SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 4, Issue 1, 2019
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

4Door Security System Based on Arduino with Multi-Factor Authentication

John Gabriel G. Rivera, Shunro E. Banayos, Jhonalyn G. Bautista
Don Mariano Marcos Memorial State University
North La Union Campus
College of Information Systems

Abstract *– Security has been playing an essential role, and that is to secure data or materials from unauthorized access. Over the past years, there are a lot of different protocol developed to strengthen security. One of which is the multi-factor authentication which means it involves multiple levels of security so that it cannot be easily breached. This study adopted this concept to secure a hostel door from unauthorized access. This involves different security protocol such as fingerprint scanner and pin code. An SMS notification is also included for additional security. This notification is sent to the hostel caretaker once there is an unauthorized access. This study followed the agile methodology with ISO 9126 - based questionnaire and interview as a mode to gather data. A sample of 18 respondents were used in this study, divided into two categories, 1) Management and 2) Guest/Client. The overall rating of the respondents is Acceptable in terms of its functionality, usability, efficiency, maintainability and portability. The implementation of the device is highly recommended.*

Keywords *– Arduino, Fingerprint Scanner, ISO 9126, Multi-factor authentication, Pin .*

INTRODUCTION

In this present and fast paced world, security is most significant than ever. Every day, people hears about losses occurring due to lack of safety on the bulletin, news or radio. Security also is not just limited to valuable tangible things. It also includes credit card and other important documents. Security has been playing a major role in different places like offices and institutions in order to keep our data confidentially so that no other unauthorized person could have an access on them. Nowadays, at every point of time, every institution needs security systems for protection of valuable data and even money (Shankar, Sastry, Ram, & Vamsidhar, 2015).

Data from FBI 2012 crime report shows that they can expect one in every thirty-six homes in the United States to be burglarized this year, resulting in an average loss of $2,230 per break in totaling $4.7 billion in property losses. These numbers do not account for any additional psychological costs to the homeowners, as burglary victims may subsequently live in fear and harbor feeling of personal violation (D. DeMille, 2019).

Door locks can be opened in a matter of minutes, yet many homeowners still rely upon them to provide a basic level of security. If a break in occurs, those homeowners instead purchase insurance at a reasonable rate to ensure their possessions could be replaced if stolen. Due to the increased risk of customer data being lost, most businesses, however, have stepped up to more aggressive controls (R. Wiedower, 2015).

BPS Residential Hostel is located at Don Mariano Marcos Memorial State University, North La Union Campus, Bacnotan, La Union. The Hostel is open for reservation and walk-in clients who wishes to stay and relax during their free times, and for a place where they can stay whenever they have seminar inside and outside the university. The management is composed only of three personnel that provides everything from maintenance up to the security. The measurement of security in the BPS Residential Hostel is a bit inadequate especially during weekends. They are using traditional lock system or doorknobs. The management allows their clients to bring their room keys whenever they wanted to go outside the vicinity. Their clients have to pay a certain amount in case they lost their room keys. The biggest disadvantage of the traditional lock is that it is not typically as strong as the other types of locks. Even with heavy-duty strength locks, an enterprising and determined burglar could break the lock by putting enough pressure on it. With the lightest locks, a strong hand can do this.

OBJECTIVES OF THE STUDY

The study aimed to design and develop a Door Security System Based on Arduino with Multi-Factor Authentication to help the employee of the BPS Residential Hostel to increase the security through fingerprint scanner, PIN (Personal Identification Number) code and SMS notification.

In addition to the study's objective, the study also aimed to assess the level of acceptability as to functionality, reliability, usability, efficiency, maintainability and portability of the Door Security System based on Arduino with Multi-factor Authentication.

MATERIALS AND METHODS

In this study, the following materials and procedures were used and followed in order to design and develop the Door Security System Based on Arduino with Multi-Factor Authentication:

Software In the development of the device, this study used an Arduino IDE with a version of 1.8.5 and C++ as a programming language. Base on Windows 10 Intel (R) Celeron (R) CPU N3160 @ 1.60GHz (4 CPUs).

Hardware The researcher used Arduino Mega 2560, fingerprint scanner, keypad for the PIN code, jumper wires, push button, solenoid lock, AC (Alternative Current) adapter, 12 volts by 3 ampere battery, RTC (Real Time Clock), LCD (Liquid Crystal Display) screen, GSM Module and power bank. A laptop with a processor of 1.60GHz.

To develop the Door Security System Based on Arduino with Multi-Factor Authentication, the researcher used the Agile Modelling System Development Life Cycle. The researcher undergone its different phases.

Phase I. Requirement Gathering. In this phase, the researchers will conduct a series of interviews to the BPS Residential Hostel Management to collect the necessary information and requirements that are needed in designing and developing the device. For the device that will be used, the researcher will use the Arduino Mega 2560 as the main controller for the system with the help of authentication devices such as fingerprint scanner and Keypad for the PIN code. It will also include the GSM technology for the SMS notification and RTC module for real time update. Multiple fingerprint can be stored in the device if necessary. The notification format will be "*An attempt to enter (room number) has been detected on (Date & Time). An Immediate action is needed. This is an auto generated message. Please do not reply*". The developed device will notify the management and the security personnel when an unauthorized fingerprint and PIN code is detected by the device on the third time of authentication errors. Upon check out of the guests or clients, the management will manually delete the stored fingerprint from the device to avoid storage shortage by using the keypad. In-case of power interruption the developed device may rely to a power bank continue its task.

Phase II. Design & Architecture. In this phase, the researchers will discuss the detailed identification in constructing the device. The researcher also used the use-case diagram and prepared a general design architecture for the device as guide on the structure of the device and to know the roles of each actor.

Phase III. Development & Coding. The researcher designed and developed the device. For the hardware, the researcher will be using Arduino Mega 2560 as the main board to construct the Door Lock Security System Based on Arduino with Multi-Factor Authentication with fingerprint scanner and Keypad along with the GSM module. For the software, this study used the Arduino IDE version 1.8.5 and C++ as programming language.

Phase IV. Quality Assurance & Software Testing. In this phase, the researchers conducted a series of testing to assure that the device is functional for the end-user. The researchers also used a prototype model and a cellular phone number to notify the management and security for the simulation process. A questionnaire based on ISO 9126 were used to evaluate the level of acceptability of the device. Comments and suggestions are analysed, and possibly, included in the final version of the device.

Phase V. Implementation. In this phase, the researchers have deployed the device to the end-user.

Phase VI. Maintenance & Support. In this phase, the researcher trained and gave support to the end user on how to use the developed device. User documentation and user manual was generated to provide information to users on how the device will be operated and maintained.

RESULTS AND DISCUSSION

The prototype of this paper is shown in fig. 1. As displayed in the figure there are 10 parts such as 1) AC Adapter, 2) Keypad, 3) Fingerprint Scanner, 4) LCD Screen, 5) Arduino Mega 2560 board, 6) GSM Module, 7) Solenoid Lock 8) 12 volts by 3 amperes battery 9) Power bank 10) RTC (real time clock). The power sources (part 1, 8, 9) are responsible to provide electricity to the developed device. In case of power interruption (part 9) will provide electricity for the device to work. (Part 8) will provide electricity to the (part 7). The GSM module (part 6) will send notification alert to the management and security personnel with the updated time and date using the (part 10). The keypad and fingerprint scanner (parts 2 and 3) are the access of the guest/client to their designated room. Arduino Mega 2560 (part 5) is the main controller of the developed device. The prototype of the developed device is shown in fig. 2. SMS notification format received by the management and security personnel when 3 consecutive unauthorized attempts have been detected by the developed device shown in fig. 3.

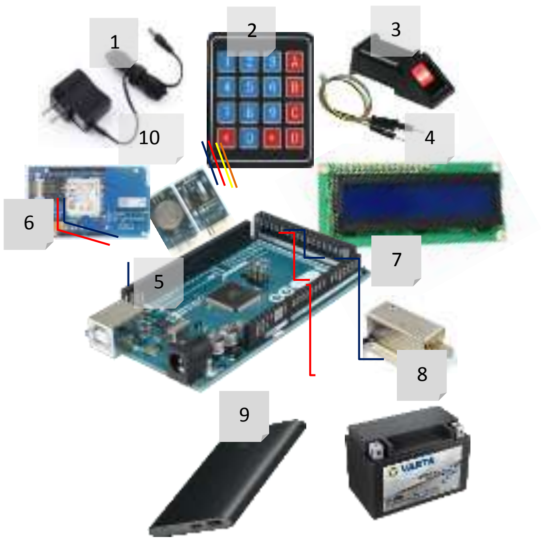


Figure 1. Device Architecture

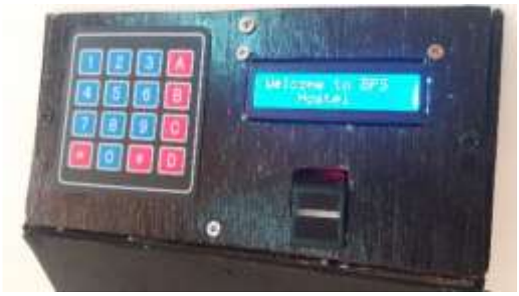
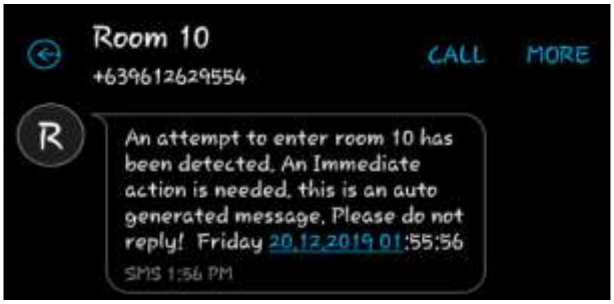


Figure 2. Prototype of the Developed Device



Room 10
+639612629554

An attempt to enter room 10 has been detected. An Immediate action is needed, this is an auto generated message. Please do not reply! Friday 20.12.2019 01:55:56

SMS 1:56 PM

Figure 3. SMS Notification Format

The summary of the evaluation of the management is shown in table 1. As perceived in the table, the respondents believed that the device is acceptable in all categories of the questionnaire with its Reliability as rated highest. This means that the management finds the device reliable and helpful to their units because it handles errors and continues working after any failure. The result of this study of reliability strengthens the reason why physical token device, such as an id card, or a credit card could be stolen by an attacker and the attacker could easily access systems. (C. Cetin 2015).

Table 1. Summary of Evaluation of the Management

Item	Mean	Descriptive Rating
Functionality	4.11	Acceptable
Reliability	4.33	Acceptable
Usability	3.33	Acceptable
Efficiency	3.83	Acceptable
Maintainability	3.33	Acceptable
Portability	3.50	Acceptable

The summary evaluation of the security personals is shown in table 2. As perceived in the table, the respondents believed that the device is acceptable in all categories of the questionnaire with its Usability as rated highest. This means that the device was easy to understand and the users can easily comprehend the device. The result of this study of usability strengthens the reason why the intruders were asked for the reason of using the door; different answers were obtained but all agreed that conventional lock is easy to get around; either by kicking or picking the lock (S. A. Dahe 2015).

Table 2. Summary of Evaluation of the Security Personnel

Item	Mean	Descriptive Rating
Functionality	4.73	Acceptable
Reliability	4.70	Acceptable
Usability	4.93	Acceptable
Efficiency	4.50	Acceptable

The summary evaluation of the guests/client's personals is shown in table 3. As perceived in the table, the respondents believed that the device is acceptable in all categories of the questionnaire with its Functionality and Usability as rated highest. This means that the device performs its task as what it was designed for. It also implies that the device was easy to understand and the users can easily comprehend the device. The result of the study on functionality strengthens why the prevention of unauthorized entry into buildings through the main doors is done by using ordinary, electronically operated locks, digital codes, and biometrics technique like the fingerprint technology or some are based on thumb printing only (P. R. Nehete, et al., 2016). The study of usability strengthens why two-factor authentication adopters found it annoying, but fairly easy to use, and believed it made their accounts more secure; experience often led to positive perceptions, sometimes translating into two-factor authentication adoption for other accounts; and the differences between users required to adopt two-factor authentication and those who adopted voluntarily are smaller than expected (J. Colnago, et al., 2018).

Table 3. Summary of Evaluation of the Guests/Clients

Item	Mean	Descriptive Rating
Functionality	4.93	Acceptable
Reliability	4.90	Acceptable
Usability	4.93	Acceptable
Efficiency	4.90	Acceptable

Conclusion and Recommendation

The results above show that the device is acceptable and can benefit the users from the management, security, and guests of the BPS Residential Hostel. This means that the device can potentially secure the belongings of the guests/clients and the property of the BPS Residential Hostel. Also, the developed device functions as a report generator by the use of the SMS notification function. Future works can include the improvement of the device by incorporating the recommendations of the respondents. Implementation of the device in a national scenario is also highly recommended.

References

Cagri C. (2015). Design, Testing and Implementation of a New Authentication Method Using Multiple Devices. Retrieved from http://scholarcommons.usf.edu/etd/5660

De Mille, D. (2019). Will Your House Be Broken Into this Year? Retrieved from https://www.asecurelife.com/burglary-statistics/

Jessica C., Summer D., Maggie O., Chelse S., Lujo B., Lorrie C., Nicolas C. (2018). It’s not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University. ACM ISBN 978-1-4503-5620-6/18/04.

Pradnya R. N., J. P. Chaudhari, S. R. Pachpande, K. P. Rane (2016). Literature Survey on Door Lock Security Systems. In *International Journal of Computer Applications (0975 – 8887) Volume 153 – No2, 2016* .

Richey, R. C., Klein, J. D., & Nelson, W. A. (2003). *DEVELOPMENTAL RESEARCH: STUDIES OF INSTRUCTIONAL DESIGN AND DEVELOPMENT*.

Shankar, A. A., Sastry, P. R. K., Ram, A. L. V., & Vamsidhar, A. (2015). Finger Print Based Door Locking System. *International Journal Of Engineering And Computer Science*, *4*(3), 10810–10814. Retrieved from www.ijecs.in

Salam, A. D. (2015). Study conceptual design of biometrics technology in door lock. Journal of *Kerbala University* (Vol. 13 No.3) *Scientifi*c.