ISSN 2087-3336 (Print) | 2721-4729 (Online)

TEKNOSAINS: Jurnal Sains, Teknologi dan Informatika
Vol 11, No. 2, July 2024, page. 238-244
http://jurnal.sttmcileungsi.ac.id/index.php/tekno
DOI: 10.37373

Design of the pistol P1 weapon storage system shelf using fingerprint electronic system in the TNI-AD units

Subaktiar Prayogi Putra[1], Dekki Widiatmoko[2*], Mokhammad Syafaat[1], Rafi Maulana[1], Aguk Sridaryanto[1]

[1] Weapon Systems Electronics Engineering, Army Polytechnic, Jl. Raya Orchid No. 01, Junrejo, Batu City, East Java-Indonesia 65321
[2*] Cyber Security Engineering, Army Polytechnic, Jl. Raya Orchid No. 01, Junrejo, Batu City, East Java-Indonesia 65321

*✉ dekkiwidiatmoko@poltekad.ac.id

Submitted: 12/12/2023 Revised: 23/01/2024 Accepted: 02/02/2024

ABSTRACT

Safe storage is one of the most crucial elements in stopping the unlawful use of firearms. Using fingerprint technology in the construction of electric firearm storage systems is a creative technique to ensure that only authorized owners can access the firearms. Fingerprint technology be used to improve gun storage security. However, conditions affecting the finger's health, such as cuts, stains, and moisture, can make the detection less accurate. To evaluate the system's accuracy, this study uses a quantitative technique and five different fingerprint detection scenarios. For the nine months that the study was carried out at the Kodiklatad Poltekad Electronics Laboratory, the Arduino ESP served as the basis for the system's execution. The test results show that the system can identify five distinct fingerprint detection scenarios with 100% accuracy. However, the system's inability to detect moist, broken, or dirty fingertips suggests limitations. Therefore, more consideration needs to be paid to these situations to increase system reliability. The security of gun storage might be improved by designing an electronic gun storage unit with Arduino ESP-based fingerprint technology, but there are still some challenges that need to be resolved to improve detection accuracy.

Keywords: Fingerprint; Arduino ESP; electric; firearms

1. INTRODUCTION

These days, there are a lot of unexpected events like robberies and thefts. For this reason, security is crucial in daily life. People who are always preoccupied with their everyday tasks also want to make sure that their treasured possessions are safe. Occasionally, people neglect to maintain their essential possessions, such as wallets, credit cards, and keys [1]. They are unable to enter their house or any other location without a security system. To gain access to traditional security systems, a user must possess an ID card, RFID card, security password, or key [2]. One of the disadvantages of this security mechanism is that it may be forgotten or taken by an unauthorized individual. Therefore, software that guarantees a better level of security needs to be developed [3].

Using biometrics can improve security and thwart theft. Although biometrics cannot completely prevent security breaches, it is crucial to understand that they can make systems more difficult to penetrate, which helps to protect information privacy [4]. In addition to being useful for personal security, biometric technology can be implemented as a security system in governmental organizations like the Indonesian Army and for warehouse security [5]. An armory is a facility used for the production, storage, and upkeep of armaments and ammunition as well as for staff training, ammo distribution, and overall management of armaments and ammunition [6]. In most nations, armories are mostly found in military formations. Because of the military's delicate position in ensuring national and territorial security through the employment of weapons, armories need to be properly controlled and secured [7]

One of the biometric traits that is easier to trace is human identification, as opposed to using pins or passwords. The practice of identifying a person based on one or more distinctive characteristics is known as human identification [8] There are numerous varieties of private verification processes available in the legal and business sectors. A password system or password identification number (PIN) is a popular personal verification technique. However, this approach is susceptible to theft, forgeries, and human memory errors. Developments in the area of digital feature-based identity verification are therefore necessary. If we wish to identify a person using their distinct biological structure, these features include fingerprint, palm, iris, retina, and face detection [9].

The iris and fingerprints are two other biometric approaches that are thought to be good metrics for identification when used with the human face. The majority of the time, the face offers sufficient information to reliably identify, even in the presence of additional biometric methods like [10], [11]. In general, fingerprint scanning yields higher accuracy. Compared to existing biometrics, our fingerprint detection and facial recognition technology is less expensive, simpler, more accurate, and less invasive [12]. This system will be separated into two groups, face detection and face recognition, similar to facial feature detection. While in the recognition phase, we must distinguish between face and non-facial regions in face detection [13]. In terms of needing to contrast several photos of the input image with the single-face images. An Arduino ESP processor is used in this job [14]. Designing and Building a P1 Pistol Weapon Storage System Rack Using a Fingerprint Electronic System in a TNI-AD Unit is the new title for this research project. Arduino ESP32 is the implementation base for this study [15]. This system refers to earlier research that used a long-barreled pistol; subsequent research uses an ESP32 Arduino to power a P1 gun [16].

2. METHOD

The P1 pistol storage system is an inventive way to enhance security and weapon management in TNI-AD units. It uses fingerprint technology and an Arduino ESP32. Analyzing demands and choosing hardware are important initial steps in planning. An efficient combination of a fingerprint sensor for identity verification, a servo/solenoid motor for the shelf opening mechanism, and an Arduino ESP32 for system intelligence [14]. To integrate the fingerprint sensor with the shelf opening mechanism, an Arduino program must be written and hardware must be connected. Verifying the fingerprint sensor, testing the opening mechanism, and testing the reaction to security events are all part of the test. Following testing that passes muster, field implementation entails user education, regular upkeep, and any required system changes. To maintain the degree of security and system performance, regular evaluation and improvement become an essential component of the overall system, taking into account user feedback and the most recent technological advancements [17]. Therefore, this technology can help with weapon management and security in a military setting.

This electronic system rack's design follows the research flow to facilitate the formulation of each task that is completed.

a. Personnel ID: Unique identification number for each personnel.
b. Personnel Name: Full name of personnel.
c. Access Status: Indicates whether personnel are permitted access or not permitted access.
d. Data Type: Type of data related to personnel (for example, face or fingerprint).

2.1 Research flow diagram

The research flow diagram in Figure 1 shows the procedures involved in creating the P1 pistol weapon rack system utilizing an Arduino ESP32 [15]. Finding a sensor that fits the required measurement range, accuracy, and precision level is the first step.

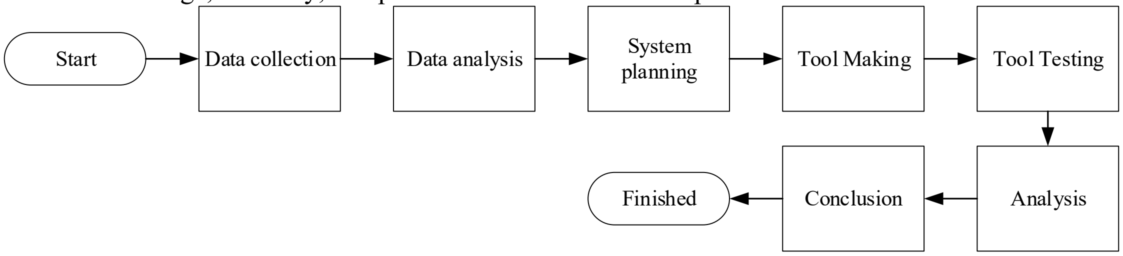

Figure 1. Research flow diagram

Additionally, this project entails designing a weapons storage rack using an electronic system and integrating components like a fingerprint reader, LCD, and keypad. The goal of this research is to develop novel approaches that can improve pistol retrieval efficiency. The system's performance was tested in the field using portable methods; evaluation results, data analysis, and a comparison with traditional methods will all be included in the research report. This will give a clear picture of the effectiveness and excellence of the suggested remedy.

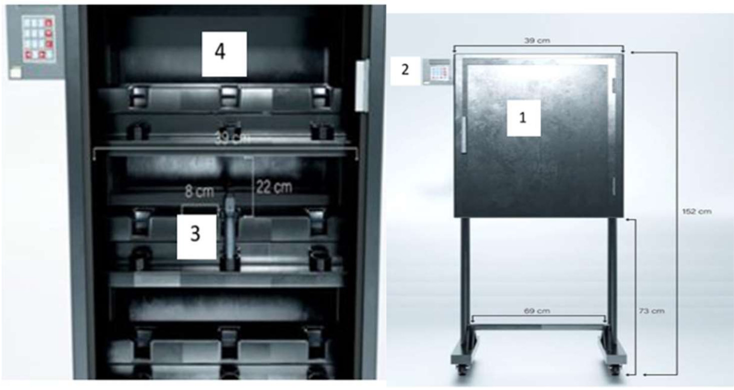

Figure 2. Tool component design

We offer a thorough explanation of each of the gun box security system's primary parts in Figure 2. A discussion of each section is given below:

1. P1 Gun and storage case:
explains the exact placement of the P1 handgun inside the box. highlights the physical safety and defense of the weapons kept inside.
2. LCD screen (Liquid Crystal Display):
The user interacts visually with the LCD panel. used to show essential notifications, registration instructions, and security status information. shows security configurations and alerts if unwanted access is attempted.
3. Keypad:
The user can enter a security code using the keypad as input. serves as a manual way to input the PIN or combination needed to open the box lock. combines with security measures to guarantee permission entry.
4. Fingerprint scanner:
The box lock is unlocked using fingerprint identification technology. A simple explanation of how a fingerprint scanner operates may be found in Figure 2. offers a high degree of security since fingerprints are distinct and hard to forge. Systems Integrating Electronic and Security:
Explains the connections and interactions between the parts. describes how to register, how to adjust the security, and how to access weapons safely.

2.2 Design specifications

By using fingerprints that are made to desired specifications, the design determination seeks to simplify the process of designing weapons system racks. Figure 3 displays the model specifications that need to be implemented. A block diagram of the tool design is shown below:

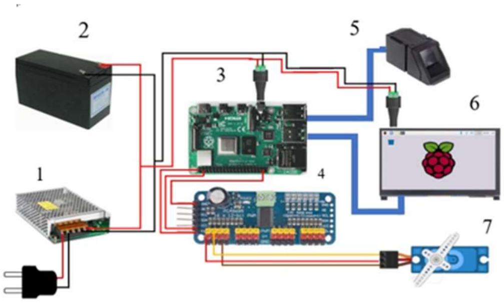

Figure 3. Block diagram of tool design

The operational steps in the design of the weapons storage rack design tool above can be explained as follows:

a) The supply component makes sure that electrical power is sent to electronic devices within the right parameters. An electrical adapter or battery power source that offers the voltage and current required to operate electronic devices to their best potential can be referred to as a supply, or power source, in this context. To ensure the stability and operational reliability of the device, it is imperative to maintain appropriate power levels.
b) Electronic systems require electrical power, which is supplied by batteries. The battery serves as a transportable power source, enabling the gadget to keep running without requiring an external power supply. The use of batteries offers protection during power outages and flexibility in how weapons are stored.
c) The data obtained from the fingerprint is processed by the Arduino Esp32 microcontroller and sent to the system output, which is shown on the LCD screen. The system's brain, the Arduino ESP32 microcontroller, is in charge of processing fingerprint sensor data and managing system functions as a whole. The microcontroller's output is shown on an LCD screen, giving the user information about the outcomes of the fingerprint identification procedure.
d) The control signals sent to the servo motor are managed by the servo motor driver. The servo motor driver serves as a mediator between the servo motor and the microcontroller. This driver helps the weapons storage system's opening and shutting mechanism by translating control signals from the microcontroller into motions on the servo motor.
e) The P1 weapon's fingerprint is accessed using fingerprint. One part that is utilized to collect and identify user fingerprints is the fingerprint sensor. The P1 weapon can only be retrieved by using the registered and authorized fingerprint as the key to unlock the weapons storage system.
f) The results of fingerprint access, which is used to register and retrieve firearms, are displayed on the LCD panel. The LCD screen gives the user a visual interface by showing details about the security status, fingerprint registration procedure, and how to retrieve the weapon. This makes it possible for the user and the system to interact intuitively.
g) The tool's lock is opened using the servo motor. The weapon storage system's lock mechanism is moved using the servo motor. Upon accurate identification and authorization, the servo motor initiates, granting entry to the P1 weapon.

3. RESULTS AND DISCUSSION

Following the completion of the tool's development, testing utilizing Arduino, servo motors, and fingerprint sensors is necessary to comprehend the properties of each component and the tool's overall functionality. The primary microcontroller, Arduino, is configured to synchronize the functions of the servo motor, LCD screen, keypad, and fingerprint sensor. The weapon storage system's unlocking mechanism heavily relies on the servo motor, which is coupled to the Arduino via a driver. As a means of identification, the fingerprint sensor works in the background to identify the user's fingerprints. Testing will entail confirming each component's response, the servo motor's speed and precision during unlocking, and the fingerprint sensor's accuracy in identifying fingerprints. The testing's outcomes will offer a comprehensive grasp of the gadget's functionality, enabling modifications or enhancements as needed to reach the required degree of efficiency and safety in the technology's application for weapon storage.

3.1 How the tool works

a) Enter fingerprint information in the fingerprint recording test. After running the application through the terminal, staff members press their thumbs against the sensor.
b) Look for prints on surfaces. The purpose of this fingerprint search test is to look for fingerprint information that has already been entered into the system. Data kept in the error graph system is used to conduct this test.

3.2 Error graph

If we examine issues with fingerprint recognition that involve several aspects that can impact the precision and dependability of the system, we can classify the fingerprint error graph. Errors in measurements might be non-linear, linear with offset, or affected by outside variables like humidity and temperature. In addition, spoofing—the possibility of false fingerprint recognition—is a significant issue that must be resolved to increase security. Erroneous fingerprint readings can also be caused by other elements like extremely dry or wet skin, sensor aging or damage, and the amount of oil or grime on the sensor. The development of more advanced sensor technology, the use of robust encryption techniques, the implementation of sound security standards, as well as regular maintenance and calibration to guarantee system accuracy over time, are all necessary to solve these issues.

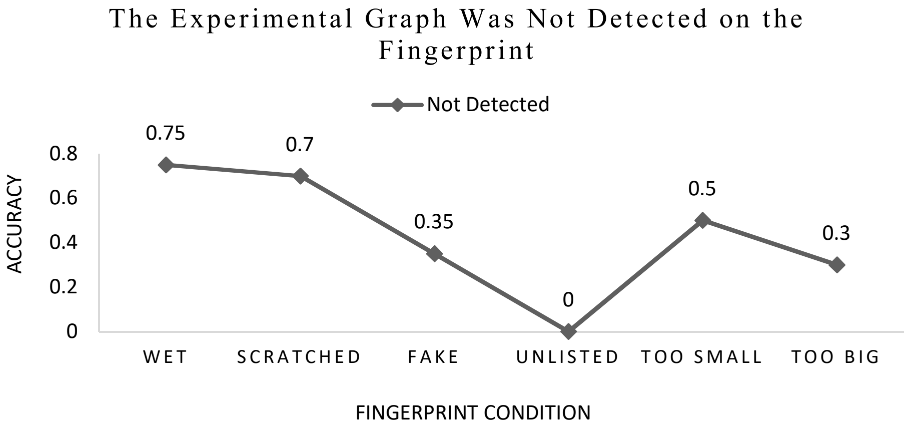

Figure 4. Graph of fingerprint experiment results

Figure 4 the test findings indicate that, with differing degrees of effectiveness, the fingerprint recognition system has trouble identifying several unique circumstances. There are still situations in which it is unable to identify wet fingerprints, despite having a 75% accuracy rate in this regard. Similar results are obtained with fingerprints that have been scratched, where the accuracy rate is 70%, suggesting good performance but still needing improvement. With an accuracy rate of only 35%, the system encounters serious problems in the false fingerprint scenario. Regarding unregistered fingerprints and too huge fingerprints, the system appears to be completely unable to provide any kind of detection. When fingerprints are too tiny, the accuracy rate displayed by the system is 50%. To raise the system's capacity to handle more drastic variations in fingerprint situations and raise the degree of accuracy overall, more advancements and upgrades are required.

Individual identity is typically included in fingerprint findings. Since each person's fingerprints are distinct, they can be used as a form of identification. Fingerprints can have a variety of patterns, including circular, fractured, and navel. The following categories of fingerprint patterns discovered during fingerprint testing are included in the discussion:

a. Test by applying a stain to your finger
b. Fingertip testing
c. Test on the left edge
d. Test on the right edge
e. Testing using the whole finger (full finger)
f. Test method

3.3 Fingerprint test results detected

The fingerprint identification system performs exceptionally well under a variety of circumstances, according to the accuracy test findings. In typical circumstances or with slight smudges on the thumb, the system can identify fingerprints with 100% accuracy. Aside from that, the thumb's entire tip, left edge, right edge, and powers are still at their best. These outcomes attest to the system's dependability in identifying fingerprints under many settings and orientations. It is crucial to remember that to increase the system's overall dependability, specific circumstances like dirty, damaged, or moist fingerprints must be addressed by ongoing system improvements. Table 1 then displays the testing experiments and data gathering.

Table 1. Detected fingerprint test results

No.	Fingerprint Condition	Test result	Accuracy
1	Fingerprint Condition	Detected	100%
2	There is a stain on the thumb	Detected	100%
3	Thumb tip	Detected	100%

No.	Fingerprint Condition	Test result	Accuracy
4	The left edge of the thumb	Detected	100%
5	The right edge of the thumb	Detected	100%
6	Full thumb section	Detected	100%

According to the test results, the fingerprint identification system has a very high accuracy of 100% under a variety of situations, including smudged thumbs. The thumb's tip, left edge, and right edge are among the areas where the system's functionality is still at its best. These outcomes attest to the system's dependability in identifying fingerprints under many settings and orientations. Still, additional enhancements are required to handle unique situations, like dry, damaged, or moist fingerprints, to raise the system's overall dependability. It is envisaged that the fingerprint identification method would become a more dependable and potent security measure by carrying out more advancements.

3.4 Fingerprint test results were not detected

The test findings are broken down individually using the unique identification number assigned to each test that is conducted. The fingerprint condition refers to a unique feature or state of the fingerprint under examination. Different conditions, including but not limited to clean, moist, scratched, fake, unclear, incomplete, not registered, too tiny, too large, and insufficient pressure, may be included in this research. Test results indicate whether or not the technology is capable of accurately detecting fingerprints. If the fingerprint is successfully recognized and verified by the system, the test result can be documented as "Detected". On the other hand, test results can be noted as "Not Detected" if the fingerprint is difficult to distinguish, damp, scratched, or in another situation where the system is unable to detect it. Table 2 then displays the testing experiments and data collecting.

Table 2. Fingerprint test results not detected

No	Fingerprint Condition	Test result	Accuracy
1	Wet fingerprints	Not detected	75%
2	Fingerprints are scratched	Not detected	70%
3	Fake fingerprints	Not detected	35%
4	Fingerprint not registered	Not detected	0%
5	The fingerprint is too small	Not detected	50%
6	The fingerprint is too big	Not detected	30%

It is evident from the fingerprint testing results that there are various degrees of detection error. Fingerprints that are too little, too large, false, wet, scratched, or unregistered cannot all be accurately identified. With only 35% accuracy, fake fingerprints displayed the highest detection mistake rate. Furthermore, the error rate for large and unregistered fingerprints is equally high—30% and 0%, respectively. It should be highlighted, nevertheless, that there is still some accuracy—75% in the case of wet fingerprints and 50% in the case of too small fingerprints. Consequently, it will be crucial to keep improving the detecting system to increase overall accuracy, particularly when handling extreme fingerprint sizes and fake fingerprints.

4. CONCLUSION

Although the accuracy varies, it can be inferred from the fingerprint test results that the system performs well in identifying a variety of circumstances. Fake fingerprints have the lowest accuracy rate at 35%, whereas wet fingerprints have the best detection accuracy at 75%. Despite this, the system was able to accurately identify situations like stains on the thumb, tip, left edge, right edge, and entire thumb. This demonstrates the system's capacity to accurately identify different fingerprint components and states, but more work needs to be done in several areas to raise detection accuracy overall**.**

REFERENCES

[1] S. Samsugi, Z. Mardiyansyah, and A. Nurkholis, "Sistem Pengontrol Irigasi Otomatis Menggunakan Mikrokontroler Arduino Uno," *Jurnal Teknologi dan Sistem Tertanam*, vol. 1, no. 1, p. 17, 2020, doi: 10.33365/jtst.v1i1.719.

[2] U. Hasanah, M. Wildan, and T. Tohazen, "Sistem Kendali dan Pemantauan Peralatan Navigasi Penerbangan Non Directional Beacon Tipe ND200S Menggunakan Nodemcu ESP8266 Berbasis

Internet of Thing," *JTEV (Jurnal Teknik Elektro dan Vokasional)*, vol. 8, no. 1, p. 67, 2022, doi: 10.24036/jtev.v8i1.113268.

[3] M. Wibowo, A. Rabi', S. Suprayogi, and I. Mujahidin, "Rancang Bangun Sistem Pengamanan Rak Senjata M16 Menggunakan Rfid Dan Fingerprint," *JASIEK (Jurnal Aplikasi Sains, Informasi, Elektronika dan Komputer)*, vol. 1, no. 2, 2019, doi: 10.26905/jasiek.v1i2.3525.

[4] M. Dimyati Ayatullah, E. Ariyanto Sandi, and G. Hendra Wibowo, "Rancang Bangun Absensi Mahasiswa Berbasis Fingerprint Menggunakan Komunikasi Wireless," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 4, no. 2, pp. 152–158, 2019, doi: 10.30591/jpit.v4i2.1123.

[5] N. K. Daulay and M. N. Alamsyah, "Monitoring Sistem Keamanan Pintu Menggunakan Rfid Dan Fingerprint Berbasis Web Dan Database," *Jusikom : Jurnal Sistem Komputer Musirawas*, vol. 4, no. 02, pp. 85–92, 2019, doi: 10.32767/jusikom.v4i2.632.

[6] D. Hermawan, A. B. Setiawan, D. A. Prasetya, and A. Rabi, "Sistem Pengaman Pintu Gudang Senjata Rudal Arhanud TNI AD dengan Identifikasi Wajah," *Seminar Nasional Sistem Informasi*, no. September, pp. 887–897, 2017.

[7] F. Hermawanto, A. A. Fajar Riyanto, and N. C. Hasyim, "Manajemen Peminjaman Kunci Menggunakan Fingerprint Pada Laboratorium Komputer Jurusan Teknik Informatika," *Jurnal Pengelolaan Laboratorium Pendidikan*, vol. 3, no. 2, pp. 77–85, 2021, doi: 10.14710/jplp.3.2.77-85.

[8] I. P. Rudi Handika, Dedy Hartama, Ika Okta Kirana, M. Safii, "Prototype Alat Pengamanan Pintu dengan Menggunakan Sensor Sidik Jari Berbasis Arduino Mega2560," *Kajian Ilmiah Informatika dan Komputer*, vol. 1, no. 6, pp. 240–247, 2021.

[9] P. Studi, T. Informatika, F. Sains, D. A. N. Teknologi, U. Islam, and N. Syarif, "Implementasi Face Recognition Dengan Opencv Pada ' Smart Cctv ' Untuk Keamanan Implementasi Face Recognition Dengan Opencv Pada ' Smart Cctv ' Untuk Keamanan," 2020.

[10] M. Wibowo, A. Rabi', S. Suprayogi, and I. Mujahidin, "Rancang Bangun Sistem Pengamanan Rak Senjata M16 Menggunakan Rfid Dan Fingerprint," *JASIEK (Jurnal Aplikasi Sains, Informasi, Elektronika dan Komputer)*, vol. 1, no. 2, 2019, doi: 10.26905/jasiek.v1i2.3525.

[11] A. Mubarok, I. Sofyan, A. A. Rismayadi, and I. Najiyah, "Sistem Keamanan Rumah Menggunakan RFID, Sensor PIR dan Modul GSM Berbasis Mikrokontroler," *Jurnal Informatika*, vol. 5, no. 1, pp. 137–144, 2018, doi: 10.31311/ji.v5i1.2734.

[12] S. Rahardiansyah, D. Siswanto, F. Rofii, and M. I. Fanani, "Kendali Pengunci Pintu Secara Nirkabel Menggunakan Wemos Arduino," *JASEE Journal of Application and Science on Electrical Engineering*, vol. 1, no. 02, pp. 63–78, Feb. 2021, doi: 10.31328/jasee.v1i02.11.

[13] M. A. L. QADIM, "Rancang Bangun Mekanisme Pembuka Pintu Pada Robot Asisten Medis," 2021, [Online]. Available: https://dspace.uii.ac.id/handle/123456789/33817%0Ahttps://dspace.uii.ac.id/bitstream/handle/123456789/33817/17525050 Muhammad Al Qadim.pdf?sequence=1&isAllowed=y

[14] "5-Sofyan+Rahardian_OK arduino".

[15] U. Latifa and J. S. Saputro, "Perancangan Robot Arm Gripper Berbasis Arduino Uno Menggunakan Antarmuka Labview," *Barometer*, vol. 3, no. 2, pp. 138–141, 2018.

[16] S. Samsugi, A. Ardiansyah, and D. Kastutara, "Arduino dan Modul Wifi ESP8266 sebagai Media Kendali Jarak Jauh dengan antarmuka Berbasis Android," *Jurnal Teknoinfo*, vol. 12, no. 1, p. 23, 2018, doi: 10.33365/jti.v12i1.42.

[17] I. R. Afandi, D. Febriawan, A. S. F. Faturohman, F. Nazihah, M. A. Andreansyah, and B. Alfian, "Aplikasi SIPEDRO 1.0 untuk pemantauan hidroponik dengan platform blynk terintegrasi ESP32," *TEKNOSAINS : Jurnal Sains, Teknologi dan Informatika*, vol. 10, no. 1, pp. 71–81, 2023, doi: 10.37373/tekno.v10i1.334.