International Journal of Synergy in Engineering and Technology
IJSET

Development of IoT Automated Door Lock System Using Blynk Application

Mohamed Affiq Mohamed Bakhory [1], Suzanna Ridzuan Aw [1,*], Nurul Huda Mat Tahir [1], Arfah Syahida Mohd Nor [2] , Farah Hanan Azimi [1] , Lia Safiyah Syafie [1], Safuan Naim Mohamad [1] , Nooraida Samsudin [1]

[1] Faculty of Engineering Technology, University College TATI, 24100, Kemaman, Terengganu, MALAYSIA.
[2] Department of Electrical Technology, Universiti Teknikal Malaysia Melaka, 75450 Ayer Keroh, Malacca, MALAYSIA.
[*]Corresponding author: suzanna_aw@uctati.edu.my

KEYWORDS

Home security
Automated Door Lock
IoT
Blynk application

ABSTRACT

The proposed method in this study uses the IoT technology and the application of smartphone communication technology to conventional device (door lock) to open or close a door remotely through authentication. In this study, door lock is designed for remote home monitoring through the Internet of Things (IOT) methods. Door lock monitoring through the IOT method is more possibly effective than other smart door system. This system consists of IoT system that was build up using the Arduino Wemos D1, ESP8266 as the microcontroller and the Blynk application as for the monitoring. The monitoring process of this door lock can be monitored anywhere and anytime. The durability of the system was tested through this system development. The results were collected by measuring the durability of servo motor to carry out the load which is door deadbolt lock. This system has successfully achieved the objectives.

1.0 INTRODUCTION

Nowadays, smartphone has variety of uses and have been designed to be used as pocket-sized personal computers. Smartphone have utilized many tool and service which are Bluetooth, Wireless Fidelity (WiFi) and Near Field Communication (NFC). Today, WiFi is provided in many smartphones. This has allowed an electronic device to exchange data or connect to the internet wirelessly. Internets are playing an important role in everyday environment. Many devices can be connected to the internet such as smartphone.

As technology develops, smartphone becomes one of the devices that can help to monitor in any aspects. Since less awareness concern on door lock system, this device will help in solving the problem. Wireless access monitoring using smartphone seems to benefit from this technology. Thus, a system for the home system entry that apply the wireless access monitoring is proposed. This system will contribute more secure and advance technology compatible to the latest invention and technology. Other than that, it will increase the security technology of the home.

Received April 2021; received in revised form May 2021; accepted June 2021.

For this study, the locking system will activate automatically. By using Blynk application, the smartphone can unlock the door within a specific range. Data transmission will be done using WiFi technology. WiFi technology can locate a signal almost anywhere. So, the user does not have to worry whether the door is lock or not because it is automatically lock and they can control unlock the door by using their smartphone within a specific range. The user also does not have to worry about the closing of the door key.

2.0 IOT TECHNOLOGY DEVELOPMENT FOR SECURITY SYSTEM

IoT should have three characteristics: comprehensive perception, reliable transmission, and intelligent processing. Comprehensive perception means by the sensor nodes of perception layer obtain object information anytime and anywhere; reliable transmission means that safely and completely transfer the information of objects through the wireless or wired network to the data center in real time; intelligent processing means that middle-ware analyses and deals with the collected information before submitting to application terminal eventually (Zhao & Ge, 2013).

IoT features should reflect the characteristics of IoT security, and reveal the related security problems. In the following security measures are the new features:

i. *The Contradiction between Security and Cost*: If each sensor node cost is too low, the large number of low performance nodes will reduce the security of sensor network. On the other hand, high-performance nodes can increase security, but the cost of network maintenance will be improved.

ii. *Lightweight*: The processor performance of sensor nodes is lower, so must be lightweight encryption algorithm and security authentication.

iii. *Asymmetric*: Comparing with network terminal, gateway nodes data processing ability is weak. Nevertheless, how to coordinate these asymmetric networks that need efficient security management measures.

iv. *Complexity*: The types of application determine the number of security issues and complexity. The security problems of each layer should be considered synthetically

The smart home is the fastest growing field of IoT technology and it provides innovative, intelligent, ubiquitous and interactive services to users using different operations. Due to internet connected, dynamic and heterogeneous nature, smart home creates new security issues and challenges. For the state of art, the Security Goals of Smart Home with one of important which is authentication. The verification about communicating parties or user, who is user and what he claims, what data send by claim author and message send. Another security goal is integration, the assurance that data is maintained in consistency and in an accurate way. Modification and losses of data will be under notice (Ali *et al*., 2017).

Enforcing security in Internet of Things environments has been identified as one of the top barriers for realizing the vision of smart, energy-efficient homes and buildings. The risks classified as high were either related to the human factor or to the software components of the system. The results indicate that with the implementation of standard security features, new, as well as, current risks can be minimized to acceptable levels albeit that the most serious risks. Next, with such a model of security and privacy in design in place, it will contribute to enforcing system security and enhancing user privacy in smart homes, and thus helping to further realize the potential in such IoT environments (Jacobsson *et al*., 2016).

IoT can provide several advantages in retail and supply chain management (SCM) operations. For example, with RFID-equipped items and smart shelves that track the present items in real

time, a retailer can optimize many applications. For example, he can make automatic checking of goods receipt, real time monitoring of stocks, tracking out-of-stocks or the detection of shoplifting. IoT can provide a large savings potential in a retail store, since it has been found that 3.9% of sales loss happens worldwide when shelves go empty and customers return with getting the desired products. Furthermore, IoT can help making the data from the retail store available for optimizing the logistics of the whole supply chain (Bandyopadhyay & Sen, 2011).

With the development of IoT technology, every device in our surroundings will be able to communicate with another device and send information to that device or control it, depending on the collected information. The Internet of Things is a network connecting objects from different environments into a single large network based on the Internet Protocol, and it is a basis for the development of the so-called smart environments, such as smart houses, factories or even cities. There are many applications for services in the IoT field, from user applications that will provide added value only to the user who defined them to entire branches of science that are provided simplified sharing of resources, collecting of data from a large number of sensors, statistical analysis of such data and conclusions in relation to data in real time (Weber & Boban, 2016).

2.1 Smart Door Towards Industry and Home-Based System

Home automation system is a computer-based application that has the ability to connect different electronic devices for the sake of monitoring and controlling the home appliances. Home automation system is an area that has caught several attentions by both the academic and business fields. The earliest effort of home security system was relied on wired home networks however, due to the appropriate planning and construction works required to offer a wired home, such effort tend to be insufficient. As a solution for this problem, wireless communication has been emerged to provide more flexible platform where the installation cost is significantly lower than the wired one. Therefore, it has been applied for different security home systems in order to provide an alarm for critical threats such as intrusions or other environmental risks such as gas leaking or fire (Hussein & Al Mansoori, 2017).

Growing interest in the Internet of Things has spurred the commoditization of many cyber-physical devices for personal use, such as smart home appliances, wearables devices, and new car models. These emerging “smart devices” extend their mechanical counterparts by integrating them with electronic components that allow external computer systems to control them. Although this integration enables new functionality, it greatly increases the system’s attack surface. While prior work on the Internet of Things (IoT) has focused on the cryptographic protocols used by these systems, limited work has studied the security implications of common network architectures used by these smart devices and the new modes of user interaction these devices enable (Ho *et al*., 2016).

A smart home is a house which is integrated with communication network using electrical equipment that can be controlled and monitored or accessed remotely. The main purpose of creating a smart home is to provide comfort to the homeowner in terms of controlling and monitoring the state of his home when they are away. If Android is used as the remote control of the smart home, homeowners can turn on and off lights regularly even though they are not at home, as if we were at home. Another advantage of implementing smart homes is that it can help the elderly and also the disabled as they can switch off and on electronic equipment and home doors more easily without the need to walk first (Romadhon, 2018).

Systems Engineering is now becoming mandatory to master complexity but also to develop innovative systems. Application of Systems Engineering requires the use of a methodology upon tool set. This paper is about the application of a Systems Engineering methodology from CESAMES on a small but complex system: an automatic sliding door in a building. We all experienced it: automatic doors have tendency to open inadvertently for example when pedestrian just walks by with no intention to enter the room. This is due to an old technological design: easiest way to

decide to open the door is to detect a person in a trigger zone. With a system approach, the door could be nicely improved with great potential developments (Kendall, 2011).

As Industrial Internet, Industrial IoT (IIoT) is another form of IoT applications favored by big high-tech companies. The fact that machines can perform specific tasks such as data acquisition and communication more accurately than humans has boosted IIoT's adoption. Machine to machine (M2M) communication, Big Data analysis, and machine learning techniques are major building blocks when it comes to the definition of IIoT. These data enable companies to detect and resolve problems faster, thus resulting in overall money and time savings. For instance, in a manufacturing company, IIoT can be used to efficiently track and manage the supply chain, perform quality control and assurance, and lower the total energy consumption (Khodadadi *et al*., 2016).

3.0 METHODOLOGY

The system will rely on three major hardware components: a microcontroller unit (Arduino), a Servo motor and, a smartphone device. The IoT Controlled Arduino that control the servo motor and the sensor. Then, the Arduino will be in standby mode and waiting for monitoring process from the user. The info through the phone will always shows at the phone apps which either it is lock or unlock. The block diagram is shown in Figure 1.

Figure 1: System Block Diagram

The system starts with ensuring the door is unlocked or lock. If the door is unlocked, the user will be notified through their phone. Then, the user may lock the door through the phone. On the other hand, the user just only locks or unlock the door only through their phone even them are far from the door.

Figure 2 shows the sketch of project which consists of servo motor that detect and monitor the door lock. The user will be notified the door is lock/unlock. Then, the user may lock/unlock the door through their phone using Blynk application.

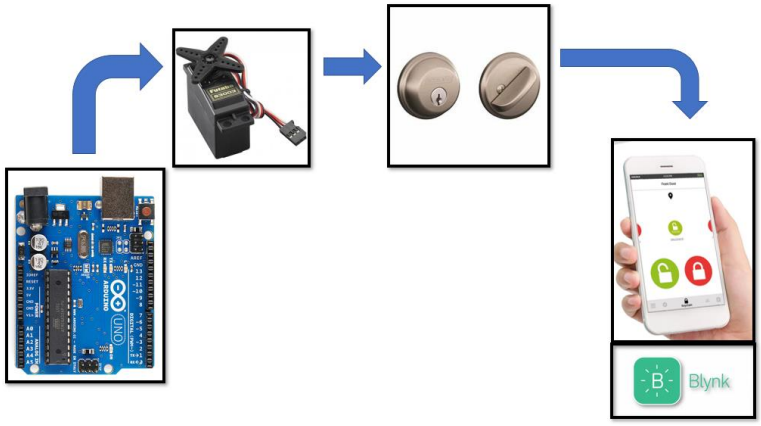

Figure 2: Project Sketch

3.1 Hardware Development

In this project, FRITZING software is used to design and also simulate the circuit. Figure 3 below shows the full design of the circuit using FRITZING software.

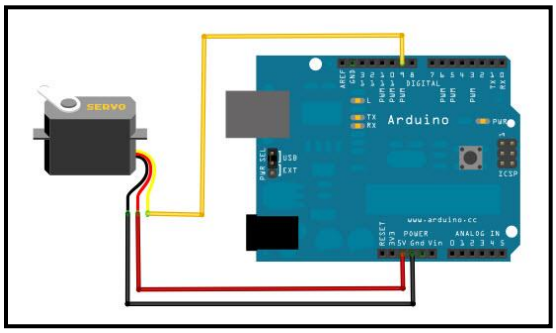

Figure 3: Circuit design

After circuit simulation is complete, all of the component used in this project were installed and assembled. Figure 4 below shows the full connection of the circuit used in this project.

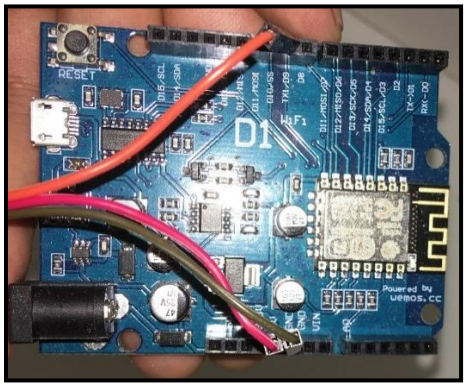

Figure 4: Circuit Connection

Automatic door closer and deadbolt were integrated together to complete the hardware. For this study, deadbolt lock is required for user to install the IoT Door Lock system at their door. Other type of door lock is not suitable and possible to install. Figure 5 shows the installation for deadbolt and servo motor.

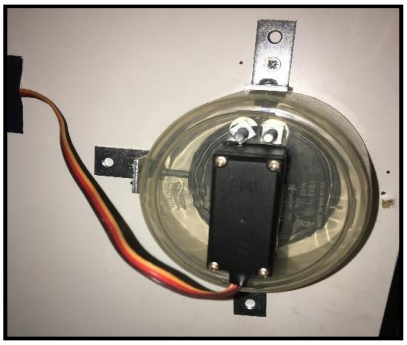

Figure 5: Installation for deadbolt

Other than that, automatic door closer was installed at the door and also the other mechanical part. Figure 6 shows the installation of automatic door closer to automatically close the door.

Figure 6: Installation of Automatic Door Closer

3.2 Software Development

This research is adopting methods approach involving develops the control system using software such as Arduino IDE and Fritzing. This software provides better programming customization and simulation on the system. Fritzing is an open-source hardware initiative that makes electronics accessible as a creative material for anyone. Software tool, a community website and services in the spirit of Processing and Arduino, fostering a creative ecosystem that allows users to document their prototypes, share them with others, teach electronics in a classroom, and layout and manufacture professional PCBs.

3.2.1 Blynk Development

Blynk has been used as the app for IoT monitoring system in this study. The Blynk application can be download through appstore for apple user or playstore for android user. The setup on Arduino WeMos was very well documented and the library briefly described the features that are possible. It is easy to use with minimal software knowledge. Numerous features added. Frequent updates to Blynk app. Support for multiple devices with different modes of communication. The Blynk application can be download through appstore for apple user or playstore for android user. After download the application, the user must create an account to use the entertainment through the applications. After successfully create an account, the home sides of the applications appeared. Then, select the new project to start create a system through the Blynk applications. Figure 7 shows the home sides of the apps.

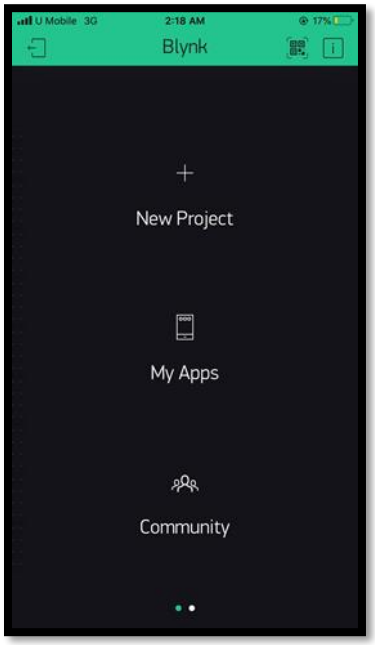

Figure 7: Blynk Home

After create the new project, select the controllers from the Widget Box. Every widget contains the energy balance. However, the user only been given 2000 amount of energy balance. If the user reaches the limits of the energy balance, the user may have some additional balance by purchase the energy balance through the application. Any Energy sale is final without any returns, refills, or account balance topping up with more Energy The button widget was used for this project to control the servo motor. Figure 8 shows the Widget Box of Blynk applications.

Figure 8: Blynk Widget Box

After that, the button that selected from the widget appeared at your project system. Figure 9 below shows the button of from Widget Box.

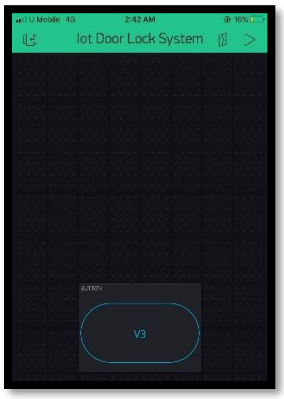

Figure 9: Widget Button

Every new project that been created from the project contain an auth token. This auth token provided for the user to put in their programming to connect the Blynk application with their controller. Auth Token is a unique identifier which is needed to connect your hardware to your smartphone. Every new project you create will have its own Auth Token. Click on devices section and selected required device as show in Figure 10 below.

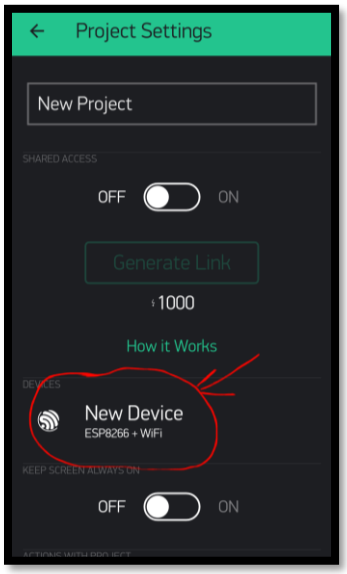

Figure 10: Device Section

After that, the user will get Auth Token automatically on their email after project creation. The user can also copy it manually. Figure 11 shows the Blynk auth token.

Figure 11: Blynk Auth Token

Programming to test run the servo motor can be found through Blynk browser. Through the Blynk browser, they provided variable libraries for the user to run their project. This example shows how value can be pushed from Arduino to the Blynk App Figure 12 below shows the Blynk browser.

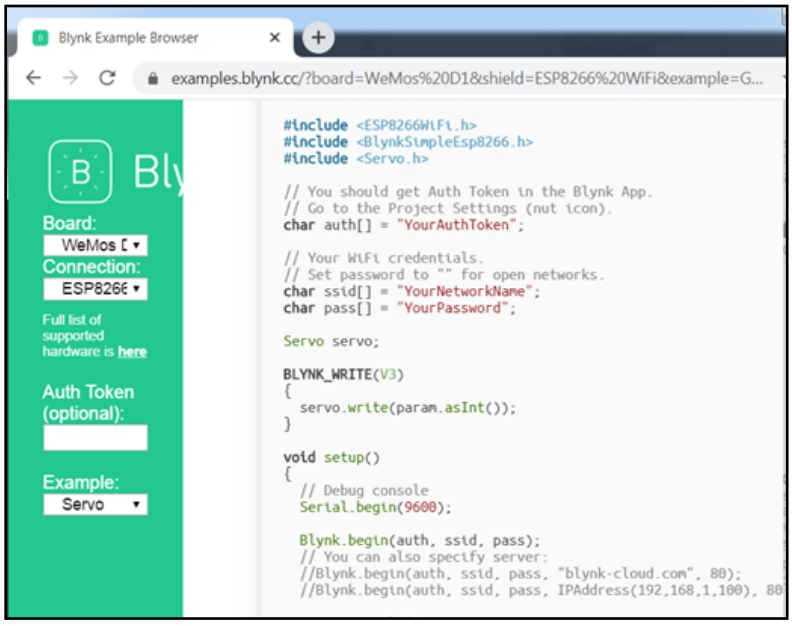

Figure 12: Blynk browser

4.0 RESULTS AND DISCUSSION

The complete hardware setup is shown in Figure 13. The door lock kept inside the door. The door lock has been demonstrated using the servo motor which has been powered here using a 9V battery. The Arduino WeMos is connected to the internet using a hotspot from smartphone. This system run in real time by pressing the button, the door will automatically lock.


Figure 13: Complete Hardware Setup

For the data analysis in this project, the data are obtained by doing a durability test of the system count by 0 until 1000. The condition of durability divided by 5 conditions. The result for this durability was Table 1 shows the condition for durability test.

Table 1: Durability conditions in real time

No.	Type of condition
5	Excellent condition
4	Very good condition
3	Good condition
2	Satisfactory condition
1	Poor condition

Every type of condition state the response reacts of servo motor to carry out the load. It is because the different type of servo motor, the different load servo motor may carry. This test run reacts happen in when the user clicks the button in Blynk app, the servo motor will react to lock or unlock the door.

The excellent condition shows there is no any overshoot during the test and its run-in real time. Next, the very good condition shows that there is a little overshoot which response late 0.5 second in real time. After that, the good condition shows the result overshoot which response late for 1 second in real time. Last but not least, the satisfactory condition shows the result the overshoot which response late for 2 second in real time. Lastly, the poor condition shows the result which response late from 3 to 5 seconds in real time.

At 20th run, the servo motor slowly overshoots because the source supply which is AC/DC Adaptor produce 4.5V for Arduino are not enough to run the servo motor. After replacing the source supply with 9V battery, servo motor start to run constantly until 200th. Below shows the result for durability test count by 0-200 in real time in Figure 14.

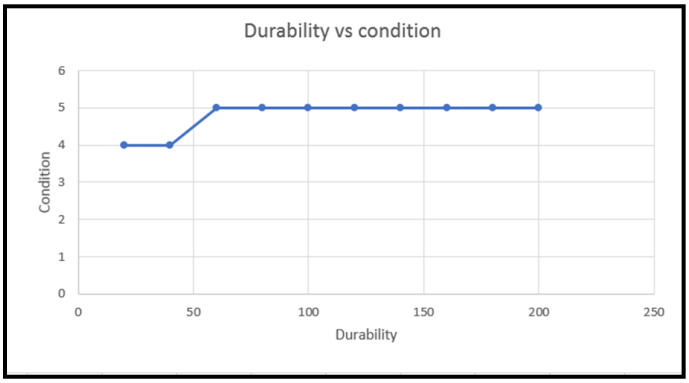

Figure 14: Graph of durability test from 0-200 in real time

Servo motor operate smoothly with Arduino WeMos and Blynk without any overshoots and lagging count by 200 until 400. Below shows the result for durability test count by 200 until 400 in real time in Figure 15.

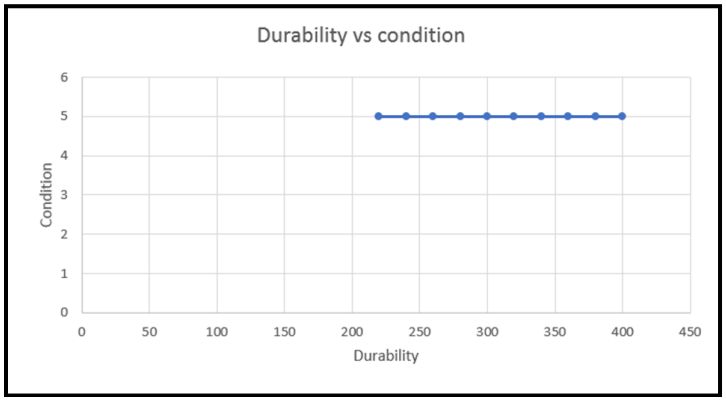

Figure 15: Graph of durability test from 200-400 in real time

Servo motor operate smoothly with Arduino WeMos and Blynk without any overshoots and lagging count by 400 until 600. Below shows the result for durability test count by 400 until 600 in real time in Figure 16.

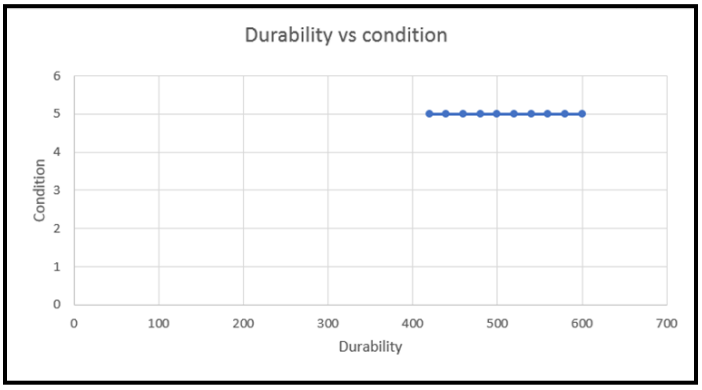

Figure 16: Graph of durability test from 400-600 in real time

Servo motor operate smoothly with Arduino WeMos and Blynk without any overshoots and lagging count by 600 until 1000. Below shows the result for durability test count by 600 until 1000 in real time in Figure 17.

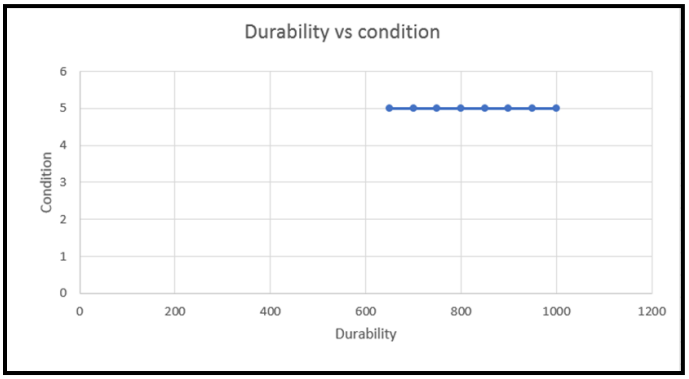

Figure 17: Graph of durability test from 600-1000 in real time

Servo motor operate smoothly with Arduino WeMos and Blynk without any overshoots and lagging count by 600 until 1000. Below shows the result for durability test count by 200 until 400 in real time in Figure 18.

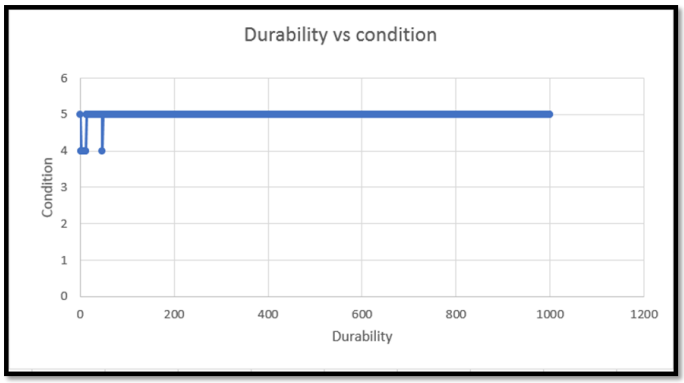

Figure 18: Graph of durability test from 0-1000 in real time

There are lots of servo motors available in the market and each one has its own specialty and applications. Servo motor MG996r that been used is quite strong, and can control them quite precisely. When going to extreme travel, the servo does not overshoot. Every AC servo motor will have their alignment checked and recorded both statically and dynamically before being disassembled. This procedure ensures correct alignment when the servo motor is repaired and rebuilt. Correct servo motor alignment is important as bad alignment will cause the servo motor to not run correctly, if it runs at all. Final servo motor repair testing involves a second round of all the initial tests to ensure the problem is fixed. All servo motors are run on matching factory drives or manufactured drives that have the correct parameters for the servo motor and feedback configuration This servo has been tested by applied a load to run for 20 mins continuously without any overshoot due to load and it works precisely. Figure 19 shows the test run for servo motor

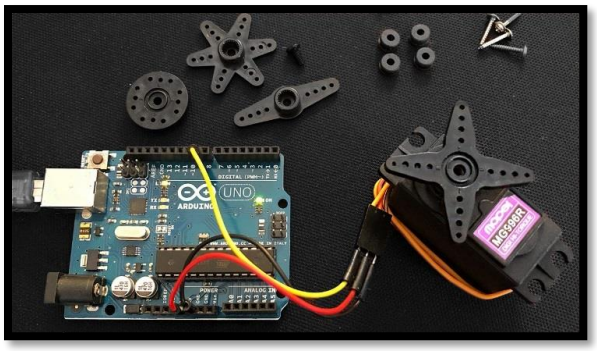

Figure 19: Test run servo motor

By connecting the Blynk with Arduino Wemos, it is constantly can be controlled without overshoot if the source of Arduino Wemos is enough and compatible. The incompatible of source will cause overshoot for servo motor. Figure 20 shows the test run for servo motor through Blynk application.

Figure 20: Test run servo motor through Blynk application

For the test, when the button widget is pressed on the app, the servo turns on and rotates based on a simple servo sweep sketch from the Arduino IDE examples. Once the button is pressed, the servo rotates continuously until the button is in the off position which is when the servo stops. This is done using virtual pins to run a certain type of code (in this case the servo angle code) when the virtual pin is set to a 0°-180°.

5.0 CONCLUSION

This project is developed in purposes the most obvious improvement smart technology delivers to door locks are keyless system that strongly simplify the entry procedures to the point that you need to try and find the best home security system. House keys stand among the most commonly misplaced items. So, it is more convenient, that the user does not have to keep track of yet another key or worry about how to pass off the key to someone else. It ensures the convenient authentication and unlocks, so you don't have to worry about lost or forgotten keys. This project has successfully achieved the objectives. The aim of this project is to build the IoT monitoring system by using Blynk application platform. This project consists of IoT system that was build up using the Arduino Wemos D1, ESP8266 as the microcontroller and the Blynk application as for the monitoring. By doing this project, virtual keys give the user a valuable security option to lock and unlock doors easily via a free app on their Android or Apple device. A single Blynk application is able to control locks and unlocks their door simultaneously. Most importantly this system should be user-friendly and even can be operated by the non-technical person by adapting IoT application towards the system.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the University College TATI for the support.

REFERENCES

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. *ICAC 2017 - 2017 23rd IEEE International Conference on Automation and Computing: Addressing Global Challenges through Automation and Computing*.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). *Smart Locks*.

Hussein, N. A., & Al Mansoori, I. (2017). Smart Door System for Home Security Using Raspberry pi3. *2017 International Conference on Computer and Applications, ICCA 2017*.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*.

Kendall, S. (2011). Developments toward a residential fit-out industry. *Open House International*.

Khodadadi, F., Dastjerdi, A. V., & Buyya, R. (2016). Internet of Things: An overview. In *Internet of Things: Principles and Paradigms*.

Romadhon, A. S. (2018). System Security and Monitoring on Smart Home Using Android. *Journal of Physics: Conference Series*.

Weber, M., & Boban, M. (2016). Security challenges of the internet of things. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings*.

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. *9th International Conference on Computational Intelligence and Security, CIS 2013*.