assessed by different users. According to the evaluation results, the proposed home automation system, which uses state-of-the-art cloud technologies and Android applications, is adequate overall.

The system is flexible regarding both the number of the houses and the number of the devices used in a house. The system is adjustable regarding the pricing. Regarding the infrastructural resources, the system is scalable, since it is mainly based on distributed cloud platform. The system is also extensible with new modules for different services; for example an intruder detection module can be added to the system by integrating motion sensors and/or cameras to monitor any movement within a house.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. They are also grateful to Umit Tarhan and Erman Selim for their contribution in the local hardware configuration of the prototype system.

References

- [1] Kovatsch M, Weiss M, Guinard D. Embedding internet technology for home automation. In: Proc of ETFA; 2010. p. 1–8.
 - [2] Moraes F, Amory A, Calazans N, Bezerra E, Petrini J. Using the CAN protocol and reconfigurable computing technology for Web-based smart house automation. In: Proc of 14th symposium on integrated circuits and systems design; 2001. p. 38–43.
 - [3] Piyare R, Tazil M. Bluetooth based home automation system using cell phone. In: Proc of IEEE 15th international symposium on consumer electronics; 2011. p. 192–5.
 - [4] Gurek A, Gur C, Gurakin C, Akdeniz M, Metin SK, Korkmaz I. An android based home automation system. In: Proc of 10th international conference on high capacity optical networks and enabling technologies (HONET-CNS); 2013. p. 121–5.
 - [5] Gill K, Yang SH, Yao F, Lu X. A ZigBee-based home automation system. *IEEE Trans Consum Electron* 2009;55/2:422–30.
 - [6] Sriskanthan N, Tan F, Karande A. Bluetooth based home automation system. *Microprocess Microsyst* 2002;26/6:281–9.
 - [7] Al-Ali AR, Al-Rousan M. Java-based home automation system. *IEEE Trans Consum Electron* 2004;50/2:498–504.
 - [8] Golzar MG, Tajozzakerin HR. A new intelligent remote control system for home automation and reduce energy consumption. In: Proc of fourth asia international conference on mathematical/analytical modelling and computer simulation (AMS); 2010. p. 174–80.
 - [9] Ardam H, Coskun I. A remote controller for home and office appliances by telephone. *IEEE Trans Consum Electron* 1998;44/4:1291–7.
 - [10] Ye X, Huang J. A framework for cloud-based smart home. In: Proc of international conference on computer science and network technology (ICCSNT '11); 2011. p. 894–7.
 - [11] Xu L, Zheng X, Guo W, Chen G. A cloud-based monitoring framework for smart home. In: Proc of IEEE 4th international conference on cloud computing technology and science; 2012. p. 805–10.
 - [12] Dickey N, Banks D, Sukitanon S. Home automation using cloud network and mobile devices. In: Proc of IEEE Southeastcon; 2012. p. 1–4.
 - [13] Das SR, Chita S, Peterson N, Shirazi BA, Bhadkamkar M. Home automation and security for mobile devices. In: Proc of IEEE PERCOM workshops; 2011. p. 141–6.
 - [14] Heierman EO, Cook DJ. Improving home automation by discovering regularly occurring device usage patterns. In: Proc of IEEE international conference on data mining; 2003. p. 537–40.
 - [15] Hjorth TS, Torbensen R. Trusted domain: a security platform for home automation. *Comput Secur* 2012;31/8:940–55.
 - [16] Jahn M, Jentsch M, Prause CR, Pramudianto F, Al-Akkad A, Reiners R. The energy aware smart home. In: Proc of 5th international conference on future information technology (futuretech); 2010. p. 1–8.
 - [17] Grid-control. <<http://www.grid-control.com/Heimautomatisierung.htm>> [last accessed: 02.14].
 - [18] Fukuoka smart house. <<http://www.smartenergy.co.jp/fukuoka/>> [last accessed: 02.14].

- [19] Mell P, Grance T. The NIST definition of cloud computing. National Institute of Standards and Technology, Information Technology Laboratory. NIST SP 800-145. <<http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>>; 2009.
- [20] Pearson S. Privacy, security and trust in cloud computing. In: Pearson S, Yee G, editors. *Privacy and security for cloud computing*. London: Springer; 2013, p. 3–42.
- [21] Google Cloud Platform. <<https://cloud.google.com/>> [last accessed: 04.14].
- [22] Google App Engine. <<https://developers.google.com/appengine/>> [last accessed: 04.14].
- [23] Google Cloud Messaging (GCM) for Android. <<http://developer.android.com/google/gcm/index.html>> [last accessed: 04.14].
- [24] Google Cloud Datastore. <<https://developers.google.com/datastore/>> [last accessed: 04.14].

Ilker Korkmaz received his B.Sc. degree in Electrical and Electronics Engineering and M.Sc. degree in Computer Science from Ege University, Izmir. He is a Ph.D. candidate at International Computer Institute, Ege University. He is currently with the Department of Computer Engineering at Izmir University of Economics. His research interests include sensor networks, security and cloud computing.

Senem Kumova Metin has taken her B.Sc. degree from Electrical and Electronics Engineering Department, Ege University (2001), M.Sc. and Ph.D. degrees from International Computer Institute, Ege University, Izmir (2005, 2011). She is mainly interested in natural language processing applications. She is currently working in Izmir University of Economics.

Alper Gurek has taken his B.Sc. degree from Department of Software Engineering, Izmir University of Economics, (2013). Currently, he is working in a well known software company in Turkey.

Caner Gur has taken his B.Sc. degree from Department of Software Engineering, Izmir University of Economics, (2013). Currently, he is working in a well known software company in Turkey.

Cagri Gurakin has taken his B.Sc. degree from Department of Software Engineering, Izmir University of Economics, (2013). Currently, he is working in a well known software company in Turkey.

Mustafa Akdeniz has taken his B.Sc. degree from Department of Software Engineering, Izmir University of Economics, (2013). Currently, he is working in a well known software company in Turkey.