Motorcycle Secondary Authentication System Using Arduino-Based HC-05 and SIM800l Module

by Nenny Anggraini

Submission date: 31-Jan-2021 12:37PM (UTC+0700)
Submission ID: 1497998703
File name: 09268891.pdf (1.05M)
Word count: 4961
Character count: 25154

Motorcycle Secondary Authentication System Using Arduino-Based HC-05 and SIM800l Module

1st Nenny Anggraini
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta, Indonesia
Nenny.anggraini@uinjkt.ac.id

2nd Imam Marzuki Shofi
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta, Indonesia
imam@uinjkt.ac.id

3rd Mahfudz Nurzamzami
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta, Indonesia
mahfudz.nurzamzami15@mhs.uinjkt.ac.id

4th Nashrul Hakiem
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta, Indonesia
hakiem@uinjkt.ac.id

5th Feri Fahrianto
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta, Indonesia
feri.fahrianto@uinjkt.ac.id

6th Tubah Rosyadi
Informatic Engineering
State Islamic Syarif Hidayatullah
Jakarta, Indonesia
tubah.rosyadi@uinjkt.ac.id

***Abstract*—Motorcycles are still the dominant means of transportation in Indonesia, marked by the number of motorcycle sales in 2018 reaching 6.3 million units. One problem that motorcycle users do not want is the loss of keys. Therefore in this study will create a motorcycle secondary authentication system with the Product Development Lifecycle method, by using the SA-RT (Situation Awareness Rating Technique) method to the analysis of functional system requirements, this research stated the authentication system is operated from an android application that is connected to an Arduino device on a motorcycle via Bluetooth and SMS. Passwords are sent through the Android application to the Arduino microcontroller to turn on or turn off the electricity on the motorcycle. The maximum distance of a Bluetooth connection on this system is 5 m, the average Bluetooth authentication response time is 344 ms, the average SMS authentication process time is 249 ms, and the suitability of the function is 100%. The results obtained show that the proposed method can be an alternative solution for motorcycle security and motorcycle secondary authentication system.**

Keywords—GSM, Motorcycle, Authentication, Bluetooth, Arduino.

I. Introduction

Every year, the number of motorbikes circulating in the community continues to grow. Judging from the sales data released by the Indonesian Motorcycle Industry Association (AISI), in 2018 motorcycles sold in Indonesia totalled 6,383,108 units. This shows that motorbikes are still the transportation of choice for residents in Indonesia [1]

Generally, motorcycles circulating in Indonesia still use conventional ignition keys which must be inserted in the vehicle keyhole. Until February 2019, there are still many motorbikes produced by carrying these features. One of them is Honda, the manufacturer that contributed the most sales throughout 2018 has 17 variants of motorcycles that use conventional keys. Honda itself managed to achieve total sales during 2018 of 4,759,202 units or controlled 74.6 percent of the market share [1]

Events that often occur when using a motorcycle is the loss of vehicle keys. This incident can happen to anyone and anywhere. Evidenced by the results of a survey conducted by the author of 100 motorbike riders in Jabodetabek with ages 20 to 50 years. From this survey, it can be concluded that 73% of motorcycle riders have lost their vehicle keys and 95% of motorcycle riders think that losing their motorcycle keys interferes with their activities. Based on the results of a survey conducted by researchers, there are three solutions that are mostly done by people who lost their vehicle keys. First, the owner takes his vehicle to a duplicate key service to make a key that is suitable for his vehicle. The second solution, the owner takes his vehicle to a garage to replace the set key. The third solution, the vehicle owner takes the spare key provided by the seller when purchasing a vehicle.

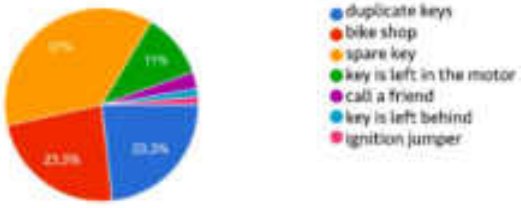

Fig. 1. Key lost solution

Based on the graph above, it can be seen that the solution is most often done when a key is lost is "taking a backup key". When purchasing a new motor vehicle, the seller will provide two keys with the aim of overcoming this problem. But the owner still has to spend more effort to take it to the place where the key is stored. The most commonplace is at home. In another case, if the loss case has happened twice; in other words, there is no other backup key. Then the solution does not apply. The owner must bring his vehicle to a duplicate key or repair shop and must pay a set key replacement fee of Rp 150,000 to Rp 300,000 according to the type of motorbike.

Based on this, additional authentication features are needed on motorbikes. One of the authentication methods commonly used today is a password. Unwittingly a password has an important role in securing personal information. In some applications related to devices such as cell phones, ATM cards, safe deposit boxes, lockers, etc., there is also a security system whose function is similar to a password, commonly known as a PIN code [2]. Based on the background description described above, the researcher wants to develop a motorcycle authentication system that adapts several modules and methods from previous studies, namely the

authentication system using a password that is connected to the android application via Bluetooth and gsm modules.

II. Literature Review

Tombeng [3]. This research authentication system is intended to reduce the risk of motorcycle theft. The conventional motorcycle lock system is connected in parallel with the RFID and password-based authentication system. So that the password in the form of numbers can be entered via the keypad that serves to turn on the motorcycle. Pratama & Rakhmadi [4], successfully used the SIM800L module and the Force Sensitive Resistor sensor to create a motorcycle safety system. The system can receive commands via incoming SMS from the SIM800L module, while it can send SMS notifications to the user's telephone number when there is an indication of motorcycle theft installed by the system. This system is installed in series between the ignition key and the motorcycle's electricity so that it can disconnect the motorcycle when receiving commands via SMS. Muthumari, 2018 [5], Create an automatic door opening system that is controlled via an Android application that is connected to the HC-05 Bluetooth module. This system will provide users with camera-recorded images via Wi-Fi. So users can see who the people who come to visit through the application. When the user is pleased, the door lock can be opened remotely via a Bluetooth connection between the smartphone and the prototype of the device. In this research there are improvements both in technology and feasibility, namely using Bluetooth technology and combined with SMS, so that it does not have an effect on signal capture distance, besides that it will be equipped with an Android application that makes it easier for users to control and monitor.

TABLE I. LITERATURE REVIEW COMPARISON

NO	Research	Technology	Interface	SMS Notification	Object
1	Tombeng et al.[4],	RFID	No	No	motorcycle
2	Pratama & Rakhmadi [5]	Force Sensitive Resistor sensor & SIM800L	No	Yes	motorcycle
3	Muthumari (2018 [6]	Wi-fi & Bluetooth	Androis	No	House Door
4	This Research	Bluetooth & SIM800L	Android	Yes	Motorcycle socket key & ignition

III. Theoretical Basis

A. Arduino Uno

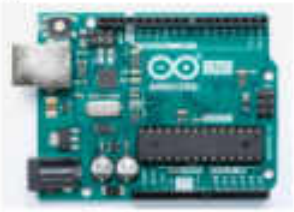

Fig. 2. Arduino Uno

Arduino is an open-source physical computing media where Arduino has simple input/output (I / O) that can be controlled using a programming language. Arduino can be connected to devices like a computer. The programming language used in Arduino is a C programming language that has been simplified with features in the library [6].

B. HC-05

Fig. 3. Bluetooth HC-05

Bluetooth HC-05 is a Bluetooth SPP (Serial Port Protocol) module that is easy to use for wireless serial communication that converts serial ports to Bluetooth. HC05 uses a 3 Mbps Bluetooth V2.0 + EDR (Enhanced Data Rate) modulation using 2.4 GHz radio waves. In use, HC-05 can operate without using special drivers [7].

C. SIM800L

The SIM800L module already has a Quadband feature, meaning that the module can operate on four frequencies, namely 850, 900, 1800, and 1900 MHz. The "auto" baud rate configuration makes the SIM800L module able to adjust the baud rate according to that applied to Arduino[8]. Another factor which is the reason for the use of SIM800L on this system is a consideration in terms of size. The device that is made will be placed on a motorcycle with limited storage space, so small components are needed so that the final result of the device is concise. [7].

Fig. 4. SIM800L Comparation

The picture is a comparison of the sizes of the SIM800L and SIM900A modules. It appears that the size of the SIM800L is smaller than the size of the SIM900A, so to make a concise system the researchers used the SIM800L as a gsm module embedded in the motorcycle secondary authentication system.

IV. Analysis and System Design

This stage contains an analysis of the functional requirements of the system using the SA-RT method. Situational Awareness (SA) is knowledge relevant to the task being performed [8]. It is a critical component of decision making and has been included in several models of decision making. SA has three levels: Level 1, perception of the elements in the environment; Level 2, comprehension of the current situation; and Level 3, projection of future status [2].

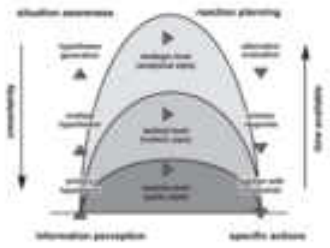

Fig. 5. Decision making under uncertainty and time pressure [2]

The need for the primary function of this secondary authentication system is presented in Data Flow Diagrams (DFD) and Control Flow Diagrams (CFD) [9].

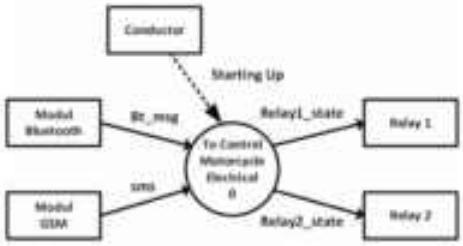

Fig. 6. Contex Diagram/DFD Level 0

Figure 7 below shows the level 1 Data Flow Diagram (DFD) of the secondary authentication system. The data processing in this system is divided into two according to the source of data entry. In the input system of each input, data will go through several processes to finally produce an output in the form of a relay status. [10].

Conducted in developing sophisticated security methods with authentication mechanisms placed in the front line of defence. Since these mechanisms are based on user conduct, they may not accomplish the intended objectives with improper use. Despite the influence of usability, little research has been focused on the balance between usability and security in authentication mechanisms when evaluating the effectiveness of these systems [11].

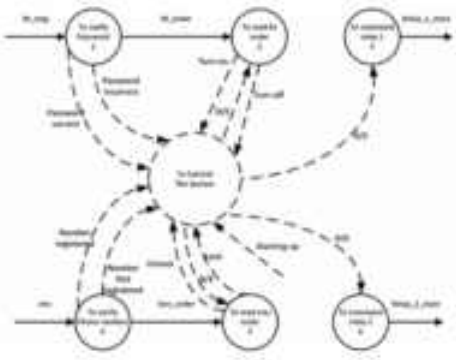

Fig. 7. Diagram/DFD Level 1 "Authentication System"

Figure 7 shows the needs of the main functions of the gender authentication system in the form of a combination of Data Flow Diagrams (DFD) and Control Flow Diagrams (CFD) level 1. From the picture shows that to be able to control the relay, input data must go through several processes, namely: (1) Password Verification Process, used to verify the password sent, if it is not appropriate then the data reading process is not perfoemed. Conversely, if appropriate, data will be sent to the next process, and the controller activates the command reading process. (2) The Bluetooth Command Reading Process is used to read data that is passed from the previous process to find out the purpose of the user. Data in the form of on/off commands which will then be translated in the form of control commands to change the status of relay 1. (3) The Relay Command Process 1, is used to change the incoming control command into data that can be recognized by relay 1. The on command will change the relay status to low while the off command will change the relay status to high. (4) The phone Number Verification Process used to verify the telephone number sent if it does not match what has been registered then the data reading process is not carried out. Conversely, if appropriate, data will be sent to the next process, and the controller activates the command reading process. (5) The Process of Reading SMS Commands used to read data passed from the previous process to find out the purpose of the user. Data in the form of a lock / unlock command which will then be translated in the form of a control command to change the relay status 2. (6) The Relay Command 2 process, is used to change the incoming control command into data that can be recognized by relay 2. The lock command will change the relay position to low while the unlock command will change the relay position to high.

The design stage is defined as a temporary system design that is made as an initial stage of making a system before entering the implementation phase. At this stage, an architectural system design scenario will be made that makes the hardware used into a unified system so that the circuit can be used and programmed at a later stage.

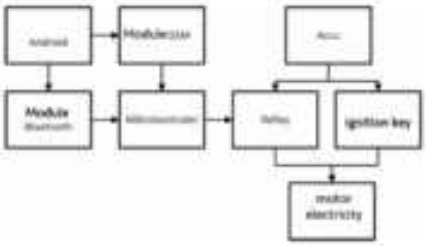

Fig. 8. Block Diagram

Arduino Uno R3 is the center of the process of the motorcycle secondary authentication system which processes the commands given to then be forwarded to the 2 channel relay. Researchers use Arduino Uno because it is easy to modify and has an EEPROM whose data is used to store data references for authentication. SIM800L GSM module functions as a medium of long-distance communication between smartphones and Arduino Uno via short messages that contain commands. This module is used because it has smaller dimensions compared to other GSM module versions. The Bluetooth HC-05 module functions as a personal communication medium between Arduino Uno and smartphones to send passwords and commands. This module is used because it carries out a personal network making it

safer. Besides that Bluetooth is a feature that can be found on every smartphone. The 2 Channel Relay Module functions as a switch that disconnects or connects the electric motorcycle to the battery according to the instructions received from Arduino Uno. This module was chosen because it has two relays combined in one PCB at a time, making it more concise. And the two relays are able to fulfill the functions and features needed in this system. The android application functions as a command giver on the motorcycle secondary authentication module via the short message media and Bluetooth.

V. Implementation and Testing

This manufacturing phase focuses on making secondary motorcycle authentication tools. The preparation of components and hardware modules in accordance with the schematic that has been made. Integration between modules is also done by referring to the pin configuration that has been determined at the design stage.

Fig. 9. Arrangement of Components

Figure 9 shows the components arranged in such a way as to produce a concise form on the secondary authentication tool. These components are integrated with each other using cables in accordance with the scheme that was created at the design stage. The following configuration pins are used to integrate all components.

TABLE II. Integrated Pin Configuration

No.	Pin Modul	Pin Arduino
1.	+5 V HC-05	Vout 5V (+)
2.	VCC SIM800L	
3.	VCC Relay	
4.	GND HC-05	GND (-)
5.	GND SIM800L	
6.	GND Relay	
7.	IN1 Relay	Pin 5
8.	IN2 Relay	Pin 6
9.	RXD HC-05	Pin10
10.	TXD HC-05	Pin 11
11.	TXD SIM800L	Pin 8
12.	RXD SIM800L	Pin 7

Table I is the entire relationship between all modules and Arduino Uno microcontrollers, for more details, here are the stages of making secondary authentication devices.

A. HC-05 Module Installation

There are 4 pins used in the HC-05 module, namely pins + 5V, GND, TXD, and RXD. Pin + 5V from the HC-05 module is connected to the Arduino 5V pin, this pin serves to provide electric current from Arduino to the module. The GND module pin is connected to the Arduino GNG pin, which functions to flow negative/reverse current from the module to the Arduino. The TXD pin of the module is connected to pin number 11 on Arduino, pin 11 which will later receive data from the HC-05 module. While the RXD pin of the module is connected to pin number 10 on Arduino, this pin 10 will send data from Arduino to be received by the HC-05 module.

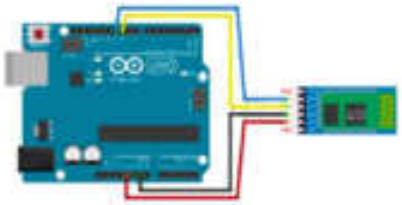

Fig. 10. Schematic Arduino with HC-05

The relationship between the HC-05 and Arduino modules is in accordance with Figure 5, the SA-RT context diagram at the analysis stage. The HC-05 module is described as a Bluetooth module in the context diagram. The module will send data in the form of "bt_msg" to the microcontroller, in the application the data is sent from the TXD HC-05 pin to pin number 11 Arduino.

B. SIM800L Module Installation

There are 4 pins used on the SIM800L module, namely the VCC, GND, TXD, and RXD pins. The VCC pin of the SIM800L module is connected to the Arduino 5V pin, this pin serves to provide electric current from the Arduino to the module. The GN800 pin of the SIM800L module is connected to the Arduino GNG pin, which functions to flow negative/reverse current from the module to the Arduino. The TXD pin of the SIM800L module is connected to pin number 8 on Arduino, pin 8 which will later receive data from the SIM800L module. While the RXD pin of the module is connected to pin number 7 on Arduino, pin 7 will later send data from Arduino to be received by the SIM800L module.

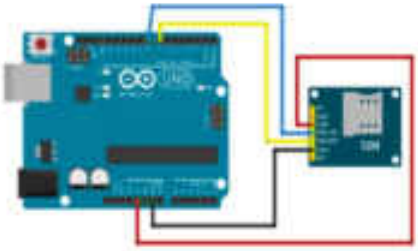

Fig. 11. Arduino schematic with SIM800L

The relationship between the SIM800L and Arduino modules is in accordance with Figure 5, the SA-RT context diagram at the analysis stage. The SIM800L module is described as a gsm module in the context diagram. The module will send "SMS" data to the microcontroller, in its application the data is sent from the SIM800L TXD pin to the Arduino number 8 pin.

C. 2 Channel Relay Installation

There are 4 pins that are used in the 2 channel relay, namely VCC, GND, IN1, and IN2 pins. The VCC pin of the relay is connected to the Arduino 5V pin, this pin serves to

provide an electric current from Arduino to the relay. The GND module pin is connected to the Arduino GNG pin, which functions to flow negative/reverse current from the relay to the Arduino. The IN1 pin of the module is connected to pin number 5 on Arduino, this pin 5 will later send the status from Arduino to control relay line 1. While the IN2 pin of the relay is connected to pin number 6 on Arduino, this pin 6 will later send the status from Arduino to control relay lines 2.

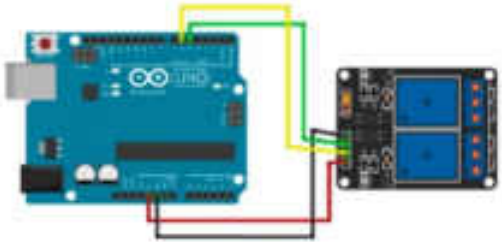

Fig. 12. Arduino Schematic with 2 Channel Relay

The relationship between relay 2 channels and Arduino is in accordance with Figure 5, the SA-RT context diagram at the analysis stage. Relay 2 of this channel is described as relay 1 and relay 2 in the context diagram. Relay 1 will receive data "relay1_state" from the microcontroller, in the application the data is sent from pin number 5 Arduino to pin IN1 on relay 2 channel. While relay 2 will receive data "relay2_state" from the microcontroller, in its application the data is sent from pin number 6 Arduino to pin IN2 on relay 2 channel.

D. Create Packaging

The packaging is made from an acrylic base to protect the components. The product is packaged as short as possible so it can be placed on a motorcycle, for that, it is made in the form of blocks measuring 10 x 8 x 3cm. Make 6 pieces of patterns that represent the sides of the packaging on acrylic, with the size of 10 x 8 cm by 2 pieces, 8 x 3 cm by 2 pieces, and 10 x 3 cm by 2 pieces. Cut each of these patterns and glue them together to form a block, leaving one side with a size of 10 x 8 as a lid.

E. Finishing

After all, pins are connected and the packaging is successfully made, the next step is to put the components that have been assembled on the package.

Fig. 13. Assembling Tools

Figure 13 is the final result of the hardware manufacturing process. The integrated component is placed in an acrylic container measuring 10 cm x 8 cm x 3 cm, with the aim that the component inside is protected and has a concise shape so that it can be placed on a motorcycle. The device is connected to the motorcycle through the two connectors provided, the connector is connected to the relay 2 channels in series and parallel as shown in the following picture.

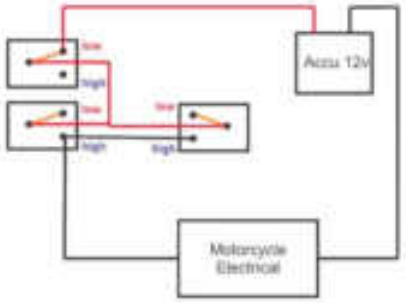

Fig. 14. Electrical Modification

The functionality test is done by user acceptance testing. The test parameters are arranged based on the main functions needed by stakeholders. This test was carried out by the target of this study, namely motorcycle users.

TABLE III. FUNCTION TESTING

Testing	Function	Expected results	Result
Bluetooth Authentication	connect	The device will connect to the smartphone via a Bluetooth connection	Approriate
Bluetooth Authentication	Turn on	The device will turn on the motorcycle electricity when the password is entered correctly	Approriate
Bluetooth Authentication	Turn off	The device will turn off the motorcycle electricity when the password is entered correctly	Approriate
Bluetooth Authentication	Notification	The device will give notification of commands received	Approriate
Bluetooth Authentication	Change Password	The device will change the saved password	Approriate

SMS Authentication	Lock	The device will disconnect the motorcycle when it receives the lock command from an sms	Appropriate
SMS Authentication	Unlock	The device will connect the motorcycle electricity when receiving unlock commands via sms	Appropriate

Test the authentication success rate using the distance parameter on Bluetooth. This trial was conducted on the Keylost Control feature, in which this feature utilizes Bluetooth connectivity as a means of communication. The distance variable will continue to increase until the test result data is deemed sufficient by the researcher to do the analysis or until the connection between devices can no longer be connected. This test is divided into two scenarios, namely with a barrier and without a barrier. This scenario intends to test whether the condition of a motorcycle when it is parked in a crowded parking lot can affect the propagation of a Bluetooth signal due to being blocked by another motorcycle. The signal propagation itself can be influenced by reflection and spread by other objects, as explained in the theoretical chapter. For this reason, barrier testing is done by parking the motorcycle next to the motorcycle with a secondary authentication system. Whereas the conditions without obstacles were carried out only with a test motorcycle. Each scenario was tested ten times. Table IV below is the result of the test.

TABLE IV. BLUETOOTH DISTANCE TESTING

No	Range	No barrier		With barrier	
		Succeed	Failed	Succeed	Failed
1.	1 m	10	0	9	1
2.	2 m	9	1	8	2
3.	3 m	7	3	2	8
4.	4 m	3	7	1	9
5.	5 m	1	9	0	10
6.	6 m	0	10	0	10

Re-open time test uses distance parameters on Bluetooth. This trial was carried out on the Keylost Control feature, in which this feature utilizes Bluetooth connectivity as a means of communication. The distance variable will adjust in the previous test. In this test, the two functions are turned on and turn off. The response time results in units of milliseconds (ms), calculated starting from the button on the application pressed until the application gets a notification from the system. Table V below is the result of the test.

TABLE V. BLUETOOTH RESPONSE TIME TESTING

Effect of distance on time on bluetooth		
Range	*Response time (ms)*	
	Turn on	*Turn off*
1 m	321	373
2 m	309	381
3 m	316	379
4 m	324	366
5 m	301	372

Re-open time test uses distance parameters on Bluetooth. This trial was carried out on the Keylost Control feature, in which this feature utilizes Bluetooth connectivity as a means of communication. The distance variable will adjust in the previous test. In this test, the two functions are turned on and turn off. The response time results in units of milliseconds (ms), calculated starting from the button on the application pressed until the application gets a notification from the system. Table v. below is the result of the test.

TABLE VI. SMS TIME TESTING PROCESS

No.	*Process time (ms)*	
	Lock	*Unlock*
1	235	254
2	265	267
3	247	257
4	233	245
5	252	243
6	266	265
7	249	239
8	246	237
9	252	264
10	233	255

Based on the results of performance testing on the secondary authentication system, the following results are obtained.

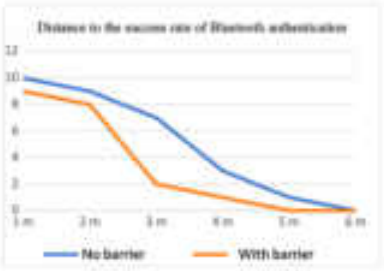

Fig. 15. Bluetooth Authentication Success Rate

Figure 15 displays a graph of the results of testing the authentication success rate if it is affected by the distance of the Bluetooth connection. In testing without a barrier, the maximum distance of a Bluetooth connection to authenticate is 5 meters with the number of successes 1 time. The ideal distance in this scenario is less than 3 meters because when testing a distance of 4 meters there was a significant decrease in success 4 times. While in testing with a barrier, the maximum distance of a Bluetooth connection is 4 meters with a success rate of 1 time. The ideal distance in this scenario is less than 2 meters because when testing a distance of 4 meters there was a significant decrease in success as much as 6 times.

Based on these data the authors know that the distance of the Bluetooth connection affects the success rate of authentication with the optimal distance in the condition without a barrier is 3 meters and the condition of obstructions as far as 2 meters and the condition of obstructed motorcycle conditions can reduce the range of Bluetooth connections due to reflection and signal spread.

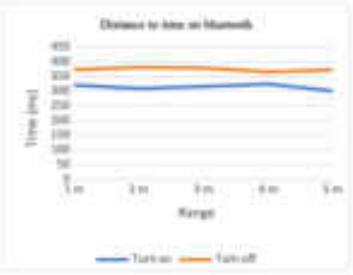

Fig. 16. Effect of Distance Against Bluetooth Response Time

Figure 16 displays a graph of the test system response time testing data if it is affected by the Bluetooth connection distance. Seen on the test chart the turn on function is marked with a blue line, showing changes in response time that are fluctuating but tend to be stable between 300 ms to 350 ms. Likewise, the turn off the function that is illustrated by the orange line, shows a change in response time that is fluctuating but tends to be stable between 350 ms to 400 ms. This is due to the connection distance below 5 m and the type of Bluetooth connection without intermediaries. Also seen is the turn on function response time is faster than the turn off function response time. This is because, in the program code, the turn off function is executed after checking the turn on function first. Based on these explanations, it can be said that the response time of the authentication system via a Bluetooth connection is not affected by the connection distance to the average value of the response time of 0.344 seconds.

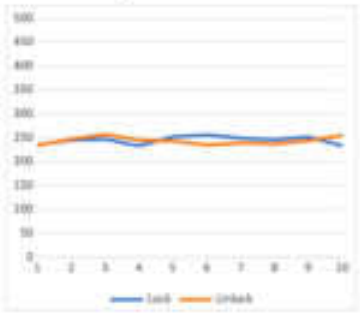

Fig. 17. SMS Authentication Process Time

Figure 17 displays a graph of the data from the results of testing the processing time of the SMS authentication system. Seen in the lock function test results marked with a blue line, there is no significant change in time in this test. The results of the testing of the lock function processing time were fluctuating with a data range of 33 ms, obtained from the difference between the longest time of 266 ms and the fastest time of 233 ms. Whereas the results of the unlock function test were marked with an orange line, something similar happened. The results of testing the processing time of the unlock function have a data range of 33 ms. Obtained from the difference between the longest time 367 ms with the fastest time 334 ms. Based on the results of the discussion it is known that the authentication system processing time via SMS can be executed with an average time of 0.249 seconds.

VI. Result

Based on the results of research and discussion in the previous chapter, it can be concluded that the secondary authentication system on a motorcycle can be made using an Arduino-based HC-05 and SIM800L module. The modification of the motorcycle electricity was successfully carried out on the motorcycle ignition in series and parallel at the same time so that it can overcome the problem of lost keys that occur in the owner of the motorcycle and can secure the motorbike when a key is lost. The maximum distance of the Bluetooth connection obtained by this system is 5 meters, which results are better than previous studies that used RFID as the authentication object. The average Bluetooth authentication response time obtained was 344 ms, the average SMS authentication process time was 249 ms, and the suitability of the function was 100%. There are several findings during the research process, namely the system created does not have independent resources so that it burdens the motorcycle batteries, and the system does not yet have a motorcycle location information feature through the emergency lock function.

References

[1] S. Ravel, "Penjualan Motor 2018 tembus 6,3 juta unit," Kompas.com, 2019," Vols. https://otomotif.kompas.com/read/2019/01/15/072200715/penjualan-motor-2018-tembus-6-3-juta-unit., no. [Accessed: 02-Feb-2019]., 2019.

[2] G. a. D. H. Durfel, "Enhancing situational awareness by knowledge-based user interfaces," Proceedings of the 2nd Annual Symposium and Exhibition on Situational Awareness in the Tactical Air Environment, pp. 197–205, 1997.

[3] M. T. Tombeng, "implementation of Wireless Xbee Authentication System of Motorcycle," Cogito Smart J., vol. 5, no. 1, p. 45–55, 2019.

[4] F. A. P. a. F. A. Rakhmadi, "Design of Motorcycle Security System Using Fsr (Force Sensitive Resistor) Sensor, Arduino Uno Microcontroller and Sim808 Module," Proceeding Int. Conf. Sci. Eng., vol. 2, p. 185–187, 2019.

[5] Muthumari, "Arduino based Auto Door unlock control system by Android mobile through Bluetooth and Wi-Fi," Int.Conf. Comput. Intell. Time (ma) Comput, pp. 1–4, 2018.

[6] H. Santoso, "Monster Arduino 3 : Implementasi Internet of Things pada Jaringan GPRS," no. Elangsakti, 2018.

[7] B. Setiawan, "Implementasi Metode Caesar Ciper pada Password Berbasis Arduino," 2017.

[8] G. V. Jane, "Measures of Situational Awareness from Human Performance and Situation Awareness Measures CRC," 2019.

[9] R. P. G. D. A. A. D. F. a. W. A. R. R. E. Peters, "Finding Lost Objects. Informing the Design of Ubiquitous Computing Services for the Home," 2004.

[10] I. Polkovnikov, "Unified Control and Data Flow Diagrams Applied to Software Engineering and other Systems.," 2016.

[11] M. J. B. J. S. Milaglov, "Quantifying Usability and Security in Authentication," IEEE International Computer Software and Applications Conference, 2011.

Motorcycle Secondary Authentication System Using Arduino-Based HC-05 and SIM800l Module

ORIGINALITY REPORT

6%	3%	5%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to UIN Syarif Hidayatullah Jakarta Student Paper	2%
2	Submitted to University of Stirling Student Paper	2%
3	Suci Ratnawati, Luthfiyyah Widianingsih, Nenny Anggraini, Imam Marzuki Shofi, Nashrul Hakiem, Fenty Eka M Agustin. "Evaluation Of Digital Library's Usability Using the System Usability Scale Method of (A Case Study)", 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020 Publication	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		

Motorcycle Secondary Authentication System Using Arduino-Based HC-05 and SIM800l Module

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7