IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 15, 2020, accepted July 5, 2020, date of publication July 10, 2020, date of current version July 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3008610

Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform

QUSAY I. SARHAN
Software Engineering and Embedded Systems (SEES) Research Group, Department of Computer Science, College of Science, University of Duhok, Duhok 42001, Iraq

e-mail: qusay.sarhan@uod.ac

ABSTRACT Smart home safety and security systems have gained much importance over the last few years owing to their notable impact in reducing and preventing losses in resources and human life caused by unwanted situations that could occur while homeowners are far away from their homes. To date, there is a lack of an in-depth literature analysis that could help researchers and developers better understand these systems and their applications in different contexts. It is therefore crucial that research evidence published in this area is presented. In this study, 63 research papers that examined smart home safety and security systems using the Arduino platform from popular literature databases were thoroughly surveyed to extract useful data. Then, the extracted data were analyzed to answer many research questions concerning state-of-the-art applications of these systems, their architectures, their enabling technologies, their components, etc. In addition, several challenges that these systems currently face and how future research could enable better implementation and use of these systems were discussed.

INDEX TERMS Arduino, smart homes, safety systems, security systems, sensors and actuators, architectures, enabling technologies.

I. INTRODUCTION

A smart home system is defined as a collection of sensors, actuators, communication devices, and computing devices that are connected to each other to provide homeowners with services and applications (e.g., safety and security, automation, entertainment, and energy management) with minimum or no intervention [1]. However, smart home safety and security systems are in high demand and always needed for many reasons including people's desire to feel safe in their own houses and to avoid a high rate of crime [2]. Additionally, recent advancements in the Internet of Things (IoT), pocket-size microcontrollers, and inexpensive sensors/actuators have provided many opportunities to enable safety and security in smart homes. Safety and security systems are employed to monitor indoor environments to provide homeowners with live updates and alarms when harmful situations may arise while they are far away. The aim of these systems is to interpret the sensory data collected (via sensors) from the surrounding environment to issue alarms or to carry out some appropriate actions (via actuators) against unwanted events. For instance, fire in homes could occur for a number of reasons, such as the burning of materials, gases, and electrical circuits, which could cause serious accidents [3]. To protect homes from fire, a fire alarm system is a must. Fire alarm systems are very useful in warning homeowners about this undesired situation and to prevent the loss of resources and human life that could result from it. Gas leakage is another unwanted situation. Liquefied petroleum gas (LPG) is the most widely used gas for cooking in homes. It is provided in cylinders and may blast due to leakage. In many cases, residents do not know that gas is leaking. They therefore may light up fire that causes a blast. To avoid this dangerous situation, a gas leakage detection system must be installed and used. Crime is rampant these days as well. The installation of security systems in homes is therefore crucial [4]. These systems can detect movements that may occur as a result of a thief entering a house. To avoid all the situations mentioned above, fire, gas leakage, and motion detection systems must be developed and used. Doing so will ensure the safety and security of homeowners and their families and will prevent them from serious accidents and undesired situations. The work of smart home safety and security systems starts with

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaolong Li.

monitoring the surrounding environment and then reacting to the abovementioned unexpected incidents that may occur while homeowners are away by sending alert notifications. In addition, some proper actions may also be taken by the systems such as stopping fire through the spraying of water and reducing the concentration of gas via air ventilation. The monitoring process of these systems is performed by means of sensors such as temperature sensors, gas sensors, and motion sensors. In event of an emergency, these systems may send notifications such as messages and emails. Additionally, they may use actuators such as buzzers, lights, and screens to notify nearby people. A communication medium is required to interact with these systems. Wireless communication, such as the Global System for Mobile Communications (GSM), Bluetooth, and WiFi, is widely used in this context. Of course, the selection of the appropriate communication medium is subject to a number of factors, including the cost, range, and technical specifications [5]. This study presents a detailed systematic survey covering the past six years to analyze the state-of-the-art research evidence related to Arduino-based smart home safety and security systems. The study begins with defining several research questions (RQs) covering several aspects of this topic. Then, it identifies the related papers that should be examined to answer the identified questions. Finally, it concludes with a discussion of potential opportunities for research in the field. To achieve the aforementioned aims, the relevant published papers were collected and extensively analyzed using a systematic process.

This systematic survey study was motivated by a number of factors: (a) Safety and security systems in smart homes are an important topic of research. Therefore, it is imperative to conduct a survey of related works to better understand the applications, implementations, and current research directions of this topic. (b) Carrying out a survey study could potentially benefit numerous researchers and developers interested in the field and aid in its future development. (c) There is no in-depth survey study that explores the topic of this paper.

The remainder of this survey paper is structured as follows: Section II presents the related works for this study. Section III describes in detail the research methodology used to conduct this study systematically. Section IV presents the results and outcomes of the study. Section V presents the threats to validity and the actions taken into account to avoid them. Finally, the conclusions of the study are provided in Section VI.

II. RELATED WORKS

This section briefly presents the most relevant literature publications on the topic. The authors in [6] provided an overview of smart homes and their main components. Then, they presented different security issues related to smart home systems. In addition, they provided a summary of the security studies that are conducted to address the security problems in smart homes and some possible solutions. The authors in [7] presented a brief survey of the works that use the IoT and big data in smart homes. Additionally, the technologies required to enable IoT and big data in smart homes were provided, along with their possible applications and services. In [8], the authors described the benefits and applications of using the IoT in smart homes. Then, they dedicated a section to IoT-based smart home security systems. In that section, they presented the use of sensors such as infrared (IR), passive infrared (PIR) sensors, and cameras for developing motion detection security systems. Additionally, the authors in [9] provided different IoT-based smart home applications. Then, they described a number of concerns about using the IoT in smart home systems such as security, data management, communication issues, etc. The authors in [10] and [11] presented different interesting functions of smart home systems. Then, they described the monitoring and controlling processes in smart homes and highlighted the advantages and disadvantages of various wireless technologies such as Bluetooth, GSM, ZigBee, and WiFi. Moreover, they provided an overview of different smart home architectures. The authors in [12]–[14] focused on the applications, enabling technologies, and security challenges in smart homes. In [15], the authors conducted a systematic review on smart home systems and their applications from the users' perspective. Additionally, they presented different types of smart home systems and their benefits. Then, they highlighted the challenges and barriers of implementing smart home systems.

The focus of the aforementioned studies was not to conduct a dedicated systematic literature study on smart home safety and security systems. In contrast, our paper presents a comprehensive and systematic literature study with a well-defined research methodology to investigate several aspects of smart home safety and security systems, such as applications, architectures, enabling technologies, challenges with possible solutions, and possible research gaps. Thus, it extends the details of other works on this topic by addressing nine important research questions that are not addressed in the literature. Potentially, this study provides a more detailed survey on the development and use of smart home safety and security systems.

III. RESEARCH METHODOLOGY

In this study, the guidelines for conducting systematic mapping studies [16] and systematic literature review studies [17] were followed. The systematic process employed in this study consists of five stages, as shown in Figure 1.

The first stage is to identify the objectives and questions of this study. Here, the study's research problem is identified, and various questions are defined to address the identified problem. The search process is performed in the second stage. Here, a search strategy for selecting the relevant publications on the topic of this study is specified. The third stage is the selecting and filtering of the publications obtained from the preceding stage. The fourth stage is the data extraction, in which the relevant publications are

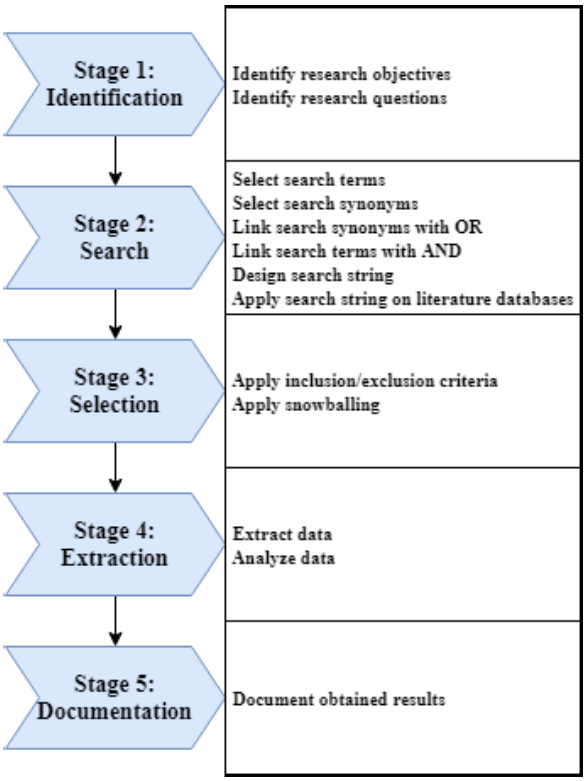

FIGURE 1. Stages of the used systematic survey process.

extensively analyzed and the useful details needed to answer the identified questions of this study are extracted. The final stage is the reporting and documenting of the results. The details of the aforementioned five stages are provided in the subsequent sections.

A. IDENTIFICATION OF RESEARCH OBJECTIVES AND QUESTIONS

1) RESEARCH OBJECTIVES

This systematic survey aims to provide a comprehensive analysis of all the studies published on smart home safety and security systems using the Arduino platform by identifying, reviewing, and categorizing the state-of-the-art contributions. This is achieved by answering several related research questions and thus helping researchers and developers to better understand these systems and contribute to their development and research.

2) RESEARCH QUESTIONS

Several research questions (RQs) have been identified and answered in this study. Each RQ addresses a particular aspect of the topic as follows.

- **RQ1.** What is the number and distribution of published studies on Arduino-based smart home safety and security systems since 2014?
- **RQ2.** Which universities are active in Arduino-based smart home safety and security systems research?
- **RQ3.** What are the applications and enabling sensors of Arduino-based safety and security systems in smart homes?
- **RQ4.** Which Arduino boards are the most commonly used in smart home safety and security systems?
- **RQ5.** What are the most commonly used alert notifications and response actions in Arduino-based smart home safety and security systems?
- **RQ6.** What are the most commonly used system architectures in Arduino-based smart home safety and security systems?
- **RQ7.** What useful details and findings can be extracted from the identified system architectures?
- **RQ8.** What are the challenges and issues of implementing and using Arduino-based smart home safety and security systems?
- **RQ9.** What are the potential future directions of research on smart home safety and security systems using Arduino?

B. SEARCH STRATEGY

1) LITERATURE SOURCES

Five standard online databases that index the publications relevant to the scope of this survey were selected as sources. Table 1 presents these sources and their web-links.

TABLE 1. Database sources used to search the literature.

Sources	Links
IEEE Xplore	http://ieeexplore.ieee.org
Elsevier ScienceDirect	http://sciencedirect.com
ACM Digital Library	http://portal.acm.org
Scopus	http://scopus.com
SpringerLink	http://springerlink.com

2) SEARCH STRING

To find the publications relevant to this study, the following search string was applied to the database literature sources:

"(arduino OR microcontroller) AND (smart OR intelligent) AND (home OR house OR building) AND (automation OR monitoring OR gas OR fire OR motion OR intrusion OR security OR system)"

All terms of the search string were linked with each other using Boolean operators [18]. The Boolean "OR" was employed to link synonyms or related terms that refer precisely or broadly to different aspects of the study topic, and the Boolean "AND" was used to link the major terms.

C. PAPER SELECTION

1) PAPER INCLUSION/EXCLUSION CRITERIA

A set of inclusion and exclusion criteria were established and employed to decide whether a publication is relevant to this study or not. These criteria, which are listed below, have been applied based on the titles, abstracts, and full text reading.

Inclusion criteria:

- Publications related directly to smart home safety and security systems using Arduino. Arduino has been selected because it represents the most used microcontroller-based board in various smart home systems. It has a user-friendly development environment and is affordable. In addition, it is appealing due to its large support community, extensive set of support software libraries, and various shields/modules boards to extend its interfacing capabilities [19].
- Publications published online over the last six years (2014–2019). According to our search and exploration of the literature, publications on smart home safety and security systems using Arduino started in 2014.

Exclusion criteria:

- Publications not published in English.
- Publications not peer reviewed (e.g., gray literature).
- Publications not published electronically.
- Publications that are duplicates of other previous publications.
- Publications without clear experimental results and evidence.

2) SNOWBALLING

To reduce the risk of missing some relevant papers, the snowballing search technique [20] was applied to the remaining papers. In snowballing, the reference list of each paper is checked with the inclusion/exclusion criteria. Then, the paper selection process is applied recursively to the papers that have just been found.

Figure 2 shows the number of included and excluded papers at each stage of the paper selection process.

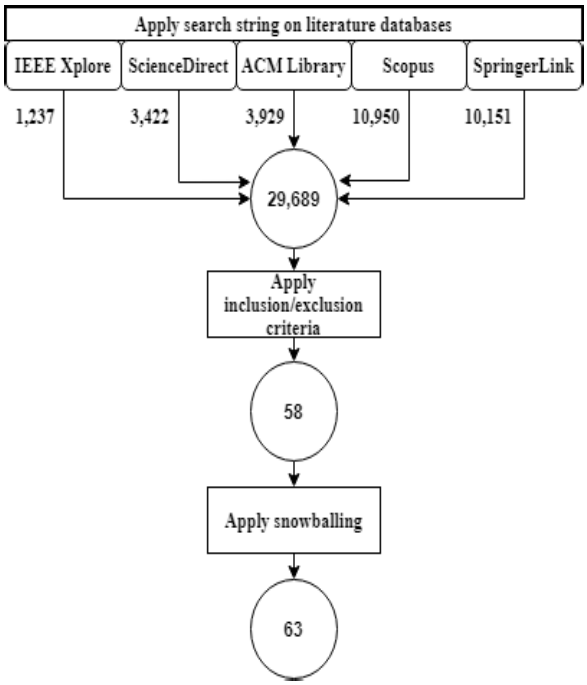

FIGURE 2. Results of the paper selection process.

In addition, Table 14 lists all papers (with their references, titles, and publication years) obtained after applying the paper selection process.

D. DATA EXTRACTION AND ANALYSIS

From the selected papers, data were extracted and extensively analyzed to answer the identified RQs. The extracted data were stored in an Excel sheet of various fields created specifically for this study. Each field has a data item and a value, as presented in Table 2. In this stage, the data were extracted first and then double-checked to ensure accuracy.

TABLE 2. Data extraction form.

Data Item	Value	RQ
Paper number	Integer ID	None
Paper title	Title of the study	None
Publication year	Calendar year	RQ1
Publication type	Category of publication type	RQ1
Publication venue	Name of publication venue	RQ1
Active university	Name of the active universities and their details	RQ2
Applications and enabling sensors	Applications and enabling sensors of Arduino-based safety and security systems in smart homes	RQ3
Arduino boards	Arduino boards used in smart home safety and security systems	RQ4
Alert notifications and actions	Alert notifications and response actions provided by Arduino-based smart home safety and security systems	RQ5
Architectures	Architectures used in Arduino-based smart home safety and security system	RQ6
Architectures: details and findings	Useful details and findings extracted from the identified system architectures	RQ7
Challenges	Challenges and issues of implementing and using Arduino-based smart home safety and security systems	RQ8
Future Research	Possible future research directions	RQ9

IV. RESULTS

To answer the identified RQs of this study, all the selected publications were intensively analyzed. Each RQ, represented by a short title, is discussed in the following subsections based on the obtained results.

A. DISTRIBUTION OF PUBLICATIONS (RQ1)

1) PUBLICATION FREQUENCY

All the selected papers of this study were analyzed to determine their publication frequency and evolution. Figure 3 shows the results of this analysis. The results show that the average number of publications per year is approximately 11 papers. Additionally, it can be noted that the interest in this topic increased in the last three years. This increase in the publication number is an indication of the successful applications of Arduino-based safety and security systems in smart homes. Another valid reason is the appearance of new technical advancements in the IoT, pocket-sized microcontrollers, and a variety of affordable sensors/actuators, providing many possibilities for implementing and using these systems.

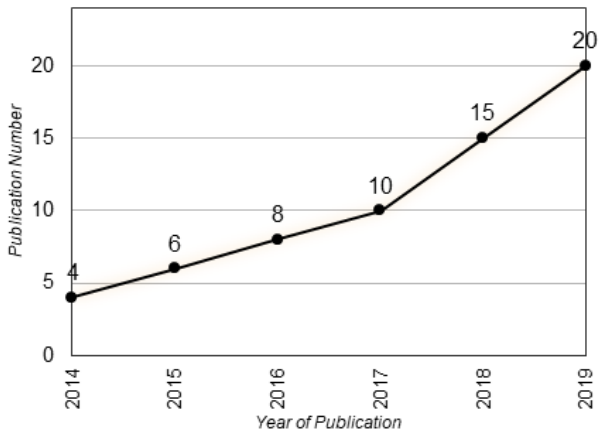

FIGURE 3. Publication per year.

2) PUBLICATION VENUE

As evident in Figure 4, the selected studies are distributed across several publication venues, of which 60 are conference papers, 2 are journal papers, and 1 is a workshop paper. This figure also shows that only 3% of the published papers have reached the maturity of a journal publication, implying that the research area is still very young or even immature [21], [22]. Some conference papers were published as book chapters. Here, their original venues, which are conferences, were considered.

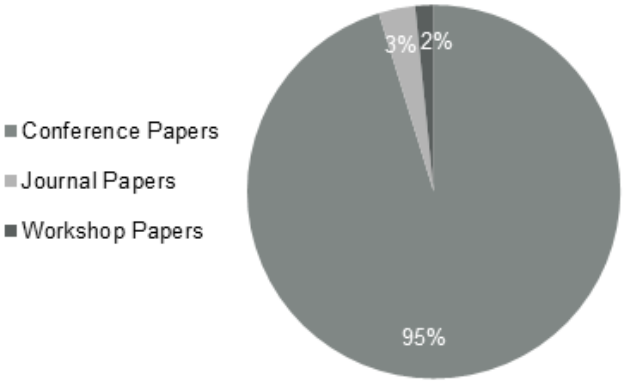

FIGURE 4. Publication ratio per each venue.

By analyzing the publications, the most active and top journals, conferences, and workshop venues that publish papers on the topic of this study can be clarified. Due to their long names, abbreviations are used in this paper. Figure 5 shows the active journals in which the relevant papers were published. The full names of the journals can be found in Table 15. The figure clearly shows that the most active journals are ''Procedia Comput. Sci.'' and ''IEEE Access'' with one published paper each.

Figure 6 shows the active conferences in which the relevant papers were published. The full names of the conferences are presented in Table 16. The most active conferences are

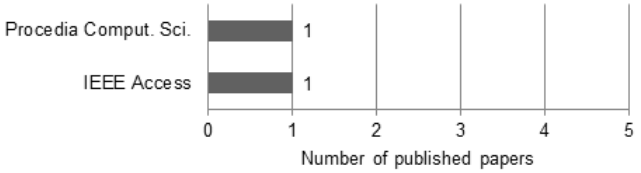

FIGURE 5. Number of published papers vs. journal name.

''ICCES'', ''ICAEE'', ''ICECA'', and ''ICOEI''. Notably, approximately 13% of the conference papers were published in these top four conferences. The greatest number (approximately 87%) of conference papers were published at individual conferences that are represented as ''Others'' in Figure 6.

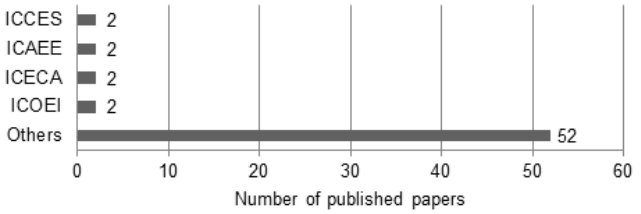

FIGURE 6. Number of published papers vs. conference name.

B. ACTIVE UNIVERSITIES (RQ2)

Many universities are interested and involved in the research topic of this study. However, the most active universities are those who have published at least two research papers on this topic. The details of these universities, the references to their published papers, and the total number of their papers are presented in Table 3. The table evidently shows that ''Vellore Institute of Technology (VIT)'' is the top university in researching the topic with approximately 6% (4/63) of the total publications.

TABLE 3. Active universities with their details.

Country	University	Published Papers	Total
India	Vellore Institute of Technology (VIT)	[23], [24], [25], [26]	4
India	Amity University	[27], [28]	2
Indonesia	Institut Teknologi Bandung	[29], [30]	2
Bangladesh	Independent University	[31], [32]	2
Bangladesh	North South University (NSU)	[33], [34]	2
Bangladesh	American International University Bangladesh (AIUB)	[34], [35]	2

C. APPLICATIONS AND SENSORS OF ARDUINO-BASED SAFETY AND SECURITY SYSTEMS IN SMART HOMES (RQ3)

The deep analysis of the selected studies shows that the applications of Arduino based safety and security systems in smart homes can be categorized into three main areas. Table 4 presents this information and refers to the published papers of each application area. It can be noted that ''Intrusion detection'', ''Fire detection'', and ''Gas detection'' have

TABLE 4. Distribution of papers by application area.

Application Areas	Published Papers	Total
Intrusion detection	[2], [36], [1], [37], [29], [38], [4], [39], [40], [30], [41], [42], [43], [44], [45], [27], [46], [47], [48], [49], [50], [32], [51], [52], [53], [54], [26], [33], [55], [56], [57], [58], [59], [60], [28], [61], [62], [34], [63], [64], [65]	41
Fire detection	[23], [66], [43], [49], [32], [67], [68], [69], [70], [71], [34], [72], [3], [29], [39], [42], [45], [73], [24], [55], [59], [74], [63], [65], [31]	25
Gas detection	[36], [39], [24], [44], [19], [45], [48], [75], [25], [76], [55], [58], [35], [71], [77], [78], [59], [79], [74], [80], [73], [64], [65]	23

41, 25, and 23 relevant published papers, respectively. Additionally, it is observable that some papers implemented more than one application area.

1) INTRUSION DETECTION

Intrusion detection systems are intelligent systems installed in homes to warn owners and prevent unwanted situations such as house break-ins and violent crimes. The analysis of the considered papers in this study reveals that intrusion can be detected via three detection methods, namely, motion-based detection, vibration-based detection, and image-based detection. Table 5 presents this information and refers to the papers of each intrusion detection method. From the identified intrusion detection methods, it can be noted that ''motion-based detection'' is the top and most commonly used intrusion detection method, with 38 published papers. It is worth mentioning that some papers employed more than one type of intrusion detection method.

TABLE 5. Distribution of papers by intrusion detection method.

Detection Method	Published Papers	Total
Motion-based detection	[2], [36], [1], [37], [29], [38], [4], [40], [30], [41], [42], [43], [44], [45], [27], [46], [47], [48], [49], [50], [32], [51], [52], [53], [54], [26], [33], [56], [57], [58], [59], [60], [28], [61], [62], [34], [63] , [64]	38
Vibration-based detection	[48], [58], [59], [62], [65]	5
Contact-based detection	[39], [48], [55], [58], [59]	5

- **Motion-based detection:** Here, motion sensors are used to detect intrusion. When there is a movement in any area inside a home, the used motion sensor will detect that movement. To detect intrusion via motion, different types of sensors can be used. Examining the considered papers in this study reveals that the ''PIR'', ''ultrasonic'', ''camera'', ''InfraRed (IR)'', and ''microwave'' motion detection sensors are the focus of researchers in the literature. Figure 7 shows this information. The figure also shows that approximately 84% (32/38), 5% (2/38), 5% (2/38), 5% (2/38), and 3% (1/38) of the total published papers considered ''PIR'', ''ultrasonic'', ''camera'', ''IR'', and ''microwave'' sensors, respectively. It is worth mentioning that some papers employed more than one type of motion sensor.

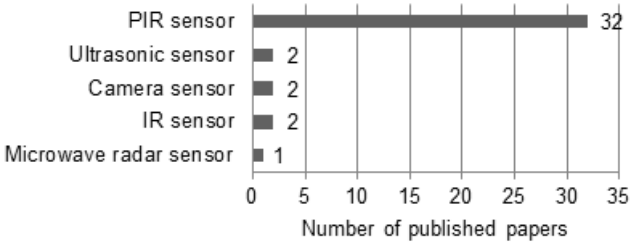

FIGURE 7. Number of published papers vs. motion sensor type.

Table 6 briefly presents the main differences between ''PIR'', ''ultrasonic'', ''IR'', and ''microwave'' motion detection sensors. The ''camera'' sensor can be used for both motion and fire detection, as explained in the image-based detection of Section IV-C2 (Fire Detection).

TABLE 6. Comparison of motion sensors.

Sensor Name	Sensitivity Range	Trigger Condition	Operating Voltage	Measurement Angle	Sensing Type	Ambient Temperature
PIR	7m	Temperature Change	3–5V	100°	Projection area	Dependent
Ultrasonic	2-4m	Movement	5V	15°	Line direction	Independent
IR	2-30cm	Movement	3–5V	35°	Line direction	Dependent
Microwave	5-9m	Movement	4-28V	360°	Projection area	Independent

- **Vibration-based detection:** In this type of detection, vibration sensors are used to detect vibrations in the surroundings. These sensors can be installed on windows and doors to detect vibrations caused by glass/door tampering or breakage. Analyzing the papers considered in this study reveals that 100% (5/5) of the total published papers considered the ''SW-420'' vibration sensor in developing their systems, as shown in Figure 8.

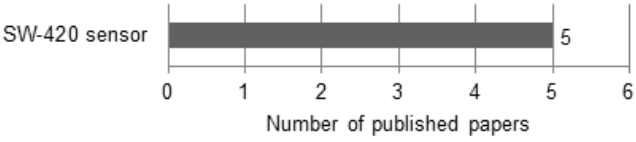

FIGURE 8. Number of published papers vs. vibration sensor type.

- **Contact-based detection:** In this type of detection, magnetic contact switch sensors are installed on windows and doors to detect if they are opened due to an intrusion activity. Each sensor is designed with two parts: one part is set on a window or door frame, and the other part is set on the window or door itself. Thus, when

the two parts are separated from each other, the contact is broken, which triggers an alarm. Analyzing the papers considered in this study reveals that 100% (5/5) of the total published papers considered the "MC-38" magnetic contact switch sensor in developing their systems as shown in Figure 9.

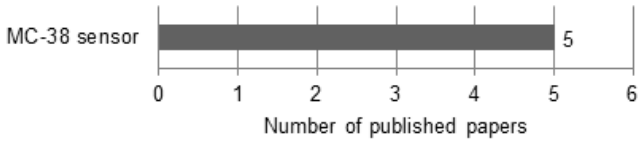

FIGURE 9. Number of published papers vs. magnetic contact switch sensor type.

2) FIRE DETECTION

Fire detection systems are commonly employed in smart homes to ensure homeowner safety and to avoid or reduce property loss. In the case of fire threat, these systems automatically notify homeowners about this emergency situation and may perform some proper actions to reduce the impact. Common causes of fire could be gas leakage, cooking outbreaks, and electrical fire including electrical contactless, faulty outlets, and faulty appliances [26]. The analysis of the considered papers in this study reveals that fire can be detected via four detection methods, namely, smoke-based detection, temperature-based detection, flame-based detection, and image-based detection. Table 7 presents this information and refers to the papers of each fire detection method. From the identified fire detection methods, it can be noted that "smoke-based detection" is the top and most commonly used fire detection method with 12 published papers. It is worth mentioning that some papers employed more than one type of fire detection method.

TABLE 7. Distribution of papers by fire detection method.

Detection Method	Published Papers	Total
Smoke-based detection	[23], [66], [43], [49], [32], [67], [68], [69], [70], [71], [34], [72]	12
Temperature-based detection	[3], [29], [39], [23], [42], [45], [68], [70], [71], [73]	10
Flame-based detection	[24], [68], [55], [59], [74], [73], [63], [65]	8
Image-based detection	[31]	1

- **Smoke-based detection:** In this type of detection, smoke sensors are used to detect the presence of smoke (which is a main indicator of fire occurrence) in the monitoring area. These sensors work on the basis of the relationship between voltage and the measured smoke concentration in the atmosphere. In other words, the higher the smoke concentration is, the higher the output voltage will be. The lower the smoke concentration is, the lower the output voltage will be. Analyzing the papers considered in this study reveals that 100% (12/12) of the total published papers considered the "MQ2" sensor in developing their systems, as shown in Figure 10.

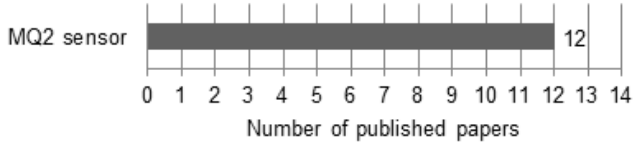

FIGURE 10. Number of published papers vs. smoke sensor type.

- **Temperature-based detection:** Here, temperature sensors are used to detect fire. When fire starts in any area inside a home, the temperature of the surrounding air increases exponentially until reaching a maximum level, while humidity decreases until reaching a minimum level or even zero [28]. To detect fire via temperature, different types of sensors can be used. Examining the considered papers in this study reveals that the "DHT11", "DHT22", "LM35", and "DS18B20" temperature measurement sensors are the focus of researchers in the literature with approximately 40% (4/10), 20% (2/10), 20% (2/10), and 20% (2/10) of the total published papers, respectively. Figure 11 shows this information. The figure also shows that the "DHT11" sensor is the top and most commonly used temperature measurement sensor.

FIGURE 11. Number of published papers vs. temperature sensor type.

It is worth mentioning that each sensor has its own set of technical specifications, and it is difficult for developers to choose the most suitable sensor for building their temperature-based fire detection systems. To help in this respect, Table 8 briefly presents the main differences between these four temperature sensors.

- **Flame-based detection:** Flame sensors can also be used to detect fire and they are available in two main types, namely, ultraviolet (UV)-based flame sensors and IR-based flame sensors. As most types of fire produce certain levels of UV radiation in the atmosphere, UV sensors can be used to detect these levels of radiation. The main drawback of these sensors is that they can produce false alarms as a result of detecting other UV sources, such as electrical sparks and lighting. Additionally, their detection could be inhibited by thick smoke, vapor, and dust. On the other hand, IR sensors

TABLE 8. Comparison of temperature sensors.

Sensor Name	Measurement	Output Signal	Operating Voltage	Temperature Range	Accuracy	Library Required
DHT11	Temperature Humidity	Digital	3-5.5V	0-50ºC	+/-2ºC (at 0-50ºC)	Yes
DHT22	Temperature Humidity	Digital	3-6V	-40-80ºC	+/-0.5ºC (at -40-80ºC)	Yes
LM35	Temperature	Analog	4-30V	-55-150ºC	+/-0.5ºC (at 25ºC)	No
DS18B20	Temperature	Digital	3-5.5V	-55-125ºC	+/-0.5ºC (at -10-85ºC)	Yes

can detect fires that emit light in the infrared spectrum. The main drawback of these sensors is that they can produce false alarms because they have poor detection performance for stable flames. Analyzing the papers considered in this study reveals that 100% (8/8) of the total published papers considered the "YG1006" IR sensor in developing their systems, as shown in Figure 12. There are many valid reasons for preferring IR sensors over UV sensors, including the fact that IR sensors are more insensitive to dust and dirt, are more insensitive to light, and provide good detection within the range of approximately 60 metre from fire sources.

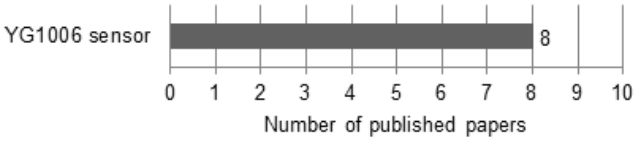

FIGURE 12. Number of published papers vs. flame sensor type.

Table 9 presents the technical specifications of the "YG1006" flame sensor.

TABLE 9. "YG1006" sensor specifications.

Specification	Detail
Operating Voltage	3.3V-5V
On-board Chip	LM393
Detection Angle	60 degrees
Wavelength Detection Range	760nm-1100nm
Distance Detection Range	Up to 60 meters
Dust/Dirt Sensitivity	Very low
Light Sensitivity	Very low

- **Image-based detection:** In this type of detection, images captured by cameras are processed with complex image processing and analysis techniques to detect changes, including fire occurrence [81]. The main advantage of using image-based fire detection systems is the wide range of their detection compared to other methods. Here, the fire detection process is performed via four main steps: (a) Image acquisition: here, images are captured from an installed camera at a regular interval. (b) Image preprocessing: captured images then might be preprocessed via different techniques (e.g., contrast adjustment, intensity adjustment, and color conversion) to enhance their quality or to reduce their computational complexity [82]. (c) Image similarity measurement: here, two captured images are compared to each other to decide how close they are. This can be performed by using different image similarity measurements (e.g., Euclidean distance, Mahalanobis distance, and Chord distance) [83]. The outcome from this step is then used to check whether there is fire in a specific monitoring area or not. (d) Image background subtraction: here, the regions of image intensity changes due to fire can be extracted for further processing. Often, the absolute image subtraction method represented by |image1-image2| is used for this purpose. Thus, the output pixels will mostly be zero values in the regions where no intensity changes are found. Otherwise, the pixels in regions where intensity changes are found will exhibit significant absolute differences between the two compared images (image before fire and image after fire). In most cases, the output from this step is not very meaningful. Thus, the representation of the output image is converted into another new image that is more meaningful and easy to analyze. To do so, the thresholding method is employed to convert the output image into a binary image that shows the impact and size of fire in a more understandable way [84].

3) GAS DETECTION

LPG is a colorless odorless liquid that readily evaporates into a gas. Normally, it is provided in cylinders, with odorants added to help detect leaks. LPG is an essential need of every household, as it is used for cooking and heating. However, its leakage could lead to disasters. When the gas meets a source of ignition, it can burn or explode. Inhaling LPG vapor at high concentrations even for a short time can cause fainting, asphyxiation, and/or death. Here, different gas sensors can be used to detect the presence of gas in the atmosphere. Analyzing the papers considered in this study reveals that the "MQ2", "MQ5", "MQ6", and "MQ9" gas sensors are the focus of researchers in the literature. Figure 13 shows this information. The figure also shows that approximately 70% (16/23), 22% (5/23), 4% (1/23), and 4% (1/23) of the total published papers considered "MQ2", "MQ5", "MQ6", and "MQ9", respectively.

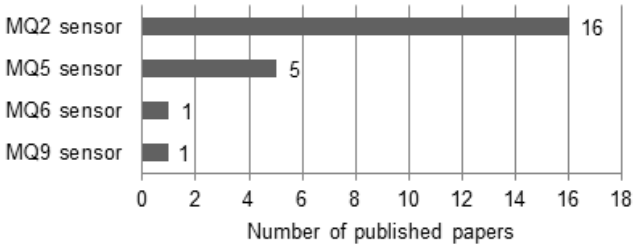

FIGURE 13. Number of published papers vs. gas sensor type.

TABLE 10. MQ sensors target gas.

Sensor Model	Target Gas	Detect Concentration
MQ2	LPG, Methane, Butane, Smoke	300-10000ppm
MQ5	LPG, Natural Gas	300-10000ppm
MQ6	LPG, Butane	200-10000ppm
MQ9	LPG, Carbon Monoxide, Coal Gas, Liquefied Gas	100-10000ppm

Table 10 presents the target gas and concentration range of these four MQ series gas sensors [85].

D. MOST USED ARDUINO BOARDS (RQ4)

The smart home safety and security systems in the considered papers of this study are based on Arduino boards. These boards are open-source microcontroller-based boards developed by "Arduino.cc" [86]. Each board has a number of digital input/output pins, a number of analog input/output pins, can be powered by a USB cable or by an external power supply, and is programmable with the Arduino programming language. Arduino pins can be interfaced with various sensors, actuators, modules, and shields to further expand each board's capabilities and thus provide more functionality to users [87]. Figure 14 shows the most commonly used Arduino boards in the selected studies. It is worth mentioning that some studies used two boards in a single system. However, it can be noted that "Arduino Uno" and "Arduino Mega" are the most used boards, with percentages of approximately 65% (41/63) and 30% (19/63) of the total publications, respectively. Table 11 presents a brief comparison of the used Arduino boards.

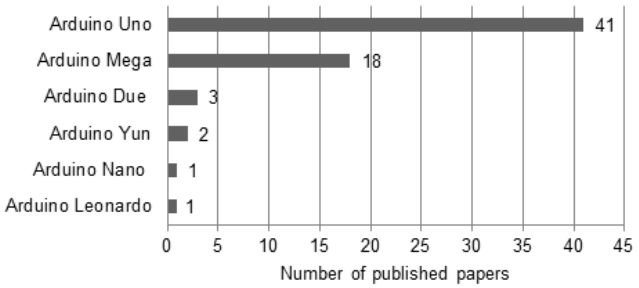

FIGURE 14. Number of published papers vs. Arduino board.

E. ALERT NOTIFICATIONS AND RESPONSE ACTIONS (RQ5)

When any unwanted situation (e.g., gas leak, fire, and intrusion) occurs while homeowners are far away, it is crucial for the installed safety and security systems to activate alert notifications to notify owners or even perform some proper actions (e.g., to stop or reduce the impact of dangerous situations) in response to these undesired situations. Analyzing the selected papers reveals that "playing sound" and "sending SMS" with approximately 60% (38/63) and 46% (29/63) of the total published papers, respectively, are the two most commonly used notification mechanisms. Figure 15 shows this information. It is worth mentioning that many studies employed more than one notification mechanism in their systems. Sound is played using buzzers/speakers. The sound of an alarm scares off intruders/infiltrators and catches the attention of nearby people towards event taking place. Sending SMS messages to designated phone numbers (e.g., to homeowners, police stations, or fire stations to enable them to take proper actions) is performed using GSM communication.

TABLE 11. Comparison of the used Arduino boards.

Board Name	Operating Voltage	Processor Type	Clock Speed	Digital I/O	Analog Inputs	PWM	Flash Memory	SRAM
Uno	5V	ATmega328P	16 MHz	14	6	6	32 KB	2 KB
Mega	5V	ATmega2560	16 MHz	54	16	15	256 KB	8 KB
Due	3.3V	ATSAM3X8E	84 MHz	54	12	12	512 KB	96 KB
Yun	5V	ATmega32U4 AR9331 Linux	16 MHz 400 MHz	20	12	7	32 KB 64 MB	2.5 KB 16 MB
Nano	5V	ATmega168 ATmega328P	16 MHz	14	8	6	16 KB 32 KB	1 KB 2 KB
Leonardo	5V	ATmega32U4	16 MHz	20	12	7	32 KB	2.5 KB

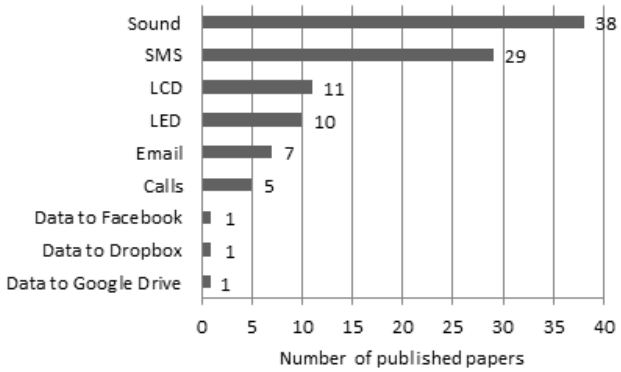

FIGURE 15. Number of published papers vs. alert/notification type.

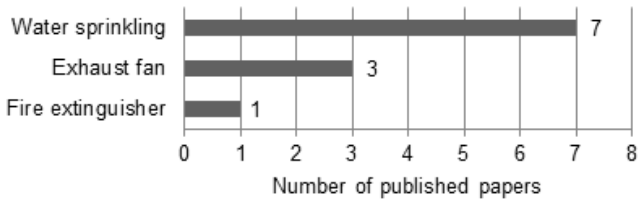

FIGURE 16. Number of published papers vs. action type.

Regarding the proper actions considered against unwanted situations, Figure 16 shows that "water sprinkling", "exhaust fan", and "fire extinguisher" with approximately 11% (7/63), 5% (3/63), and 2% (1/63) of the total published papers, respectively, are the only three proper actions used. Water sprinkling is performed via a solenoid valve, which is a valve switch controlled by an electromagnet. The used valve is a normally closed (NC) valve, which means that

if pressurized water is supplied to an NC solenoid valve, water will not flow through the valve. If a suitable power is supplied to the valve, the valve will open, and the water will flow. An exhaust fan is a device used to pull out (by moving the air from inside to outside) the air in a room/house via fans or blowers. Using exhaust fans helps to clear smoke or leaked gas. A fire extinguisher is a fire protection device used for extinguishing or preventing fires. In smart homes, the extinguisher is controlled and turned on by a servo motor.

F. SMART HOME ARCHITECTURES (RQ6)

According to the papers analyzed in this study, it has been found that a number of different architectures were employed in the design and implementation of smart home safety and security systems using Arduino. Figure 17 shows this information. It can be noted that the top three used system architectures are "Architecture 15" with approximately 37% (23/63), "Architecture 14" with approximately 14% (9/63), and "Architecture 5" with approximately 8% (5/63) of the total publications.

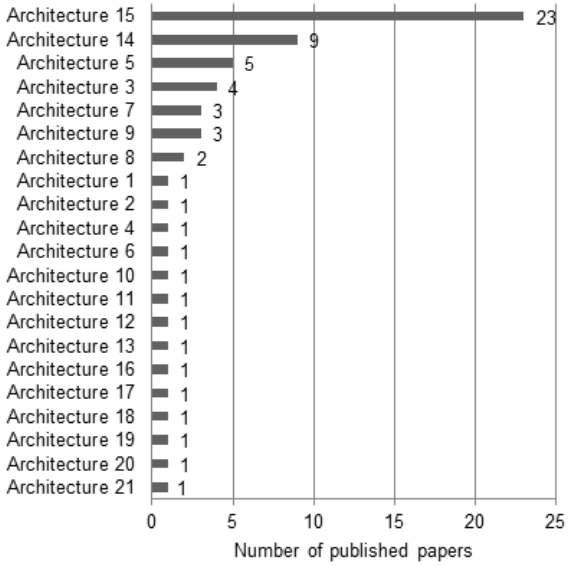

FIGURE 17. Number of published papers vs. architecture used.

- **Architecture 1:** The smart home system architecture consists of sensors connected to the transmitter XBee board using wires. The transmitter XBee board is connected to the receiver XBee board using a wireless communication medium (ZigBee). The receiver XBee board is then connected to the Arduino board. The Arduino board is connected to the Internet using the Arduino Ethernet shield. This connection provides the opportunity to use an embedded web server that can be accessed remotely from everywhere. The Arduino board continuously uploads the readings from the sensors to the embedded web server. Thus, the user can use his/her mobile phone for example to wirelessly access and display the readings stored in the web server. Figure 18 shows this architecture type.

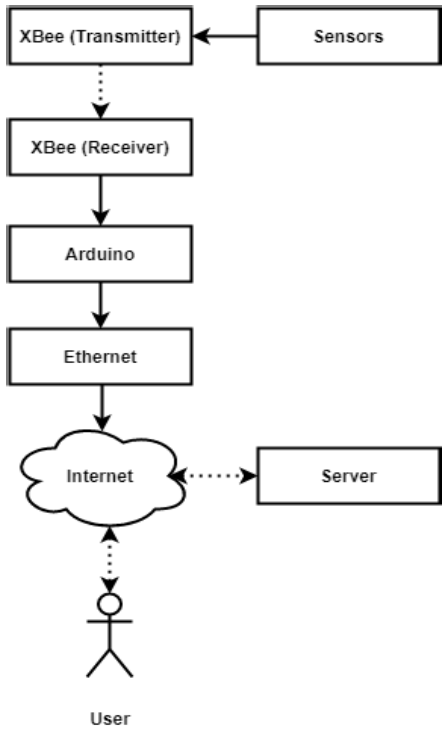

FIGURE 18. Smart home architecture 1.

- **Architecture 2:** This smart home system architecture consists of sensors connected to the transmitter Arduino board using wires. The transmitter Arduino board is connected to the receiver Arduino board using a wireless communication medium. The receiver Arduino board is connected to the Internet using the Arduino Ethernet shield. In case of an emergency, the receiver Arduino board will activate alarms via the actuators. Then, it will upload the status of sensors to the embedded web server. Thus, the user can use his/her mobile phone, for example, to wirelessly access (via the Internet) the readings stored in the web server. Alternatively, he/she can use another wireless communication medium, Bluetooth, to interact with the system directly when there is no Internet connectivity. In addition, the user here is able to deactivate the alarms when needed. Figure 19 shows this architecture type.
- **Architecture 3:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. The Arduino board is connected to the Internet using the Arduino Ethernet shield. In case of an emergency, the Arduino board will activate alarms via the actuators. Then, it will upload the status of sensors to the embedded web server. Thus, the user can use his/her mobile phone for example to wirelessly access (via the Internet) the sensor

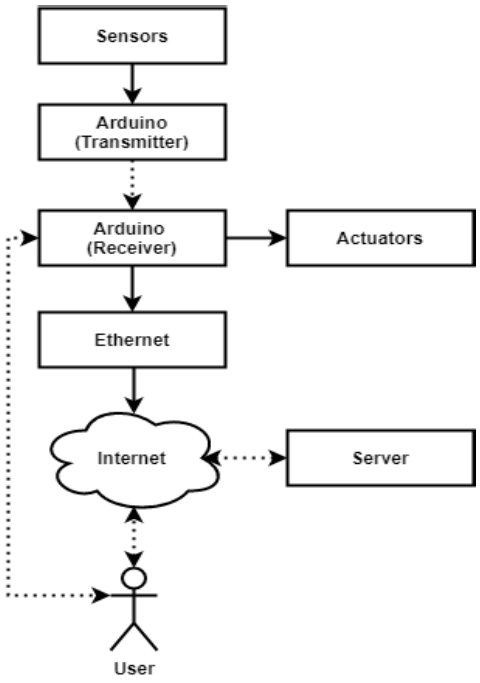

FIGURE 19. Smart home architecture 2.

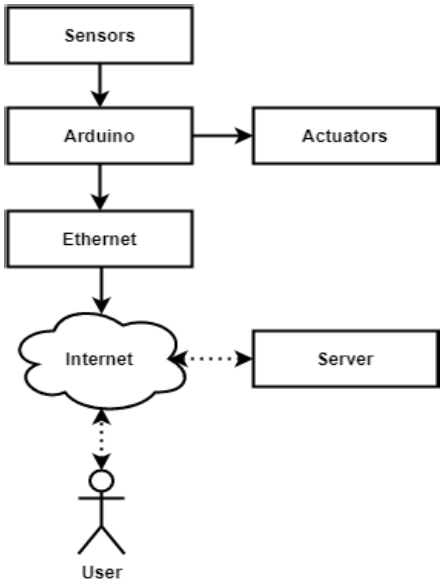

FIGURE 20. Smart home architecture 3.

readings stored in the web server. Figure 20 shows this architecture type.

- **Architecture 4:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. The Arduino board is connected to the transmitter XBee board using wires. The transmitter XBee board is connected to the receiver XBee board wirelessly using ZigBee technology. The receiver XBee board is then connected to a computer using a USB cable. In the event of an emergency, the Arduino board will activate alarms via the actuators and will send the sensors readings to a personal computer wirelessly. Thus, the user can use a desktop application (e.g., Arduino IDE or a dedicated application) installed on his/her personal computer to read the sensors data. Figure 21 shows this architecture type.

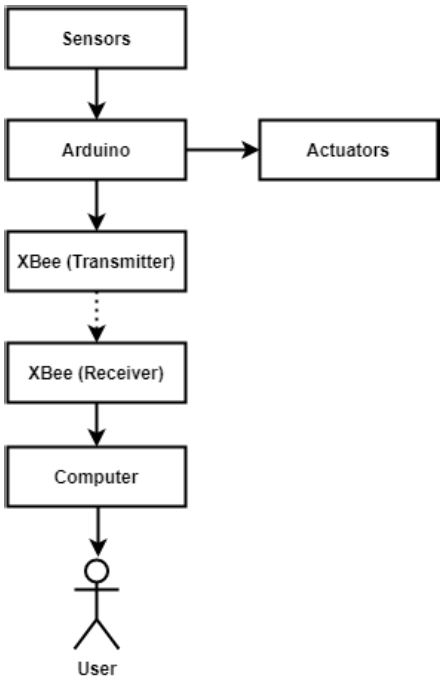

FIGURE 21. Smart home architecture 4.

- **Architecture 5:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. The Arduino board is connected to the Internet using WiFi. In response to an emergency situation, the Arduino board will activate alarms via the actuators. Then, it will upload the status of the sensors to a web server. Thus, the user can use his/her mobile phone, for example, to wirelessly access (via the Internet) the sensors readings stored in the web server. Figure 22 shows this architecture type.
- **Architecture 6:** This smart home system architecture consists of sensors connected to the Arduino board using wires. The Arduino board is connected to the transmitter XBee board using wires. The transmitter XBee board is connected to the receiver XBee board wirelessly using ZigBee technology. The receiver XBee board is then connected to a computer using a USB cable. The computer is interfaced with a GSM device. In case of an emergency, the computer will send an alarm notification wirelessly to the user. Figure 23 shows this architecture type.
- **Architecture 7:** This smart home system architecture consists of sensors connected to the Arduino board using wires. The Arduino board is connected to a computer using a USB cable. The computer uploads the status of

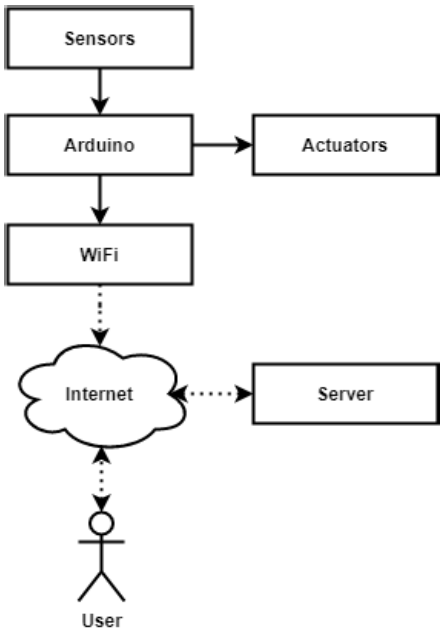

FIGURE 22. Smart home architecture 5.

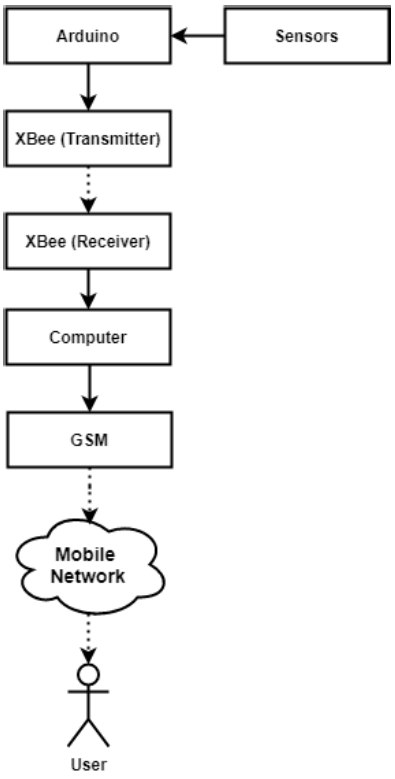

FIGURE 23. Smart home architecture 6.

sensors to a web server. Thus, the user can use his/her mobile phone, for example, to wirelessly access (via the Internet) the sensors readings stored in the web server. Figure 24 shows this architecture type.

- **Architecture 8:** This smart home system architecture consists of sensors connected to the Arduino board using wires. The Arduino board is connected to the Internet using an Ethernet connection. The Arduino board continuously uploads the readings from the sensors to the embedded web server. Thus, the user can use his/her mobile phone, for example, to wirelessly access and display the readings stored in the web server. Figure 25 shows this architecture type.

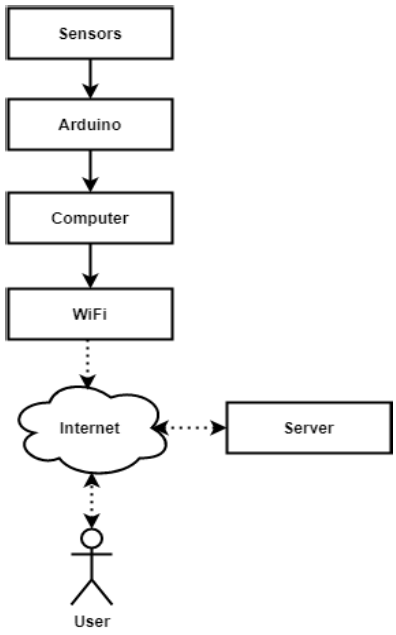

FIGURE 24. Smart home architecture 7.

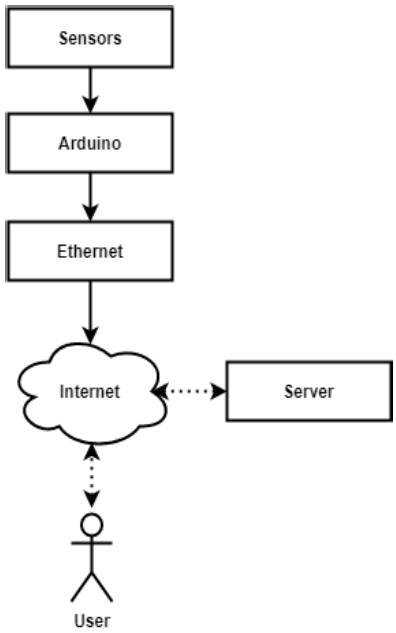

FIGURE 25. Smart home architecture 8.

- **Architecture 9:** This smart home system architecture consists of sensors connected to the Arduino board using

wires. The Arduino board is connected to the Internet using WiFi. In case of an emergency, the Arduino will upload the status of sensors to a web server. Then, the server will send an alarm notification wirelessly to the user. Figure 26 shows this architecture type.

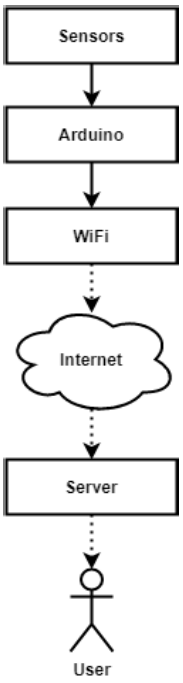

FIGURE 26. Smart home architecture 9.

- **Architecture 10:** This smart home system architecture consists of sensors (camera) connected to a computer using wires. The Arduino board is connected to the computer using a USB cable. In the event of an emergency, the Arduino board will activate alarms via the actuators and then will send an alarm notification wirelessly using GSM to the user. Figure 27 shows this architecture type.
- **Architecture 11:** This smart home system architecture consists of sensors (camera) connected to a computer using wires. The Arduino board is connected to the computer using a USB cable. In response to an emergency situation, the Arduino board will activate alarms via the actuators. Then, the computer will send sensor data wirelessly to Dropbox so that the user can access the stored data. Figure 28 shows this architecture type.
- **Architecture 12:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. In case of an emergency, the Arduino board will activate alarms via the actuators. Additionally, the user has the ability to wirelessly access the sensor readings via Bluetooth by using a mobile application installed on his/her mobile phone. Figure 29 shows this architecture type.

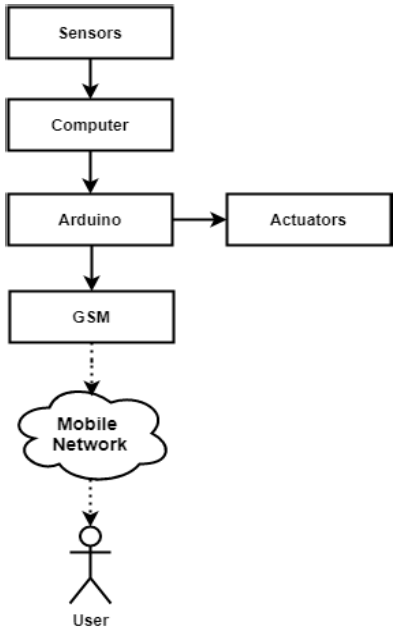

FIGURE 27. Smart home architecture 10.

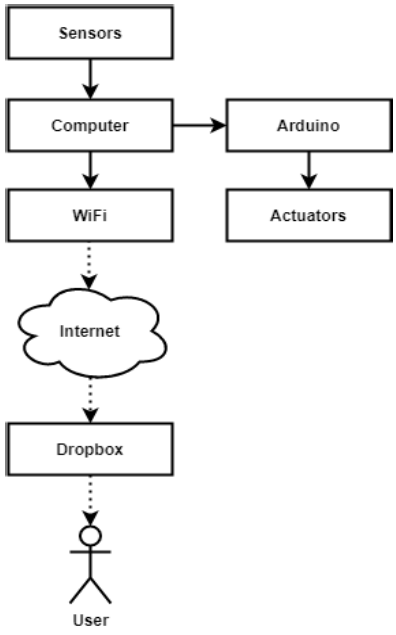

FIGURE 28. Smart home architecture 11.

- **Architecture 13:** This smart home system architecture consists of sensors connected to the transmitter Arduino board using wires. The transmitter Arduino board is connected to the receiver Arduino board using a wireless communication medium. The receiver Arduino board is connected to the Internet using WiFi. The receiver Arduino board uploads the status of sensors to a web server. Thus, the user can use his/her mobile phone, for example, to wirelessly access (via the Internet) the sensors readings stored in the web server. Figure 30 shows this architecture type.

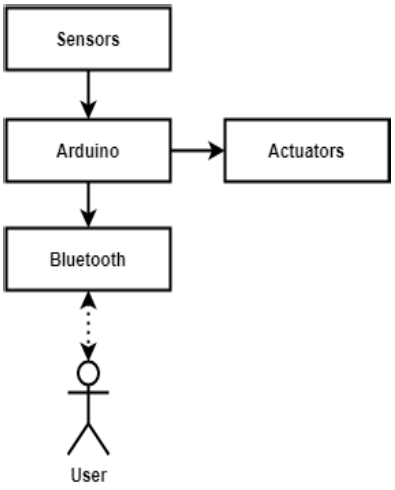

FIGURE 29. Smart home architecture 12.

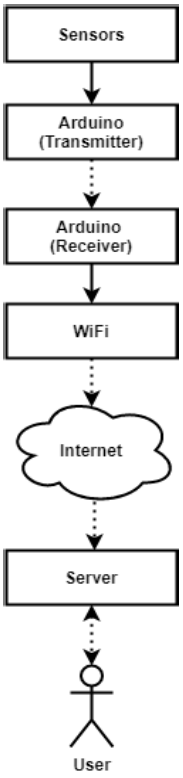

FIGURE 30. Smart home architecture 13.

- **Architecture 14:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. In case of an emergency, the Arduino board will activate alarms via the actuators. Thus, the user will notice the sensor readings and alarms. Figure 31 shows this architecture type.
- **Architecture 15:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. The Arduino board is connected to the mobile network using GSM. In case of an emergency, the Arduino board will activate alarms via the actuators and then will send an alarm notification wirelessly to the user. Figure 32 shows this architecture type.

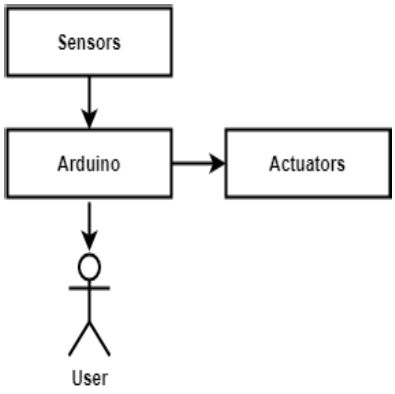

FIGURE 31. Smart home architecture 14.

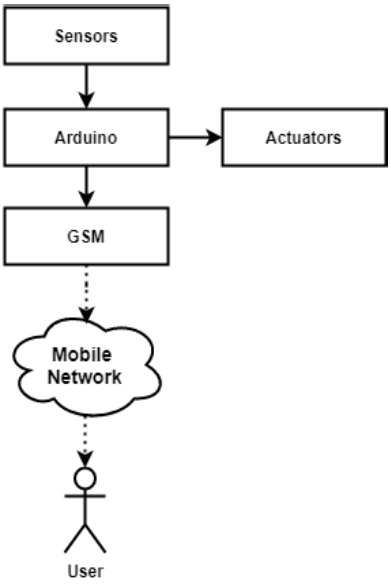

FIGURE 32. Smart home architecture 15.

- **Architecture 16:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. The Arduino board is connected to a computer using wires. A camera is connected to the computer using wires. The computer is connected to the Internet using WiFi. In the event of an emergency, the Arduino board will activate alarms via the actuators and then will send a notification to the computer to capture pictures. Then, the computer will upload the pictures to the server. The user can use his/her mobile phone for example to wirelessly access (via the Internet) the pictures stored in the server. Figure 33 shows this architecture type.
- **Architecture 17:** This smart home system architecture consists of sensors connected to the transmitter Arduino

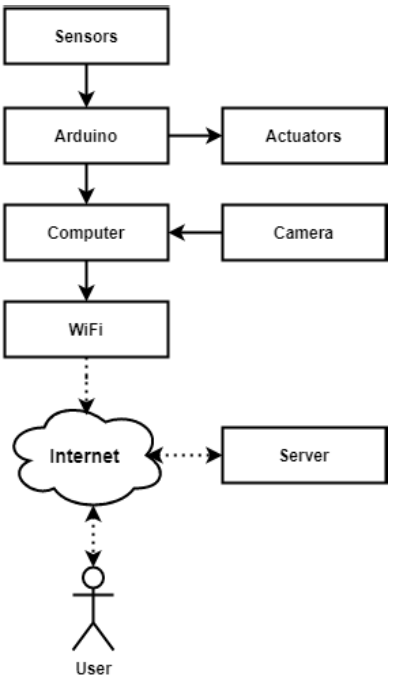

FIGURE 33. Smart home architecture 16.

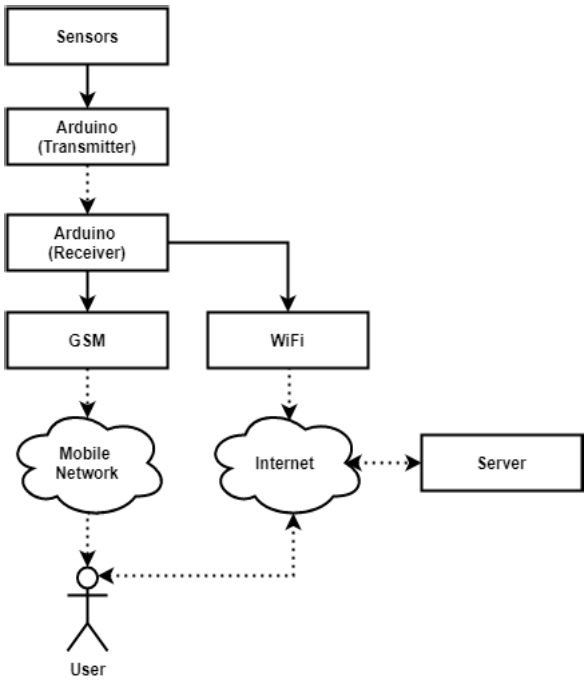

FIGURE 34. Smart home architecture 17.

board using wires. The transmitter Arduino board is connected to the receiver Arduino board using a wireless communication medium. The receiver Arduino board is connected to the mobile network and to the Internet using GSM and WiFi, respectively. In the event of an emergency, the receiver Arduino board will send an alarm notification wirelessly to the user via the mobile network then it will upload the status of sensors to the server. Thus, the user can use his/her mobile phone, for example, to wirelessly access (via the Internet) the sensors readings stored in the server. Figure 34 shows this architecture type.

- **Architecture 18:** This smart home system architecture consists of sensors connected to the Arduino board using wires. The Arduino board is connected to the mobile network using GSM. In an emergency situation, the Arduino board will send an alarm notification wirelessly to the user. Here, the user also has the ability to send back a deactivation notification to the Arduino board to stop the operation of the system. Figure 35 shows this architecture type.
- **Architecture 19:** This smart home system architecture consists of sensors connected to the Arduino board using wires. The Arduino board is connected to the mobile network using GSM and to the Internet using an Ethernet connection. In the case of an emergency, the Arduino board will send an alarm notification wirelessly to the user via the mobile network and then uploads the status of sensors to the server. Thus, the user can use his/her mobile phone, for example, to wirelessly access

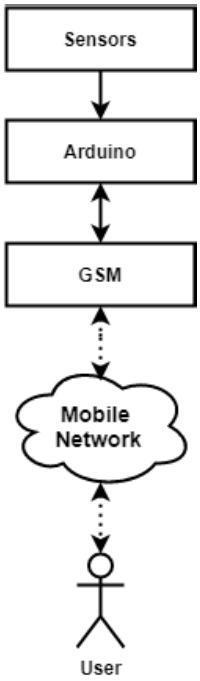

FIGURE 35. Smart home architecture 18.

(via the Internet) the sensors readings stored in the server. Figure 36 shows this architecture type.

- **Architecture 20:** This smart home system architecture consists of sensors connected to the transmitter Arduino board using wires. The transmitter Arduino board is connected to the receiver Arduino board using a wireless communication medium. The receiver Arduino board

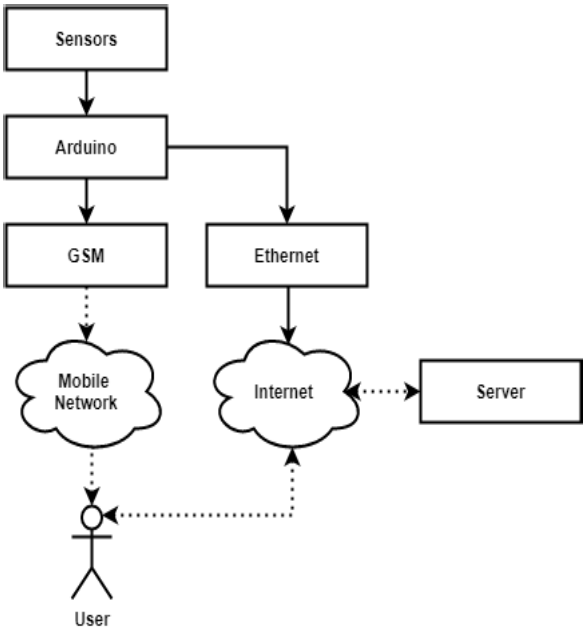

FIGURE 36. Smart home architecture 19.

is connected to a computer using a USB cable. The computer is connected to the Internet via WiFi. In an emergency situation, the receiver Arduino board will activate alarms via the actuators connected to it and then will send sensor readings to the computer to be uploaded to the server. Thus, the user can use his/her mobile phone, for example, to wirelessly access (via the Internet) the sensors readings stored in the server. Figure 37 shows this architecture type.

- **Architecture 21:** This smart home system architecture consists of sensors and actuators connected to the Arduino board using wires. The Arduino board is connected to the mobile network using GSM. In an emergency situation, the Arduino board will activate alarms via the actuators and then will send an alarm notification wirelessly to the user. Here, the user also has the ability to send back a deactivation notification to the Arduino board to stop the operation of the actuators. Figure 38 shows this architecture type.

G. DETAILS AND FINDINGS EXTRACTED FROM SYSTEM ARCHITECTURES (RQ7)

Analyzing the selected papers of this study based on the system architectures obtained from them reveals several useful details and interesting findings as follows:

1) COLLECTING SENSORS DATA

It has been found that sensors data can be collected by Arduino boards via two connection mediums, namely, wired and wirelessly. Figure 39 shows the connection types used, i.e., ''wired connection'' and ''wireless connection'', with

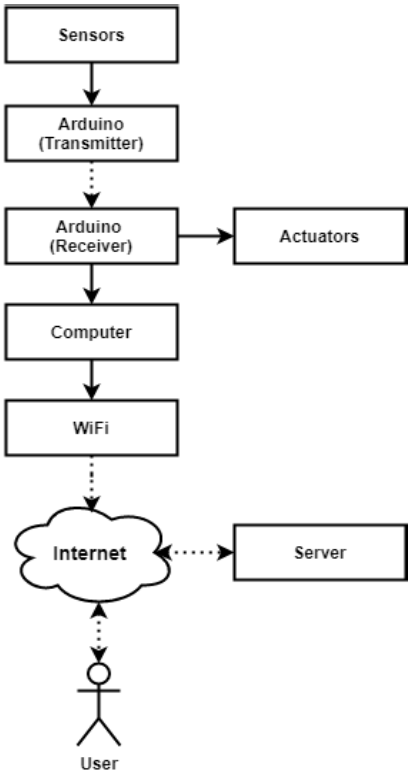

FIGURE 37. Smart home architecture 20.

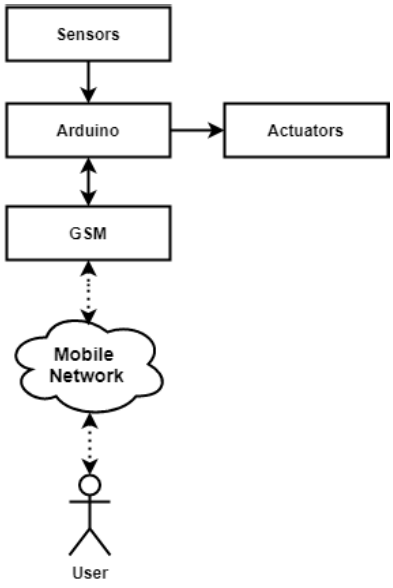

FIGURE 38. Smart home architecture 21.

percentages of approximately 89% (56/63) and 11% (7/63) of the total publications, respectively.

- **Wired connection:** In a wired connection, the sensors are connected directly to the main Arduino boards via wires. Thus, the main boards directly read their readings except in architectures 10 and 11, where the readings of the sensors are collected by a computer that

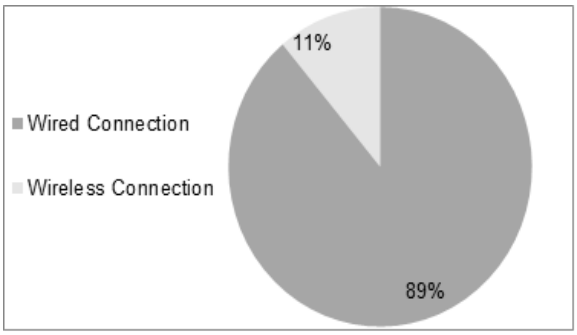

FIGURE 39. Number of published papers vs. sensor connection type.

decides whether there is an emergency situation or not. In an emergency situation, the computer will inform the Arduino board to activate some actuators to generate alarm notifications.

- **Wireless connection:** In a wireless connection as in architectures 1, 2, 4, 6, 13, 17, and 20, transmitter and receiver nodes are employed. Examining the aforementioned seven architectures reveals that the ZigBee module was used in five papers and that the NRF24L01 module was used in two papers. Only these two modules were used as wireless communication mediums between the transmitters and receivers. Table 12 presents a brief comparison of these two wireless communication modules. For more details, please refer to [88].

TABLE 12. Comparison between ZigBee and NRF24L01 wireless communication modules.

Module	Typical Range	Data Rates	Power
ZigBee	10-100m	20-250kbps	Low
NRF24L01	10-150m	250kbps-Mbps	Ultra-Low

2) DATA STORAGE SERVERS

Different types of servers/platforms were used in the considered papers for two purposes: (a) To store sensors readings to be accessed by users. (b) To send alarm notifications. Figure 40 shows the different types of servers used. Clearly, ''Local server'', ''Ethernet server'', ''ThingSpeak server'', and ''Ubidots server'' are the most commonly used servers, with percentages of approximately 13% (8/63), 8% (5/63), 6% (4/63), and 3% (2/63) of the total publications, respectively.

Additionally, it can be noted that many of these servers are cloud based. To help developers select the most suitable server to be used in their systems out of many available options, the following main points can be considered in the selection process [89]:

- **Availability:** The selected server or platform should have high availability (the probability that it will be run with no outage for many years). This can be ensured by asking current and past customers and by investigating

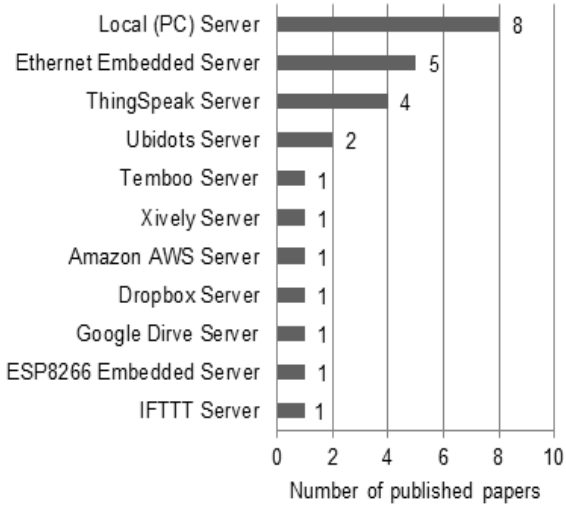

FIGURE 40. Number of published papers vs. server type.

reviews that reflect what each server can offer in this context.

- **Scalability:** Because an installed system may grow over time due to users' needs, the selected server should be able to scale well with that without compromising the integrity and functionality of the installed system. This can be ensured by searching for real-world projects that a specific server has been deployed for and what the results were.
- **Features:** The selected server should meet both user and developer requirements. Additionally, it is crucial to check whether the offered features are free of cost or not. Some advanced features are provided only after paying some amount of money.
- **Support:** The selected server should provide support to its users when they are faced with any technical issues while using it.
- **Documentation:** The selected server should provide users with full documentation of how to use it. The documentation should be written in a simple and informative way and should always be available for download.

3) INTERNET CONNECTIVITY

It has been found that 25 out of the 63 papers employed the Internet in their systems via two connection methods, namely, WiFi and Ethernet connections. Figure 41 shows the connection types used, i.e., ''WiFi connection'' and ''Ethernet connection'', with percentages of approximately 64% (16/25) and 36% (9/25) of the total publications, respectively.

Table 13 briefly presents the main differences between the WiFi and Ethernet connections [90].

Examining the papers that used WiFi to connect to the Internet reveals that ''ESP8266 WiFi'', ''PC Builtin

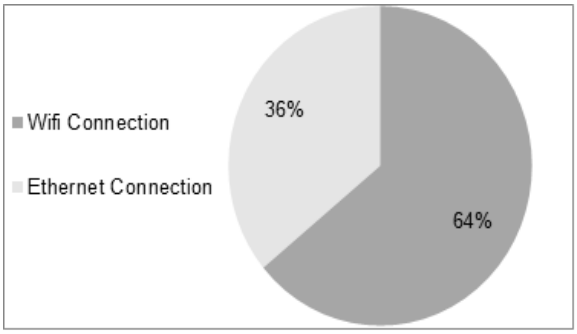

FIGURE 41. Number of published papers vs. connection type.

TABLE 13. Comparison between Wifi and Ethernet connections.

Factors	Wifi	Ethernet
Speed	Slow data transfer speed	Faster data transfer speed
Reliability	Suffers from signal interference to due environmental conditions	Does not suffer from signal interference
Security	Data needs to be encrypted	Data does not require to be encrypted
Latency	Higher	Lower
Cable Installation	Not required	Required
Deployment	Easy to install and deploy	Difficult to install and deploy

WiFi'', and ''Arduino Yun Builtin WiFi'' have percentages of approximately 44% (7/16), 44% (7/16), and 12% (2/16) of the total publications, respectively. Figure 42 shows this result.

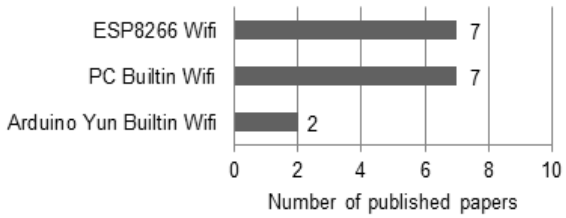

FIGURE 42. Number of published papers vs. sensor connection type.

H. CHALLENGES AND ISSUES (RQ8)

A variety of challenges and issues are posed by implementing and using smart home safety and security systems using Arduino and their enabling technologies. The following points summarize those challenges and issues.

- **Physical attacks:** The distributed and unattended nature of sensors and actuators installed in smart homes makes them susceptible to different types of physical attacks [91]. They may physically be destroyed (e.g., via physical force, heat, or counterfeiting of their associated circuitry), disabled, or even stolen. Therefore, it is essential to install and deploy these devices in secure locations to protect them against physical attacks [12].
- **Device failure:** Because there are a number of sensors, actuators, and microcontrollers that communicate with each other, failure in one of these devices may lead to failure of the entire system. It is recommended that when the installed system starts working, it should display the status of all connected devices to the user. Thus, the user from the beginning will notice if any device is not working properly. Otherwise, the developed system should be adaptable and continue working in case of simple failures or immediately warn users about the occurrence of any failure.
- **Power outage:** A power outage due to damaged electrical transmission lines, short circuits, etc., prevents the deployed system from delivering its services to the user. One valid solution to this issue is to use power backups such as solar panels with rechargeable batteries to power the system [59]. There are many benefits of using solar energy, including the fact that it does not harm the environment/atmosphere and can be collected every day, even on cloudy days [65].
- **Internet outage:** Many of the proposed systems depend on the Internet to send alarm notifications or to upload readings obtained from different sensors to the cloud to be accessed by users. Without Internet connectivity, users will not be notified of any unwanted situations. To overcome this issue, the installed system should periodically check the Internet connectivity. In the case of Internet outages, the system should be able to send its notifications and upload its readings once the Internet is available again. Another valid solution is to employ GSM technology in addition to using the Internet [47], [55]. When there is no Internet, GSM communication can be used.
- **Software compatibility:** In the papers considered in this study, all the proposed systems that enable homeowners to use mobile applications to access the readings of sensors or interact with the system have associated Android native mobile applications that were created for this purpose. The rationale for developing mobile applications for only Android-based devices is the fact that Android has become the most popular operating system for mobile phones and tablets [57]. Considering that all homeowners have Android-based devices is not viable. To overcome this issue, web applications or hybrid mobile applications that are developed using web technologies (e.g., HTML, CSS, and JavaScript) can be used instead of native mobile applications. Doing so will enable users to utilize the proposed systems using smart phones with any operating system installed or by using computers. Web applications provide full interoperability or cross-platform compatibility features. Therefore, they can be accessed and used by any software platform. On the other hand, developing native mobile applications limits their use [92]. In addition, any large change occurring in that platform means that the whole application will need to

TABLE 14. List of all papers included in this study.

No.	Ref.	Paper Title	Year
1	[2]	A tablet-controlled, mesh-network security system: an architecture for a secure, mesh network of security and automation systems using Arduino and Zigbee controllers and an Android tablet application	2014
2	[36]	Android based smart home system with control via Bluetooth and internet connectivity	2014
3	[1]	Design of Small Smart Home System Based on Arduino	2014
4	[3]	HOME FADS: A Dedicated Fire Alert Detection System Using ZigBee Wireless Network	2014
5	[37]	A comparative study and implementation of real time home automation system	2015
6	[29]	Intelligent home management system prototype design and development	2015
7	[38]	Prototype utilization of PIR motion sensor for real time surveillance system and web-enabled lamp automation	2015
8	[4]	Smart home automation system for intrusion detection	2015
9	[39]	Smart home for elderly care, based on Wireless Sensor Network	2015
10	[23]	Xively based sensing and monitoring system for IoT	2015
11	[24]	A 24 hour IoT framework for monitoring and managing home automation	2016
12	[40]	ADDSMART: Address Digitization and Smart Mailbox with RFID Technology	2016
13	[31]	An automatic fire detection and warning system under home video surveillance	2016
14	[30]	Design and implementation of Smart Home Surveillance system	2016
15	[41]	Design and implementation prototype of a smart house system at low cost and multi-functional	2016
16	[42]	Home Monitoring and Security system	2016
17	[66]	Smoke Detection Alert System via Mobile Application	2016
18	[43]	Wireless Home monitoring using Social Internet of Things (SIoT)	2016
19	[44]	Customary homes to smart homes using Internet of Things (IoT) and mobile application	2017
20	[19]	Design and implementation of a low-cost Arduino-based smart home system	2017
21	[45]	Design and implementation of security system for smart home	2017
22	[27]	Economical Home Monitoring System Using IOT	2017
23	[46]	Home automation system using wireless network	2017
24	[47]	IoT based intrusion detection system using PIR sensor	2017
25	[48]	IoT: Secured and automated house	2017
26	[49]	Low-cost home automation using Arduino and Modbus protocol	2017
27	[50]	RFID Device Based Home Security System to Detect Intruder Trespassing	2017
28	[32]	Smart home solutions with sun tracking solar panel	2017
29	[67]	A Home Environment Monitoring Design on Arduino	2018
30	[75]	A User-Friendly Low-Cost Mobile App Based Home Appliance Control And Circuit Breaker	2018
31	[51]	Arduino-based Wireless Motion Detecting System	2018
32	[52]	Design and Implementation of IoT-Based Automation System for Smart Home	2018
33	[25]	Design of Weather Monitoring System and Smart Home Automation	2018
34	[53]	Development of Voice Control and Home Security for Smart Home Automation	2018
35	[76]	Effective Environmental Monitoring and Domestic Home Conditions by Implementation of IoT	2018
36	[54]	ElectriCare – Care, Protection and Automation	2018
37	[68]	Fire Safety and Alert System Using Arduino Sensors with IoT Integration	2018
38	[69]	GSM based Home Environment Monitoring System	2018
39	[26]	Home Security System Using GSM	2018
40	[33]	Microcontroller Based Smart Home System with Enhanced Appliance Switching Capacity	2018
41	[70]	Prototype of Fire Symptom Detection System	2018
42	[55]	Prototype Residence Monitoring and Automation System Using Microcontroller Arduino	2018
43	[56]	Smart Home System - Remote Monitoring and Control Using Mobile Phone	2018
44	[57]	Design and Validation of a Multifunctional Android-Based Smart Home Control and Monitoring System	2019
45	[58]	Developing System from Low-Cost Devices to Build a Security and Fire System as a Part of IoT	2019
46	[35]	Domicile - An IoT Based Smart Home Automation System	2019
47	[71]	Early Detection System for Gas Leakage and Fire in Smart Home Using Machine Learning	2019
48	[77]	Gas Leakage Detection Based on IOT	2019
49	[78]	GSM Based Low-cost Gas Leakage, Explosion and Fire Alert System with Advanced Security	2019
50	[59]	Internet of Things (IoT) enabled Sustainable Home Automation along with Security using Solar Energy	2019
51	[79]	IoT based LPG cylinder monitoring system	2019
52	[74]	IoT based smart gas management system	2019
53	[60]	IoT based Smart Security System using PIR and Microwave Sensors	2019
54	[28]	Iot Based Smart Wireless Home Security Systems	2019
55	[61]	IOT Controlled Home Automation Technologies	2019
56	[62]	Neural controller for smart house security subsystem	2019
57	[80]	Ogrodut: GSM based Gas Leakage Detection and Ventilation System using Arduino and Servo Motor	2019
58	[73]	Quick Fire Sensing Model and Extinguishing by Using an Arduino Based Fire Protection Device	2019
59	[34]	Service Development of Smart Home Automation System	2019
60	[72]	Smart Fire-Alarm System for Home	2019
61	[63]	Smart Home Automation System Using Internet of Things	2019
62	[64]	Smart home monitoring and automation energy efficient system using IoT devices	2019
63	[65]	Smart Old Age Home Using Zigbee	2019

be changed accordingly, which is not feasible and time consuming.

- **Arduino clones:** Most of the proposed systems in the literature used Arduino clones, not original devices, in their systems. This may lead to problems in the long run for many reasons owing to the following: (a) They are not made from the best hardware components (e.g., integrated circuits (ICs), I/O pins, communication ports, and soldering materials). (b) They have the issue of drivers not working on some operating systems. (c) They are not fully tested for better quality before being shipped.
- **Security:** Many of the proposed systems utilize the IoT to deliver services to homeowners. However, the IoT core physical components, such as wireless sensor networks (WSNs) and wireless communication

TABLE 15. List of active journals with abbreviations.

Acronym	Journal Full Name
Procedia Comput. Sci.	Procedia Computer Science
IEEE Access	IEEE Access

devices, are vulnerable to various security threats [93]. This is because these components suffer from resource limitations, computing constraints, small storage spaces, and limited wireless channel bandwidth. Any security threat in this respect may lead to the entire system being compromised. To overcome this security issue, software and hardware enhancements may be useful in some cases. To address the issue properly and comprehensively, sophisticated countermeasures must be applied, such as malicious node detection techniques, lightweight encryption algorithms, secure key management mechanisms, and secure routing protocols [94].

I. FUTURE DIRECTIONS OF RESEARCH (RQ9)

Several possible directions for future research were identified based on the analysis of the papers included in this study. These future directions are summarized and categorized under the following points:

- **Extendability**: The installed Arduino-based smart home safety and security systems should allow homeowners to add new types of sensors and actuators when needed without making large changes to the software and hardware design. This can be achieved by allowing owners to add new devices and then register (e.g., by providing the type of device, type of device output, and device pin) them using a new software feature called ''add new sensor/actuators'' that should be provided by the software application developed for this purpose. Here, one issue that developers may face could be understanding how the software functionality for a specific added device will be added or generated. In addition, what will the impact, cost, or effort be in achieving this? An intensive investigation in this regard can therefore be considered a successful step forward.
- **Satisfaction**: The goal of using smart home safety and security systems is to help notify homeowners in the event of an unwanted situation while they are far from home. However, are homeowners truly satisfied with using the developed systems? In the considered papers, there is no research addressing this important concern. Thus, it is crucial to measure user satisfaction and even involve it in some parts of the development process.
- **Performance**: Arduino devices suffer from resource limitations and computing capabilities (e.g., limited code storage space, limited data memory size, and limited processing power). Therefore, it is crucial to efficiently program these devices, especially when the aim is to develop time-sensitive applications where each second matters. To increase the performance of Arduino programs in terms of execution time, flash memory usage, and SRAM usage, different coding strategies (optimization) can be employed. However, analyzing the considered papers reveals that no study analyzed and measured the impact of writing efficient code for programming Arduino-based safety and security systems. Additionally, to use sensors such as DHT11 and DHT22 for measuring humidity and temperature, an external software library must be included in the code. For example, the libraries: [95], [96], and [97] can all be used to program the DHT11 sensor, but one of them provides better performance and outperforms the others in terms of runtime, flash memory usage, and SRAM space. There is no study in the literature addressing this important issue. Therefore, it will be interesting to examine the capabilities and performance of each available library to help developers select the most suitable one.
- **Visualization**: Using a large number of different sensors in homes can create a large amount of data related to what is happening in one's home. However, if these data are not reduced and visualized in a meaningful and understandable way, they will overwhelm the homeowner. One solution to this issue is to apply filters to separate the sensors readings into different abstraction levels. Thus, the homeowner can look for the data within a specific level only instead of going through all the displayed data. In this way, the user can better understand the displayed data. Additionally, it has been found that most developed systems display raw sensors data to users who are mostly nontechnical and thus cannot understand the data without it being processed and displayed in an informative format.
- **Testing**: Smart home safety and security system testing requires a variety of connected sensors, actuators, and devices to be deployed and then actually tested. In practice, certain situations such as considering fire in all the rooms of a house are difficult and not safe to be provided. Therefore, developers should be equipped with various types of simulation software to resolve this deployment issue. These tools should allow various critical scenarios to be simulated and should also allow testing systems under these scenarios before they are used in reality.

V. THREATS TO VALIDITY

Different threats may affect the validity of literature survey studies. For this paper, the following actions were taken into consideration to avoid threats to validity.

- **Finding related papers:** It cannot be ensured whether all the related studies can be found. Thus, several literature databases were used and a search string with several term synonyms was applied to obtain the relevant studies. However, there may still remain

TABLE 16. List of active conferences with abbreviations.

Acronym	Conference Full Name
ICCES	International Conference on Communication and Electronics Systems (ICCES)
ICAEE	International Conference on Advances in Electrical Engineering (ICAEE)
ICECA	International conference on Electronics, Communication and Aerospace Technology (ICECA)
ICOEI	International Conference on Trends in Electronics and Informatics (ICOEI)

some undiscovered papers. To address this threat, there was intensive application of the snowballing search technique to reduce the probability of missing important relevant papers.

- **Accuracy of data extraction:** Many mistakes may occur when extracting data from the selected papers. To tackle this threat, the data extraction process was performed manually. Automatic mining and filtering provided by Microsoft Excel were also used in the spreadsheet. The results from both methods were then compared to determine the differences and reach a final dataset.
- **Study reproducibility:** Another threat is whether other researchers could obtain similar results if they perform/duplicate this study. To address this threat, all the steps of the research methodology followed and performed in this study were described in detail (see Section III).

VI. CONCLUSIONS

This survey systematically reports the state-of-the-art contributions in smart home safety and security systems using Arduino. Thus, to classify, compare, and discuss the applications, the enabling sensors, the Arduino boards, the alert notifications, and the architectures that have been employed and used in these systems were identified. In this study, 63 relevant research papers from five well-known literature databases published over the past six years from 2014-2019 were selected. The published papers were a mixture of contributions from conferences, journals, and workshops, with the majority of papers being published in conferences. The considered papers were extensively reviewed and analyzed from different perspectives and were based on a set of RQs. The obtained results yielded many categories. For example, statistics regarding the selected papers, publication venues, and active universities were given. Then, the applications of these systems were classified. All the sensors, actuators, notifications, and architectures that enabled the operation of these systems were also discussed. The findings presented in this survey could be of great value to other researchers interested in the topic. Therefore, we hope this systematic survey will be considered a primary reference that can facilitate the process of finding the most relevant information.

REFERENCES

[1] A. Adriansyah and A. W. Dani, "Design of small smart home system based on arduino," in *Proc. Electr. Power, Electron., Commun., Control Informat. Seminar (EECCIS)*, Aug. 2014, pp. 121–125.

[2] J. W. Lartigue, C. McKinney, R. Phelps, R. Rhodes, A. D. Rice, and A. Ryder, "A tablet-controlled, mesh-network security system: An architecture for a secure, mesh network of security and automation systems using Arduino and Zigbee controllers and an Android tablet application," in *Proc. ACM Southeast Regional Conf.*, 2014, pp. 33:1–33:4.

[3] M. F. M. Fuzi, A. F. Ibrahim, M. H. Ismail, and N. S. A. Halim, "HOME FADS: A dedicated fire alert detection system using ZigBee wireless network," in *Proc. IEEE 5th Control Syst. Graduate Res. Colloq. (ICSGRC)*, Aug. 2014, pp. 53–58.

[4] D. Chowdhry, R. Paranjape, and P. Laforge, "Smart home automation system for intrusion detection," in *Proc. Can. Workshop Inf. Theory (CWIT)*, Jul. 2015, pp. 75–78.

[5] W. Anani, A. Ouda, and A. Hamou, "A survey of wireless communications for IoT echo-systems," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–6.

[6] M. B. Yassein, I. Hmeidi, F. Shatnawi, W. Mardini, and Y. Khamayseh, "Smart home is not smart enough to protect You–protocols, challenges and open issues," *Procedia Comput. Sci.*, vol. 160, pp. 134–141, 2019.

[7] A. Daissaoui, A. Boulmakoul, L. Karim, and A. Lbath, "IoT and big data analytics for smart buildings: A survey," *Procedia Comput. Sci.*, vol. 170, pp. 161–168, Jan. 2020.

[8] V. Williams, S. Terence J., and J. Immaculate, "Survey on Internet of Things based smart home," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Feb. 2019, pp. 460–464.

[9] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *J. Netw. Comput. Appl.*, vol. 97, pp. 48–65, Nov. 2017.

[10] M. Asadullah and A. Raza, "An overview of home automation systems," in *Proc. 2nd Int. Conf. Robot. Artif. Intell. (ICRAI)*, Nov. 2016, pp. 27–31.

[11] M. Hasan, P. Biswas, M. T. I. Bilash, and M. A. Z. Dipto, "Smart home systems: Overview and comparative analysis," in *Proc. 4th Int. Conf. Res. Comput. Intell. Commun. Netw. (ICRCICN)*, Nov. 2018, pp. 264–268.

[12] K. Karimi and S. Krit, "Smart home-smartphone systems: Threats, security requirements and open research challenges," in *Proc. Int. Conf. Comput. Sci. Renew. Energies (ICCSRE)*, Jul. 2019, pp. 1–5.

[13] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[14] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 67–72.

[15] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technol. Forecasting Social Change*, vol. 138, pp. 139–154, Jan. 2019.

[16] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[17] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Dept. Comput. Sci., School Comput. Sci. Math., EBSE Softw. Eng. Group, Keele Univ., U.K., Univ. Durham, version 2.3., Tech. Rep. EBSE-2007-01, 2007.

[18] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.

[19] S. Gunputh, A. P. Murdan, and V. Oree, "Design and implementation of a low-cost Arduino-based smart home system," in *Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2017, pp. 1491–1495.

[20] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng. (EASE)*, 2014, pp. 1–10.

[21] O. Pedreira, F. García, N. Brisaboa, and M. Piattini, "Gamification in software engineering—A systematic mapping," *Inf. Softw. Technol.*, vol. 57, pp. 157–168, Jan. 2015.

[22] R. E. Lopez-Herrejon, L. Linsbauer, and A. Egyed, "A systematic mapping study of search-based software engineering for software product lines," *Inf. Softw. Technol.*, vol. 61, pp. 33–51, May 2015.
[23] N. Sinha, K. E. Pujitha, and J. S. R. Alex, "Xively based sensing and monitoring system for IoT," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jun. 2015, pp. 1–6.
[24] G. Kesavan, P. Sanjeevi, and P. Viswanathan, "A 24 hour IoT framework for monitoring and managing home automation," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Aug. 2016, pp. 1–5.
[25] I. Majumdar, B. Banerjee, M. T. Preeth, and M. K. Hota, "Design of weather monitoring system and smart home automation," in *Proc. IEEE Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN)*, Jul. 2018, pp. 1–5.
[26] P. Mahalakshmi, R. Singhania, D. Shil, and A. Sharmila, "Home security system using GSM," in *Proc. Int. Conf. Emerg. Res. Comput., Inf., Commun. Appl.*, 2018, pp. 627–634.
[27] K. S. Obheroi, A. Chaurasia, T. Choudhury, and P. Kumar, "Economical home monitoring system using IOT," in *Proc. 2nd Int. Conf. Comput. Intell. Inform.*, in Adv. Intell. Syst. Comput., Singapore: Springer, 2017, pp. 627–637.
[28] K. Sehgal and R. Singh, "Iot based smart wireless home security systems," in *Proc. 3rd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Jun. 2019, pp. 323–326.
[29] A. I. Nurrahman and K. Mutijarsa, "Intelligent home management system prototype design and development," in *Proc. Int. Conf. Inf. Technol. Syst. Innov. (ICITSI)*, Nov. 2015, pp. 1–6.
[30] T. Juhana and V. G. Anggraini, "Design and implementation of smart home surveillance system," in *Proc. 10th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2016, pp. 1–5.
[31] M. M. Hasan and M. A. Razzak, "An automatic fire detection and warning system under home video surveillance," in *Proc. IEEE 12th Int. Colloq. Signal Process. Appl. (CSPA)*, Mar. 2016, pp. 258–262.
[32] F. B. Shahin, P. Tawheed, M. F. Haque, M. R. Hasan, and M. N. R. Khan, "Smart home solutions with sun tracking solar panel," in *Proc. 4th Int. Conf. Adv. Electr. Eng. (ICAEE)*, Sep. 2017, pp. 766–769.
[33] M. Hasan, M. H. Anik, and S. Islam, "Microcontroller based smart home system with enhanced appliance switching capacity," in *Proc. 5th HCT Inf. Technol. Trends (ITT)*, Nov. 2018, pp. 364–367.
[34] J. Miah and R. H. Khan, "Service development of smart home automation system," in *Proc. 2nd Int. Conf. Comput. Intell. Intell. Syst.*, New York, NY, USA, Nov. 2019, pp. 161–167.
[35] M. S. Mahamud, M. S. R. Zishan, S. I. Ahmad, A. R. Rahman, M. Hasan, and M. L. Rahman, "Domicile—An IoT based smart home automation system," in *Proc. Int. Conf. Robot., Elect. Signal Process. Techn. (ICREST)*, Jan. 2019, pp. 493–497.
[36] S. Kumar and S. R. Lee, "Android based smart home system with control via Bluetooth and Internet connectivity," in *Proc. IEEE Int. Symp. Consum. Electron. (ISCE)*, Jun. 2014, pp. 1–2.
[37] A. R. Behera, J. Devi, and D. S. Mishra, "A comparative study and implementation of real time home automation system," in *Proc. Int. Conf. Energy Syst. Appl.*, Oct. 2015, pp. 28–33.
[38] H. T. Sukmana, M. G. Farisi, and D. Khairani, "Prototype utilization of PIR motion sensor for real time surveillance system and Web-enabled lamp automation," in *Proc. IEEE Asia–Pacific Conf. Wireless Mobile (APWiMob)*, Aug. 2015, pp. 183–187.
[39] R. S. Ransing and M. Rajput, "Smart home for elderly care, based on wireless sensor network," in *Proc. Int. Conf. Nascent Technol. Eng. Field (ICNTE)*, Jan. 2015, pp. 1–5.
[40] J. R. Tew and L. Ray, "ADDSMART: Address digitization and smart mailbox with RFID technology," in *Proc. IEEE 7th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2016, pp. 1–6.
[41] A. Howedi and A. Jwaid, "Design and implementation prototype of a smart house system at low cost and multi-functional," in *Proc. Future Technol. Conf. (FTC)*, Dec. 2016, pp. 876–884.
[42] S. Suresh, J. Bhavya, S. Sakshi, K. Varun, and G. Debarshi, "Home monitoring and security system," in *Proc. Int. Conf. ICT Bus. Ind. Government (ICTBIG)*, 2016, pp. 1–5.
[43] B. Jadhav and S. C. Patil, "Wireless home monitoring using social Internet of Things (SIoT)," in *Proc. Int. Conf. Autom. Control Dyn. Optim. Techn. (ICACDOT)*, Sep. 2016, pp. 925–929.
[44] V. Govindraj, M. Sathiyanarayanan, and B. Abubakar, "Customary homes to smart homes using Internet of Things (IoT) and mobile application," in *Proc. Int. Conf. Smart Technol. Smart Nation (SmartTechCon)*, Aug. 2017, pp. 1059–1063.
[45] M. A. Raja, G. R. Reddy, and Ajitha, "Design and implementation of security system for smart home," in *Proc. Int. Conf. Algorithms, Methodol., Models Appl. Emerg. Technol. (ICAMMAET)*, Feb. 2017, pp. 1–4. [Online]. Available: https://ieeexplore.ieee.org/document/8186705
[46] S. A. Joshi, S. Poojari, T. Chougale, S. Shetty, and M. K. Sandeep, "Home automation system using wireless network," in *Proc. 2nd Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2017, pp. 803–807.
[47] K. C. Sahoo and U. C. Pati, "IoT based intrusion detection system using PIR sensor," in *Proc. 2nd IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2017, pp. 1641–1645.
[48] H. M. Saber and N. K. Al-Salihi, "IoT: Secured and automated house," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2017, pp. 1–6.
[49] V. Hassanpour, S. Rajabi, Z. Shayan, Z. Hafezi, and M. M. Arefi, "Low-cost home automation using arduino and modbus protocol," in *Proc. 5th Int. Conf. Control, Instrum., Autom. (ICCIA)*, Nov. 2017, pp. 284–289.
[50] S. Minocha and A. Dumka, "RFID device based home security system to detect intruder trespassing," in *Proc. Int. Conf. Intell. Commun., Control Devices*, 2017, pp. 1445–1454.
[51] S. S. S. M. Soleh, M. M. Som, M. H. A. Wahab, A. Mustapha, N. A. Othman, and M. Z. Saringat, "Arduino-based wireless motion detecting system," in *Proc. IEEE Conf. Open Syst. (ICOS)*, Nov. 2018, pp. 71–75.
[52] W. A. Jabbar, M. H. Alsibai, N. S. S. Amran, and S. K. Mahayadin, "Design and implementation of IoT-based automation system for smart home," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Jun. 2018, pp. 1–6.
[53] M. E. Abidi, A. L. Asnawi, N. F. Azmin, A. Z. Jusoh, S. N. Ibrahim, H. A. M. Ramli, and N. A. Malek, "Development of voice control and home security for smart home automation," in *Proc. 7th Int. Conf. Comput. Commun. Eng. (ICCCE)*, Sep. 2018, pp. 1–6.
[54] A. Nagaria, H. Ansari, M. Qadeer, and E. M. K. Shaikh, "ElectriCare—Care, protection & automation," in *Proc. 2nd Int. Conf. Smart Sensors Appl. (ICSSA)*, 2018, pp. 88–92.
[55] F. Nurpandi, A. Musrifalr, and I. Rizaldi, "Prototype residence monitoring and automation system using microcontroller arduino," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Oct. 2018, pp. 1–5.
[56] M. Škrgić, U. Drakulić, and E. Mujčić, "Smart home system—Remote monitoring and control using mobile phone," in *Proc. Int. Symp. Innov. Interdiscipl. Appl. Adv. Technol.*, 2018, pp. 409–419.
[57] L. D. Liao, C. C. Chuang, T. R. Ger, Y. Wang, Y. C. Tsao, I. J. Wang, D. F. Jhang, T. S. Chu, C. H. Tsao, C. N. Tsai, and S. F. Chen, "Design and validation of a multifunctional android-based smart home control and monitoring system," *IEEE Access*, vol. 7, no. 1, pp. 1–9, 2019.
[58] V. S. Koprda, Z. Balogh, and M. Magdin, "Developing system from low-cost devices to build a security and fire system as a part of IoT," in *Proc. Int. Conf. Intell. Comput.*, 2019, pp. 142–154.
[59] S. Amit, A. S. Koshy, S. Samprita, S. Joshi, and N. Ranjitha, "Internet of Things (IoT) enabled sustainable home automation along with security using solar energy," in *Proc. Int. Conf. Commun. Electron. Syst. (ICCES)*, Jul. 2019, pp. 1026–1029.
[60] M. Z. Saeed, R. R. Ahmed, O. B. Samin, and N. Ali, "IoT based smart security system using PIR and microwave sensors," in *Proc. 13th Int. Conf. Math., Actuarial Sci., Comput. Sci. Statist. (MACS)*, Dec. 2019, pp. 1–5.
[61] S. Adamu, U. I. Bature, A. Y. Nasir, A. M. Hassan, K. I. Jahun, and U. S. Toro, "IOT controlled home automation technologies," in *Proc. 2nd Int. Conf. IEEE Nigeria Comput. Chapter (NigeriaComputConf)*, Oct. 2019, pp. 1–7.
[62] V. Teslyuk, P. Denysyuk, N. Kryvinska, K. Beregovska, and T. Teslyuk, "Neural controller for smart house security subsystem," *Procedia Comput. Sci.*, vol. 160, pp. 394–401, 2019.
[63] U. Singh and M. A. Ansari, "Smart home automation system using Internet of Things," in *Proc. 2nd Int. Conf. Power Energy, Environ. Intell. Control (PEEIC)*, Oct. 2019, pp. 144–149.
[64] K. Suneetha and M. Sreekanth, "Smart home monitoring and automation energy efficient system using IoT devices," in *Proc. Int. Conf. Comput. Commun. Data Eng.*, 2019, pp. 627–637.
[65] N. Shubha, S. Sahana, K. Pavithra, M. S. Meghana, and K. Panimozhi, "Smart old age home using Zigbee," in *Proc. Int. Conf. Comput. Netw., Big Data IoT (ICCBI)*, 2019, pp. 100–111.
[66] W. H. W. Ismail, H. R. M. Husny, and N. Y. Abdullah, "Smoke detection alert system via mobile application," in *Proc. 10th Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, New York, NY, USA, 2016, pp. 1–6.
[67] H. Zhang, G. Li, and Y. Li, "A home environment monitoring design on Arduino," in *Proc. Int. Conf. Intell. Transp., Big Data Smart City (ICITBS)*, Jan. 2018, pp. 53–56.

[68] F. S. Perilla, G. R. Villanueva, N. M. Cacanindin, and T. D. Palaoag, "Fire safety and alert system using arduino sensors with IoT integration," in *Proc. 7th Int. Conf. Softw. Comput. Appl. (ICSCA)*, New York, NY, USA, 2018, pp. 199–203.
[69] T. M. Jothi, A. Periyanayaki, R. Srimathy, M. Vinotha, and G. Gopika, "GSM based home environment monitoring system," in *Proc. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, May 2018, pp. 1263–1268.
[70] O. Giandi and R. Sarno, "Prototype of fire symptom detection system," in *Proc. Int. Conf. Inf. Commun. Technol. (ICOIACT)*, Mar. 2018, pp. 489–494.
[71] L. Salhi, T. Silverston, T. Yamazaki, and T. Miyoshi, "Early detection system for gas leakage and fire in smart home using machine learning," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–6.
[72] J. Kang, S. Basnet, and S. M. Farhad, "Smart fire-alarm system for home," in *Proc. Conf. Complex, Intell., Softw. Intensive Syst.*, 2019, pp. 474–483.
[73] M. R. Habib, N. Khan, K. Ahmed, M. R. Kiran, A. K. M. Asif, M. I. Bhuiyan, and O. Farrok, "Quick fire sensing model and extinguishing by using an Arduino based fire protection device," in *Proc. 5th Int. Conf. Adv. Electr. Eng. (ICAEE)*, Sep. 2019, pp. 435–439.
[74] S. Shrestha, V. P. K. Anne, and R. Chaitanya, "IoT based smart gas management system," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 550–555.
[75] H. U. Zaman, Rafiunnisa, and A. M. Shams, "A user-friendly low-cost mobile app based home appliance control and circuit breaker," in *Proc. 2nd Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Feb. 2018, pp. 203–208.
[76] A. Chaudhari, B. Mapari, and S. Jog, "Effective environmental monitoring & domestic home conditions by implementation of IoT," in *Proc. 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Aug. 2018, pp. 1–5.
[77] V. Suma, R. R. Shekar, and K. A. Akshay, "Gas leakage detection based on IOT," in *Proc. 3rd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Jun. 2019, pp. 1312–1315.
[78] P. Ghosh and P. K. Dhar, "GSM based low-cost gas leakage, explosion and fire alert system with advanced security," in *Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–5.
[79] A. K. Srivastava, S. Thakur, A. Kumar, and A. Raj, "IoT based LPG cylinder monitoring system," in *Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES)*, Dec. 2019, pp. 268–271.
[80] A. Samiha, F. H. Sarker, R. N. K. Chowdhury, A. K. M. R. R. Habib, and R. Rahman, "Ogrodut: GSM based gas leakage detection and ventilation system using Arduino and servo motor," in *Proc. Int. Energy Sustain. Conf. (IESC)*, Oct. 2019, pp. 1–6.
[81] R. J. Radke, S. Andra, O. Al-Kofahi, and B. Roysam, "Image change detection algorithms: A systematic survey," *IEEE Trans. Image Process.*, vol. 14, no. 3, pp. 294–307, Mar. 2005.
[82] P. Vasuki, J. Kanimozhi, and M. B. Devi, "A survey on image preprocessing techniques for diverse fields of medical imagery," in *Proc. IEEE Int. Conf. Electr., Instrum. Commun. Eng. (ICEICE)*, Apr. 2017, pp. 1–6.
[83] C.-C. Chen and H.-T. Chu, "Similarity measurement between images," in *Proc. 29th Annu. Int. Comput. Softw. Appl. Conf. (COMPSAC)*, 2005, pp. 41–42.
[84] D. C. C. Wang, A. H. Vagnucci, and C. C. Li, "Digital image enhancement: A survey," *Comput. Vis., Graph., Image Process.*, vol. 24, no. 3, pp. 363–381, Dec. 1983.
[85] A. Nayyar, V. Puri, and D.-N. Le, "A comprehensive review of semiconductor-type gas sensors for environmental monitoring," *Rev. Comput. Eng. Res.*, vol. 3, no. 3, pp. 55–64, 2016.
[86] *Arduino Website*. Accessed: Jan. 5, 2020. [Online]. Available: https://www.arduino.cc/
[87] A. Nayyar and V. Puri, "A review of Arduino board's, Lilypad's Arduino shields," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2016, pp. 1485–1492.
[88] H. Saha, S. Mandal, S. Mitra, S. Banerjee, and U. Saha, "Comparative performance analysis between nRF24L01+ and XBEE ZB module based wireless ad-hoc networks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 7, pp. 36–44, Jul. 2017.
[89] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," in *Proc. IEEE Int. Conf. Future IoT Technol. (Future IoT)*, Jan. 2018, pp. 1–8.
[90] A. Jame. *Wi-Fi vs. Ethernet: Which Connection to Use?*. Accessed: Jan. 5, 2020. [Online]. Available: https://ubidots.com/blog/wi-fi-vs-ethernet-which-connection-to-use/
[91] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensor network configuration under physical attacks," in *Proc. Int. Conf. Netw. Mobile Comput. (ICCNMC)*, 2005, pp. 23–32.
[92] N. Fernandes, D. Costa, C. Duarte, and L. Carriço, "Evaluating the accessibility of Web applications," *Procedia Comput. Sci.*, vol. 14, pp. 28–35, Jan. 2012.
[93] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur.*, Dec. 2013, pp. 663–667.
[94] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *Proc. Int. Conf. Syst. Netw. Commun. (ICSNC)*, 2006, p. 40.
[95] *Class for DHTXX Sensors*. Accessed: Jan. 5, 2020. [Online]. Available: https://playground.arduino.cc/Main/DHTLib/
[96] *Efficient DHT Library for Arduino*. Accessed: Jan. 5, 2020. [Online]. Available: https://github.com/markruys/arduino-DHT
[97] *Arduino Library for DHT11, DHT22, Etc Temperature & Humidity Sensors*. Accessed: Jan. 5, 2020. [Online]. Available: https://github.com/adafruit/DHT-sensor-library

QUSAY I. SARHAN received the B.Sc. degree in software engineering from the University of Mosul, Iraq, in 2007, and the M.Tech. degree in software engineering from Jawaharlal Nehru Technological University, India, in 2011. He is currently a Lecturer and the Leader of the Software Engineering and Embedded Systems (SEES) Research Group, University of Duhok, Iraq. He has a couple of national and international publications. His research interests include software engineering, the Internet of Things, and embedded systems.