

6

SMART HOME SECURITY SYSTEM

Muhammad Harith Bahrin, Ruzairi Abdul Rahim, Tee Kian Sek, Mohamad Shukri Abdul Manaf, Ahmad Ridhwan Wahap, Shahrulnizahani Mohamed Din, Nasarudin Ahmad, Norkharziana Mohd Nayan, Rasif Mohd Zain, Jaysuman Pusppanathan

6.1 INTRODUCTION

The most common Internet of Things (IoT) component is the smart home, which is described as a home with technology features that ensure the safety and well-being of its inhabitants. A smart home is a networked home with numerous sensors, actuators, and devices that can be managed and accessed remotely through network communication.

The latest project that we can see for now is the usage of application by phone and connected to the devices to control what happen at our home and get notify if there is something wrong. However, in the IoT world, an increase in the phenomenon of user privacy data leakage and security vulnerability should not be ignored. Describes a range of important research needs for future IoT systems, including protection and privacy, and depicts the general meanings for the key security aspects within the IoT domain. If the service infrastructure is built without understanding predictable security vulnerabilities, outsiders with malicious intent can cause consumer privacy data leakage, social infrastructure paralysis, and economic losses, as well as a risk to human life in extreme cases. [1]

6.2 PROBLEM BACKGROUND

Home security device system are invented to produce a safety requirement among family members which can be related to a camera system and application about the system device. Nowadays, the security system use for our house are totally depends on guard and human. the security level for the current system is very low because there is lack of sight-seeing from surrounding.

Secondly, the alarm system provides a very good security only outside of the house. Supposedly, the house alarm system must be loud and can be heard by the neighborhoods such as the bank alarm system but it only can be heard by sided house which less circumference included in the area. Users can't totally hope guard to take a good care of our house, therefore the system should be more details about the surrounding of the user house and can be reach by other people easily when there is a case happen in their neighborhoods.

This section will describe some related projects done by other researcher and some news regarding cases of child left in a car. Overall, those projects have some disadvantages which make it incomplete as home security system.

6.2.1 Control the home security by using smart phone

One of the most important smart home-smartphone security requirements is the data encryption. Since the communication between the smartphone and home devices is based on the internet, which means that it is possible to have cybersecurity problems. Many attacks may threaten the user's security and the security of his data as an example man-in-the-middle attack (MITM). This attack is used to monitor and steal information between the two parties also it is may be used for update or change the exchanged data. To address these types of attacks, it is required to implement an encryption mechanism that encrypts the data exchanged among the network.

Many types of research have been conducted for cryptographic techniques for smart homes systems. There are a lot of approaches and algorithms to encrypt data, protect information and privacy of users. Actually, two categories of cryptographic algorithms: symmetric and asymmetric algorithms. Advanced Encryption Standard (AES) is the most used symmetric algorithms for encrypting data because it is secure and is used to insure data confidentiality. For the asymmetric algorithm, there are a lot of them like Shamir Adelman (RSA), Secure Hash Algorithms (SHA), Diffie-Hellman (DH) and Elliptic curve cryptography (ECC) [3].

All these algorithms are secure but the heterogeneous nature of the system device and their limitations requires the combination of these algorithms or development of a new algorithm for better protect and secure data exchange. Figure 6.1 shows the block diagram of the projects.

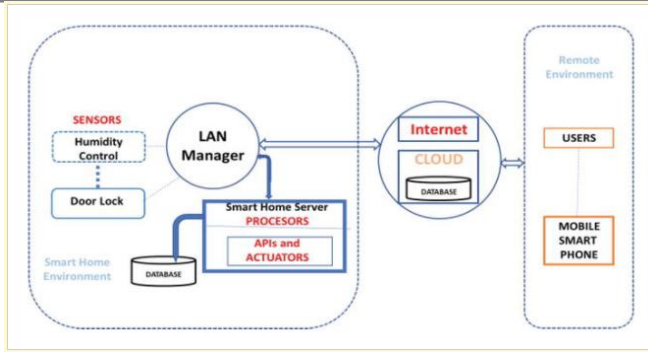


Figure 6.1: The block diagram of the project

6.2.2 IoT for Smart Home using

A smart home-smartphone system is a network of devices (sensors, microcontrollers, actuators, and a smartphone app) that communicates using one or more communication protocols such as Wi-Fi, ZigBee, and others, as shown in Figure 6.2. This form of system’s network must be monitored in order to ensure the system’s security.

These communication systems are susceptible to network layer attacks such as denial of service (DoS), routing attacks, message corruption, and traffic analysis due to a lack of data transmission security on the network.

As a result, a number of academics and industrial researchers have proposed a mechanism for network monitoring.

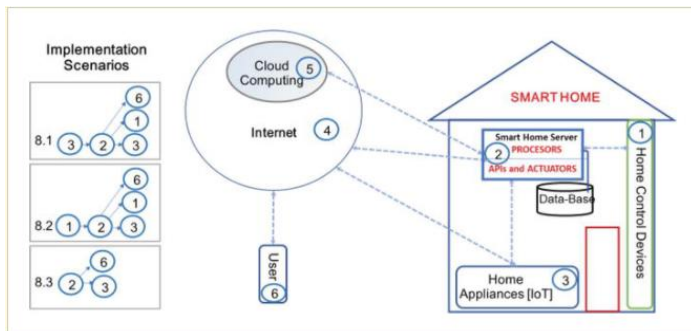


Figure 6.2: Advance smart security system

6.2.3 Burglar Alarm using Arduino and PIR Sensor- with SMS Alarm using GSM Module

This system is using the Arduino as a microcontroller. The input is the PIR Sensor. The system will detect any movement inside the house and will send a SMS to the owner to inform there is a movement inside the house. The system also will trigger the buzzer and the buzzer will not turn off until the owner pressed the reset button. The circuit diagram of the system is illustrating in Figure 6.3.

The system does not have the locking system using GSM module to lock and unlock the door. Furthermore, this system can only be applied in house.

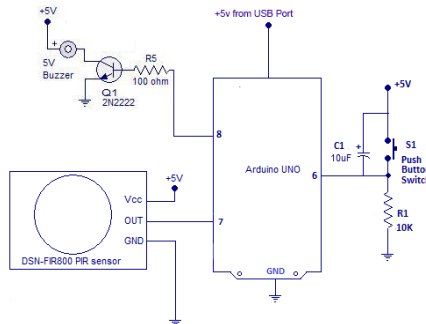


Figure 6.3: Circuit Diagram of Burglar Alarm System

6.2.4 Internal safety for home appliances

1) Water Leaking

First step is deploying water sensors under every reasonable potential leak source and an automated master water valve sensor for the whole house, which now means the house is considered as an IoT. In case the water sensor detects a leak of water (3), it sends an event to the hub (2), which triggers the “turn valve off” application. The home control application then sends a “turn off” command to all IoT (3) appliances defined as sensitive to water stopping and then sends the “turn off” command to the main water valve (1). An update message is sent via the messaging system to these appearing in the notification list (6). This setup helps defending against scenarios where the source of the water is from the house plumbing. The underlying configuration assumes an integration via messages and commands.

2) Smoke detector

Most houses already have the typical collection of smoke detectors (1), but there is no bridge to send data from the sensor to a smart home hub. Connecting these sensors to a smart home app (2), enables a comprehensive smoke detection system. It is further expanded to notify the elevator sensor to block the use of it due to fire condition (1), and so, it is even further expanded to any IoT sensor (3), who may be activated due to the detected smoke alert.




They designed a wireless sensor network for early detection of house fires. They simulated a fire in a smart home using the fire dynamics simulator and a language program. The simulation results showed that the system detects fire early.

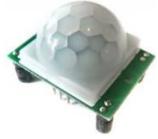



6.3 METHODOLOGY

6.3.1 Hardware Requirement

In making of these projects there is some hardware and software required to make sure the system working properly. The list of hardware is tabulated in Table 6.1.

Table 6.1: List of Component Used

Hardware	Purpose	Detection range	Photo
Arduino Uno	As microcontroller to control the process	Microcontroller ATmega 328	
Robot Motor	To control the lock and unlock of the car system.	Voltage 6V, no-load current 200mA, no-load speed 200±10% rpm	
SIM 800 GSM Module	To receive the command from user and to send the alarm to user.	Quad-band 850/900/1800/1900MHz	

PIR Motion Sensor	To detect if there is any motion inside the car.	Up to 20 feet (6 meters) 110° x 70° detection range	
Sound sensor module	To detect if there is any sound inside the car.	Microphone sensitivity (1Khz): 52-48dB Microphone Frequency: 16-20Khz	
Water Leaking sensor	Leak sensors, also referred to as leak detectors, are devices that serve to provide an alarm condition or visual indication of the presence of a leak	leak detection methodologies have an accuracy rate of over 90%	
Smoke sensor	A <i>smoke detector</i> is a device that senses smoke, typically as an indicator of fire	spacing of 30 feet between detectors	

For the microcontroller, the system will be using Arduino Uno as it uses a simple programming language making it easier to be programmed. For the sensor to detect the movement and sound, the project will be using PIR motion sensor and sound sensor module. The PIR and sound sensor schematic is shown in Figure 6.4 and Figure 6.5, respectively.

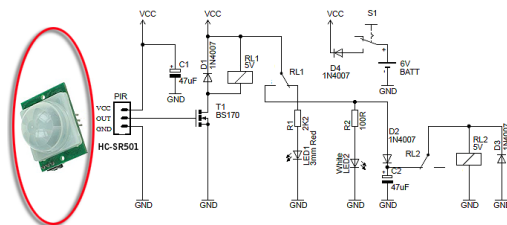


Figure 6.4: Schematic Diagram of PIR Motion Sensor

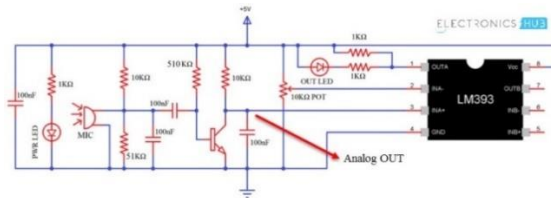


Figure 6.5: Schematic Diagram of Sound Sensor Module

6.3.2 Software Requirements

For the software requirement, the system needs to use Arduino Ide software to program and upload the language into the microcontroller.

6.3.3 Project Flowcharts

The flowchart (Figure 6.6) of the alert system connected to the mobile phone application where we get the data from the sensor and transfer to the controller and send a signal to our phone that already synchronize with the particular object system.

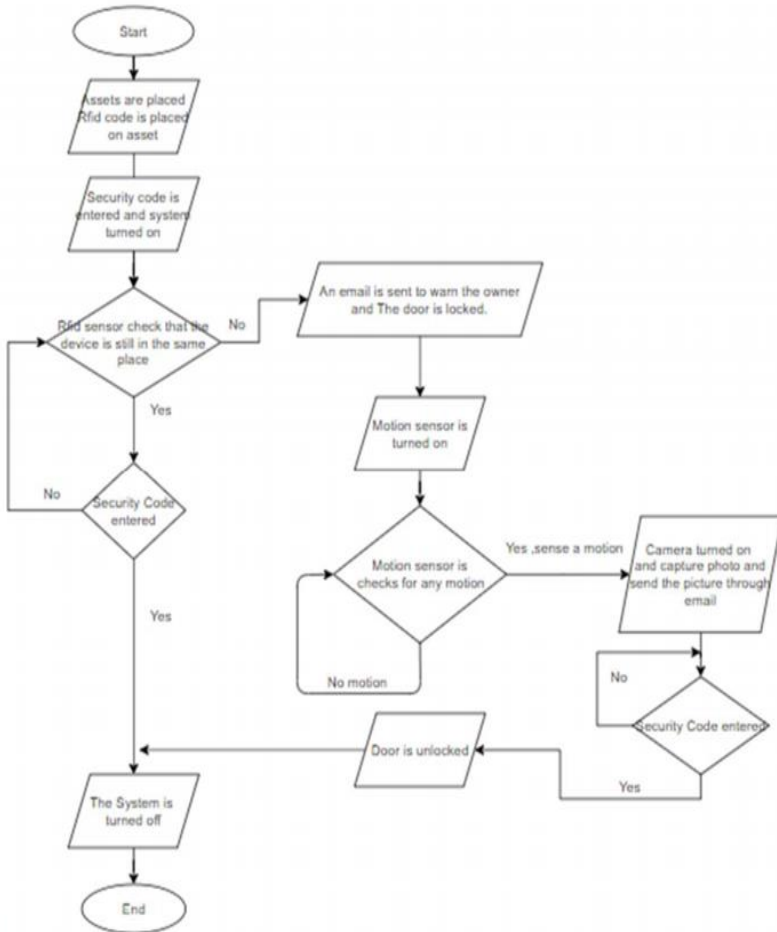


Figure 6.6: Flow chart of the whole system to operate

6.4 RESULTS AND DISCUSSION

6.4.1 Sensitivity of sensor

The following sensors' sensitivity has been identified during the study:

The sensitivity of the Sound Sensor can be adjusted at the module itself ranging:

- Microphone sensitivity (1Khz): 52-48dB
- Microphone Frequency: 16-20Khz

The sensitivity of the Motion Sensor can be adjusted at the module itself ranging:

- Up to 20 feet (6 meters) 110° x 70° detection range

The sensitivity of smoke detector is weak due to range:

- spacing of 30 feet between detectors

The sensitivity of water level sensors

- leak detection methodologies have an accuracy rate of over 90%

Table 6.2 show the result of the problem occurred.

Table 6.2: Table for Failure and Analysis

No	Problem & finding	Root Cause	Action	Result
1.	The power supply for this system needs to be on, if using the cigarettes port from the car, it will switch off when the car engine is off.	Power source	Replace with a rechargeable battery.	The system can be use even if the car engine is turn off.
2.	Some of the SMS feedback didn't reach back to the customer hand phone.	Sensor SMS and feedback SMS send at the same time.	Increase the delay for the sensor to detect any movement or sound.	The system working fine.

3.	The sound sensor is too sensitive.	Sensor specification	Adjust the sensitivity of the sensor.	Only certain frequency will be detected by the sensor.
----	------------------------------------	----------------------	---------------------------------------	--

6.5 CONCLUSION

Several cases of depression among Malaysians have been recorded as a result of heavy workloads. As a result, the parents could forget about their daily routine. The most of the cases in the news are due to parents not seeing their children in the car while speeding. By using this device, the risk of an injury is minimized and the system would notify the parent if a child or perhaps pets are left inside the vehicle.

There are some improvements that can be done by the inventors due to demands now days about the system that created more invention and more creative towards the upgraded technology. But somehow the supply and demands right now are totally follow the needs of customer. The security system nowadays really needs to be practices either for actual self-protection and databased protection. As the self-protection services is this IoT project which related to home security system and we hope for a better improvement in this system which it can be use and normalize in our daily usage with no compromise and feel more safer outside.

REFERENCES

- [1] J. Han, Y. Jeon and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, 2015, pp. 1116-1118, doi: 10.1109/ICTC.2015.7354752.
- [2] V. D. Vaidya and P. Vishwakarma, "A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation," *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, 2018, pp. 1-4, doi: 10.1109/ICSCET.2018.8537381.
- [3] I. Ali, S. Sabir and Z. Ullah, "Internet of things security device authentication and access control: a review", 2019.

-
- [4] Menachem Domb (February 28th 2019). Smart Home Systems Based on Internet of Things, Internet of Things (IoT) for Automated and Smart Applications, Yasser Ismail, IntechOpen, DOI: 10.5772/intechopen.84894. 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] M. Schiefer, "Smart Home Definition and Security Threats," 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, 2015, pp. 114-118, doi: 10.1109/IMF.2015.17.
- [6] G. M. S. Mahmud Rana, A. A. Mamun Khan, M. N. Hoque and A. F. Mitul, "Design and implementation of a GSM based remote home security and appliance control system," 2013 2nd International Conference on Advances in Electrical Engineering (ICAEE), 2013, pp. 291-295, doi: 10.1109/ICAEE.2013.6750350.
- [7] D. Teixeira, L. Assunção and S. Paiva, "Security of Smart Home-Smartphones Systems," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020, pp. 1-5, doi: 10.23919/CISTI49556.2020.9141025.
- [8] R. C. Luo, P. K. Wang, Y. F. Tseng and T. Y. Lin, "Navigation and Mobile Security System of Home Security Robot," 2006 IEEE International Conference on Systems, Man and Cybernetics, 2006, pp. 169-174, doi: 10.1109/ICSMC.2006.384377.

