INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Efficient and robust security implementation in a smart home using the internet of things

Irfan Abbas[1,2]*, Munib Ahmad[2], Hafiz Subhan Sarfraz[2], Muhammad Nadeem[2], Rizwan Subhan[2]

1 Lecturer, Department of Computer Science, University of Central Punjab, Natt Road, 50700, Gujrat, Pakistan. Tel.: +92-306-647-3003
2 Department of Computer Science and IT, Minhaj University Lahore, Hamdard Road, Pakistan

OPEN ACCESS

Received: 27-03-2020

Accepted: 27-04-2020

Published: 04-06-2020

Editor: Dr. Natarajan Gajendran

Citation: Abbas I, Ahmad M, Sarfraz HS, Nadeem M, Subhan R (2020) Efficient and robust security implementation in a smart home using the internet of things. Indian Journal of Science and Technology 13(15): 1563-1569. https://doi.org/10.17485/IJST/v13i15.9

***Corresponding author**.
Irfan Abbas

Lecturer, Department of Computer Science, University of Central Punjab, Natt Road, 50700, Gujrat, Pakistan. Tel.: +92-306-647-3003

Department of Computer Science and IT, Minhaj University Lahore, Hamdard Road, Pakistan
abbasirfan440@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

Abstract

Background/Objectives: Internet of Things (IoT) is considered as a new paradigm in a computing environment. The devices connected to the internet perform different functionalities. The objective of this paper is to present a model that consists of devices having different sensing capabilities. **Methodology:** The system would use ``Wi-Fi scanner'', ``Heat sensor'', "Motion sensor" etc. for sensing the movement of different physical objects to implement security in the smart home. **Findings:** The system based on our presented model has capabilities to replace the faulty devices in order to improve the efficiency and robustness for the implementation of security in smart homes.

Keywords: Internet of Things; Security; Robustness; Efficiency; Smart homes systems

1 Introduction

Internet of Things (IoT)[(1)] is a newly emerging area in the field of computer science. Researchers and practitioners show great interest in IoT as It is being used by different devices. It has makes the world intelligent by creating smart environments. It enables billions of devices to be interconnected with each other anywhere and anytime without any disturbance. It has made a technological revolution by interconnecting devices and objects[(2)]. Multiple technologies of IoT are being used for the deployment of the system related to security[(3)]. It is being used for monitoring and controlling security by using web interfaces. The user interacts with devices by using smartphones to control and automate appliances. Home appliances like TV, refrigerator, Air conditioner, and automatic door opening can be easily controlled through simple web interfaces by using IoT[(4)].

It can be more successful if there will be direct interaction between devices without any interruption. The interaction between devices must be without any kind of user involvement for the purpose of security. The implementation of security at the home must be efficient and vigorous. It predicts a future in which different physical objects and devices can be linked by the use of technologies. There should be direct interaction between devices which is a difficult task because IoT devices are heterogeneous[(5)].

In heterogeneous computing different devices performs different activities by using high speed communication links with different frequencies. Different computational tasks can be performed by different devices in distributed computing[6]. InIoT, there is much significance of distributed computing as devices perform completely different activities. In case of a home security system where different sensors are being used for the implementation of security such as a camera for video recording, door sensor for automatic door opening by perceiving any physical object, a sensor for face recognition to authenticate person identity, etc. So there is less possibility of applying fault-tolerant techniques to IoT systems.

In this study, we present a model that would be competent and hearty for implementing security in the smart home. Different devices will work for completely different scenarios. The model will create an overlap between the capabilities of devices to save energy. Hence our model can easily handle faulty devices and replace them with other devices. As a faulty security camera can be easily replaced with another sensing device like heat or motion sensor. As per our knowledge, there is no previous work like this to present such type of solution.

We will apply our method to check the implementation of security in a smart home. The most important requirement to be live in a home is safety and security. An alarm system can be used as a sensor for security in the smart home. Usage of alarm systems have been already well studied and can be easily added to any system for security implementation[7]. A number of IoT systems can be entertained by this method. The outcomes of our model will preserve energy and will provide a robust IoT system for security in the smart home.

Robustness is a compulsory element for IoT systems and has been already well discussed and implemented in IoT systems with heterogeneous IP packets[8]. Distributed systems are actually decentralized systems and have the mechanism of fault handling. To achieve fault tolerance replicate services have been used by the author to recover the system from failure. Similarly, IoT systems are mostly distributed and decentralized and fault tolerance in devices of IoT has been studied earlier as like[9]. Here author requires that different devices provide identical services. Faults in IoT devices that are not permanent have been discussed in[10] where authors proposed a method that can handle the coherence of IoT systems. Our model deals with permanent failures to recover without any choreography. Newly developed systems require a strong environment to be operated easily without any disturbance. An efficient system with respect to energy is considered important for next-generation IoT systems[11]. To save energy in IoT systems better technologies have been developed by addressing energy efficiency. Efficiency in the form of energy can be achieved through the use of motion harvesting systems[12]. Energy may be associated with moving objects or it can be generated by monitoring human activities as relaxing, walking, etc.[13]. Communication systems such as “RFID” can also be used to achieve energy efficiency and the same systems have been already applied to many smart home projects[14].

An impressive approach to gain energy efficiency in IoT systems is through the use of machine learning, Where learning patterns can be used to reduce the usage of energy[15]. Activity patterns can also be used to gain energy efficiency to make these systems efficient[16]. To maintain power consumption Sleep schedule is an interesting phenomenon, where devices go to sleep mode to save energy[17]. Our model for implementing IoT based security system also uses the sleep scheduling phenomenon. There have been a number of projects related to smart homes have already been addressed but the actual outcome has not achieved[18]. Interesting embedded devices have been used to implement security in smart homes as an android phone for remote controlling of different objects. In[19] Different devices and sensors have been embedded in the system for the feasibility purpose. Some special operating systems such as ”RIOT” OS have already been used for IoT systems[20]. Ontology-based systems can be used to create smart environments[21] and we will organize our sensors in the same way. Another interesting project is ”Home Web” where an IoT based home is developed by the use of web ”APIs” as ”REST”. The authors of this project using “WSDL” to define the capability of each device[22] that is interesting. Another interesting feature of the home security system is the use of an alert engine through the use of mobile phone notification or through camera[23]. As the features like notifications have already been well studied in literature so we leave the integration of alert engine in our system. However, the integration of an alert engine with our system is so simple.

2 Developing of IoT based model

As multiple devices communicate with the internet and with each other to develop an IoT systems. The developed system composed of multiple devices and the interesting thing is that all the devices belong to the same owner. High-level goals can be achieved if the devices communicate with each other in the most effective way. In our proposed model the high-level goals are an effective use of energy and robust IoT system.

Our proposed model can also be applied to other IoT systems to achieve high-level goals. The efficiency of energy will be achieved by our model by powering on only those devices to which we need at most and powering off those devices to which we don’t need at all. Devices with equal capabilities provide robustness to the IoT system even devices show different functions. Devices used with low power mode capabilities as sleep and hibernation are known to us but the same capabilities are not suitable for embedded platforms[24].

There is a need to list down all the devices that will be part of our model to develop an IoT system. The devices will perform completely different functionalities according to the location where they located, and each device has different sensing capabilities as a video camera can be located on the entrance of the home for face recognition. After the identification of all devices that will be the part of system, the capabilities of all devices will be categorized. There can be overlaps between the capabilities of devices as the same type of devices can have different capabilities and different type of devices can have the same capabilities, it depends on the use cases. There can be an ordered relationship between the capabilities of devices. Some devices may be considered as superior due to more capabilities. Consider the following relation $C_X > C_Y$ that shows type x capabilities are superior to capabilities of type y. We can consider that the sensors of device x are more accurate than sensors of device y. As discussed earlier the capabilities and relationships of devices, the system needs to make the decision for selecting the device in order to achieve the efficiency of energy and robustness.

To enable low energy consumptions in our model we define some important rules. There can be an ordered relationship or an overlap between the capabilities of devices. There is a need to power on those devices that have more capabilities. When some device triggers any signal there is a need to power on a device with more capabilities and with low consumption of power. In our case for implementing security in the smart home the sensor which is located at door, power on the camera when the door sensor feels that someone is coming towards the door.

$$D_T P.ON = \{ Dj \mid MIN\ E\ j\hat{}C\ j > CT \} \tag{A}$$

By using the equation (A) multiple devices can be powered on by the request of a trigger generated by device D_T andonly that device will be powered on that have more capabilities and low consumption of energy. During working the devices may be damaged or get faults and it is common in cheap embedded systems. Our model has the capabilities to deal with this type of issues by replacing the faulty devices with other devices.[25].

$$D_{FU}\ Rep = \{ Dj \mid MIN = \sum_{Dj} E\hat{}C_F = U\ \complement\ j\hat{}Is\ Faulty\ (D\ j) = 0 \} \tag{B}$$

Equation (B) shows the available list of all devices that will perform the same capabilities in case of failure of device D_{FU}. Here

1. D_J represents the device exists in the system
2. D_{FU} represents the faulty device,
3. D_T represents the device that triggers an upgrade for selecting the device with more capabilities
4. E_J represents the consumptions of energy for device J
5. C_J represents the capabilities of device J
6. U Represents the Union between different variables

If there is no any fault in the device D_J then it returns 0 as represented in equation (B) and 1 if faults occur in device. Some other rules can also be added to achieve the efficiency of energy and robustness for our system. Timeout phenomenon for devices is also important and brings improvements in system efficiency. Finally, we implement these rules in our system. There will be effective communication between all devices and the system will take decision for powering on devices that will be needed for security purpose.

3 Efficient and robust security implementation

There can be multiple forms of IoT devices, different sensors and actuators can perform different functions. The devices can perform single functions or many functions. The connection between devices may consist of cables or through wireless. Our proposed model consists of one function, one sensor, and a wireless device and this is the simplest form of our model. The interesting thing is that our model can be extended easily to accommodate multiple sensors. For implementing security in a smart home we have used multiple sensors and each sensor will completely perform different functionality. The main thing is the implementation of security, so we will use the following sensors as described below:

For face recognition, security cameras have been used. Security cameras offer video feeds. Here require some advance processing algorithms[26]. This is an effective method but needs vast resources. And the consumption of energy used by security cameras is 0.071 Wh/min. For voice recognition microphone has been used. It is also an important sensor as a camera but it lacks some important information as it only recognizes the voice when someone talks. It cannot recognize the voice of door opening. The consumption of energy used by the microphone is 0.018 Wh/min. For the identification of the homeowner, the information of the MAC address of his smartphone will be used by Wi-Fi scanner. This is a good approach for security implementation in smart homes because the only homeowner can enter the home. The consumption of energy used by Wi-Fi scanner

is 0.003 Wh/min. To distinguish between humans and animals heat sensors have been used. Heat sensor differentiates humans and animals by sensing their body heat. The consumption of energy used by heat sensors is 0.02 Wh/min. Some special sensors such as a respiration sensor have also been used to distinguish between humans and animals remotely by sensing their heartbeats.The consumption of energy used by the respiration sensor is 0.02 Wh/min.

If someone forcefully tries to enter into the home vibration sensor will indicate it by creating vibrations onto the windows or doors. The consumption of energy used by the vibration sensor is 0.04 Wh/min. The hall sensor has been used to know about the door or windows positions whether they are open or closed. The consumption of energy used by hall sensor is 0.02 Wh/min. To monitor the movement in home motion sensor has been used. The consumption of energy used by the motion sensor is 0.03 Wh/min. To provide access to authenticate persons for entering into the home, pin code or bio-metrics sensors has been used. User authentication can be done through the use of thumb impression or scanning the eye retina. The consumption of energy used by bio-metrics sensors is 0.005 Wh/min.

Table 1. Sensors and their capabilities

Sensor	Identity	Is Person	Is Moving	Access Detection
Camera	Yes	Yes	Yes	Yes
Microphone	No	No	Yes	-
Wi-Fi scanner	-	-	-	-
Heat Sensor	-	Yes	Yes	-
Vibration Sensor	-	-	-	Yes
Motion sensor	-	-	Yes	Yes
Biometrics sensor	Yes	-	-	Yes

Table 1 represents the sensors and their capabilities. A camera is used here for face recognition and identity of a person entering into the home. The sensors used to implement security in smart home may be viewed in Figure 1.

Similarly, identification of moving objects and access detection inform us that the door or window is opened. The ordered relationship between the capabilities can be represented as (Table 1):

Identity > is person > is moving> Access detection.

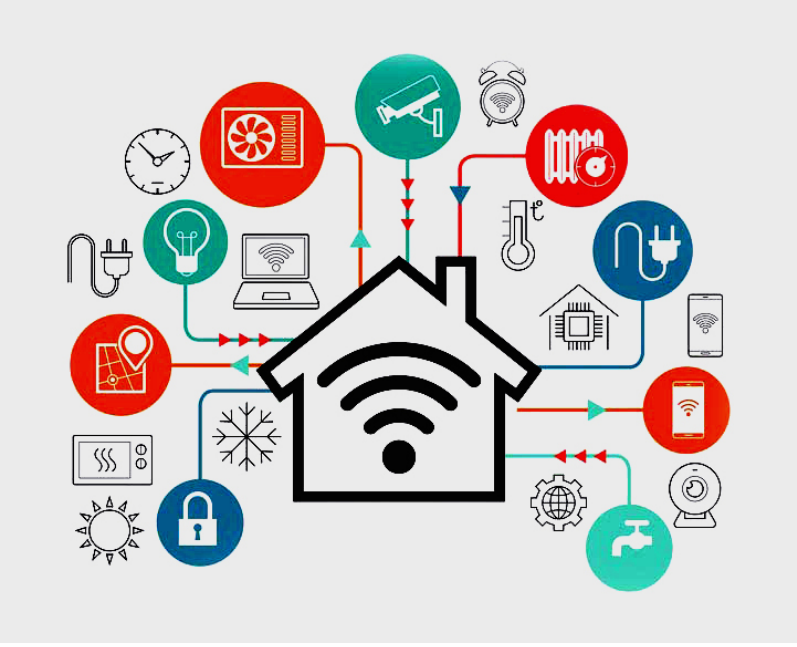

Fig 1. Sensors used in smart home security system

4 Outcomes of the model

In order to show the results of our model, the resulting IoT system provides efficient and robust security implementation in a smart home in terms of energy. To monitor the energy efficiency improvements, we consider a simulation. The simulation will take a 15 min. time and a person (Purab) will trigger some events. Timeout for each sensor will be 5 min. The simulation will start when nobody will be at home. Access sensors will remain powered on from start to the end of the simulation. If we consider the simulation, then at the 3rd minute Purab opens the door. The event will be detected by the hall sensor, and hall sensor will power on the motion and microphone sensor for getting more information. Camera and heat sensor will be get started by motion sensor when Purab will look around the room at the 4th minute. After 4th minute completion, the WiFi scanner will be get activated for the personal identity through a smartphone. After 5th minute Purab sits on the sofa placed in the hall of the house for almost 5 minutes, and at this time all the existing sensors will remain power on. After 10th minute the time, out will occur for microphone and Wi-Fi sensor, and they will stop responding. All the other sensors will detect personal identity. At the 13th minute, Purab will stand up and leave the house. Here the hall sensor will detect the event and will notify the camera and heat sensor to stop responding. In the above simulation, the consumption of energy is 1.49 Wh, and it is 46.3 % less than the consumption of energy when all sensors were in a working state. Our proposed system is robust IoT security system. As we have seen that different sensors have been used here for the implementation of security in a smart home. The purpose of each sensor is the same, the working may be different but the purpose is the implementation of security in the smart home is the same. If one component stops working or fails, the other component can take its place in order to make the system in working condition. In this way, our model gets efficiency and robustness. The given scenario demonstrates the robustness of our presented model.

At the very first minute, our system is in standby mode only the sensors related to the unauthorized access group are in running mode. At the 3rd minute someone walks near the home and opens the door, our system will detect access based on equation (A); the motion sensor will be activated. At the 4th minute, the system will detect someone is moving, and then based on equation (A) the sensor related to the camera will be activated. At the 5th-minute camera-sensor fails to start, the heat sensor will be activated to distinguish between the human and animal. At the 6th minute, the heat sensor of our system will detect the identity as "is a person"; the Wi-Fi scanner will be activated to identify the person by his smartphone MAC address. At the 8th minute the person sits down on sofa and motion sensor will be deactivated. Similarly, at the 11th and 12th minute, the Wi-Fi and heat sensor will be deactivated to save the energy.

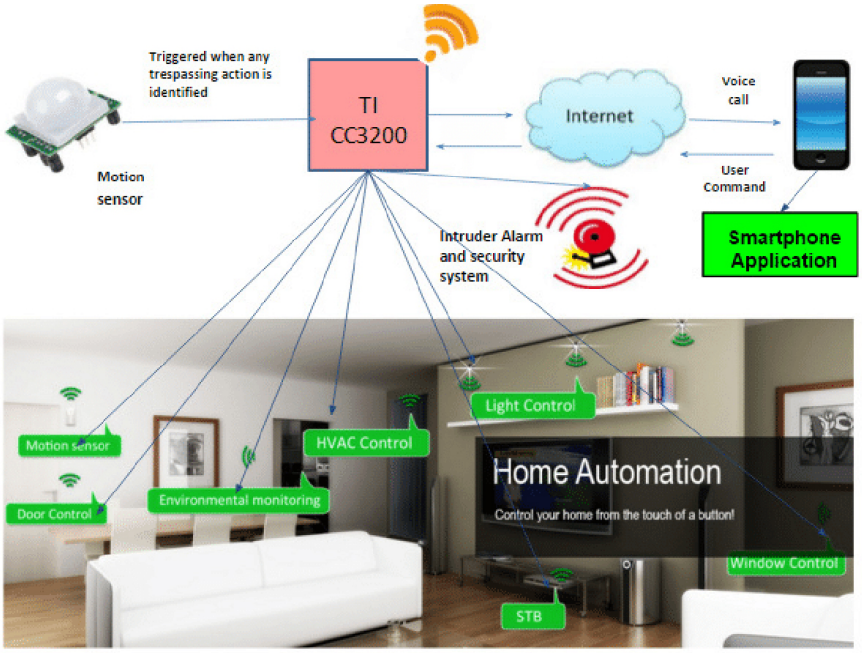

Fig 2. Prototype of proposed security system

Let takes another scenario to demonstrate the robustness of our presented model. At the very first minute, our system is in

standby mode only the sensors related to the unauthorized access group are in running mode. At the 3rd minute someone walks near the home and opens the door, our system will detect access based on equation (A); the motion sensor will be activated. Here the motion sensor will fail to start, and then the heat sensor will take its place based on the equation mentioned earlier. Heat sensor also fails to start at the 6th minute; by following the same logic the camera sensor will be activated. At the 6th minute, the identity of a person will be detected by face recognition through the camera. And at the 10th minute, the timeout occurs and the camera sensor will be detected to save the energy. Prototype of our proposed work may be viewed in Figure 2.

5 Conclusion

We present a model that is used by the Internet of Things (IoT) system to implement security in the smart home. The presented model enables devices to work with each other, even each device has completely different capabilities. The devices used in our model are heterogeneous. Our model has the capabilities to handle faults and provides energy efficiency by powering on only those devices that we need the most. Our presented model can be used to build real-time IoT systems that can be used for different purposes. We also showed how our model provides energy efficiency and robustness by demonstrating different scenarios. Our proposed model can be applied to other IoT systems such as "smart farming" and "smart healthcare" to create a smart environment. The model we presented can be extended to multi-user and multi-room environments by using fuzzy logic techniques. We also showed how different sensors combine with each other to improve security and accuracy. Further with our model, we will initiate to implement multiple IoT systems in the future.

References

1) Mezghani E, Exposito E, Drira K. A Model-Driven Methodology for the Design of Autonomic and Cognitive IoT-Based Systems: Application to Healthcare. *IEEE Transactions on Emerging Topics in Computational Intelligence*. 2017;1(3):224–234. doi:10.1109/tetci.2017.2699218.
2) Kukunin S. Popoa iicoї mesc Toooiї opaiaiї сисsc Tem sc Тиу «роумий уио» рамах араиmи «isc Tepesc Ty peeй». *Computer-Integrated Technologies: Education, Science, Production*. 2020;38:40–45. Available from: http://cit-journal.com.ua/index.php/cit/article/view/98.
3) Pulkkinen V. 2019. Available from: https://www.theseus.fi/handle/10024/263946.
4) Domb M, IoT and Smart Home Automation. Smart Home Systems Based on Internet of Things. 2019. Available from: https://www.intechopen.com/books/internet-of-things-iot-for-automated-and-smart-applications/smart-home-systems-based-on-internet-of-things.
5) Shouran Z, Ashari A, Kuntoro T. Internet of Things (IoT) of Smart Home: Privacy and Security. *International Journal of Computer Applications*. 2019;182(39):3–8. doi:10.5120/ijca2019918450.
6) Yang H, Lee W, Lee H. IoT Smart Home Adoption: The Importance of Proper Level Automation. *Journal of Sensors*. 2018;2018:1–11. doi:10.1155/2018/6464036.
7) Elhoseny M. Secure medical data transmission model for IoT-based healthcare systems. *Ieee Access*. 2018;6:20596–20608.
8) Solanki V, Kumar M, Venkatesan S, Katiyar. Conceptual Model for Smart Cities: Irrigation and Highway Lamps using IoT. *International Journal of Interactive Multimedia and Artificial Intelligence*. 2017;4(3):28–33. doi:10.9781/ijimai.2017.435.
9) Das A, Dash PK, Mishra BK. An intelligent parking system in smart cities using IoT. In: and others, editor. Exploring the convergence of big data and the Internet of Things. IGI Global. 2018;p. 155–180. doi:10.4018/978-1-5225-2947-7.ch012.
10) Vadivukarasi K, Krithiga S. Home security system using IOT. *International Journal of Pure and Applied Mathematics*. 2018;119:1863–1868.
11) Al-Ali, Abdul-Rahman. A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*. 2017;63(4):426–434. doi:10.1109/TCE.2017.015014.
12) Wadhwani S, Singh U, Singh P, Dwivedi S. Smart home automation and security system using Arduino and IOT. *International Research Journal of Engineering and Technololgy*. 2018;5(2):1357–1359.
13) Al-Ali, Abdul-Rahman. A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*. 2017;63:426–434.
14) Anitha A. Home security system using internet of things. *IOP Conference Series: Materials Science and Engineering*. 2017;263(4):042026–042026. doi:10.1088/1757-899x/263/4/042026.
15) Sruthy S, George SN. WiFi enabled home security surveillance system using Raspberry Pi and IoT module. In: and others, editor. 2017 IEEE International Conference on Signal Processing. .
16) Han D, Kim H, Jang J, IEEE. Blockchain based smart door lock system. In: and others, editor. International conference on information and communication technology convergence (ICTC). 2017. Available from: https://ieeexplore.ieee.org/abstract/document/8190886.
17) Tao M. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*. 2018;78:1040–1051.
18) Mannapur SJ. IoT based home security through image processing algorithms. *International Journal of Advance Research, Ideas and Innovations in Technology*. 2018;4:1598–1602.
19) Abbas I, Muneer U. The Prediction of death causes using regression models and moving averages. *International Journal of Data Science and Advanced Analytics*. 2019;1:39–46.
20) Chilipirea C, Ursache A, Popa DO, Pop F. Energy efficiency and robustness for IoT: building a smart home security system. *Intelligent Computer Communication and Processing (ICCP)*. 2016;p. 43–48.
21) Pirbhulal S, Zhang H, Alahi ME, Ghayvat H, Mukhopadhyay S, Zhang YT, et al. A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. *Sensors*. 2016;17(12):69–69. doi:10.3390/s17010069.
22) Stergiou C, Psannis KE, Kim BG, Gupta B. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*. 2018;78:964–975. doi:10.1016/j.future.2016.11.031.

23) Kumar PM, Gandhi UD. A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Computers & Electrical Engineering*. 2018;65:222–235. doi:10.1016/j.compeleceng.2017.09.001.
24) Sahoo K, Chandra UC, Pati, IEEE. IoT based intrusion detection system using PIR sensor. In: and others, editor. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017. Available from: https://ieeexplore.ieee.org/abstract/document/8256877.
25) Tanwar S, IEEE. An advanced internet of thing based security alert system for smart home. In: and others, editor. 2017 International Conference on Computer, Information and Telecommunication Systems (CITS). 2017. Available from: https://ieeexplore.ieee.org/abstract/document/8035326.
26) Taryudi, Adriano DB, Budi WAC. Iot-based Integrated Home Security and Monitoring System. *Journal of Physics: Conference Series*. 2018;1140(1):1–8. doi:10.1088/1742-6596/1140/1/012006.