Door Security System Using e-KTP and One Time Password (OTP) Code with Telegram Messenger Notification

Putri Pajria Syalbilla[1], Lilik Anifah[2], Farid Baskoro[3], Pradini Puspitaningayu[4]
Bachelor of Electrical Engineering, Faculty of Engineering, Surabaya State University
putri.21095@mhs.unesa.ac.id
lilikanifah@unesa.ac.id
faridbaskoro@unesa.ac.id
pradinip@unesa.ac.id

Abstract - The large number of cases of theft cases can be evidence that this crime is a social phenomenon that is always faced and always sought by various parties to reduce the intensity or level of crime that occurs. Improving the door security system is an effort that can be made to reduce theft that occurs because the existence of this door is often used by thieves as the main access to be able to enter a room and open it by breaking into the door. Therefore, the development of a door security system is needed to provide convenience in monitoring the condition of the door. This system is based on the NodeMCU ESP32 microcontroller as the working controller of the entire range, using the verification of the registered owner's e-KTP and OTP code as the second password to be able to open the door. Equipped with a solenoid door lock as door lock, magnetic sensor, SW 420 vibrating sensor, and buzzer as a security alarm. The Telegram application acts as a notification when there is an attempted theft or break-in on the door and as a messenger regarding who accesses the door. The test results obtained are tools that are designed as a whole to have good performance and can work according to their respective specifications, with the telegram application that can work optimally in monitoring all activities on the door.

Keywords: RFID, e-KTP, One Time Password, NodeMCU ESP32, monitoring

INTRODUCTION

Crime is now a real threat in society. The existence of this criminal behavior can indirectly damage the norms or rules used as guidelines to create social order. One of the crimes that often occurs in the community is theft of property [1]. The large number of theft cases can be evidence that this crime is a social phenomenon that is always faced and always tried by various parties to reduce the intensity or quality of crimes that occur [2].

The efforts that can be made to reduce theft are by strengthening security in a room. The door is an important part of a room, where all activities in and out of humans are carried out through a door [3]. The existence of this door is often used by thieves as the main access to be able to enter the room and open it by breaking the door. Generally, today's door security systems still use manual locking in the form of keys or padlocks. This locking system is considered less effective because thieves can access the door using only simple tools such as wires, paperclips, screwdrivers, and so on. Therefore, the development of the door security system is very necessary to do [4].

Some similar studies on security systems have been conducted, including [5] proposing a safe security system based on e-KTP cards and utilizing technology Internet Of Things (IoT) to monitor the condition of the safe in case of theft. This designed system cannot monitor anyone who has accessed the vault whether a user with a registered e-KTP or not. Designed security system [6] Produce the design of a Punia fund box security system using fingerprints with telegrams as message recipients in case of theft. This tool only uses fingerprints to be able to access the fund box and does not use double security.

Research by [7] Produce the design of a safe security system with Arduino-based fingerprints and a buzzer as Output if access is denied. Research by [8] designing a storage box with a security system equipped with fingerprints and Passwords as Double Protection on the safe, then [9] successfully researched security systems using fingerprint sensors and SMS notifications in the form of OTP codes to open safes. This designed system has also been equipped with Double Protection in the form of fingerprints and OTP codes to open the safe. Of the three studies described above, it is still not equipped with a condition monitoring system that occurs on the door and is not IoT-based.

Research conducted by [10] generates a safe security design using an e-KTP card and OTP code sent via SMS to the user. Equipped with a double key in the form of e-KTP and OTP to open the safe, it's just that this system is not yet IoT-based and [11] Conducted research on fingerprint-based bank locker security system with Bluetooth module and vibrating sensor as protection on the locker. This designed system is not equipped with the provision of information related to who has opened the safe, either users or strangers who try to open the safe.

Based on the description of the problem above, the researcher proposed the design of a security system with doors as the object of research. This design can be called two-step verification because verification is required through the owner's e-KTP first and the OTP code as a password to open the door. In addition, this system is equipped with a telegram application as a notification to the owner in the event of an attempted theft or break-in at the door. Telegram also acts as a recipient of messages or information from the system related to anyone who has accessed the door, with a registered or unregistered e-KTP ID.

This study aims to change the manual locking system to digital and provide convenience in supervising every activity on the door, by utilizing the e-KTP ID that has been registered as an electronic key and OTP code as a form of double protection on the door. So it is hoped that this system can contribute to reducing the crime rate of theft or burglary that occurs, considering that the e-KTP itself has different data from one another can add security value to the door because the system will immediately reject the unregistered e-KTP card. Likewise, the OTP code in the form of a password that is constantly changing will increase the security value of the door because this change makes it difficult for unauthorized people to be able to access the door.

METHOD

Research Flow

This research was carried out following predetermined stages, which aim to achieve maximum results in this study. The flow of research carried out is in Figure 1.

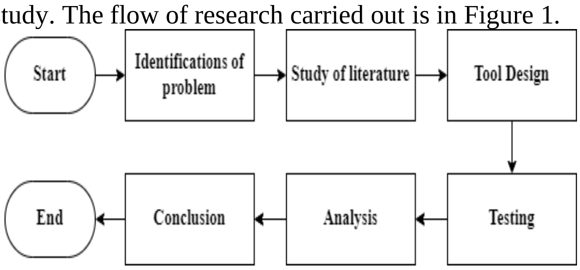


Figure 1. Research Flow

Block diagram

System design begins with making block diagrams, where each block has its function, thus forming an interconnected system. The block diagram also illustrates in general terms how the circuit as a whole works. Block diagram as shown in figure 2.

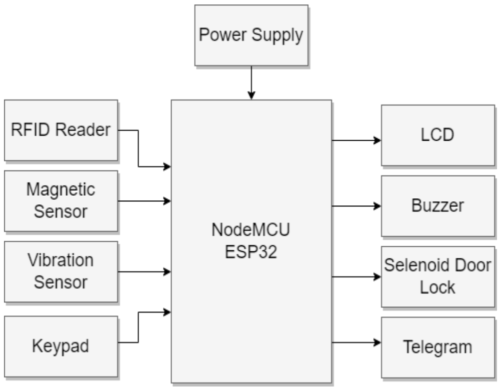


Figure 2 Block diagram

Technical Drafting Design

The technical drafting design aims to provide an overview of the use of sensors and components in the design to be carried out. In this study, the tools and materials used are:

Table 1. Tools and Materials

No.	Tools and Materials	Specifications
1.	Laptop	Ideapad Flex 5
2.	Multimeter	DT9205A
3.	Adapter	12 V
4.	Microcontroller	NodeMCU ESP32
5.	Solenoid door lock	12 V
6.	Keypad	3x4
7.	Buzzer	5V
8.	Magnetic Sensor	MC-38
9.	Vibrating Sensor	SW-420
10.	12C LCD	16x2
11.	RFID	RC522
12.	Relay	1 channel
13	Step Down	LM2596

Wiring or wiring is done to identify how the systematics of the hardware circuit works on the tool to be designed. The wiring design is shown in Figure 3.

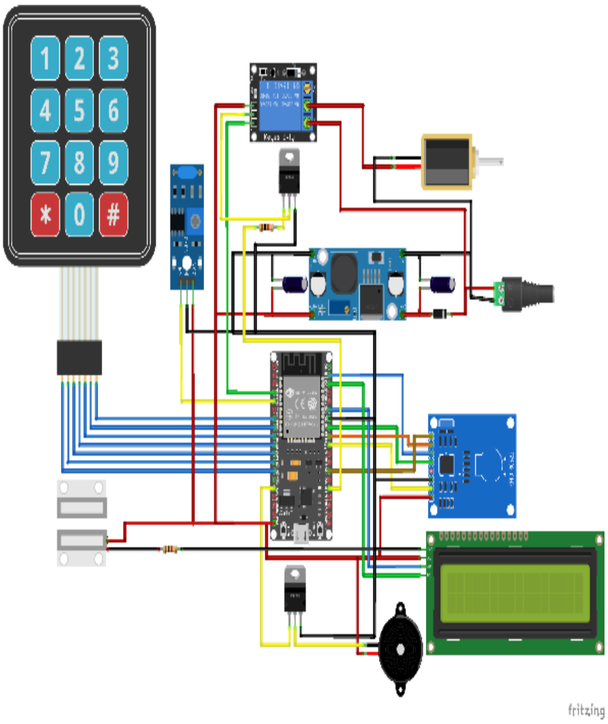


Figure 3. Technical Drafting Design

Flowchart

Software design aims so that the designed hardware can function properly according to the instructions that have been programmed before. Figure 4 is a flowchart display showing the overall working steps of the system.

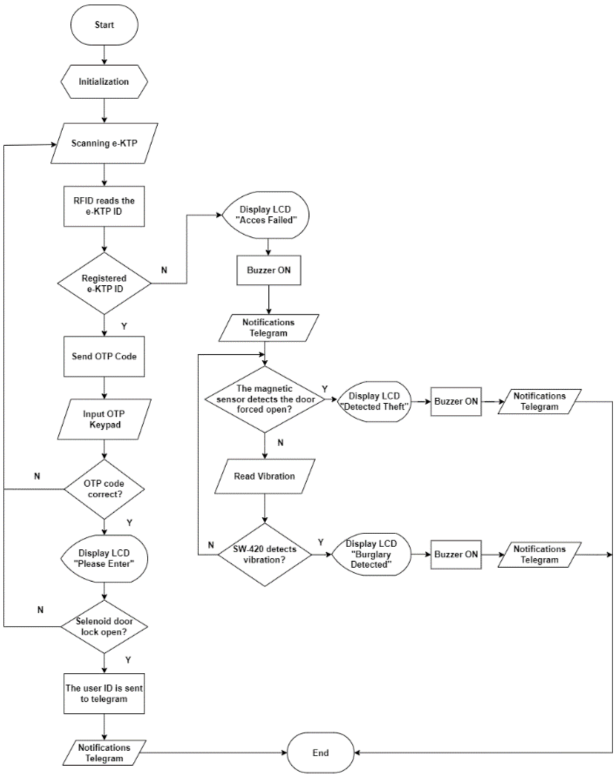


Figure 4. Flowchart

RESULTS AND DISCUSSION

Testing is carried out to determine whether the designed tool has good performance and ensure that each component of the entire tool series has functioned as planned. The results of designing a security system on the door are shown in Figure 5.

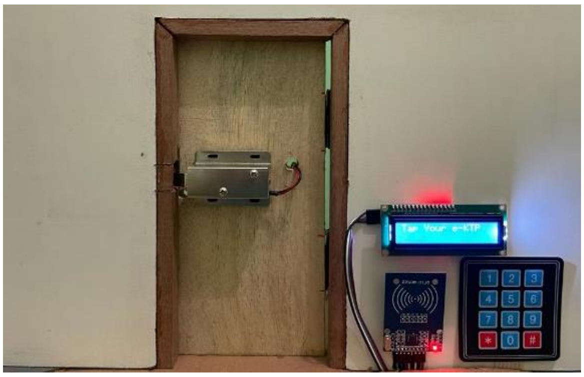


Figure 5. Miniature doors as a whole

12V Adapter Testing

This test aims to determine whether the voltage source coming from the adapter of 12V has good performance. The output of this voltage will be used as a door lock solenoid input and as a microcontroller input which will be processed first through a 5V step down. The results of the test are shown in Table 2.

Table 2. 12V Power Supply Output Testing

Experiment to-	Vout	Vout Measurement	Error%
1.	12 V	12.39 V	3.14%
2.	12 V	12.41 V	3.30%
3.	12 V	12.44 V	3.53%
4.	12 V	12.35 V	2.83%
5.	12 V	12.42 V	3.38%
Average error			3.24%

After obtaining the measurement data, an error calculation is performed using the equation:

$$\text{error\%} = \frac{|\text{estimated value} - \text{exact value}|}{\text{exact value}} \quad (1)$$

$$\text{Average} = \frac{\sum \text{Amount of result data}}{\text{Lots of test data}} \quad (2)$$

Based on measurement data, the average error in the test was 3.24%. This value is still acceptable because it has a relatively small percentage of error, so it is concluded that the 12V power supply can work properly.

Step Down Testing LM2596

The use of step-down serves as a voltage reducer that converts a high DC input voltage into a lower DC voltage. This test is carried out by measuring the output of the LM2596 step-down. Results from testing as in Table 3.

Table 3. LM2596 step-down testing

Experiment to-	Vout	Vout measurement	Error%
1.	5 V	4.94	1.21%
2.	5 V	4.93	1.42%
3.	5 V	4.94	1.21%
4.	5 V	4.92	1.62%
5.	5 V	4.93	1.42%
Average error			1.38%

Based on the calculation results, the average error of the step-down output voltage calculated using equations (1) and (2) is 1.38%. It can be seen that this step-down module can work well by lowering the input voltage by 12V to 5V. This obtained value will be used as a voltage source by the NodeMCU ESP32 microcontroller. This 5V voltage will later provide working voltage to the entire circuit of the tool.

RFID Testing

Tests are carried out to find out whether the RFID reader works properly reading data on a tag whose ID has been registered and that has not been registered. In addition, distance testing is also carried out to find out what the maximum reading distance is between the tag and the RFID reader. Test results as in Table 4.

Table 4. RFID Testing

Tag Type	Registered /Not	Status	Reader distance	
			0-2 cm	3-5cm
e-KTP 1	Registered	Access Accepted	Unreadable	Not Unreadable
e-KTP 2	Registered	Access Accepted	Unreadable	Not Unreadable
e-KTP 3	Registered	Access Accepted	Unreadable	Not Unreadable
e-KTP 4	Registered	Access Accepted	Unreadable	Not Unreadable
RFID Card	Not	Access fail	Not Unreadable	Not Unreadable
RFID Key chain	Not	Access fail	Not Unreadable	Not Unreadable

Based on the test result data, RFID readers can only read and allow access to tags that have a pre-registered ID. So it can be concluded that the RFID reader has good performance and has successfully read 4 registered e-KTPs with a maximum reading distance of between 0-2 cm. This registered card is used as an electronic key to open the door, which can add security value because the system will reject cards or tags that are not registered.

Solenoid Door Lock Testing

A Solenoid door lock serves as a locking device on the door. This door lock solenoid will open if the system successfully verifies the e-KTP and OTP code used as security on the door. The device works with the help of a relay that serves as a switch. The Solenoid door lock will be active if it gets a voltage of 9V-12V. Solenoid door lock test results as shown in Table 5.

Table 5. Solenoid door lock testing

Experiment to-	Condition	Rated voltage
1.	Solenoid door lock works	11.78 V
2.	The Solenoid door lock does not work	0 V

Based on the measurement data in the table above, it is known, that when the measured voltage of 11.78 V solenoid door lock can work well, and 0 V when the solenoid door lock does not work.

MC 38 Magnetic Sensor Testing

This magnetic sensor test is useful to find out if this sensor can detect if there is a forced opening attempt on the door. The results of magnetic sensor performance testing are as in Table 6.

Table 6. MC 38 magnetic sensor testing

No.	Condition	Voltage Measurable	Buzzer
1.	Adjacent sensors	0.07 V	OFF
2.	Remote sensors	4.90 V	ON

Based on the data in the table, it is explained that the MC 38 magnetic sensor can work according to its function, where when the door is closed it produces a rated voltage of 0.07 V. While when the door opens it produces a rated voltage of 4.90 V, which causes the buzzer as a security alarm ON as an indication if there is theft by forcibly opening the door.

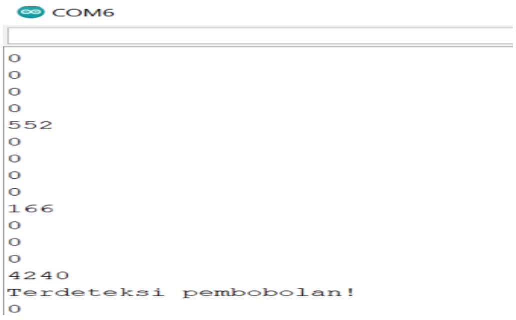
SW-420 Vibrating Testing

This vibrating sensor test serves to determine whether the vibrating sensor has a good response in detecting vibration. Test results as in Table 7.

Table 7. SW-420 vibrating sensor testing

No.	Vibration	SW-420 sensitivity to vibration	Vibration Value	Buzzer
1.	Slow	Not detected	0	OFF
2.	Slow	Not detected	0	OFF
3.	Slow	Not detected	0	OFF
4.	Slow	Not detected	0	OFF
5.	Slow	Not detected	0	OFF
6.	Moderate	Not detected	552	OFF
7.	Moderate	Not detected	166	OFF
8.	Moderate	Not detected	738	OFF
9.	Moderate	Not detected	439	OFF
10.	Moderate	Not detected	1342	OFF
11.	Strong	Detected	4240	ON
12.	Strong	Detected	2794	ON
13.	Strong	Detected	7552	ON
14.	Strong	Detected	2382	ON
15.	Strong	Detected	4577	ON

The test results as shown in the table above are carried out with 3 knock conditions, namely slow, medium, and strong. When the blow or vibration received by the vibrating sensor is <2000, the vibrating sensor does not detect the blow as a breach of the door and the buzzer remains OFF. Conversely, when a blow is worth >2000, the vibrating sensor will activate immediately and the buzzer as a security alarm will sound. From this test, it is concluded that the vibrating sensor can work well according to the design. This value can be seen in the display as shown in figure 6.



```
0
0
0
0
552
0
0
0
0
166
0
0
0
4240
Terdeteksi pembobolan!
0
```

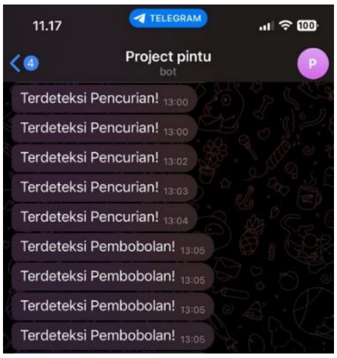
Figure 6. Serial monitor display

Telegram Notification Testing

This test was carried out to determine the effectiveness of telegram work in receiving notifications. When interference is detected in the MC 38 sensor and vibrating sensor as an attempted theft or break-in. Test results as in Table 8 and Table 9.

Table 8. Testing the delivery time of theft messages

No.	Status	Incoming messages	When to receive messages
1.	Remote magnetic sensors	Detected Theft!	1.43
2.	Remote magnetic sensors	Detected Theft!	1.40
3.	Remote magnetic sensors	Detected Theft!	1.20
4.	Remote magnetic sensors	Detected Theft!	1.33
5.	Remote magnetic sensors	Detected theft!	1.46
6.	Remote magnetic sensors	Detected theft!	1.49
7.	Remote magnetic sensors	Detected theft!	1.21



Terdeteksi Pencurian! 13:00
Terdeteksi Pencurian! 13:00
Terdeteksi Pencurian! 13:02
Terdeteksi Pencurian! 13:03
Terdeteksi Pencurian! 13:04
Terdeteksi Pembobolan! 13:05
Terdeteksi Pembobolan! 13:05
Terdeteksi Pembobolan! 13:05
Terdeteksi Pembobolan! 13:05

Figure 7. Telegram messages receive a view

Table 9. Break-in message delivery time testing

No.	Status	Incoming messages	When to receive messages
1.	Sensor detects vibration	Detected break-in!	1.52
2.	Sensor detects vibration	Detected break-in!	1.43
3.	Sensor detects vibration	Detected Break-in!	1.63
4.	Sensor detects vibration	Detected break-in!	1.39
5.	Sensor detects vibration	Detected Break-in!	1.61
6.	Sensor detects vibration	Detected break-in!	1.50
7.	Sensor detects vibration	Detected break-in!	1.28

Based on the test results, the average telegram response time when theft is detected is 1.36 seconds, and when a burglary is detected on the door for 1.48 seconds. The display of theft and break-in messages on the telegram is shown in Figure 7.

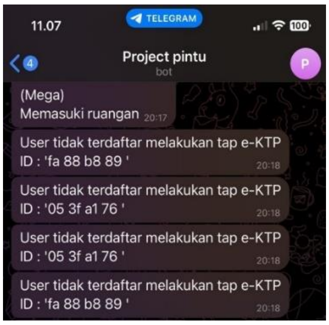
Testing Door Access Monitoring On Telegram

This test serves to determine the response time of telegrams in providing messages related to door activity to the owner. Test results as in Table 10.

Table 10. Testing the time of sending door access messages to telegrams

No.	Status	Incoming messages	When to receive messages
1.	Registered ID	Putri entered the room	1.62
2.	Registered ID	Gita entered the room	1.88
3.	Registered ID	Putri entered the room	1.72
4.	Registered ID	Hepta enters the room	1.58
5.	ID not registered	Unregistered user taps e-KTP	2.78
6.	ID not registered	Unregistered user taps e-KTP	2.56
7.	ID not registered	Unregistered user taps e-KTP	2.30

The test results showed that the fastest time in sending telegram messages was 1.58 seconds with an overall average time calculated using 2.1 seconds. Display of messages sent to the telegram application as shown in Figure 8.



(Mega)
Memasuki ruangan 20:17

User tidak terdaftar melakukan tap e-KTP
ID : 'fa 88 b8 89 ' 20:18

User tidak terdaftar melakukan tap e-KTP
ID : '05 3f a1 76 ' 20:18

User tidak terdaftar melakukan tap e-KTP
ID : '05 3f a1 76 ' 20:18

User tidak terdaftar melakukan tap e-KTP
ID : 'fa 88 b8 89 ' 20:18

Figure 8. Door monitoring message display

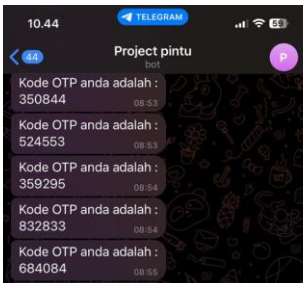
Time Testing To Receive OTP Code To Telegram

This telegram application test serves to determine the speed of the telegram in receiving the OTP code sent when the system successfully verifies the owner's e-KTP. Test results as in Table 11.

Table 11. OTP code delivery time testing

No.	Status	Message enter	Time Receive messages
1.	Send OTP code	OTP: 435262	2.23
2.	Send OTP code	OTP: 401044	2.75
3.	Send OTP code	OTP: 174486	2.57
4.	Send OTP code	OTP: 834643	2.29
5.	Send OTP code	OTP: 705613	2.77
6.	Send OTP code	OTP: 283245	2.42
7.	Send OTP code	OTP: 661839	2.30

The fastest test time in OTP code delivery is 2.23 seconds with an overall average time of 2.47 seconds. After some software testing on the telegram application, it is known that network factors greatly affect the time in receiving messages on telegram, where the better and more stable a network is, the speed in sending messages or notifications to the telegram application is also faster. The display of the OTP code sending a message to telegram is shown in Figure 9.



Kode OTP anda adalah :
350844 08:53

Kode OTP anda adalah :
524553 08:53

Kode OTP anda adalah :
359295 08:54

Kode OTP anda adalah :
832833 08:54

Kode OTP anda adalah :
684084 08:55

Figure 9. Display of telegram OTP messages

CONCLUSION

The door security system uses RFID technology to be able to read the information stored on the e-KTP and OTP code as a password to open the door. Equipped with magnetic sensors, vibration sensors, and buzzers that will be active when there is a theft or break-in with telegram as a notification to the owner. The door security system that has been designed as a whole has good performance and the telegram application can work according to its function in receiving messages when there is a theft or break-in and can record users who open the door.

This designed system still has shortcomings, suggestions for future research are that it can be added with a locking system manually so that the door can still be accessed even though there is no internet network and add the use of batteries as a backup power supply so that the designed tool can still function optimally in the event of a power outage.

REFERENCES

[1] A. Suharsoyo, “Karakter pelaku tindak pidana pencurian dalam tipologi kejahatan pencurian di wilayah sukoharjo,” *Jurisprudence*, vol. 5, no. 1, pp. 64–74, 2015.

[2] R. P. Saputra, “Perkembangan Tindak Pidana Pencurian Di Indonesia,” *J. Pahlawan*, vol. 2, no. 2, pp. 1–8, 2019, doi: 10.1088/1751-8113/44/8/085201.

[3] A. Iskandar, M. Muhajirin, and L. Lisah, “Sistem Keamanan Pintu Berbasis Arduino Mega,” *J. Inform. Upgris*, vol. 3, no. 2, pp. 99–104, 2017, doi: 10.26877/jiu.v3i2.1803.

[4] A. G. Aditya, I. P. Solihin, and Y. Widiastiwi, “Sistem Kunci Pintu Rfid Dan Password Berbasis Arduino,” pp. 81–91, 2020.

[5] A. T. Mahesa, H. Rahmawan, A. Rinharsah, and S. Arifin, “Sistem Keamanan Brankas Berbasis Kartu Rfid E-Ktp,” *J. Teknol. dan Manaj. Inform.*, vol. 5, no. 1, 2019, doi: 10.26905/jtmi.v5i1.3105.

[6] I. W. Suriana, I. G. A. Setiawan, and I. M. S. Graha, “Rancang Bangun Sistem Pengaman Kotak Dana Punia berbasis Mikrokontroler NodeMCU ESP32 dan Aplikasi Telegram,” *J. Ilm. Telsinas Elektro, Sipil dan Tek. Inf.*, vol. 4, no. 2, pp. 75–84, 2021, doi: 10.38043/telsinas.v4i2.3198.

[7] O. R. Arsyad and K. P. Kartika, “Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino,” *JATI (Jurnal Mhs. Tek. Inform.*, vol. 5, no. 1, pp. 1–6, 2021, doi: 10.36040/jati.v5i1.3285.

[8] T. Wisjhnuadji, A. Narendro, and H. Peristiwa, “Kotak Penyimpanan Dengan Sistem Keamanan Berbasis Arduino,” *Semnas Ristek (Seminar Nas. Ris. dan Inov. Teknol.*, vol. 6, no. 1, pp. 947–952, 2022, doi: 10.30998/semnasristek.v6i1.5834.

[9] F. Rahmat and W. Widyastuti, “Sistem Pengaman Brankas Menggunakan Finger Print Dengan Notifikasi SMS Berbasis Arduino Uno,” *2nd Semin. Nas. dan Pros. Scitech 2023*, pp. 432–440, 2023.

[10] M. Zurairah, M. Adam, P. Harahap, and Z. Zaharuddin, “Sistem Keamanan Brankas Berbasis Mikrokontroller Atmega 328 Dengan Munggunakan Kode One Time Password (OTP),” *J. MESIL (Mesin Elektro Sipil)*, vol. 3, no. 1, pp. 1–6, 2022, doi: 10.53695/jm.v3i1.681.

[11] A. Thomas, K. M. Varghese, S. E. Kurian, and E. A. John, “Fingerprint Based Bank Locker Security System,” *Int. Res. J. Eng. Technol.*, vol. 8, no. 7, pp. 2076–2082, 2021.