

Research Article

IoT in Action: Design and Implementation of a Building Evacuation Service

Selahattin Gokceli, Nikolay Zhmurov, Gunes Karabulut Kurt, and Berna Ors

Department of Electronics and Communication Engineering, Istanbul Technical University, Istanbul, Turkey

Correspondence should be addressed to Selahattin Gokceli; gokcelis@itu.edu.tr

Received 9 September 2016; Revised 29 November 2016; Accepted 12 December 2016; Published 22 January 2017

Academic Editor: Sabrina Gaito

Copyright © 2017 Selahattin Gokceli et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of sensor technologies, various application areas have emerged. The usage of these technologies and exploitation of recent improvements have clear benefits on building applications. Such use-cases can improve smart functions of buildings and can increase the end-user comfort. As a similar notion, building automation systems (BAS) are smart systems that target to provide automated management of various control services and to improve resource usage efficiency. However, buildings generally contain hardware and control services from a diverse set of characteristics. The automated and central management of such functions can be challenging. In order to overcome such issues, an Emergency Evacuation Service is proposed for BAS, where requirements of such central management model are analyzed and model content and subservice definitions are prepared. A crucial scenario, which could be a necessity for future BAS, is defined and an approach for evacuation of people in the buildings at emergency situations is proposed. For real-life scenarios, the Evacuation Service is implemented by using a low-cost design, which is appropriate for Internet of Things (IoT) based BAS applications. As demonstrated, the proposed service model can provide effective performance in real-life deployments.

1. Introduction

In accordance with the development of sensor technologies that has been recently surging, smart system deployments to the buildings increase. Smart systems that are deployed in buildings increase user comfort and management of building resources becomes more efficient. These systems are referred to as building automation systems (BAS). Automated management of functions like heating, ventilation, lighting, security, and energy management is provided with BAS by using hardware and software based techniques. Specifically, utilization of BAS in schools, hospitals, factories, offices, and homes brings certain quality improvements [1]. Furthermore, BAS can provide significant cost advantages. According to a research conducted by Navigant Research, BAS industry is expected to reach 91.9 billion dollars in 2023 which is quite high compared to its size, 58 billion dollars, in 2013 [2].

Management of buildings, especially those which have high commercial value, is a challenging task due to complexity and size of the included control mechanisms, systems, and

functions. On the other hand, advancing sensor technologies create an expectation on the improvement in smart content of buildings. However, BAS contains several deployment difficulties because of facts like increasing number of users and diversity of expected services and utilized hardware. Integration of BAS with information and communications technology (ICT) and other related technologies is a certain requirement in order to provide full smart building functionalities. At this point, modeling of properties and functions of a building plays a crucial role and eases the management of the building in accordance with smart building approaches. In parallel with the need for integrated management of different control systems, European Union funded BaaS project aims to meet comprehensive, open cross-domain management and control services requirements of buildings [3]. A generic service platform for commercial buildings is developed where integration of BAS with ICT infrastructures is provided.

In this study, an Emergency Evacuation Service model is proposed as part of the BaaS project and details of this model are explained. At emergency situations, especially in densely

populated buildings, evacuation of people to safe places is a very challenging task because of complexity of the building floor plans. An emergency service is targeted in this study in order to solve this issue. Requirements and suitable hardware selection are analyzed in order to render the service applicable to variety of scenarios with various hardware configurations and systems. Evacuation service model and sub-service definitions are prepared accordingly. The system design is then implemented and demonstrated.

Internet of Things (IoT) is a global-scale network that covers usage of virtual objects or virtual things with attributes, auto-IDs, and self-configuration, receptivity [4]. IoT notion mostly involves low power devices with diverse set of characteristics. As demonstrated in [4], integration of IoT and BAS can provide various benefits. In this paper, similar facts are considered and, in order to provide suitability to real-life IoT based solutions, hardware and software components are determined with regard to IoT requirements. Applicability of the service is investigated with a real-time implementation. Details of this implementation are also explained.

This paper is outlined as follows. In Section 2, related studies are summarized. In Section 3, design requirements of the target service and suitable hardware selection for a real-life implementation are detailed. Content of Emergency Evacuation Service model is explained in Section 4 and sub-service definitions are given in Section 5. Implementation details are explained in Section 6 and the paper is concluded in Section 7.

2. Related Works

In [5], the importance of the utilized communication system in the building is highlighted due to necessity of joint control and management of mechanisms targeting diverse characteristics, through BAS applications' perspectives. Thus, standards such as LonWorks and BACnet are analyzed and detailed literature review is given. It can be concluded that, because of components with various differences, an efficient and practical BAS model is hard to be proposed, however; such an effort provides many benefits. Similarly, in [6], possible benefits of BAS utilization on daily life are mentioned and a communication system deployment is analyzed. As part of these systems, BACnet and LonWorks are evaluated, and the related principals are detailed. After highlighting the importance of increasing energy costs in the recent term, an intelligent energy consumption model within the scope of BAS is proposed in [7]. According to the model, system consumption is tracked by analyzing the usage profile of the building user, and the alarm is generated when usage exceeds the determined level. In [8], usage of BAS with computer-integrated facility management (CIFM) systems is evaluated with the aim of decreasing limitations of combined usage of BAS with different technologies. Accordingly, possible usage models are proposed. Usage of wireless communication technologies in BAS solutions is detailed and corresponding advantages as well as disadvantages are explained in [9]. Similar to this study, commercial wireless communication technologies that are utilized in the BAS solutions are analyzed from distinct perspectives such as implementation costs,

reliability, and flexibility that allow suitable joint usage with other systems. Moreover, benefits and limitations of corresponding systems are detailed.

In [10], in order to increase usage efficiency of BAS, communication networks are evaluated and wireless communication based approaches are highlighted. Due to insufficient ontologies that target only limited use-cases, a solution that models BAS to be used with different use-cases and provides modularity is proposed in [11]. The proposed solution is called BASont and has suitable usage for various use-cases. Moreover, BASont integrates building information modeling (BIM) that is used for data collection of the building and BAS models by supporting retrieval operations, data access, and synchronization with the previously deployed system. The proposed ontology is implemented with a Web service in order to provide efficient usage with self-commissioning and data access, and, as demonstrated with these use-cases, the solution has suitable functionalities for such deployments. It is highlighted in [12] that recent developments about ambient intelligent paradigm lead to a growing interest on autonomous home and building automation (HBA) solutions. However, most of the corresponding solutions do not include dynamic functionalities. To this end, a flexible multiagent approach that contains semantic-based resource discovery and orchestration functions is proposed in [12]. Semantic annotation of user profiles and device capabilities is supported within the proposed solution. Accordingly, environment is monitored by devices in the building, and data from users or devices are collected by a component called home mediator. This process is managed with one-to-one negotiations between home and device agents. By characterization of usage profiles of components in the building, semantic model is used to manage corresponding scenario efficiently. With real-time experiments, performance measurements for agents such as mediator, KNX device, and user agents are done and functionality of the solution is demonstrated.

In [13], a service-oriented architecture- (SOA-) based BAS model is proposed, where Web technologies are included. As the most important aspect of this study, BAS is integrated with a Web service, SOA, and semantic Web, where dynamic management of devices/services is provided within changing contexts. Such integration brings two crucial difficulties; it is hard to serve diverse and complex requirements of different services, and dynamic context changes are difficult to be tracked. These issues can be solved by composing services based on predefining policies and defining user requirements with composite service plans by using Composition Plan Description Language (CPDL) [13]. These functionalities are combined in the proposed solution. Performance of the model is quantified with experiments and two key results that show the effectiveness of the solution are obtained. The composition time is kept low even in critical conditions, and the service cache provides a significant improvement in service execution process. As mentioned in [14], the well-known BAS types such as KNX, BACnet, or ZigBee have suitable properties to local control scenarios by using non-IP communications. However, for large-scale BAS design and deployment, such technologies may not be sufficient due to the need for heterogeneous system interaction. In order to overcome this

problem, an integration approach for BAS is proposed in [14], where an IPv6-based service-oriented architecture is considered. The most important property of this solution is the suitability to the smart city cases. Implementation of this approach is given in detail and its applicability is shown.

Cybersecurity concerns in BAS are critical and any security leakage could cause serious problems. This is detailed in [15] and the lack of proper solutions that integrate cybersecurity and BAS effectively is mentioned as a serious threat for the future of BAS applications. Furthermore, importance of the security is explained with comprehensive examples. Possible solution points and approaches that could be effective for real-life deployments are highlighted. It is almost impossible not to care about security threats because of commercial value of BAS. Thus, it is suggested that compatibility between software-hardware and traditional-new deployed systems is a must in order to overcome security challenges. Moreover, the best option is to prepare a plan for the worst case while not totally obeying assertions suggested by software and hardware providers.

3. Design Requirements and Hardware Selection

3.1. Design Requirements. As stated earlier, BAS solutions are limited with implementation related obstacles and these limitations need to be overcome if an increase of the BAS usage is targeted. A flexible solution is a must for user comfort, which can only be provided with coordinated management of different hardware and software configurations. Thus, generated solution should be compatible with the previously deployed BAS solutions in the building and with other solutions that have probability of being deployed. This is a huge advantage because of certain cost and engineering benefits that are provided. Such compatibility can be provided with a modular approach and when required, new services can be deployed easily without harming other processes. One other significant issue is the security of the information. BAS solutions are based on information exchange within system components and a reliable communication is a must. This creates an inevitable concern about possible information leakages, since such buildings usually have users that produce valuable data. Moreover, privacy of the personal data must be protected according to legal procedures and any leakage may cause serious problems. Therefore, security of the data transmission must be provided in the BAS solution. A secure BAS solution should include security components demonstrated as follows:

- Mutual authentication protocols

- Cryptographic primitives for confidentiality

- Privacy preserving listing and searching a database

- Privacy preserving localization protocols

- Implementation of localization protocols by using radiofrequency identification (RFID), related security issues

- Implementation of localization protocols by using ultrasonic sensors, related security issues

- Implementation of counting algorithms by using stationary passive infrared (PIR) sensors, related security issues

A database is required with the assumption that most of the solutions store some data and hence contain a database or a similar component. Moreover, since we specifically target emergency evacuation scenario in BAS, localization of person is a necessity for a comprehensive service and related facts that are ordered above. Possible hardware that can be used within Localization Service is mentioned in the previous list. One other important issue is the suitability of service definitions to the real-life hardware usage. Hardware that can be used in BAS applications usually has common technical capabilities and software features. Services that are defined as part of a BAS solution should be defined according to a comprehensive hardware analysis. Such services can be different from each other in most cases, but there are certain common points from the implementation perspective. As mentioned earlier, the used hardware for each service can be different, but technical definitions include similarities. Hardware requirements of the implementation of a service should be thoroughly analyzed and definitions should match technical capabilities of such hardware; that is, type of the analog-to-digital converter (ADC) that is used and operating frequency of radiofrequency identification (RFID) can be suitable design points. Efficiency of the system operation and management of the tasks also need to be considered when a BAS solution is designed. Tasks that are assigned to the hardware must be planned well in order to protect technical efficiency and life cycle of the hardware. Hardware that is used in such applications usually consumes a low amount of energy. However, the system could consist of a central computer unit that has various tasks to implement and energy consumption during implementation of these tasks could be very high. In order to keep these values low, tasks should be divided well and data obtained by hardware should be managed efficiently on the software side. Any recursive task could create certain energy inefficiency especially in large-scale buildings. Currently, green building is an important and beneficial concept that is aimed at being deployed in almost all countries. For realization of this notion, the mentioned energy management must be considered.

3.2. Utilized Hardware. To provide modularity in the proposed Emergency Evacuation Service model, different hardware modules were chosen to realize the system. Each different module is used to perform a particular task. Aside from central computer used for decision making and further evacuation maintenance, there are four modules used that are Arduino Uno microcontroller-based board, RFM23B radiofrequency module, HC-05 Bluetooth module, and LM35 temperature sensor.

3.2.1. Arduino Uno. Arduino Uno is a microcontroller-based board with an ATmega328 microcontroller. Arduino Uno has every needed component to maintain ATmega328; it can simply be attached via USB cable to a computer or by using an AC-to-DC adapter or a battery to start working.

Specific software called Arduino IDE is available to program any Arduino compatible board with C-like programming language. This software supplies a serial monitor which allows not only reading but also sending data through serial connection. With growing number of product-specific libraries, Arduino offers useful tools for designs related to embedded systems.

Arduino has several technical specifications such as containing ATmega328 microcontroller and having 5 V operating voltage, 14 digital I/O pins, and 6 analog input pins, with 16 MHz clock speed [16].

3.2.2. RFM23B Radiofrequency Module. HopeRF's RFM22B/23B is an integrated, cost effective, 433/470/868/915 MHz wireless industrial, scientific, and medical (ISM) transceiver module. Extended range and refined connection performance guaranteed by low receive sensitivity (-121 dBm) are coupled with industry leading $+20$ dBm output power [17].

This module has a proper design to be used directly with a microcontroller, which enables the creation of a very low-cost system. RFM23B also supports digital Received Signal Strength Indicator (RSSI). RFM23B radiofrequency (RF) module is used for RFID active tag and reader hardware configurations. This module is used in various applications such as remote control, sensor networks, industrial control, and home automation.

RFM23B module communicates with microcontroller by SPI communication protocol. To connect microcontroller-based Arduino with RFM23B, connections between SDI and MOSI, SDO and MISO, NSEL and SS, and SCK and SCK must be provided for SPI communication. Communication protocol is used for writing to registers and reading from registers on the module.

RFM23B consumes low power and has data rate capability from 0.123 to 256 kbps [18]. It has a temperature sensor and 8-bit ADC and supports temperature range from -40 to $+85^{\circ}\text{C}$. It can also provide frequency hopping.

3.2.3. HC-05 Bluetooth Module. HC-05 Bluetooth module is a well-known Bluetooth serial module. Designed for clear wireless serial connection establishment, HC-05 is an easy-to-employ Bluetooth Serial Port Protocol (SPP) module. Serial port Bluetooth module is a completely competent Bluetooth V2.0 + EDR (Enhanced Data Rate) 3 Mbps modulation with complete 2.4 GHz radio transceiver and baseband [19]. In master mode, HC-05 module can both search and pair with a Bluetooth device automatically.

This module has -80 dBm typical sensitivity, can support RF transmit power up to $+4$ dBm, and has UART interface with programmable baud rate [19]. Bluetooth module can support baud rates 9600, 19200, 38400, 57600, 115200, 230400, and 460800 and 8 data bits with 1 stop bit are included [19].

3.2.4. LM35 Temperature Sensor. The LM35 is an accuracy temperature integrated-circuit, which has linearly proportional output voltage to the Centigrade temperature. Since the user is not demanded to subtract a large constant voltage from the output to get handy Centigrade scaling, the LM35

device has an advantage over Kelvin-calibrated linear sensors. No outer calibration or trimming is needed to provide typical precision of $\pm 1/4^{\circ}\text{C}$ at room temperature and $\pm 3/4^{\circ}\text{C}$ over a full -55°C to 150°C temperature range [20]. The sensor can be calibrated directly in Celsius (Centigrade), and 0.5°C ensured accuracy [20]. It is also suitable for remote applications.

4. Emergency Evacuation Service Model

The proposed emergency evacuation solution for BAS consists of two important structures, the Alarm Server (AS) and the Building Management System (BMS), which play central roles in the evacuation process. The AS has initial responsibilities and mainly deals with alarm generation. Sensor sources constantly send information to the AS and by evaluating certain conditions, data received from sensor sources is analyzed. Depending on the values, an alarm is generated (or not). If an alarm is generated, AS communicates with BMS informing about the alarm. BMS is a BaaS application that manages services and conducts service procedure. Moreover, BMS stores the information about the employee and visitors having entered the building. This information is accessible in a way which keeps personal data private. Stored information within BMS also includes age and disability status of users in a database, capacity and usage status of each room or office in the building. As a significant security component, access to this database is valid only for authorized administrators. Furthermore, the communication between BMS and AS is authenticated by both parties. After receiving alarm information, BMS activates a procedure depend on the scenario.

The block diagram of the Evacuation Service is shown in Figure 1. Main part in the architecture is the EVAC which includes Web&Provisioning, Media and Application, location-based servers (LBS) and Alarm Servers. There is also Database Cluster included where EVAC Management and EVAC Reporting Interface are located. Communication between this Database Cluster and Media and Application and LBS and Alarm Servers is provided with TCP/IP protocol. Moreover, Session Initiation Protocol (SIP) and Integrated Services Digital Network (ISDN) services which are controlled over voice channels by Media and Application server are included in the private automatic branch exchange (PABX) structure of the building. LBS Server has two options to obtain location information: fixed passive infrared (PIR) sensors which are used in dynamic setup and wearable devices (WD) which are used in controlled setup. Evacuation procedure over this architecture is realized as follows:

- (i) AS receives an alarm from Fire Alarm System or from BaaS.
- (ii) After determination of the alarm, employees or the people in the building are first informed via internal alarm system by voice message or calling them.
- (iii) At the same time, an onscreen mask at the reception desk carries out a dedicated evacuation of the individual floors or the entire building complex.
- (iv) To carry out the evacuation efficiently and quickly, the language of the client is identified via interface to the

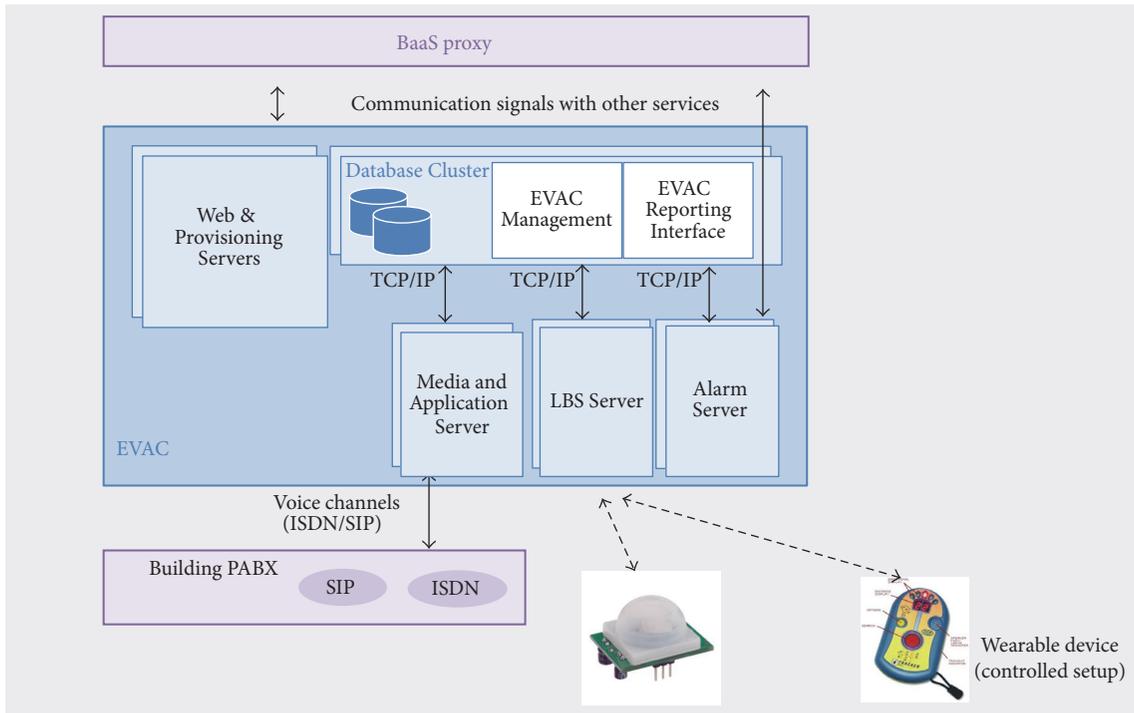


FIGURE 1: The block diagram of the Evacuation Service.

BaaS. The evacuation message is then sent in the user's native language.

- (v) Occupancy is controlled by the system by getting results from the WD with controlled setup or from PIR detectors with dynamic setup.
- (vi) AS calls the building sections-rooms/people via all available lines. The system collects every reaction in every call status mode, that is, ringing, busy, pick-up, answer, and hang-up.
- (vii) If the call is not answered during the ring phase (20 sec.) the system continues and flags this room/guest.

There are two BaaS emergency evacuation scenarios, controlled and dynamic setups. Contents of these two setups are demonstrated in Figures 2 and 3. Common and different requirements of content in these two figures can be given with explanations of steps as follows:

- (1) *Alarm*. Corresponding alarm should be triggered and authenticated by AS successfully. If an alarm is valid and type of the emergency situation is found out, emergency evacuation scenario becomes active.
- (2) *Info Request*. In this step, AS requests some information about database content from BMS. That request has to be compatible with BaaS components.
- (3) *Alarm System Info-Set*. BMS responses request from the AS some information that can contain identity (ID.EU), language, age, disability information of the person, and room/office fullness. Information content

can change according to the emergency type stated with Info Request step. It is important to protect confidentiality of the information set to be sent.

- (4) *Match ID_EUs and ID_WDs*. This step is only valid for the controlled setup. Privacy is a must. In order to preserve the privacy of the end users, pseudo ID_P_EUs can be sent rather than actual ID_EUs which are kept at BMS in that case. Access to this matched list must be limited to authenticated users.
- (5) *Calls and Actions*. Mutual authentication between AS and SIP Proxy is needed.
- (6) *ID_WD/ID_SEN Measurements*. ID of WD or ID of Stationary Sensors (SEN) is shared and confidentiality has to be ensured.
- (7) *ID_DCN and ID_WD/ID_SEN Measurements*. Similar to previous one, confidentiality of measurements must be provided.
- (8) *Localization/Counter*. Localization/counter measurements have to be analyzed and data for each user has to be produced according to the processed analysis. However, certain security protection must be provided. Obtained matched list should not violate the privacy of the end users. There must be authenticated access to this list.
- (9) *Action Feedback*. AS has to send back localization/counter information to the BMS after or during the evacuation. Confidentiality of that localization/counter information has to be ensured.

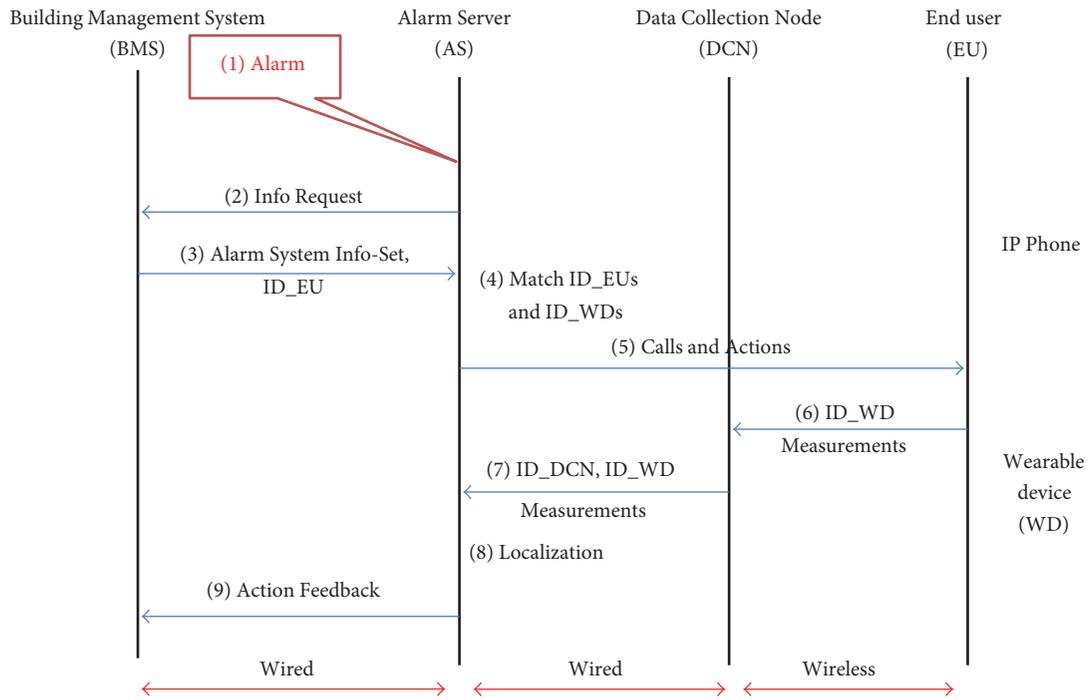


FIGURE 2: Content of the controlled setup.

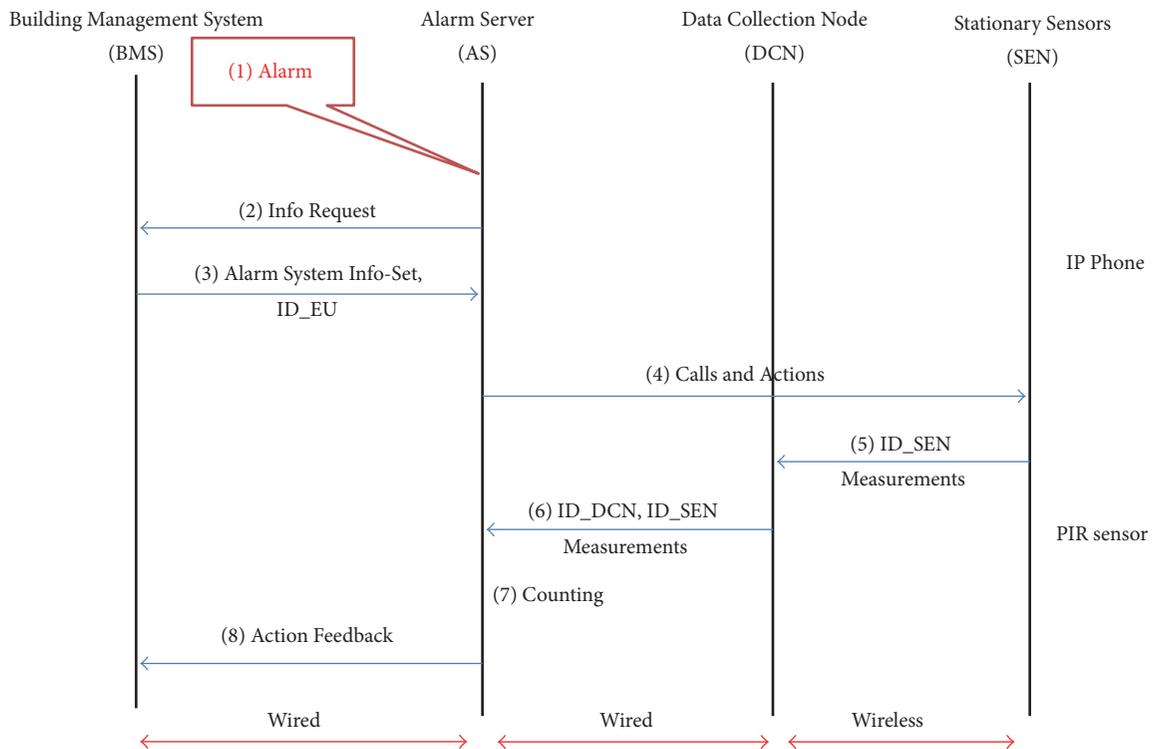


FIGURE 3: Content of the dynamic setup.

For both setups, communication between BMS-AS and AS-Data Collection Node (DCN) is provided with wired based methods. However, wireless communication methodology is valid for the communication between DCN and SEN. As mentioned earlier, one other difference between two setups is usage of PIR sensor in dynamic setup and WD in controlled setup. Few details need to be mentioned about these setups. For localization, passive RFID ultrasound tags will be on certain places on the walls and positions of the tags will be determined according to the floor plan. At real-life deployment stage of these setups, design and implementation of a handheld device that includes RF reader, ultrasonic sensor, and counting protocol by using PIR measurements should be considered. Moreover, wireless channel between DCN and WD or PIR sensors is important. This can be determined according to three types of wireless networks: personal area network (PAN), local area network (LAN), and wide area network (WAN). From our perspective, Bluetooth or ZigBee, Wi-Fi, and 2G/3G/4G can be used for PAN, LAN, and WAN respectively. Usage of Bluetooth RFID reader and tags is decided because of their several benefits. These can be summarized as follows.

4.1. Bluetooth. Bluetooth technology is a global wireless standard that enables short range wireless data communication. It has been proposed by major companies in the communication industry in order to create an alternative data transmission standard that is not based on cable connections. Bluetooth is widely used because usage cost is not high and it is compatible with almost all devices. It is very suitable to IoT applications with its advantages like being power-efficient and low-cost. 2.4 GHz industrial, scientific, and medical (ISM) radio band is the operating frequency band of the Bluetooth technology. In most countries, 80 MHz band is allocated to this band. Some radio front end features are detailed in [21, 22].

Due to Bluetooth's suitability to IoT applications and its related benefits, we used this technology in our system. Hardware settings and communication configuration are quite easy with Bluetooth technology. The communication quality obtained with this usage is another advantage. One disadvantage would be distance limitation of such usage. Bluetooth does not support long distances. However, building environment usually does not include long distances and if a sufficient number of hardware components are used with suitable distances, distance is no more an issue as in our implementation scenario.

4.2. Radiofrequency Identification. Nowadays, mobility and thus wireless communication are primary concern in consumer computing. Radiofrequency identification is one of the most widely used wireless technologies for automatic identification and data capture applications. Due to its light weight, low power consumption, cost-effectiveness, and non-line-of-sight readability RFID offers practical technology for context-aware computing like indoor localization systems [23]. An RFID module uses electromagnetic waves and employs a chip

and an antenna for two-way transfer of the data. RFID systems can be classified as tag and reader, where reader reads data generated by tag as the names suggest. Currently, various types of applications such as asset tracking, supply chain management, and payment systems (electronic tickets) include RFID systems [24].

The most distinctive property of RFID from earlier barcode technology is that it does not require a line of sight. RFID provides identification from a distance varying according to type of the module employed. Based on their power consumption, RFID tags can be categorized as active tags, passive tags, and semipassive (battery-assisted) tags [24]. Another categorization can be made by frequency range since RFID systems operate at a variety of radiofrequencies from 120 Hz to 10 GHz, which is explained in [25].

4.3. RFID Tags. For object identification, tags are used in radiofrequency identification systems. Depending on the battery property, tags can be categorized into three types which are passive, active, and semipassive. Two parts are specific main components of RFID tag. These parts are an integrated-circuit and an antenna. Processes like information storage and processing and RF signal modulation and demodulation are controlled with integrated-circuit. Transmission and reception of signals are realized via antennas.

4.4. RFID Readers. An RFID reader is a device that is used in RFID systems in order to provide connection between tag and system software [26]. Readers connect with tags which are located in the area of readers and start to perform some operations such as classifying tags in terms of meeting a criteria and encoding of tags. Readers also contain antennas for signal transmission with tags. Received data is sent to a computer for processing. Readers can be used in a stationary position or can be used with a microprocessor or mobile unit.

As the most important step of the emergency evacuation solution, subservices (where each one realizes part of the solution process) are defined according to these hardware details. Details of subservices are explained in the next section.

5. Subservice Definitions

According to the evacuation model, data obtained by sensors is processed, alarms are defined in accordance with predetermined criteria, and alarms are activated when corresponding conditions are valid. Moreover, location information of the people in building is monitored by using RFID technology and voice based help is provided to the people based on the Evacuation Service. In order to render model practical and efficient, subservices are defined and service management is organized accordingly. Services and relation between these are shown in Figure 4. Subservices are detailed below.

5.1. Alarm Monitoring Service. With this service, received data from the sensors is collected and a table that includes that data is created. This service is a key service for the Alarm Generation Service. Sensor IDs, type of the services (fire

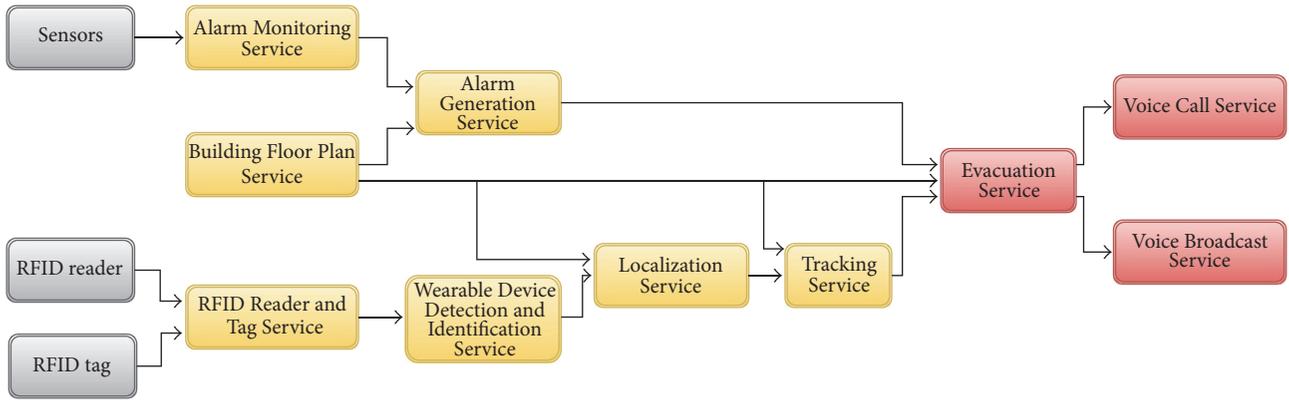


FIGURE 4: Services defined in Emergency Evacuation Service model and input-output relationship.

TABLE 1: Output table of the Alarm Monitoring Service.

Sensor ID (unsigned long)	Sensor type (short)	Measurement (short)
Sensor_ID1	1	5
Sensor_ID2	2	1

TABLE 2: Output table of the Building Floor Plan Service.

Building/Floor/Room ID (integer)	Building/Floor/Room Geometry X, Y, and Z coordinates (float)
Building/Floor/Room_ID1	X = 5, Y = 3, Z = 10
Building/Floor/Room_ID2	X = 10, Y = 4, Z = 6
Building/Floor/Room_ID3	X = 4, Y = 8, Z = 12

or gas), and measurement data that is sent by sensors are received by this service and collected data is sent to the Alarm Generation Service. An exemplary output table is shown in Table 1. Definitions like ID and measurement information are defined in accordance with technical properties of sensors that have wide-usage in the market.

5.2. Building Floor Plan Service. Building Floor Plan Service is a core service for other services. This service does not get any input; it stores some information such as room, floor, building ID, and three-dimensional location information as shown in Table 2. Building Floor Plan Service is crucial, especially for the Evacuation Service.

5.3. Alarm Generation Service. This service makes decision of alarm generation by evaluating the table and location information received from the Alarm Monitoring Service and Building Floor Plan Service, respectively. Depending on the sensor type, measurement result is compared with predetermined threshold and alarm generation decision is made by evaluating these inputs. Alarm generation is a necessity for the Evacuation Service; thus proper operation of Alarm Generation Service is very crucial. As an output of

this service, if an alarm is valid, then location and level of the alarm are sent to corresponding services as shown in Table 3.

5.4. RFID Reader and Tag Service. This service has a crucial role in the process, where evacuation plan is activated and specific plan for each person is presented. Location information is very critical in such plan and RFID Reader and Tag Service generates an important part of the location information. RFID readers obtain ID and RSSI information of tags that are located in the range of readers and give as output a table that is created by readers with obtained ID and RSSI information. RSSI information is used because RSSI level demonstrates the distance between tag and reader. Output table is similar to table shown in Table 4.

5.5. Wearable Device Detection and Identification Service. This service receives the table that is generated by the RFID Reader and Tag Service for a corresponding reader and also receives the table that includes list of the RFID readers located in the building. Firstly, it scans the registered readers IDs in order to find corresponding ID of the reader, and decides whether this reader is in the list or not. Then, if a reader is registered, Wearable Device Detection and Identification Service request RSSI levels from the reader. As a result, a table is created that contains the same content as table of RFID Reader and Tag Service. The difference is that only registered readers are included in this table, rather than all readers.

5.6. Localization Service. Localization Service receives table of registered RFID readers from the Wearable Device Detection and Identification Service and corresponding information from the Building Floor Plan Service. By evaluating the building plan, exact locations of RFID readers in the floor plan are calculated and given as output table as shown in Table 5.

5.7. Tracking Service. Tracking Service takes output table of Localization Service as input and calculates velocity and direction of the corresponding person for tracking. A table that includes these is given as output similar to Table 6.

TABLE 3: Output table of the Alarm Generation Service.

Sensor ID (unsigned long)	Measurement (short)	Alarm level (integers (1 to 5))	Zone ID (unsigned long)	System time
Sensor_ID1	1	1	Zone_ID1	16:24
Sensor_ID2	8	5	Zone_ID2	10:12

TABLE 4: Output table of the RFID Reader and Tag Service.

RFID Reader ID (integer)	RFID Tag ID (string)	RFID RSSI level (float)
Reader_ID1	Tag_ID1	-43
Reader_ID2	Tag_ID1	-57

TABLE 5: Output table of the Localization Service.

RFID Reader ID (integer)	X, Y, and Z coordinates (float)	System time
Reader_ID1	5, 3, 10	11:23
Reader_ID2	10, 8, 3	17:00

TABLE 6: Output table of the Tracking Service.

RFID Reader ID (integer)	Velocity (float)	Direction (integer)	System time
Reader_ID1	3	Direction_1	10:47
Reader_ID2	4	Direction_2	12:26

5.8. Evacuation Service. Evacuation Service is one of the most important services in the service model. A variety of information is taken as input which includes list of people inside the building received from Access Control Management; emergency type, place, and level received from the Alarm Generation Service; output table that includes velocity and direction information, received from the Tracking Service; and corresponding details received from the Building Floor Plan Service. Duty of this service is to combine generated data from previous services and decide whether to start evacuation process. Combined data is given as output and Voice Call or Voice Broadcasting Services are activated. Output consists of these elements: Voice Call ID (integer), Caller ID (integer), User ID (integer), Voice Broadcast ID (integer), and Area (integer).

5.9. Voice Call Service. Voice that is generated by Evacuation Service is taken as input and voice call is directed. Output content is as follows: Voice Call ID (integer), Caller ID (integer), and User ID (integer)

5.10. Voice Broadcast Service. Voice that is generated by Evacuation Service is taken as input and voice is broadcasted. Output content is as follows: Voice Broadcast ID (integer) and Area (integer).

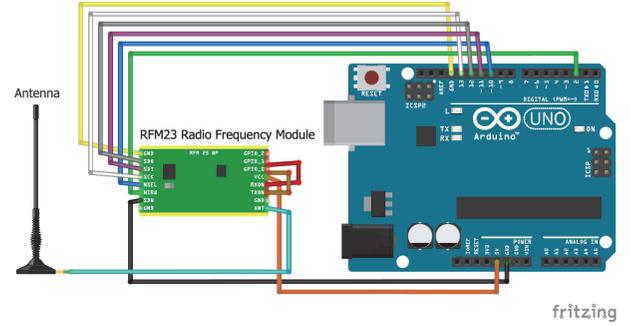


FIGURE 5: Scheme of tag configuration.

6. Implementation Details

6.1. Hardware Configurations. To implement the proposed Emergency Evacuation Service, three configurations are determined by using the previously explained modules. They are tag, reader, and sensor configurations.

6.1.1. Tag Configuration. The RFID tag is planned as an active device which continuously sends a message, supplying RSSI knowledge to a reader. Moreover, in terms of reliability, tag should supply an appropriate ID to the reader. According to the demands explained above, tag configuration is planned as a RFM23B module attached to an Arduino Uno card (Figures 5 and 6). The role of Arduino Uno is to drive RFM23B electrically and make RFM23B module transmit the message, which is a program embedded into Arduino's microcontroller. Hence, in tag configuration, Arduino Uno transfers the message through SPI to RFM23B which sends the message via radiofrequency antenna. It depends on the power supply of Arduino Uno whether tag is stationary or moving.

6.1.2. Reader Configuration. The messages sent by tag configurations should be read and transferred to the central computer by a reader configuration. Therefore, reader configuration has a RFM23B module and an Arduino Uno. Moreover, reader configuration has an HC-05 module (in slave mode) for redirecting tag data to central computer. This way, reader receives messages from tags and redirects it to central computer contemporaneously via HC-05 Bluetooth module over serial port protocol. Configuration is depicted in Figures 7 and 8. It should be mentioned that Arduino Uno has enough power to drive both RFM23B and HC-05 modules simultaneously. Additionally, reader configuration can be mobile or stationary depending on the power source type.

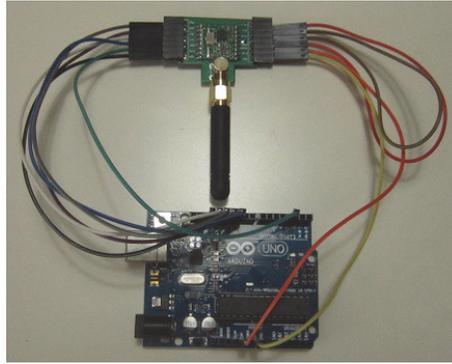


FIGURE 6: Real-time implementation of tag configuration.

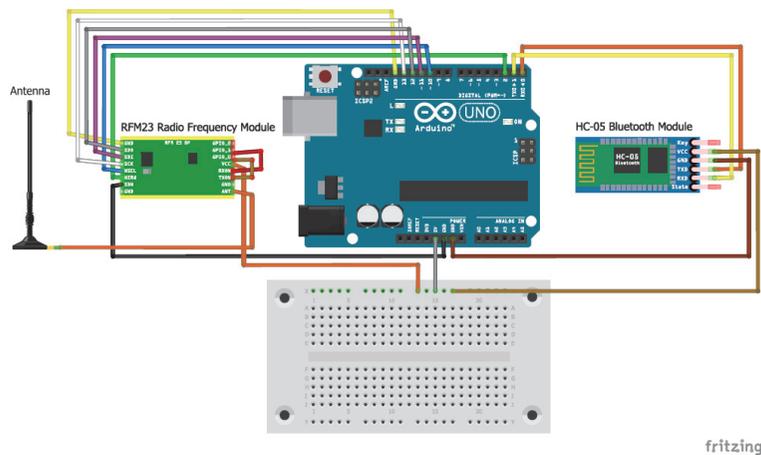


FIGURE 7: Scheme of reader configuration.

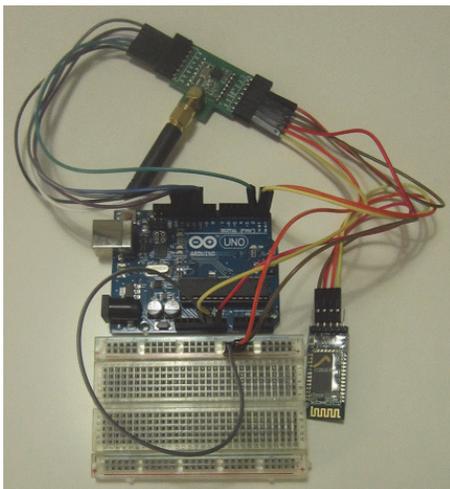


FIGURE 8: Real-time implementation of reader configuration.

6.1.3. Sensor Configuration. If a dangerous situation emerges, to create an alarm, sensory data is needed. To provide sensory data, sensor configuration is planned as an Arduino Uno

with attached LM35 temperature sensor and HC-05 module (Figures 9 and 10). Thus, while LM35 supplies sensory data through analog input to Arduino Uno, it computes the right temperature and redirects new data to a central computer via HC-05 Bluetooth SPP module in slave mode. Because LM35 sensor's supply voltage can be 5 V and its current drain is very low, Arduino Uno easily drives both LM35 temperature sensor and HC-05 module. Similar to the previous two configurations, sensor configuration can be either immovable or mobile with dependence on the type of the power supply used.

6.2. Hardware Scenario. To implement the proposed Emergency Evacuation Service model, a demo is planned. The aim is to gather central computer with all configurations in a big enough room and to test the proposed Emergency Evacuation Service model. The room is thought to be separated into four areas. Each area is planned to have stationary reader and static sensor configurations. Also, each area is thought to have people with tags inside. The model of the room is depicted in Figure 11 and real-time implementation views of readers and tags used in the demo are shown in Figure 12.

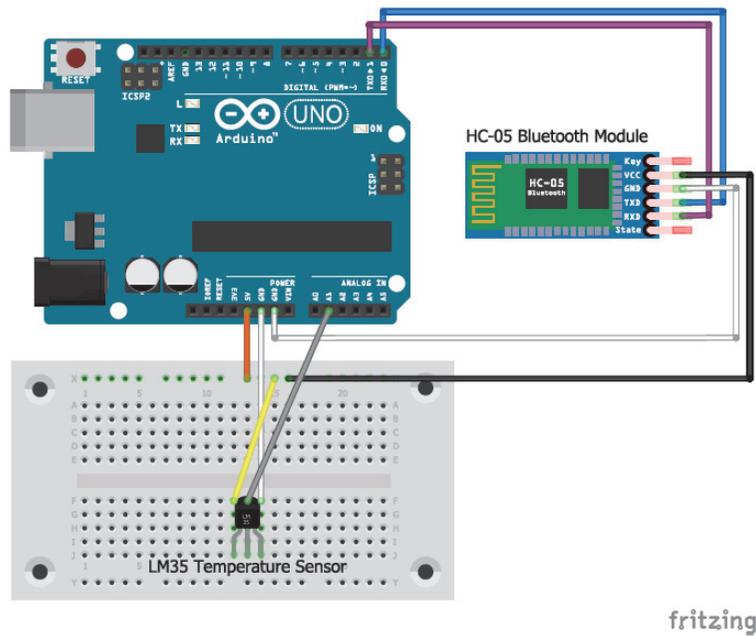


FIGURE 9: Scheme of sensor configuration.

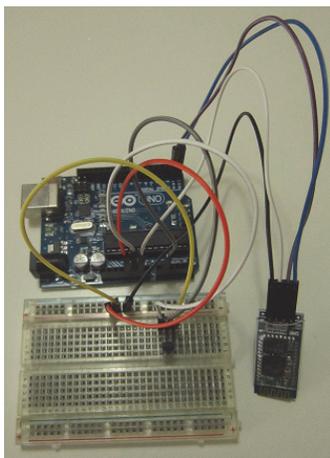


FIGURE 10: Real-time implementation of sensor configuration.

Fixed readers are planned to watch mobile tags on the people. First, each tag configuration sends its ID and message continuously by using RFM32B module. While tags send messages, readers are supposed to get messages and measure their RSSI values via RFM32B modules. Then, readers redirect collected data to the central computer via embedded programs inside Arduino Unos through HC-05 modules. Next, the data received by the central computer via its Bluetooth SPP module is thought to come through as many serial ports as readers and, by using serial Python program, processed and saved in a steady-size file as a table similar to the one shown in Figure 13 which is called the table of tags.

At the same time, stationary sensors are planned to send temperature data, through as many different serial ports as sensors, to the central computer, which decides whether there

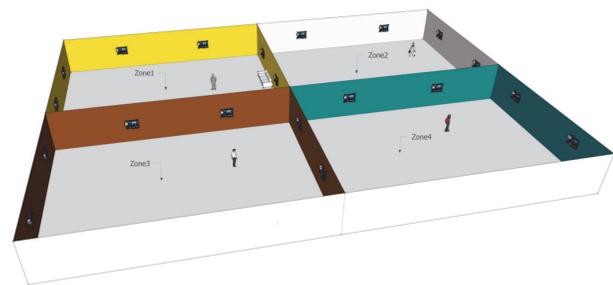


FIGURE 11: Figure of the room plan.

is a fire or not. In the first step, because each sensor configuration sends its data through independent serial port (Figure 14 depicts receiving continuous temperature data from one serial port) via HC-05 Bluetooth SPP modules, by using serial Python program, a table of all temperature sensors, similar to the table of RSSI values, is planned to be created as a fixed-size file called the table of temperature sensors. Then, the central computer decides whether there is a fire or not by checking the table of temperature sensors via BaaS application. In the next step, if there is no fire, the central computer continues to collect and monitor data. Otherwise, BaaS application activates Emergency Evacuation Service.

By reading RSSI values from the table of tags, it computes each person's position in the room (localization algorithm), then computes a safe route, and, by using voice signals, guides people to the safe location.

7. Conclusions

In this study, an effective Emergency Evacuation Service for BAS is proposed. Requirements of such services that can be

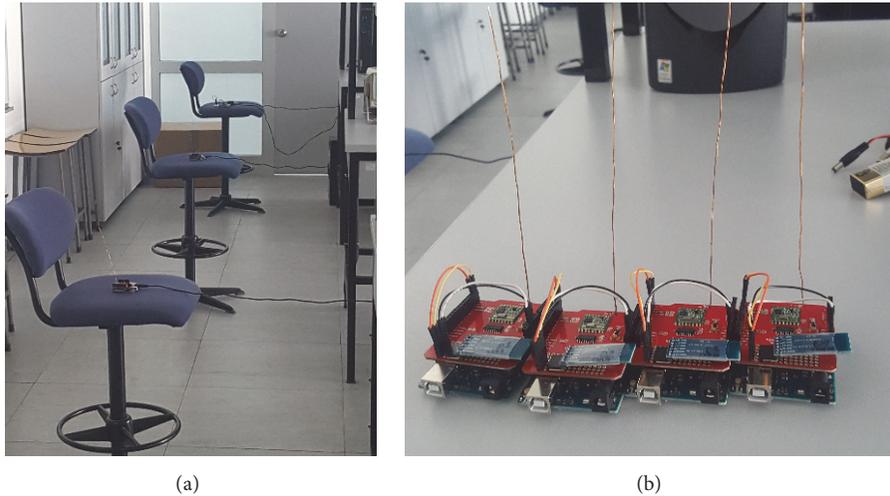


FIGURE 12: Implementation of demo scenario, (a) positions of three readers, and (b) tags carried by people.

```
Administrator: C:\Windows\system32\cmd.exe - python
ID: 1 | RSSI: 108
ID: 2 | RSSI: 106
ID: 1 | RSSI: 108
ID: 2 | RSSI: 108
ID: 1 | RSSI: 108

Ordered List Of Tags

ID: 2 | RSSI: 107 | Message: Hello From ID_2!
ID: 1 | RSSI: 108 | Message: Hello From ID_1!
```

FIGURE 13: An example of the table of data collected from tags.

```
Administrator: C:\Windows\system32\cmd.exe - python
TEMPERATURE = 27.34 °C
TEMPERATURE = 27.34 °C
TEMPERATURE = 26.37 °C
TEMPERATURE = 26.86 °C
TEMPERATURE = 26.37 °C
```

FIGURE 14: An example of a serial connection of a sensor.

implemented with complex and separate functions are analyzed and, in accordance with these, a service model structure is created. This structure consists of several functions and services that are defined with hardware compatibility. Details of these are given. Applicability of this model is observed with real-time implementation and corresponding details are mentioned. As a result, suitability of model to real-life BAS deployments is observed.

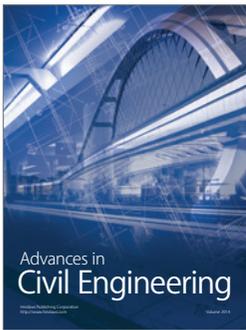
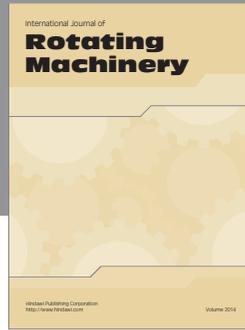
Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

- [1] F. Shu, M. N. Halgamuge, and W. Chen, "Building automation systems using wireless sensor networks: radio characteristics and energy efficient communication protocols," *Electronic Journal of Structural Engineering*, vol. 9, pp. 66–73, 2009.
- [2] N. Research, "Commercial building automation systems market report," October 2015, <https://www.navigantresearch.com/research/commercial-buildingautomation-systems>.
- [3] BaaS, September 2016, <http://www.baas-itea2.eu/cms/home-menu-item>.
- [4] J. Yu, M. Kim, H.-C. Bang, S.-H. Bae, and S.-J. Kim, "IoT as a applications: cloud-based building management systems for the Internet of Things," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14583–14596, 2016.
- [5] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman, "Communication systems for building automation and control," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1178–1203, 2005.
- [6] D. Snoonian, "Smart buildings," *IEEE Spectrum*, vol. 40, no. 8, pp. 18–23, 2003.
- [7] H. Wicaksono, S. Rogalski, and E. Kusnady, "Knowledge-based intelligent energy management using building automation system," in *Proceedings of the Conference Proceedings (IPEC '10)*, pp. 1140–1145, October 2010.
- [8] A. Bozány, "Integration of building automation systems and facility information systems," *Hungarian Electronic Journal of Sciences*, vol. 7108, HU ISSN 1418, 2003.
- [9] C. Reinisch, W. Kastner, G. Neugschwandtner, and W. Granzer, "Wireless technologies in home and building automation," in *Proceedings of the 5th IEEE International Conference on Industrial Informatics (INDIN '07)*, pp. 93–98, IEEE, Vienna, Austria, June 2007.

- [10] A. Pinto, M. D'Angelo, C. Fischione, E. Scholte, and A. Sangiovanni-Vincentelli, "Synthesis of embedded networks for building automation and control," in *Proceedings of the American Control Conference (ACC '08)*, pp. 920–925, June 2008.
- [11] J. Ploennigs, B. Hensel, H. Dibowski, and K. Kabitzsch, "BAS-ont—a modular, adaptive building automation system ontology," in *Proceedings of the 38th Annual Conference on IEEE Industrial Electronics Society (IECON '12)*, pp. 4827–4833, IEEE, Montreal, Canada, October 2012.
- [12] M. Ruta, F. Scioscia, G. Loseto, and E. D. Sciascio, "Semantic-based resource discovery and orchestration in home and building automation: a multi-agent approach," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 730–741, 2014.
- [13] S. N. Han, G. M. Lee, and N. Crespi, "Semantic context-aware service composition for building automation system," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 752–761, 2014.
- [14] M. Jung, J. Weidinger, W. Kastner, and A. Olivieri, "Building automation and smart cities: an integration approach based on a service-oriented architecture," in *Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA '13)*, pp. 1361–1367, IEEE, Barcelona, Spain, March 2013.
- [15] D. Fisk, "Cyber security, building automation, and the intelligent building," *Intelligent Buildings International*, vol. 4, no. 3, pp. 169–181, 2012.
- [16] Arduino UNO, September 2016, <http://datasheet.octopart.com/A000066-Arduino-datasheet-38879526.pdf>.
- [17] Hoperf Electronic, "RFM22B/23B ISM transceiver module," RFM22B/23B Datasheet, 2016.
- [18] RF22 Library for Arduino, September 2016, <http://www.airspayce.com/mikem/arduino/RF22/>.
- [19] HC Serial Bluetooth Products User Instructional Manual, September 2016, http://www.tec.reutlingenuniversity.de/uploads/media/DatenblattHC-05_BT-Modul.pdf.
- [20] LM35 Temperature Sensor, September 2016, <http://www.ti.com/lit/ds/symlink/lm35.pdf>.
- [21] P. Bhagwat, "Bluetooth: technology for short-range wireless apps," *IEEE Internet Computing*, vol. 5, no. 3, pp. 96–103, 2001.
- [22] Bluetooth Radio Architecture, September 2016, <https://developer.bluetooth.org/TechnologyOverview/Pages/Radio.aspx>.
- [23] B. Violino, "RFID business applications," September 2016, <http://www.rfidjournal.com/article/view/1334>.
- [24] S. A. Weis, "RFID (radio frequency identification): principles and applications," *System*, vol. 2, no. 3, 2007.
- [25] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.
- [26] RFID, September 2016, <http://www.impinj.com/resources/about-rfid/how-do-rfid-systems-work/>.



Hindawi

Submit your manuscripts at
<https://www.hindawi.com>

