INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 11, Issue 7, (2021) E-ISSN: 2222-6990

Development of Key Management System 2.0 (KeMas 2.0) using RFID and Biometric Scanner based on Arduino Mega 2560 Pro and NodeMCU

Faizah Amir, Noor Hayati Hamzah, Najmi Hafizi Zabawi

Electrical Engineering Department, Politeknik Sultan Haji Ahmad Shah, Kuantan, Pahang

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v11-i7/10517 DOI:10.6007/IJARBSS/v11-i7/10517

Published Date: 19 July 2021

Abstract

Key Management System 2.0 (KeMas 2.0) is successfully developed in order to overcome lecture room/lab key lost problem and unidentified key user in Electrical Engineering Department, Politeknik Sultan Haji Ahmad Shah (POLISAS), Kuantan, Pahang, Malaysia. This project has been developed in line with industry 4.0 revolution by using internet of thing (IoT) technology. The design of KeMas 2.0 is done using Arduino Mega 2560 Pro as microcontroller and ESP8266 NodeMCU wi-fi module which sends data over the cloud. KeMas 2.0 also utilizes the Telegram chat application bot as notification and monitoring the retrieval and return of the keys. KeMas 2.0 is equipped with two sensors, namely RFID reader and fingerprint scanner as biometric sensor. These two sensors provide an alternative to the users, either to use identification card or fingerprint. Once the user swipes his or her identification card or place fingerprint, the key is allowed to be taken and signal will be sent to Telegram application through mobile phone to notify the name of the person who takes the key and the name of room/lab key that he or she took. Subsequently, when the key is returned, notification will also be sent via Telegram application. Hence, users will always get the latest information on the availability of the keys. KeMas 2.0 is proven to be effective in solving key lost problem in Electrical Engineering Department, Politeknik Sultan Haji Ahmad Shah (POLISAS).

Keywords: IoT, RFID, Biometric Sensor, Arduino, NodeMCU, Bot, Telegram

Introduction

Security has become the primary concerned to most of educational institution nowadays. In addition to providing knowledge and skills to students, educational institution is also responsible for managing high value assets located in its lecture rooms and workshops.

Electrical Engineering Department, POLISAS is equipped with 12 lecture rooms and 22 laboratories/workshops. All the facilities in the workshops, labs and lecture rooms must be kept safely stored. Only authoritative staffs are given the access to use the keys to those rooms. One of the problems that occur is the missing or untraceable key due to human attitude. To trace the missing keys manually has become a real challenge.

In line with the industry 4.0 revolution, IoT technology becomes the top choice to answer the challenge. IoT can be defined as a network of physical objects, devices that contain embedded technology such as intelligent sensors, and controllers which can communicate, sense, or interact with internal or external systems (Vyas, Bhatt & Jha, 2015). KeMas 2.0 is developed based on IoT technology with the objective of providing an effective method of retrieval and return of the keys and to identify the key user in real time.

At the beginning, KeMAs 1.0 was developed whereby user has to use his or her identification card in order to obtain the key. Unfortunately, problem arises when the user does not bring an identification card while getting the key. To overcome this problem, biometric sensor is added to the design. The biometric system is considered as one of the most efficient and trusted security system. Biometric systems by definition is to recognize individuals based on their physiological or behavioral characteristics, such as fingerprints, face, iris, and voice (Kukula & Elliot, 2006). Therefore, KeMas 2.0 is redesigned as an improved version of KeMas 1.0.

Literature Review

This project is developed based on the previous research on smartphone and IoT. The research proves that the application of smartphone has been able to monitor the condition of any situation in real time anywhere and anytime. Smartphones have significant storage and computing capability. This feature makes them ideal candidates to carry out the delicate task of linking the world of the Internet and the world of "things" (Aloi et. al, 2016).

Previous researchers have developed a door locking system that is controlled using the Android App and Bluetooth. Android App is interfaced with door microcontroller through Bluetooth. Bluetooth is convenient and easy to use, but it also has security flaws which make it vulnerable to attacks. There are some tools and techniques that are currently available to attackers to exploit the vulnerabilities in Bluetooth (Cope, Campbell & Hayajneh, 2017).

Another previous project was developed by Nagaraja & Arthi (2017) which is a smart locker equipped with biometric scanner. Whenever the locker has to be opened or closed, the finger- print has to be recognized. If the unknown fingerprint is identified or the locker is under heavy vibration, the GSM module connected to the Arduino will send text message to the owner of the locker which is already fed in the system. This alert message can be sent to one or more mobile numbers.

KeMas 2.0 utilizes Telegram chat application bot as notification and monitoring the retrieval and return of the keys instead of Bluetooth. Bot telegram chat application as a media access smartphone application has advantages compared to using android applications or using web pages because it can be accessed with multi platforms both Android, iOS, Windows, and Linux (Findawati et. al, 2020). Also, this Telegram chat application bot can send notifications via smartphone directly when the sensor in the monitoring system detects keys taken and return.

Methodology

KeMas 2.0 was developed based on PDCA (plan–do–check–adjust) methodology. PDCA is an iterative four-step management method for the control and continuous improvement of processes and products.

Figure 1 shows the block diagram of KeMas 2.0 which consists of the input, controller and the output.

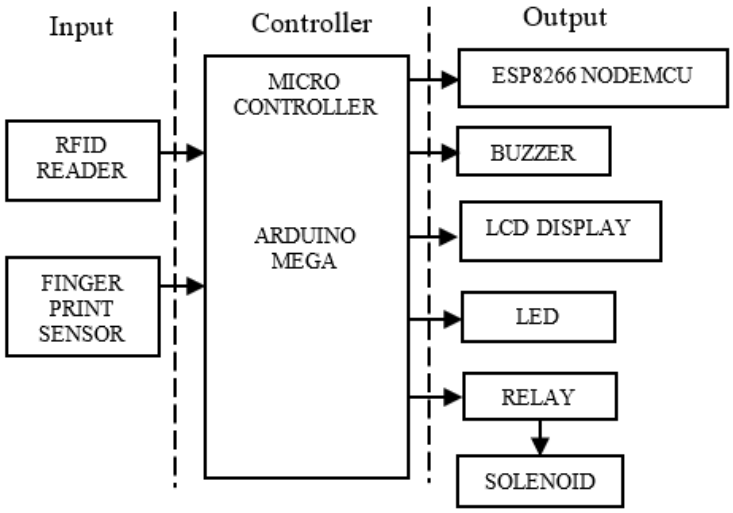

Figure 1. Block Diagram KeMas 2.0

The controller will be programmed using Arduino IDE to process the input signal in order to trigger the output. The function of each block diagram is shown in Table 1.

Table 1
Component Function

No.	Component	Function
1	Microcontroller Arduino Mega	To process the input and gives command to the outputs.
2	RFID Reader	To read the information on the tag and send the information to Arduino to be processed.
3	Fingerprint Sensor	To compare an image of one fingertip and compares it against the data of a previously scanned fingerprint.
4	ESP8266 NodeMCU	The ESP8266 is a microcontroller with Wi-Fi capability. It communicates with the smartphone, sending and receiving text in both directions.
5	Buzzer	To give alarm sound if the key is taken without authority.
6	LED	To indicate that the system is functioning properly.
7	LCD Display	To display the name of the person who takes the key.
8	Relay	To control the on/off path of the solenoid.
9	Solenoid	To open the lock latch when relay is on.

The dimension of KeMas 2.0 is 610mm x 457mm x 203mm. Figure 2 and Figure 3 show the front and side view of KeMas 2.0. The parts of KeMas 2.0 are listed in Table 2.

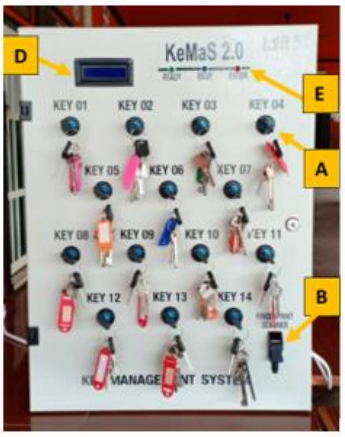

Figure 2. Front View

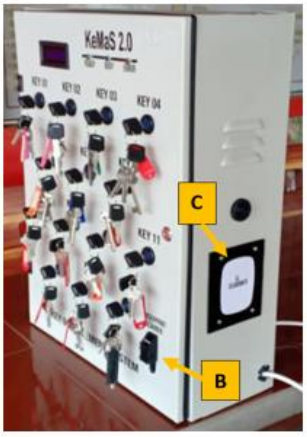

Figure 3. Side View

Table 2
Parts List

Item	Parts
A	Key holding house
B	Fingerprint sensor
C	RFID reader
D	LCD display
E	LED indicator

A flowchart in Figure 4 represents a workflow or process before the program is developed.

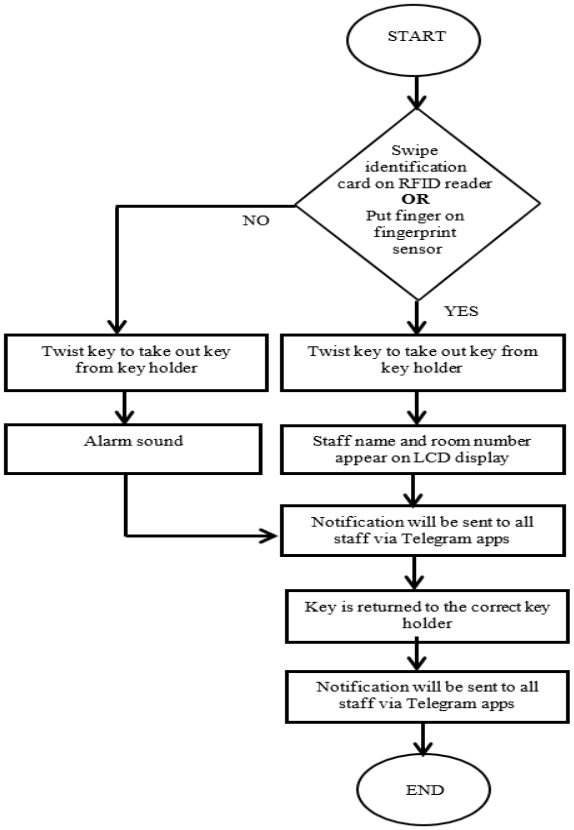

Figure 4. Flowchart of KeMas 2.0

KeMas 2.0 has been undergone a test run for a month to get feedback from 67 staffs and 3 support staffs in Electrical Engineering Department. Figure 5 shows the test run process of KeMas 2.0.

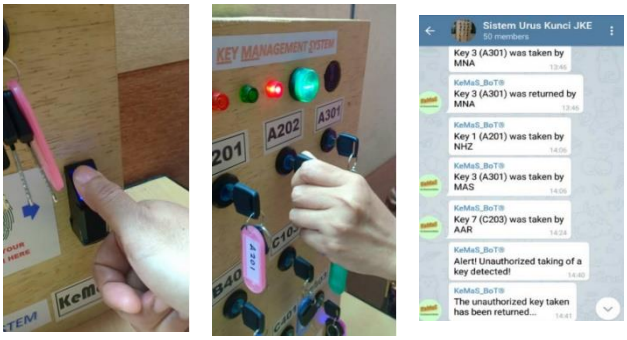

Figure 5. KeMas 2.0 Test Run

A survey has been conducted among the staffs after a month of Kemas 2.0 test run. The result is shown in Figure 6. The result shows that 95% of the staffs are satisfied with Kemas 2.0 performance. Figure 7 shows that the number of complaints regarding key loss is reduced after KeMas 2.0 is applied for two months.

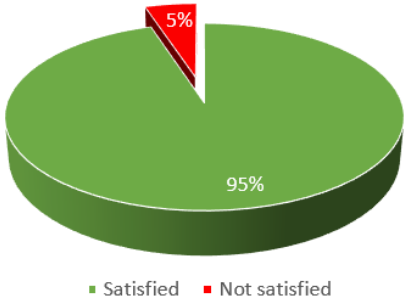

Figure 6. Staffs Satisfaction

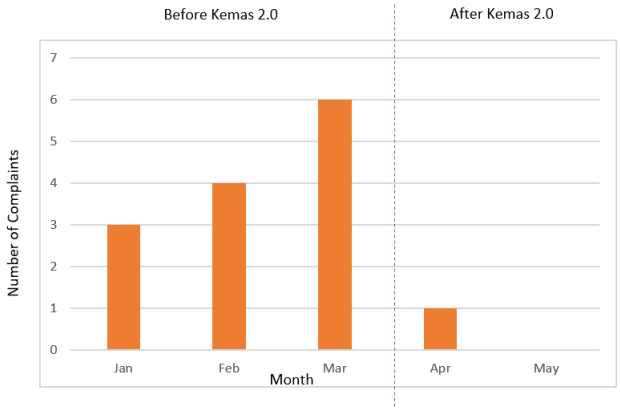

Figure 7. Number of Complaints Before and After KeMas 2.0

Conclusion

KeMaS 2.0 was developed to allow the retrieval and return of keys to be implemented systematically. Users need to register and follow a set of procedures. The user can either scan his or her identification card or fingerprint on the scanner provided. IoT technology is used in the development of KeMaS 2.0 where users can get the latest information about the identity of the person and the key taken and returned through Telegram application.

For future improvement, our team would try to facilitate visual detection system to Kemas 2.0 which can visually record the user who took the key. If in case of unauthorized user takes the key, the visual detection system will record the image of the user and display the image in Telegram application. KeMaS 2.0 has been proven to solve the room/lab key lost problem and unidentified key user in Electrical Engineering Department, Politeknik Sultan Haji Ahmad Shah (POLISAS), Pahang, Malaysia.

References

Aloi, G., Calicuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., & Savaglio, C. (2016). A Mobile Multi-Technology Gateway to Enable IoT Interoperability. *IEEE 7th Annual Computing and Communication Workshop and Conference,* 259-264

Cope, P., Campbell, J., & Hayajneh, T. (2017). An investigation of Bluetooth Security Vulnerabilities. *IEEE 7th Annual Computing and Communication Workshop and Conference,* 1-7

Findawati, Y., Idris, A., Suprianto, Rachmawati, Y., & Suprayitno, E. A. (2020). IoT-Based Smart Home Controller Using NodeMCU Lua V3 Microcontroller and Telegram Chat Application. *IOP Conf. Series: Materials Science and Engineering 874,* 1-5

Kukula, E. P., & Elliott, S. J. (2006). Implementing Ergonomic Principles in a Biometric System: A Look at The Human Biometric Sensor Interaction (HBSI). *40th Annual IEEE International Carnahan Conferences Security Technology,* 86–91

Nagarajan, L., & Arthi, A. (2017). IOT Based Low Cost Smart Locker Security System. *International Journal of Advance Research, Ideas and Innovations in Technology*, *3*(6), 510-515

Vyas, D. A., Bhatt, D., & Jha, D. (2015). IoT: Trends, Challenge & Future Scope. *International Journal of Computer Science (IJCSC), 7*, 186-197.