Fingerprint based smart door lock system using Arduino and smartphone application

Tole Sutikno¹,²,³, Moh Ainur Faqih Ubaidillah², Watra Arsadiando³, Hendril Satrian Purmana³
¹Master Program of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
²Department Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
³Embedded System and Power Electronics Research Group, Yogyakarta, Indonesia

ABSTRACT
In 2023, crime cases in Indonesia will reach 105,133. Cases of theft with aggravation dominate the majority of cases. Everyone is concerned about safety, but doors are typically opened and closed using physical keys. This is vulnerable to being tampered with with fake keys, which can lead to house break-ins and theft. In this research, we propose a fingerprint-based wireless door lock design using Arduino and a smartphone. We offer this solution as a preventive measure to reduce the high rate of theft in homes or other buildings. The devices used are Arduino UNO R3, fingerprint sensor, HC-05 Bluetooth module, buzzer, and door lock solenoid. The results of the fingerprint-based wireless door lock using Arduino and a smartphone can function well, with an average response time of 1.20 seconds. Furthermore, testing the HC-05 Bluetooth when sending signals to a smartphone shows that it can read data accurately with an average response time of 1.54 seconds.

Keywords: Bluetooth HC-05, Fingerprint, Security system, Smart home, Wireless door lock

1. INTRODUCTION
Crime cases in Indonesia in 2023 will increase by 30.7% from 2022, with a total of 105,133 cases. According to data from the National Police of the Republic of Indonesia, 30,019 cases of aggravated theft make up the majority of these cases [1]. One of the crimes of cheating is theft in the house or yard by damaging and uncovering it to enter the house and cause a criminal case. The National Police of the Republic of Indonesia urges everyone to always be alert and to always provide a proper security system for their homes.

When talking about home security systems, doors are the most important part of a building because they are the main access to go in or out. For this reason, a proper security system is needed on the door to prevent theft [2]. Currently, the only doors available on the market have physical keys to securely open or close the door of a building. However, physical keys are vulnerable to being tampered with with fake keys, which can lead to house break-ins and theft. [3], [4]. With rapidly developing technology, people are looking for devices to ensure safety and comfort in their homes. There are currently several types of security device technology, such as facial recognition [5]–[7], fingerprint [3], [4], [8]–[10], finger geometry (finger size and position), iris recognition, vein recognition, retina scan, and voice recognition [2], [3], [6], [7], [9]–[18].

Smart door locks using biometrics have the advantage of higher security. In a smart home, the security system is a very important part [19]–[24]. Fingerprint recognition is one of the most secure systems because a person's fingerprint is never coordinated with anyone else's [24]–[26]. So, someone's access to the door lock
can be limited. This makes fingerprints the new automatic ID for every person [26]–[29]. With this idea, a plan and model of a fingerprint-based door lock framework will be presented in this paper. This study proposes security device technology using a fingerprint sensor as the main access to unlock. Furthermore, in certain conditions, an alternative to unlocking the door remotely is to use an application on a smartphone with Bluetooth HC-05 as a wireless data transmitter.

2. METHODS

This research focuses on security aspects in the context of using fingerprint sensors and smartphones to control home door locking. Through the use of this technology, data will be sent wirelessly via the HC-05 Bluetooth module to smartphone applications designed using the MIT App Inventor platform [30]–[38]. The process of recognizing and extracting fingerprint data for the smart door lock device being developed can be seen in Figure 1.

The expected result is the ability to unlock home doors automatically using a fingerprint sensor and hardware that is connected to a smartphone. In this research, there are several stages involving various research materials and resources. This sub-chapter includes hardware design, software development, and the preparation of wiring diagrams. The hardware design process begins with creating block diagrams and flowchart diagrams to plan the steps to be taken. The next step is to create a system schematic circuit design by combining all device components into a single, integrated, and controllable system.

2.1. System configuration

Figure 2(a) shows the block diagram system and becomes a reference for how the system works. Arduino UNO acts as the brain of the system and manages data from fingerprints and smartphones. The Arduino is then connected to various output components, including LEDs, buzzers, and relays. The relay functions as a link between the Arduino and the door lock solenoid. The fingerprint-based wireless door lock system is implemented using Arduino hardware and smartphone software. In this figure, the main steps and components of this system are shown sequentially, making it possible to understand clearly and in detail how the system can operate. The flow diagram starts with system initialization, where the system will wait for input data from the fingerprint or Bluetooth sensor. When Bluetooth sends data in the form of an integer 1, the LED, buzzer, and solenoid connected to the relay will light up for 5 seconds, then turn off while waiting for the data to be input again. Likewise with fingerprints, if the finger detected by the sensor is registered, then the LED, buzzer, and solenoid connected to the relay will turn on for 5 seconds, then turn off, and the door lock solenoid will close automatically until you wait for fingerprint data again to open it. If the attached fingerprint is not registered, the buzzer will flash three times, indicating that the attached fingerprint is not registered. This process is shown in Figure 2(b). The implemented hardware schematic diagram is shown in Figure 2(c).

Figure 1. The process of extracting features from the finger surface and storing them in a database.
Figure 2. Hardware design: (a) Block diagram, (b) Flowchart, (c) Schematic circuit
3. RESULTS AND DISCUSSION

In this research, a smart door lock device has been successfully designed using fingerprint sensor technology and remote control with a smartphone. Figure 3 shows a photograph of the developed device prototype. In this research, tests were carried out on the device to determine its success in responding to and recognizing fingerprints registered on the system and testing the remote control using a smartphone application that had been designed using the HC-05 Bluetooth module [31]–[39] as the signal transmitter.

3.1. The test of fingerprint sensor

This test aims to find out whether the fingerprint sensor is connected and whether the fingerprint sensor is working according to its function. The first time the device is turned on, the fingerprint sensor has not yet saved the fingerprint ID, so when you attach the fingerprint, it will read on the serial monitor that it did not find a match. The fingerprint sensor can store fingerprints ranging from 1 to 127. The storage process begins by typing the numbers 1–127 to save the fingerprint. After that, the sensor will wait for the fingerprint that will be registered or that you want to save to be attached to the sensor. When the fingerprint has been obtained, the program will ask you to stick the same finger again for authentication purposes, and the fingerprint will be registered or stored in the number that was typed earlier.

3.2. Bluetooth testing

In this research, mobile applications are built using a website-based compiler developed by MIT. Application creation begins by entering or logging in to the website https://appinventor.mit.edu and clicking “Create Apps.” This data delivery test uses an application that has been created using the MIT App Inventor platform [31], [39]. This test is carried out by opening the Bluetooth settings on the smartphone and connecting it to the HC-05 Bluetooth module [31]–[39].

Figure 4 shows the appearance of the application after the Bluetooth button is pressed, and after selecting Bluetooth, which was previously connected to the smartphone, the connectivity information indicator next to the open button becomes connected, indicating that the application and the Bluetooth module are connected. This shows that applications created using MIT App Inventor can send data. It can be seen that when the open button is pressed, the Bluetooth HC-05 will receive and open the door. The data sent by the application when the open button is pressed can be used as conditioning to activate the relay so that the door lock solenoid can open.

3.3. System testing

Placing a registered finger on the fingerprint sensor and timing how long it takes for the relay to activate in order to open the doorlock solenoid serve as the test’s inputs. It can be seen that the response time required for the system to open the doorlock solenoid varies. This can be caused by the finger being attached incorrectly, so the finger must be placed in the right position so that the sensor can read the fingerprint correctly and the system can immediately open the doorlock solenoid.

The test results are carried out using a smartphone application created using the MIT App Inventor platform. Firstly, press the open button on the application after a Bluetooth connection with the connected device, then calculate the time needed for the system to respond and activate the relay so that it opens the door lock solenoid. Testing is also carried out by measuring the distance between the smartphone and the system in order to find out the ideal distance for this system to work. So, in testing the response time of smartphone applications with this system, it can be concluded that distance is one of the factors that influences the response time it takes for the system to receive data from the smartphone and respond, thereby opening the doorlock solenoid. The results of this test also show that at a distance of 15 meters, the system is no longer able to respond to or receive data sent by the application, so the system does not open the solenoid door lock.

The data in Table 1 shows the results of testing the entire system on the fingerprint sensor. It can be seen in the table that the fastest time required for the system to open the doorlock solenoid immediately after the registered fingerprint is attached is 1.08 seconds, and the longest time is 1.28 seconds. So, in this test, the average time needed for the system to read fingerprints and open the doorlock solenoid was 1.20 seconds.

Based on Table 2, it can be seen that the fastest time in this test was at a distance of 2 meters with a time of 1.02 seconds, and the longest time for the system to respond to open the doorlock solenoid was at a distance of 14 meters with a time of 3.35 seconds. From the existing response time data, it was found that the average time required for the system to respond to data sent by the application on the smartphone was 1.54 seconds.
Fingerprint based smart door lock system using arduino and smartphone application (Tole Sutikno)

Figure 3. Photograph of hardware and fingerprint sensor testing

Figure 4. Testing data transmission from smartphone to HC-05 module

Table 1. Testing Data Results of Fingerprint Sensor Response Time to Door Locks

<table>
<thead>
<tr>
<th>Test No.</th>
<th>ID Fingerprint</th>
<th>Time Respond (s)</th>
<th>Selenoid Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1.1</td>
<td>Open</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1.22</td>
<td>Open</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1.23</td>
<td>Open</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1.28</td>
<td>Open</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1.19</td>
<td>Open</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>1.08</td>
<td>Open</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>1.21</td>
<td>Open</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>1.17</td>
<td>Open</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>1.27</td>
<td>Open</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>1.25</td>
<td>Open</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td>1.20</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Results of Bluetooth application response time to door locks

<table>
<thead>
<tr>
<th>Distance (m)</th>
<th>Respon Time (s)</th>
<th>Bluetooth HC-05</th>
<th>Selenoid Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.08</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>2</td>
<td>1.02</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>3</td>
<td>1.3</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>4</td>
<td>1.33</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>5</td>
<td>1.56</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>6</td>
<td>1.37</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>7</td>
<td>1.86</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>8</td>
<td>1.2</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>9</td>
<td>1.12</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>10</td>
<td>1.39</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>11</td>
<td>1.56</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>12</td>
<td>2.02</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>13</td>
<td>1.52</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>14</td>
<td>3.35</td>
<td>ON</td>
<td>Open</td>
</tr>
<tr>
<td>15</td>
<td>-</td>
<td>OFF</td>
<td>Close</td>
</tr>
<tr>
<td>Average</td>
<td>1.54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CONCLUSION

Following the stages of design, system development, and trial implementation, a wireless door lock device utilizing fingerprint technology was successfully created. The device is powered by an Arduino and can be connected to a smartphone. This study has successfully designed and implemented an automatic door lock system that incorporates a fingerprint sensor as an input component. The system has undergone verification testing ten times, demonstrating the reliability of the fingerprint sensor. The door lock solenoid operates with a 100% accuracy rate. During a separate trial, the smartphone transmitted data to the HC-05 Bluetooth module, enabling the module to accurately retrieve the data from within a maximum range of 14 meters. The average response time for this process was 1.54 seconds.

ACKNOWLEDGEMENTS

This project is supported by Embedded Systems and Power Electronics Research Group (ESPERG).

REFERENCES


Fingerprint based smart door lock system using arduino and smartphone application (Tole Sutikno)

**BIOGRAPHIES OF AUTHORS**

**Tole Sutikno** received his B.Eng. in Electrical Engineering from Universitas Ahmad Dahlan, Indonesia. He is currently an Editor-in-Chief of the TELKOMNIKA and the Head of the Embedded Systems and Power Electronics Research Group (ESPERG). His research interests include the field of digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded system, artificial intelligence, intelligent control, information technology and digital library. He can be contacted at email: tole@te.uad.ac.id.

**Moh Ainur Faqih Ubaiddillah** received his B.Eng. in Electrical Engineering from Universitas Ahmad Dahlan, Indonesia, in 2023. His research interests include robotics and Internet of Things. He can be contacted at email: moh1800022115@webmail.uad.ac.id.
Watra Arsadiando received B. Eng. in electrical engineering from Universitas Ahmad Dahlan, Indonesia, in 2017. He is a member of the Embedded Systems & Power Electronics Research Group (ESPERG). His current research interests include renewable energy, robotics, and digital control system. He can be contacted at email: watra24arsadiando@gmail.com or watra@journal.uad.ac.id.

Hendril Satrian Purnama received his B.Eng. degree in Electrical Engineering from Universitas Ahmad Dahlan, Yogyakarta, Indonesia in 2017. After receiving his degree, he became a member of the Embedded Systems and Power Electronics Research Group (ESPERG), and worked there as a researcher. In addition, he is also active as assistant editor in several international journals in the field of electrical engineering, computer and informatics. His research interests include power electronics, renewable energy technology, robotics and the Internet of Things. He can be contacted at email: lfriyan220@gmail.com.