Available *online* at : http://jitce.fti.unand.ac.id/
JITCE (Journal of Information Technology and Computer Engineering)
| ISSN (Online) 2599-1663 |

Two Sequential Authentication Method on Locker Security System Using Open-Sourced Smartphone.

Dodon Yendri, Mohammad Hafiz Hersyah ,Yulivia Dyan Sakinah

Jurusan Sistem Komputer, Fakultas Teknologi Informasi, Universitas Andalas, Padang, 25163

ARTICLE INFORMATION

Received: August 8th, 2019
Revised: September 15th, 2019
Available online: September 30th, 2019

KEYWORDS

Security, Locker, Two-Ways Authentication, *Smartphone, Personal Identification Number*

CORRESPONDENCE

Phone: +62 81374538790
E-mail: dodon@fti.unand.ac.id

A B S T R A C T

Lockers are commonly used to store luggages temporarly. For security purposes, lockers are equipped with conventional lock keys to keep it safe. In order to enhance the security aspects, there are several options by optimalizing current emerging technology that is two-factors authentication. This method is commencing by inputting some PIN (Personal Identification Numbers) code then it would trigger confirmation access by smartphone to unlock the lockers. By having this security schemes, any unauthorized users could not allowed any attempt to unseal the locker. More over, the owner could immediately recognize if there was any suspicious access. The result of this research shows that the system could unlock the locker by inputting the correct PIN and verified access by achieving the successful percentage of 100%. The averages response time is around 6.647 seconds, while any attempt to unlock the locker by inputting the incorrect access gain 100% percentages.

INTRODUCTION

At the visiting time, locker is a temporary storage of goods that are usually provided in tourist attractions, libraries, schools, colleges, sports venues and other public places. The current locker security system still uses conventional keys which are deemed ineffective to guarantee the safety of the items inside. With this security allows lockers easily broken into without the knowledge of their owners.

Nowadays science and technology are developing very rapidly. The application of security technology by combining electronic devices and computers and wireless communication is very possible to be able to provide a better level of security. Two-factor authentication method (two-factor authentication) which is usually used in account protection has the next higher level of security. Two-factor authentication is an authentication method using two of three factors to determine the user's identity. Three factors that are commonly found are "something that is known to the user", "something that the user has", and "something that is in the user" [1].

In previous studies, the locker security system has been modified for enhancing better security. The first study was securing lockers using passwords [2]. The second study securing lockers using android-based voice recognition method [3]. Whereas the third study used fingerprints to open locker doors [4]. The three studies only use one factor to secure lockers so that the level of security is still not strong. This study aims to improve locker security with a two-factor authentication method. In addition to protecting it with a password, the system will also perform a second authentication to ensure that authorize users are able to access the locker.

THEORITICAL BACKGROUND

Locker

Lockers are usually form in small cabinets that are usually used as temporary storage. Lockers are designed to provide efficient storage. Usually lockers are used in offices, sports venues, tourist attractions, and schools and colleges.

Arduino Mega

Arduino Mega is a microcontroller based on ATMega 2560 microcontroller which can be used to realize electronic circuits. With the addition of certain components, Arduino Mega can be used for remote control and control via wireless communication, as is widely used in IoT systems on various topics [5].

Matrix Keypad

This keypad is a electronic device that is used as input is a series of buttons arranged in a matrix called a matrix keypad. Each button on the keypad has a switch below it. And every switch in the row is connected, so is the switch in the column. However, row and column pins are not connected, if the button is pressed then the row and column pin switches will be connected [6].

Liquid Crystal Display

Liquid Crystal Display (LCD) is a type of electronic media that uses liquid crystal as the main viewer. The LCD screen uses two

https://doi.org/ 10.25077/jitce.3.02.65-69.2019

sheets of material that can polarize the liquid liquid between the two sheets. Electric current passing through the liquid causes the crystal to be evenly distributed so that light cannot pass through each crystal and can change the shape of the liquid crystal into the display of numbers or letters on the screen [7].

Solenoid Door Lock

Solenoid door lock is an electronic component that is used as a door lock. Solenoid will work if given a voltage. Inside the solenoid there is a wire coiled at the iron core. When an electric current flows through a wire, a magnetic field occurs to produce energy that will pull the iron core inside. Conversely, if not given an electric current, the energy from the magnetic field will be lost and the iron core returns to its initial position [8].

ESP8266 Module

ESP8266 is a Wi-Fi module that functions as a microcontroller enhancement to be able to connect to Wi-Fi. This module operates at a voltage of 3.3V. In general, ESP8266 is programmed via AT Command via UART communication serials and uses the Arduino IDE by adding the ESP8266 library [9].

ThingSpeak Server

ThingSpeak is a web service platform that can be used to collect, store and receive data using the HTTP protocol via the internet. ThingSpeak can be used as a sensor data application, location tracking, and others. Data can be sent from or to microcontroller hardware such as Arduino, Raspberry Pi and others. The main elements in ThingSpeak activity are channels that contain data fields, location fields, and status fields [10].

Two-Factor Authentication Method

Two-factor authentication is an authentication method that aims to verify a person's identity, whether the person is legitimate to access something. In general, the two-factor authentication method is used at login or access request. This method uses two of three factors. According to Fred B. Schneider, the factors used in authentication are something the user knows, something the user has, and something in the user [1].

Android

Android is a Linux-based mobile operating system that has been modified. Android provides an open platform and is open source, making it easier for developers to create their applications [11]. Android SDK is an API tool that is used to develop applications on the Android platform using the Java programming language [12].

SYSTEM DESIGN

General System Design

The general design of a locker security system with a two-factor authentication method (two-factor authentication) can be used as multiple security. Dual security is done by entering the code in the form of a PIN on the locker and confirm access using a smartphone to open the locker. The general design of a locker security system with a two-factor authentication method can be seen in Figure 1 below:

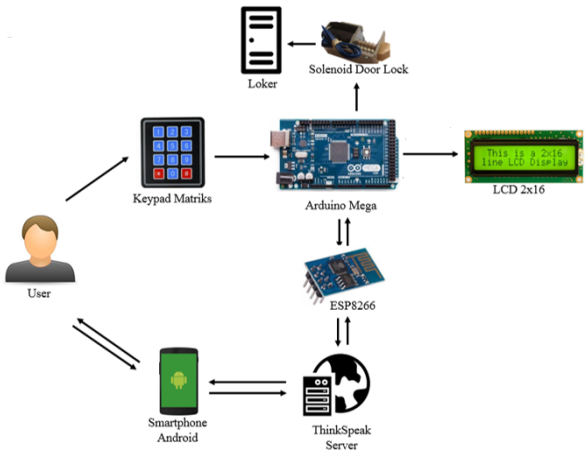
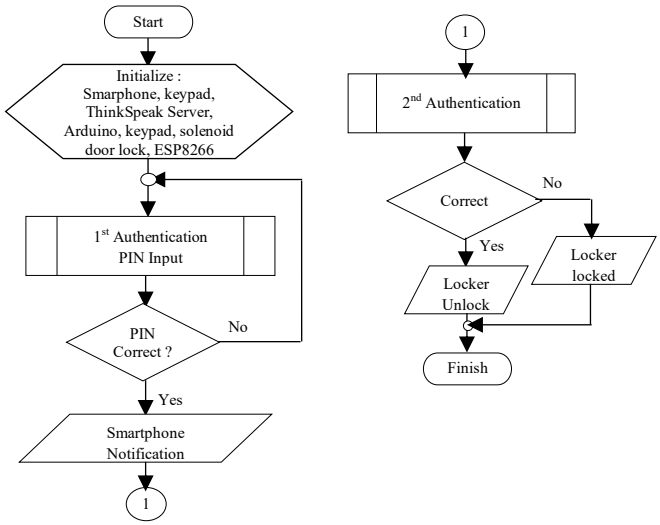


Figure 1. General System Design

Based on Figure 2 it can be explained that the user's locker and smartphone must be connected to the internet network and the Android application in order to check the telephone number on the system. Then the user enters the code or PIN on the keypad in the locker. The system will check, if the PIN entered is incorrect then the locker will not open. Conversely, if the PIN entered is correct, then Arduino will send data to the server and be forwarded to the smartphone. The smartphone receives a notification to confirm the user based on the PIN entered on the locker. The locker will open if the user has verified or agreed.

Software Design

The software is designed to regulate the workings of systems controlled by the microcontroller as the brain of the system. The system works starting with activating the application on the user's smartphone, entering the PIN on the keypad, authenticating and verifying the user's validity on the smartphone. Flowchart locker



security system with two-factor authentication method can be seen in Figure 2, Figure 3 and Figure 4.

Figure 2. Overall Flowchart Design

Figure 2 shows that the system starts by initializing the components used in the system. When the user opens the android application on the smartphone, the application will connect to the server. The system invokes the first authentication function to enter the PIN code on the keypad. Furthermore, authentication is performed, if the PIN code entered is appropriate then the system will send a notification to confirm to the android smartphone via the ThingSpeak server, if not the user is asked to repeat the first authentication again.

https://doi.org/ 10.25077/jitce.3.02.65-69.2019

When the first authentication is correct, the user is confronted with the second authentication by verifying the phone number and asking the owner of the locker for approval on the smartphone. If the second authentication is approved, the locker will open and the process is complete. Conversely, if not approved, the locker will not be opened.

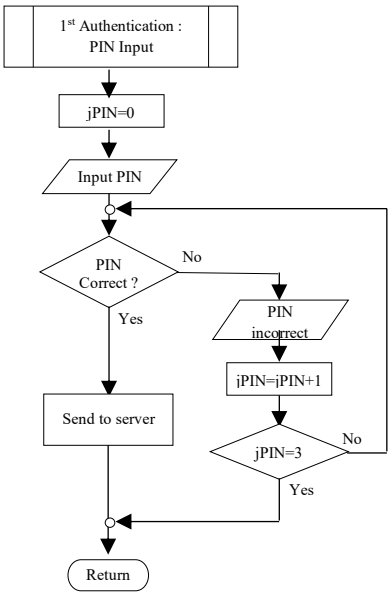


Figure 3. First Authentication Flowchart

In figure 3 the first authentication flowchart explains that the user is asked to enter the PIN code. Each PIN code entered will be checked for correctness, if the PIN entered is correct then the system will send authentication to the server, but if it is wrong the system will calculate an error entering the PIN. Users are given three times opportunity in a row to enter a PIN.

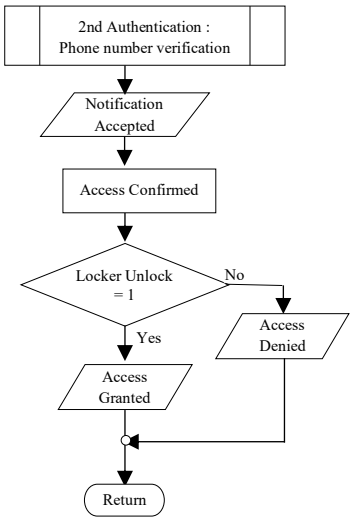


Figure 4. Second Authentication Flowchart

Figure 4 The second authentication flowchart depicts that the authentication is executed to verify the telephone number and request for access confirmation to open the locker. If the owner approves, then access is accepted and the locker will open, but if reverse, then access is denied and the locker will not be unlock.

RESULTS

System Implementation

Lockers made with iron plate with a size of 35x35x35 cm. In this locker installed several hardware components such as keypad, arduino mega, ESP8266 module, LCD, adapter, relay, and door lock solenoid. Hardware system implementation can be seen in Figure 5 below.

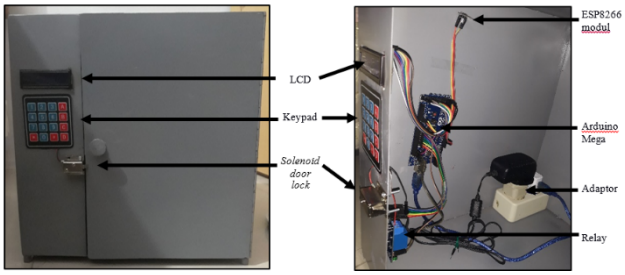


Figure 5. Hardware Implementation

Keypads are used as PIN input media, LCD 2x16 as information display media, Solenoid door lock as locker door lock, ESP8266 module as wi-fi module to connect the microcontroller to the internet network. Arduino Mega as a microcontroller to control the system, Adapter as a power supply, 1-channel Relay as a switch to set the Solenoid door lock which is controlled by a microcontroller.

Besides hardware, the locker security system with two-factor authentication method has software in the form of an android application. Android application is built as a regulator of the system that will be used and confirm access to the owner who will give permission to open the locker. When the PIN code entered is correct, the notification and access approval will appear on the owner's smartphone. Figure 6 shows the notification received and figure 7 confirming user access on the smartphone.

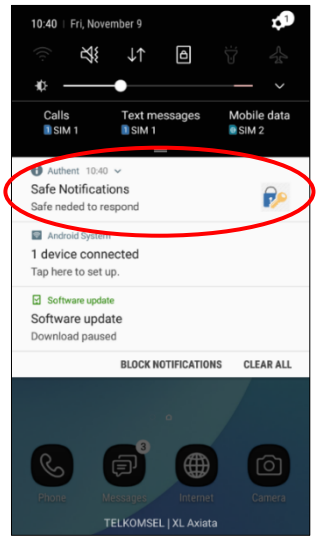


Figure 6. Security Notification

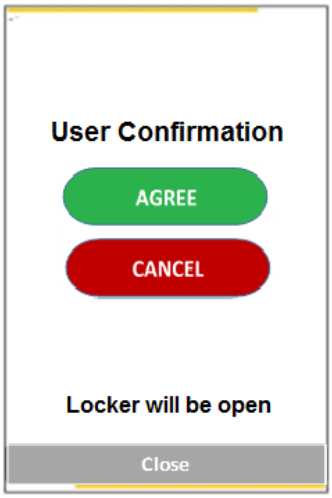


Figure 7. Security Confirmation

There are three confirmation display functions, namely 'Agree' as a key to open the locker, 'Cancel' to refuse to open the locker and 'Close' to close the android application.

System Testing

Signal Strength Testing

This test is conducted to determine the performance of the locker security system when the internet network conditions are different. dBm or decibel-milliwatt is a unit to measure the signal strength received by a smartphone from the nearest BTS (Base Transceiver Station) operator. The test is carried out by the same operator on three types of internet networks namely 4G LTE, HSPA + or H + and UMTS, known as 3G. The test parameter for response time is how long the smartphone receives a notification that starts when the user enters the PIN code on the keypad. The test results can be seen in the following Table 1.

Table 1. Signal Strength Result

No.	Type of Network	dBm	Response
1	4G LTE	- 87	4,45
2	4G LTE	-94	6,59
3	4G LTE	-103	5,73
4	4G LTE	-119	11,27
5	HSPA+	-91	8,67
6	HSPA+	-95	11,76
7	HSPA+	-95	-
8	UMTS	-93	13,78
9	UMTS	-93	16,03
10	UMTS	-99	-

Based on Table 1 it can be seen that the greater the dBm value, the faster the smartphone receives notification. On HSPA + and UMTS networks there is a dBm value but smartphones do not receive notifications, while on 4G LTE networks smartphones always receive notifications. Thus it can be said that the 4G LTE network is more stable compared to the HSPA + and UMTS networks.

Relay Solenoid Lock Testing

Solenoid lock testing is carried out to determine whether the door lock solenoid can work well when connected to Arduino. Door lock solenoid will work if given a voltage of 12 volts. When there is no voltage, the condition of the door lock solenoid is closed / locked and will open when there is voltage. The solenoid is connected to the relay so that it can work at the 5 volt voltage released by the arduino foot pin. This solenoid test is carried out by programmatically giving high (active) and low (inactive) input signals to the Arduino pin. The test results can be seen in Table 2.

Table 2. Relay and Solenoid Door Lock Testing Result

No	Input Signal	Relay	Solenoid Lock Condition	Status
1	HIGH	Active	Iron Core Not Pulled	Locked
2	LOW	Inactive	Iron Core Pulled Inside	Open
3	HIGH	Active	Iron Core Not Pulled	Locked
4	LOW	Inactive	Iron Core Pulled Inside	Open
5	HIGH	Active	Iron Core Not Pulled	Locked
6	LOW	Inactive	Iron Core Pulled Inside	Open
7	HIGH	Active	Iron Core Not Pulled	Locked
8	LOW	Inactive	Iron Core Pulled Inside	Open
9	HIGH	Active	Iron Core Not Pulled	Locked
10	LOW	Inactive	Iron Core Pulled Inside	Open

From the overall ten tests in Table 2 by giving high and low input signals on the Arduino pin with each of the five tests alternately, a percentage of success was obtained at 100%.

Locker Timing Response and User Confirmation Granted Testing.

This testing plan objective is to open the locker using a correct PIN code. Lockers can be opened if the PIN code entered on the keypad is correct and access is approved by a valid telephone number. The response time is calculated starting from the user pressing the PIN code until the solenoid / locker is open. Table 3 shows the test results opened 10 times with response time as follows.

Table 3. Correct PIN Input and Access Granted Testing Result

No	Smartphone Notification	LCD Result	Locker Condition	Time Response
1	Received	Access Granted	Opened	5.38
2	Received	Access Granted	Opened	7.90
3	Received	Access Granted	Opened	8.93
4	Received	Access Granted	Opened	5.74
5	Received	Access Granted	Opened	8.26
6	Received	Access Granted	Opened	4.79
7	Received	Access Granted	Opened	3.85
8	Received	Access Granted	Opened	7.00
9	Received	Access Granted	Opened	8.72
10	Received	Access Granted	Opened	5.90
Total				66.47

In table 3 above, it appears that out of ten tests to open a locker with the correct PIN code and access approved, all notifications are received by a smartphone, information on the LCD appears and the locker is open. This shows that the system is able to work 100% with an average response time of 66.47 / 10 = 6,647 seconds.

https://doi.org/ 10.25077/jitce.3.02.65-69.2019

Locker Timing Response and User Confirmation Rejected Testing.

This testing condition is carried out 10 times in a row. The test results are shown by displaying information notification "Access denied" on the LCD. The average response time needed to display information from inputting the PIN code until the notification appears as table 4 below.

Table 4. Correct PIN and Access Rejected Testing Result

No	Smartphone Notification	LCD Result	Locker Condition	Time Response
1	Received	Access Rejected	Locked	3.55
2	Received	Access Rejected	Locked	5.58
3	Received	Access Rejected	Locked	5.71
4	Received	Access Rejected	Locked	6.29
5	Received	Access Rejected	Locked	5.94
6	Received	Access Rejected	Locked	5.76
7	Received	Access Rejected	Locked	3.07
8	Received	Access Rejected	Locked	5.99
9	Received	Access Rejected	Locked	8.43
10	Received	Access Rejected	Locked	5.47
Total				55.79

Based on table 4 it can be seen that the ten tests opened the locker with the correct PIN code and access was denied / canceled, all notifications entered on the smartphone, information on the LCD appeared and the locker was locked. This proves that the system can provide security to lockers from unauthorized users. Thus it can be said that the system successfully maintains the security of the locker 100% of the access that is denied / canceled. The average response time required from the PIN code is inputted on the keypad until the notification 'Access is denied' on the LCD is 55.79 / 10 = 5,579 seconds.

Buffer Overflow Testing

Buffer overflow is a condition that occurs when there is excessive input on a program so that it is overloaded and memory cannot allocate it.

This test aims to determine whether there is a gap to open the locker without confirmation on the smartphone. Testing will be done by entering a PIN with a length of more than 8 characters to more than 255 characters. The system must be able to ensure that the PIN code entered is incorrect. There is no buffer overflow in this security system because the system stores PINs using string data. The string data type dynamically allocates memory where it can still store data as long as there is space left to store it.

Table 5. Buffer Overflow Testing Result

Testing	PIN length Inputted	LCD Output
1	11 Character	Wrong PIN !
2	16 Character	Wrong PIN !
3	32 Character	Wrong PIN !
4	40 Character	Wrong PIN !
5	48 Character	Wrong PIN !
6	54 Character	Wrong PIN !
7	More than 255 Character	Wrong PIN !

CONCLUSION

Based on the research that has been done, the following conclusions are obtained:

1. The locker security application system can open the locker if the PIN code entered is correct and the user's access confirmation is approved by a valid phone number.
2. The success rate of the locker security application system to open the locker is 100% with an average response time of 6,647 seconds.
3. The system can provide security to lockers from unauthorized users with a 100% success rate.

REFERENCES

[1] Schneider, B.F. *Something You Know, Have or Are*. https://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html, diakses pada 28/9/2017 pukul 8:12.

[2] Prawiroredjo, Kiki., dkk. 2016. *Locker Dengan Pengamanan Kata Kunci Berbasis Mikrokontroler*. Jurnal JETri Volume 13 Nomor 2 – Februari 2016 Hal 29 - 42.

[3] Triyono. 2017. *Rancang Bangun Loker Penyimpanan Aset Menggunakan Voice Berbasis Arduino Uno pada Dinas Marga dan Pengairan Kabupaten Tanggerang*. Jurnal IJCCS Volume 1 – November 2017 Hal 283 – 287.

[4] Herwandi. 2017. *Rancang Bangun Sistem Keamanan Loker dengan Menggunakan Fingerprint*. Jurnal Eltek Vol.15 No.1 Hal 59-70 – Oktober 2017.

[5] Marza, I. (2019, March 29). Pembuatan Alat Tracking Artefak pada Museum Menggunakan Modul GSM Berbasis Mikrokontroler dan Short Massage System. *Journal of Information Technology and Computer Engineering*, *3*(01), 18-24.

[6] Parallax Inc. *Datasheet 4x4 Matrix Membrane Keypad*. https://www.parallax.com/sites/default/files/downloads/27899-4x4-Matrix-Membrane-Keypad-v1.2.pdf. Diakses pada 27/02/2018 pukul 14:04.

[7] Parallax Inc. *Datasheet Parallax Serial LCD*. https://www.parallax.com/sites/default/files/downloads/27979-Parallax-Serial-LCDs-Product-Guide-v3.1.pdf. Diakses pada 27/02/2018 pukul 14:07.

[8] Shandy, Yan Detha., dkk. 2015. *Implementasi Sistem Kunci Pintu Otomatis Untuk Smart Home Menggunakan SMS Gateway*. Jurnal e-Proceeding of Engineering Vol.2, No.2 Agustus 2015.

[9] WiFi Module ESP8266 Datasheet. Sparkfun Electronics. www.sparkfun.com. Diakses pada 20/07/2018 pukul 13.54.

[10] ThingSpeak. http://www.mathworks.com/help/thingspeak/. Diakses pada 27/10/2018 pukul 12:32.

[11] Yendri, D., & Putri, R. (2018, March 29). Sistem Pengontrolan Dan Keamanan Rumah Pintar (Smart Home) Berbasis Android. *Journal of Information Technology and Computer Engineering*, *2*(01), 1-6.

[12] Suprianto, Dodit. 2012. *Pemrograman Aplikasi Android*. Jakarta: MediaKom.