Original Research Paper

Smart Door Lock

Athirah Nabihah Mas Erwan[1], Mohamad Norul Hafiz Muzaffar Alfian[1], Mohamad Syafiq Mohamad Adenan[1]

[1] *Department of Computing, Faculty of Arts, Computing and Creative Industry. Universiti Pendidikan Sultan Idris, Malaysia.*

Abstract: Internet of Things (IoT) has become a phenomenon in many researchers. A smart digital automated system based on IoT plays major role which helps in reducing human work by applying interaction technology in daily life. This research introduces the IoT Smart Door Lock where smartphone uses Wireless Fidelity (Wi-Fi) to activate the door lock. By using Android software, the smartphone will automatically activate the door lock within a specific range. Data transmission will be done using Wi-Fi technology. So, the user does not have to worry whether the door has been locked or not because user can control it by using their smartphone within a specific range. The user also does not have to worry about losing the door key anymore because there is no device required except user's smartphone. This research consists of hardware and software development. The main purpose on the design is to prevent the situation where the user is unable to unlock the door when the key is missing also to give a solution for users to monitor door status when they forget the door has been locked or not. This system aims to eliminate the use of keys to access the door, where the daily struggle faced to bring along a bunch of keys anywhere. Besides that, the door locking system must function efficiently. The prototype of this system is successfully done, the procedure and the software and hardware requirement has been compiled in this report.

1. Introduction

A door is one of the first defense features to maintain physical security of the house. If the door of the house can be opened easily, a thief can easily enter and steal one's possessions. At first, a door only incorporates a physical key to lock or unlock the door but then, with advancement of technology, a more modern door has been innovated, namely the smart door lock that can lock or unlock doors without requiring physical key. However, the digital door can also be broken or damaged when the house is empty and the house occupants will only find out when arriving home. To always maintain the home security, the user or house occupants will always have to make sure that they have locked the door anytime they enter or leave the house. However, sometimes they forget to lock the door due to hurry when leaving the house or they may have the doubt whether they have locked the door or not. This is one factor that can be a threat to home security.

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. An IoT ecosystem consists of web-enabled smart devices that use embedded processor, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud or analyzed locally.

IoT Smart Door Lock is an Arduino and IoT based system and is a prototype of door access system which allows user to monitor the door system by using mobile phone application via Wi-Fi connection [1]. This research is designed as an alternative method to lock and unlock the door for those who forgets to lock the door and whom always losing the key.

Most people always in urgency situation or being careless sometimes. This might be the cause of forgetting to lock the door of their home or premises. It has become a problem on how to lock and unlock the door from a different place and how to make sure that the door is fully secured if we are at somewhere else. Furthermore, bringing around a bunch of keys at a time could be a problem whenever it comes to store them. It is also a problem to enter our premises if we lost or misplace the keys and there is no other way to unlock the door except by preparing spare keys [2]. Other than that, it might be hard for handicap to lock and unlock the door if they need some privacy for themselves or they are having difficulties to move towards the door [3].

The aim of this research is to build an Internet of Things (IoT) device to simplify the task of locking and unlocking the door. This research will also enhance home security as it only allows authorized user to perform the task.

2. Literature Review
2.1. Internet of Things

Internet of Things (IoT) is involved in all aspects of human life, work, health and social areas, which will have a significant impact on the future development of the global economy society. Several innovative applications of research related with IoT is shown in Table 1 below. Perception and recognition technology are the basis of the IoT and data fusion and anti-collision technology are the sensor network and radio frequency identification research focus [4]. Because current definitions of IoT invariably imply a similar approach to the high-level architecture of a system, the ubiquitous use of the term IoT refer to the use of digital technologies in industry is unhelpful as it hinders the analysis of alternative system architectures, including the location and the nature of the data or information processing and associated performance and security issues [5].

According to the forecast, there will be more than 22 million IoT devices in operation by 2020. Whether it is a health monitoring system or a remote-control home thermostat, IoT equipment provides comfort and convenience. However, as more IoT devices are connected to the Internet, the probability of these devices being attacked is increasing. Especially at risk are the sensors that send important data to users or IoT devices. Without adequate security, leakage of user privacy data and unnecessary damages are likely. The previous method was to send data or instructions to the IoT device from a central device, through a user name and password authentication mechanism. However, most IoT devices are used by non-technicians who may not modify the default factory username and password. In recent years, hackers have launched several major network attacks using this vulnerability [6].

Table 1. IoT Research on Several Fields

Research	Description
Smart Mirror for Home Automation [7]	Smart Mirrors is designed to help users check daily updates while multi-tasking. For example, user can conveniently brush teeth while still got information through voice control on weather or traffic or even stock updates.
Displaying Health Status Based IoT [8]	This IoT use pulse sensor to help user understand whether their pulse rate is normal or not. This can help user minimize potential further health issue by taking necessary prevention when the pulse rate is not normal.
Smart Water Level Indicator [9]	Smart Water Level Indicator use IoT to provide early warning notification to the residents that live near river. When the water reaches dangerous level, the indicator will send alert through sirens and messages so the workers can control the dam of the river.
A Design Remote Control System to Feed Birds Using ESP8266 [10]	This research use ESP 8266 connected to NodeMCU to design automatic system for feeding birds.
Intelligent Egg Incubator [11]	This research use temperature and motion sensor to make smart incubator that can hatch eggs automatically. The temperature sensor will control the temperature remain certain temperature range.
Smart Cane based on IoT [12]	This research use GPS module, GPS Antenna, Arduino, ultrasonic sensor and buzzer to design smart cane to help blind disability. This cane can help user reach destination safely and avoiding obstacles. User will be notified by using sound.
Smart Charger based on IoT Concept [13]	This research use Arduino to control charging time so user will not overcharge their smartphone. This can help prolong battery lifetime.

The work process of IoT can be broadly divided into data collection, data transmission, data processing and service, according to these three different processes, its architecture is divided into perception layer, network layer and application layer. As shown in Figure 1. Perception layer is mainly used to collect all kinds of data information in the real world, says object identify, made up of all kinds of information collection equipment, including various types of sensors, labels, reading and writing, code label, laser, scanner, etc.

The network layer is responsible for receiving perception layer information, carries on the preliminary processing, will forward it to the Internet network for the transmission and it is connected to the Internet and traditional networking ties, composed of various networks, including broadband network, etc., can transmit data by way of broadband network or networks, etc. The application layer is mainly responsible for the information collected by the perceptual layer and the information needed by the function user and it can provide the specific application of the Internet of Things to the user with the specific application requirements [14].

In the modern days, people become more aware to install home security system because of reliability. All these applications and devices make IoT become a thing nowadays and will continue to expand in the future.
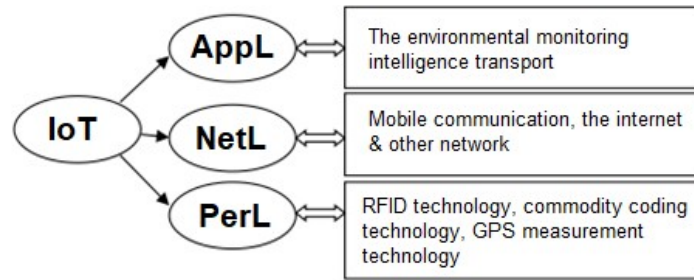
Figure 1. Architecture of Internet of Things

2.2. Home Security

Home security is both the security hardware in place on a property as well as personal security practices. Security hardware includes doors, locks, alarm systems, lighting, motion detectors, security systems, etc. that are installed on a property; personal security involves practices such as ensuring doors are locked, alarms activated, windows closed, extra keys not hidden outside, etc [15].

The most basic definition of any security system is found in its name. It is literally a means or method by which something is secured through a system of interworking components and devices. In the instance, networks of integrated electronic devices working together with a central panel to protect against burglars and other potential home industries [16].

2.3. Related Research
2.3.1. Lockitron Bolt

Lockitron is made by Apigy, a start-up based in Mountain View, California. Multiple models of Lockitron have been manufactured, including one that fits over the lock control mechanisms. Lockitron started a crowd-funding campaign to create a Wi-Fi enabled smart lock, one that could connect instantly to a Wi-Fi network and also be controlled remotely over the Internet. After more than a year invested in developing the product, the company announced it was pulling the plug on the original device and would soon begin shipments of a next-generation Bluetooth-only smart lock called the Bolt. The company also created a separate WiFi-to-Bluetooth bridge accompanying the Bolt, in order to enable remote connectivity via the Internet. The migration to a Bluetooth low-energy (BLE)-only solution was justified by Lockitron because fundamentally, they could not get around how power hungry Wi-Fi is, in nonideal circumstances and the substandard customer experience this creates. By switching to BLE and providing a bridge, they eliminated the hard problem of Wi-Fi power management and gave users instantenous remote control over the Internet [17].

Figure 2. Lockitron Bolt

2.3.2. Unikey Kevo

Unikey Technologies is an alternative access control company based in the United States that designs and licenses keyless entry technology worldwide. In order to further improve the security of wireless communication, Unikey totally replaces the BLE's security protocol and introduces a public-key infrastructure between the smartphone and smart lock is a unique transaction. So, even if someone

were able to overhear the wireless communication containing the key, they would not be able to use it again. As a second step to further improve security, Unikey provides a wireless system on both sides of the door, thus letting the smart lock understand if the user is on the inside or the outside. Essentially, Unikey eliminates any false unlocks [16].

Figure 3. Unikey Kevo

2.4. Components of Internet of Things
Nowadays, we can see a lot of research that implied IoT concept. There are many components that the developer use to build an IoT research. For this section will focus on all the components used in order to develop this research.

Components of Internet of Things used are:
1. Arduino
2. Servo Motor
3. Magnetic Contact Switch
4. LED
5. Breadboard
6. Jumper Wire
7. USB Type-B Cable
8. NodeMCU (ESP 8266)
9. Micro USB Cable

3. Research Methods
The methodology that has been chosen for this research is the Prototype methodology. The reason why this methodology was chosen is because the basic idea in this methodology is that instead of freezing the requirements before a design or coding can proceed, a throwaway prototype is built to understand the requirements. This prototype is developed based on the currently known requirements. Prototype methodology is a software development model. By using this prototype, the client can get an "actual feel" of the system, since the interactions with prototype can enable the client to better understand the requirements of the desired system [18] [19] [20]. Prototyping is an attractive idea for complicated systems for which there is no manual process to help determining the requirements. It is an iterative, trial and error method which take place between the developer and the client.

Prototype methodology is defined as a Software Development model in which a prototype is built, test and then reworked when needed until an acceptable prototype is achieved. It also creates a base to produce the final system. Software prototyping model works best in scenarios where the research's requirement is unknown. At this stage, there is a reasonable understanding of the system and its needs are unclear or likely to change. After the prototype has been developed, the end users and clients are given an opportunity to use the prototype. They provide feedback to the developers regarding the prototype: what is correct, what needs to be modified, what is missing, what is not needed, etc. Based on the feedback, the prototype is modified to incorporate some of the suggested changes that can be done easily, and then the users and the clients are again allowed to use the system. This cycle repeats until, in the judgement of the prototypes and analyst. Based on the feedback, the initial requirements are modified to produce that final requirements specification, which is the used to develop the production quality system. Figure below shows the phases of the prototype methodology.
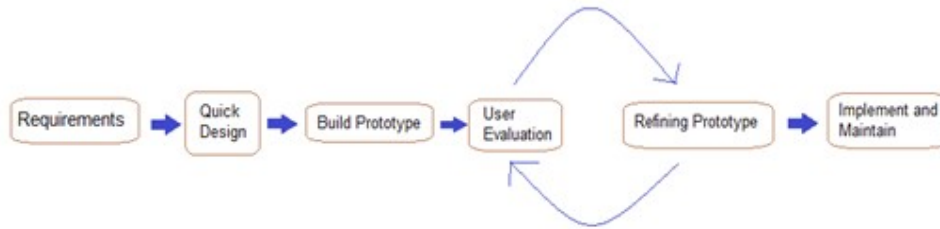
Figure 4. Prototype Methodology Diagram

3.1. Requirements Gathering and Analysis Phase
A prototyping model starts with requirement analysis. In this phase, the requirements of the system are defined in detail. During the process, the users of the system are interviewed to know what their expectations from the system. Aside from that, a questionnaire also has been made for the users to answer and found that most of the respondents think that this research will decrease the threat of their homes' security.
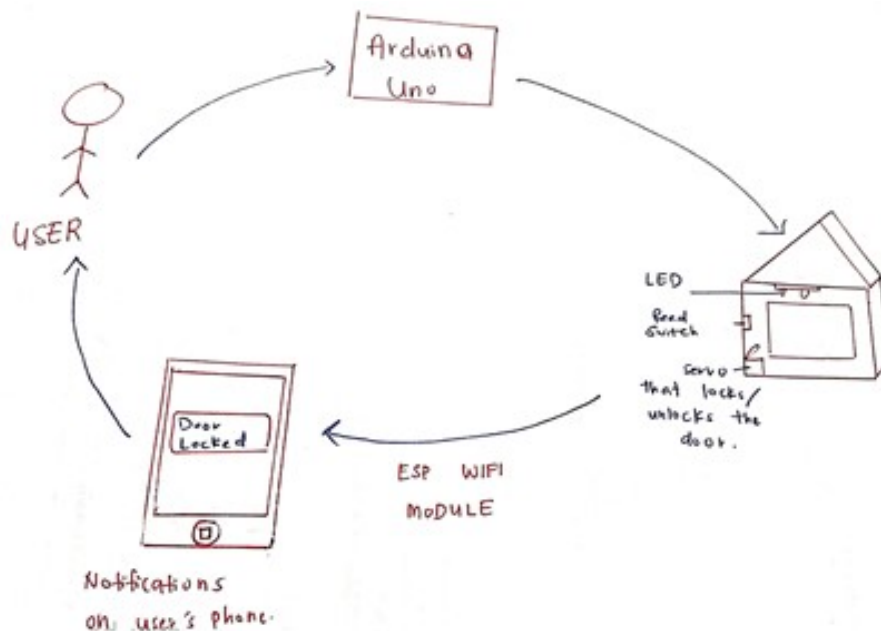

Figure 5. Sketch Diagram

3.2. Quick Design Phase
The second phase is a preliminary design or a quick design. In this stage, a simple design of the system is created. However, it is not a complete design. Design are drawn in a sketch. It gives a brief idea of the system to the user. This phase helps in developing the prototype.

3.3. Build Prototype Phase
In this phase, an actual prototype is designed based in the information gathered from quick design phase. It is a small working model of the required system. The prototype that will be build must match all the requirement that have already documented earlier to avoid untallied between document and the prototype.

3.4. Initial User Evaluation Phase

In this stage, the proposed system is presented to the client for an initial evaluation. It helps to find out the strength and weakness of the working model. Comments and suggestions are collected from the client and provided to the developer.

3.5. Refining Prototype Phase

If the user is no happy with the current prototype, the prototype is refined according to the user's feedback and suggestions. This phase is not over until all the requirements specified by the user are met. Once the user is satisfied with the developed prototype, a final system is developed based on the approved final prototype.

3.6. Implement Product and Maintain Phase

Once the final system is developed based on the final prototype, it is thoroughly tested and deployed to production. The system undergoes routine maintenance for minimizing downtime and prevent large-scale failures.

4. Results and Discussion
4.1. Implementation
4.1.1. Hardware

Hardware implementation involves the use of device that are being used. Know your device's workflow from a microcontroller for reading sensors and data transmission to the server. The prototype system that has been made can be seen in Figure 6.
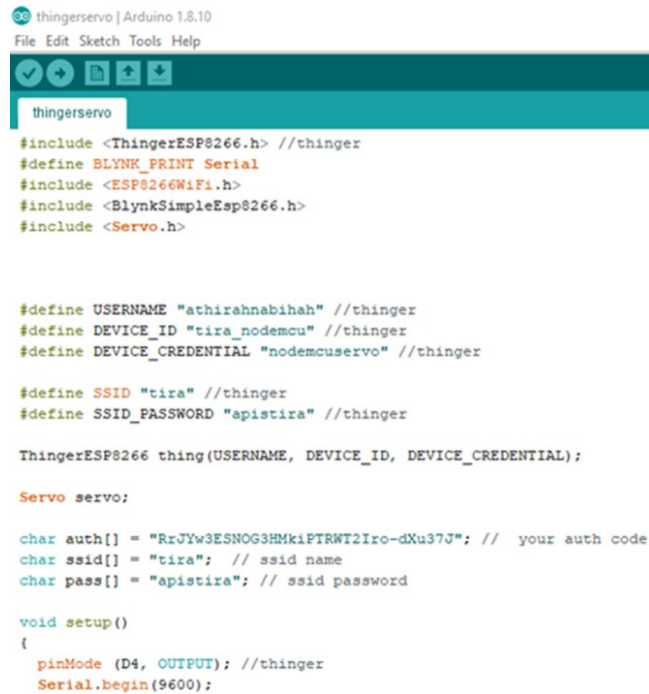

1) Magnetic Contact Switch.
2) Servo Motor.
3) Breadboard.
4) Red and Blue LED.
5) Jumper Wires.
6) Arduino Uno.
7) NodeMCU (ESP 8266).
8) USB Cable Type B.

Figure 6. System Prototype

4.1.2. Software

Software implementation is intended for deployment and the use of application into the system.

Software Configuration

The coding for servo, LED, and Magnetic Contact Switch is done using Arduino Uno and NodeMCU (ESP 8266) and can be seen in Figure 7 and Figure 8.


```
#include <ThingerESP8266.h> //thinger
#define BLYNK_PRINT Serial
#include <ESP8266WiFi.h>
#include <BlynkSimpleEsp8266.h>
#include <Servo.h>


#define USERNAME "athirahnabihah" //thinger
#define DEVICE_ID "tira_nodemcu" //thinger
#define DEVICE_CREDENTIAL "nodemcuservo" //thinger

#define SSID "tira" //thinger
#define SSID_PASSWORD "apistira" //thinger

ThingerESP8266 thing(USERNAME, DEVICE_ID, DEVICE_CREDENTIAL);

Servo servo;

char auth[] = "RrJYw3ESNOG3HMkiPTRWT2Iro-dXu37J"; //  your auth code
char ssid[] = "tira";  // ssid name
char pass[] = "apistira"; // ssid password

void setup()
{
  pinMode (D4, OUTPUT); //thinger
  Serial.begin(9600);
```

Figure 7. Coding of the servo connecting to Blynk application and Thinger.io


```
int ledOpen=9;
int ledClose=10;
int switchReed=6;

void setup(){
  pinMode(ledOpen, OUTPUT);
  pinMode(ledClose, OUTPUT);
  pinMode(switchReed, INPUT);
  Serial.begin(9600);
}

void loop(){

  if (digitalRead(switchReed)==HIGH){
    digitalWrite(ledOpen, LOW);
    digitalWrite(ledClose, HIGH);
    Serial.println("Your Door is Closed");
  }
  else {
    digitalWrite(ledOpen, HIGH);
    digitalWrite(ledClose, LOW);
    Serial.println("Your Door is Open");
  }
  delay(1);
}
```

Figure 8. Coding of the LED and Magnetic Contact Switch

Database

Thinger.io is an Internet of Things platform designed for building vertical applications. It has been designed with the developer in mind, so it is really easy to create an IoT solution from scratch. This is the database software which I worked with and this platform can be freely deployed in your own cloud using Ubuntu Core, have Sigfox integration, and can be connected to other microcontrollers or systems for real-time sensing and actuating over a REST API. The main features of the platform are: full device management and API interaction; endpoints for interacting with third party services or sending notifications; data buckets for storing and exporting information; access management for granting to access your devices and data from other applications; and dashboards for real-time data visualization.

Data Visualization: Home Menu

The Home menu displays the number of devices that connected to, dashboards, data buckets and endpoints as shown in Figure 9.
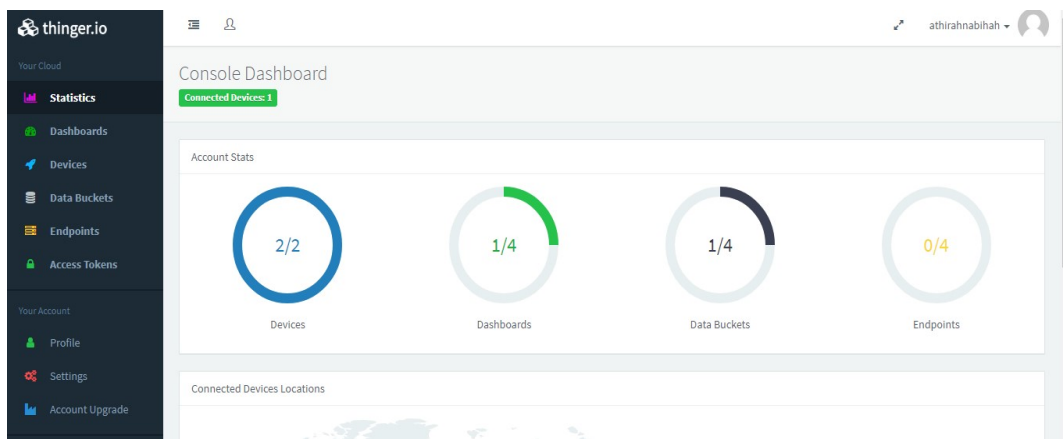
Figure 9. Home Menu Display of the Thinger.io

Data Visualization: Data Transmission

The right-side graph shows the data transmission of the NodeMCU. Whenever the NodeMCU is connected to the database, we can see the data transmission of the system as shown in Figure 10.
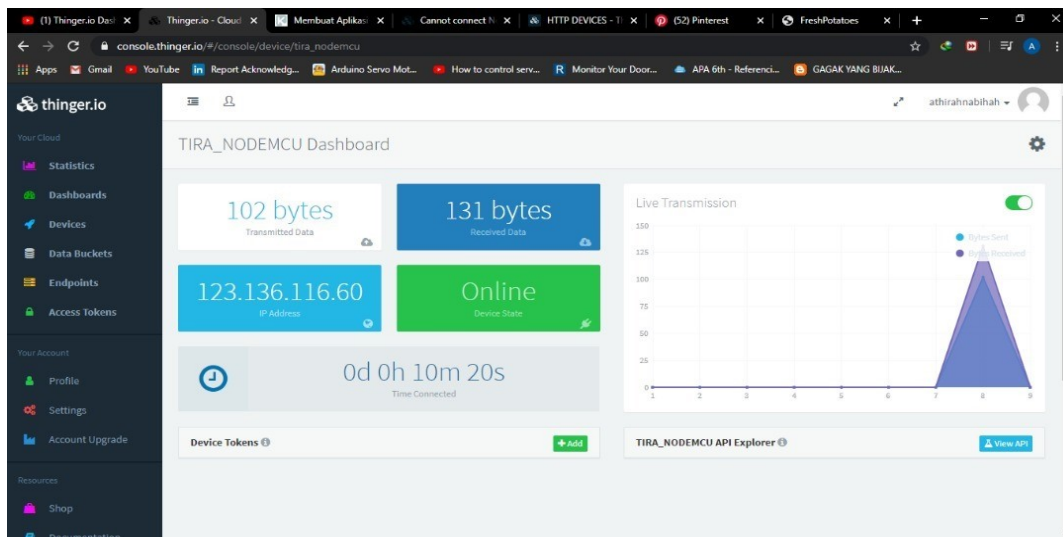

Figure 10. Dashboard of the Thinger.io

4.2. Testing
4.2.1. Testing for the System
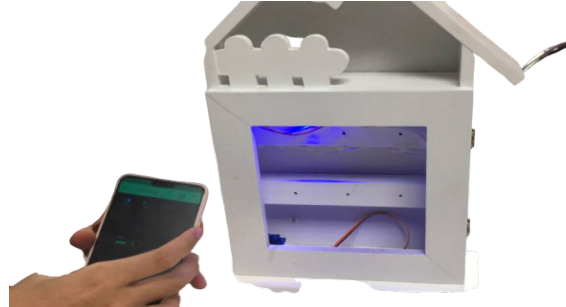System testing is to test whether all components and functionality of systems behaves according to specifications.

Figure 11. Testing

4.2.2. Evaluation
Evaluation for the testing carried out using Google Form under several criteria. This survey consists of five sections which are Usability, Functionality, Performance, Compatibility and Security. There are almost 10 questions was asked to respondent who tested the prototype. Majority of them likes the Usability of the research where people can lock and unlock the door from anywhere and anytime and receive notification about door accessibility through their smart phones. The results can be seen as below.

Usability Testing
13 over 20 users agreed that Smart Door is useful for current and future generation as shown in Figure 12. This is because people can realize that they are often forget and misplace their house and premises keys.
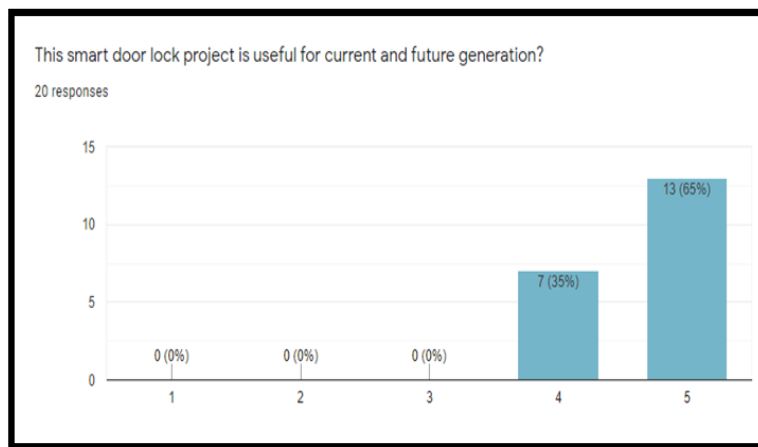

Figure 12. Usefulness in the Future

Functionality Testing
Functionality Testing consists of three sub-testing as shown in Figure 13, 14, 15: test whether the sensors are working, test LED show blue color when door is open and red color when door is close, also test whether user receive notifications on their phone whenever door is open/close. Results from user show high satisfactory towards the product's functionality.
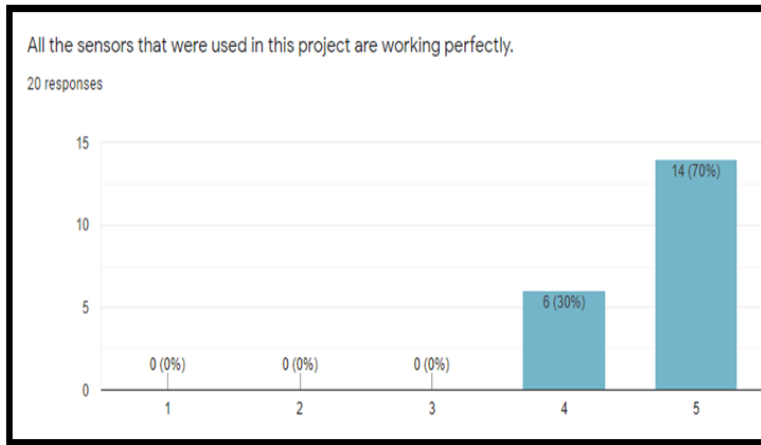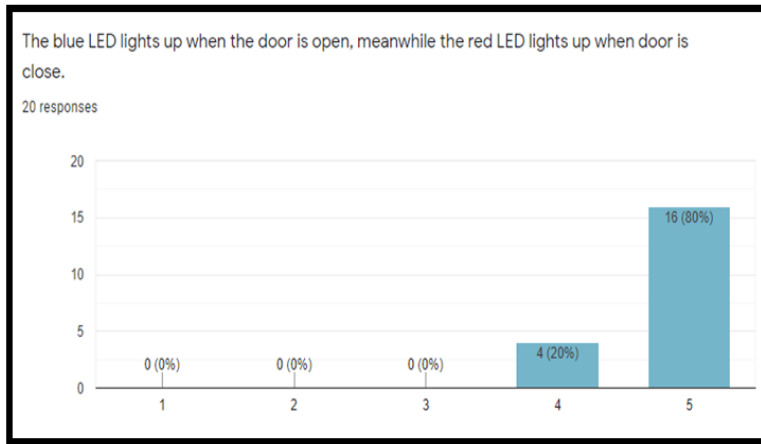
Figure 13. Sensor Functionality Testing

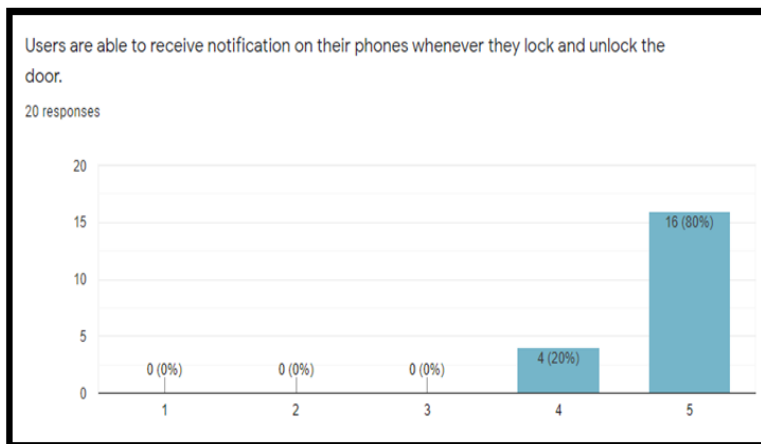Figure 14. LED Functionality Testing

Figure 15. Door Lock and Notification Functionality Testing

Performance Testing
On performance testing, 13 out of 20 users show high satisfaction towards the performance as shown in Figure 16.
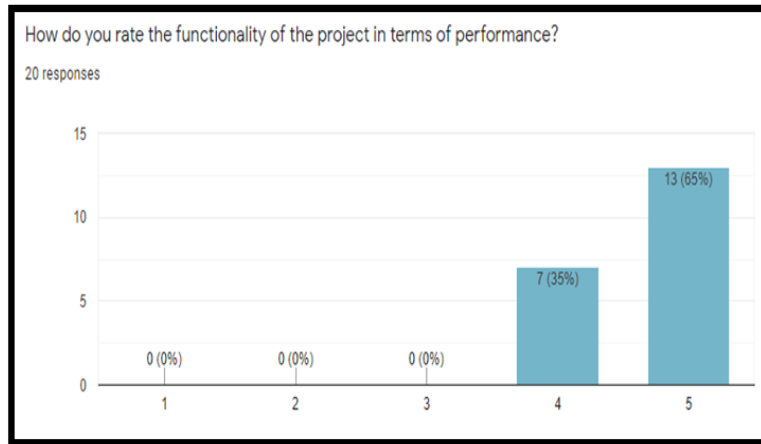
Figure 16. Door Lock and Notification Functionality Testing

Compatibility Testing

Compatibility testing consists of 2 sub-tests as shown in Figure 17 and 18. First, to test whether the sensor and the servo are working together with the component. Second, user invited to comment whether the research related to the Internet since it is related to Internet of Things.
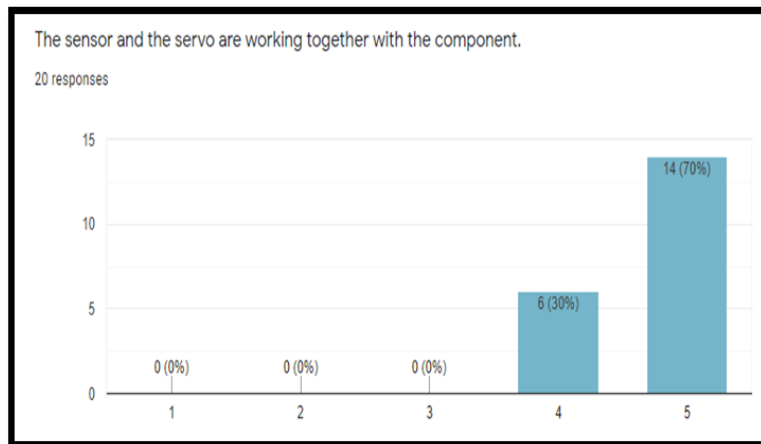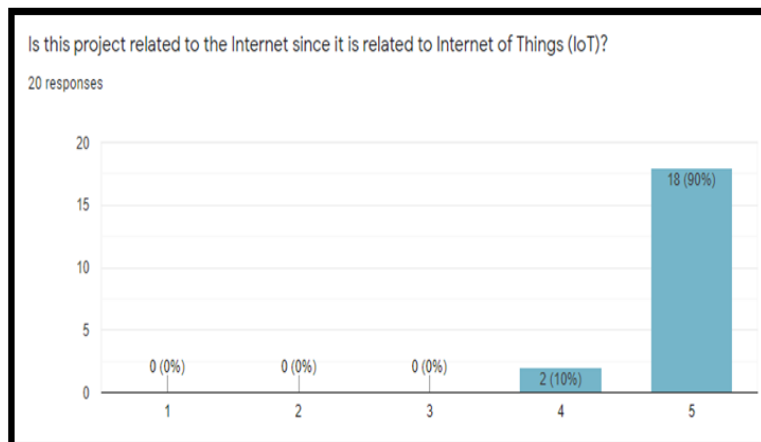

Figure 17. Compatibility Testing

Figure 18. Internet Compatibility Testing

Security Testing

For security testing, 1 out of 20 respondents choose that the research isn't safe to use by people of all age as shown in Figure 19 and 20. However, the rest of respondents show high satisfaction.
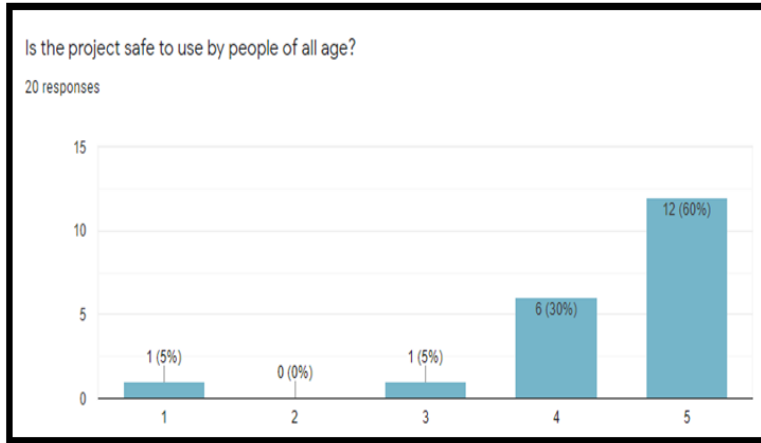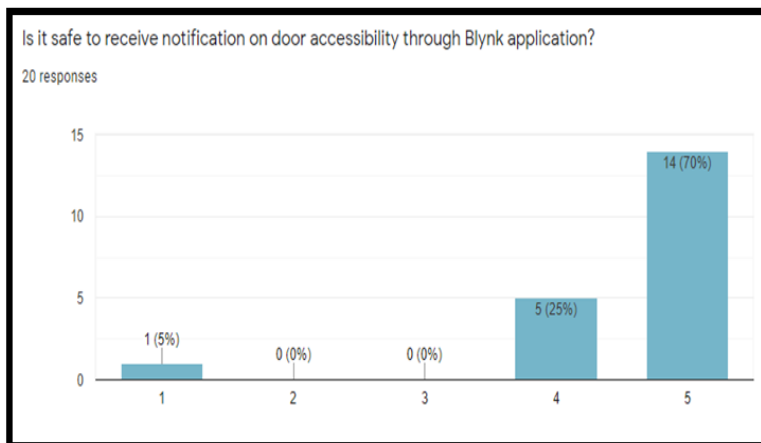

Figure 19. Safety Testing

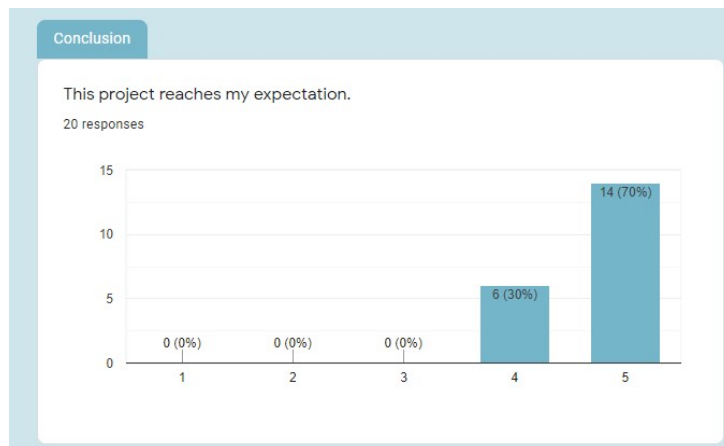Figure 20. Security with Blynk Application Testing

Figure 21. Satisfaction

5. Conclusion
Overall, the prototype received positive satisfaction based on user evaluation. In designing a prototype, there are still shortcomings so that further improvements or developments can be made:
- Make the LED can change its color by following the movement of the servo.
- Make the door open wider for the magnetic switch to detect the movement.
- Use a more suitable house model for the prototype.
- Add fingerprint scanner onto the application to increase security.
- Build my own app that can accommodate this research instead of using a built-in app, such as Blynk.

References
[1]   A. Andreas, C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo, and A. Wibisurya, "Door Security System for Home Monitoring Based on ESP32," *Procedia Computer Science*, vol. 157, no. 673-682, 2019 10.1016/j.procs.2019.08.218

[2]   J. Jeong, "A Study on the IoT Based Smart Door Lock System," *Lecture Notes in Electrical Engineering Information Science and Applications (ICISA) 2016*, no. 1307-1318. (2016, 10.1007/978-981-10-0557-2_123

[3]   N. F. Azmi, *Smartphone activated door lock using wifi*. Universiti Teknikal Malaysia Melaka, 2015.

[4]   Y. Cui, Y. Ma, Z. Zhao, Y. Li, W. Liu, and W. Shu, "Research on data fusion algorithm and anti-collision algorithm based on internet of things," *Future Generation Computer Systems*, no. 85, pp. 107-115, 2018, 10.1016/j.future.2018.03.016

[5]   H. Boyes, B. Hallaq, J.Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry,* no. 101, pp. 1-12, 2018, 10.1016/j.compind.2018.04.015

[6]   Y. Liu, and S. Zhang, "Information security and storage of Internet of Things based on block chains," *Future Generation Computer Systems*, no. 106, pp. 296-303, 2020, 10.1016/j.future.2020.01.023

[7]   M. S. Ab Latif, A. A. Ismail, and A. Zariman, "Smart Mirror for Home Automation", *International Journal of Recent Technology and Applied Science*, vol. 1, no. 1, pp. 1-11, Feb. 2020.

[8]   M. A. Azizi and A. Zariman, "Displaying Health Status Based IoT ", *International Journal of Recent Technology and Applied Science*, vol. 2, no. 1, pp. 25-35, Mar. 2020.

[9]   A. A. Ismail, M. A. Azizi, and A. Zariman, "Smart Water Level Indicator", *International Journal of Recent Technology and Applied Science*, vol. 2, no. 1, pp. 48-58, Mar. 2020.

[10]   N. Saidatin, S. Nurmuslimah, and P. Bagus, "A Design Remote Control System to Feed Birds Using ESP8266", *International Journal of Recent Technology and Applied Science*, vol. 2, no. 2, pp. 81-90, Sep. 2020.

[11]   K. B. Azahar, E. E. Sekudan, and A. M. Azhar, "Intelligent Egg Incubator", *International Journal of Recent Technology and Applied Science*, vol. 2, no. 2, pp. 91-102, Sep. 2020.

[12]   F. A. Ghani and A. Zariman, "Smart Cane based on IoT", *International Journal of Education, Science, Technology, and Engineering*, vol. 2, no. 1, pp. 12 - 18, Jun. 2019.

[13]   M. H. Husin, and I. D. Hisham, "Smart Charger Based on IoT Concept", *International Journal of Education, Science, Technology, and Engineering*, vol. 2, no. 1, pp. 39 - 44, Jun. 2019.

[14]   Y. Zhou, K. Wang, and H. Liu, "An Elevator Monitoring System Based On The Internet Of Things," *Procedia Computer Science*, no. 131, pp. 541-544. 2018, 10.1016/j.procs.2018.04.262

[15]   F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of Things," *International Journal of Communication Systems,* vol. 25, no.9, pp. 1101-1102, 2012, 10.1002/dac.2417

[16]   V. P. Ribeiro, L. D. Oliveira, D. A. Nascimento, D. B. Alencar, and J. D. Júnior, "Application of the Internet of Things in the Development of a "Smart" Door," *International Journal of Advanced Engineering Research and Science,* vol. 6, no. 5, pp. 345-349, 2019, 10.22161/ijaers.6.5.46

[17] I. Chatzigiannakis, "Apps for smart buildings: A case study on building security," *Start-Up Creation*, pp. 465-479, 2016, 10.1016/b978-0-08-100546-0.00019-4

[18] J. Morgan, "A Simple Explanation of 'The Internet of Things'," [Online] Available: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ [Acessed On: May 13, 2014]

[19] M. F. Zulkarnain, *Internet of Things (IoT) Enabled for Door Access System*. Universiti Teknikal Malaysia Melaka, 2017.

[20] P. Li, and G. Zhu, "IMC-based PID control of servo motors with extended state observer," *Mechatronics*, no. 62, 2019, 10.1016/j.mechatronics.2019.102252