Journal of Technomaterial Physics
Journal homepage: https://talenta.usu.ac.id/JoTP

Design and Development of a Door Access Prototype Using a Voice Recognition and Password Module Based on the NodeMCU ESP32

Putri Nur Azmina and Nini Firmawati*
Department of Physics, Faculty of Mathematics and Natural Sciences, Universitas Andalas, Padang 25163, Indonesia
*Corresponding Author: ninifirmawati@sci.unand.ac.id

ARTICLE INFO

Article history:
Received 30 April 2026
Revised 9 July 2026
Accepted 17 July 2026
Available online 15 August 2026

E-ISSN: 2656-0755
P-ISSN: 2656-0747

How to cite:
P. N. Azmina and N. Firmawati, "Design and Development of a Door Access Prototype Using a Voice Recognition and Password Module Based on the NodeMCU ESP32," Journal of Technomaterial Physics, vol. 08, no. 02, pp. 122-130, Aug. 2026, doi: 10.32734/jotp.v8i2.25417.

ABSTRACT

Door access security is an important aspect of room protection systems, yet conventional locking methods still have limitations in preventing unauthorized access. This study designed and implemented a NodeMCU ESP32-based smart door prototype integrating voice recognition and password authentication to provide a dual-layer authentication mechanism for smart door access. The system consists of a NodeMCU ESP32 as the main controller, a voice recognition module for voice input, a keypad for password entry, a relay as an actuator, a solenoid door lock as the locking mechanism, and an LCD to display system status. The voice recognition module detects previously trained and stored voice commands to grant access, while unregistered voices are rejected automatically. The keypad password serves as a secondary layer of security. The system was evaluated based on voice recognition performance at different distances and environmental conditions, including quiet, normal, and rainy conditions. Experimental results show that the voice recognition module can detect voices effectively at distances up to 1,250 cm in quiet conditions, 400 cm in normal environments, and 100 cm in noisy or rainy conditions. Overall, the prototype successfully implemented a dual-security access mechanism combining voice recognition and password authentication, while providing additional real-time security monitoring through the integrated system.

Keywords: Keypad, NodeMCU ESP32, Relay, Solenoid Doorlock, Voice Recognition Module

ABSTRAK

Keamanan akses pintu merupakan aspek penting dalam sistem perlindungan ruangan, namun metode penguncian konvensional masih memiliki keterbatasan dalam mencegah akses yang tidak sah. Penelitian ini merancang dan mengimplementasikan prototipe pintu pintar berbasis NodeMCU ESP32 yang mengintegrasikan pengenalan suara dan otentikasi kata sandi untuk menyediakan mekanisme otentikasi berlapis ganda bagi akses pintu pintar. Sistem ini terdiri dari NodeMCU ESP32 sebagai pengontrol utama, modul pengenalan suara untuk masukan suara, papan tombol untuk memasukkan kata sandi, relai sebagai aktuator, kunci pintu solenoida sebagai mekanisme penguncian, dan layar LCD untuk menampilkan status sistem. Modul pengenalan suara mendeteksi perintah suara yang telah dilatih dan disimpan sebelumnya untuk memberikan akses, sementara suara yang tidak terdaftar ditolak secara otomatis. Kata sandi pada papan tombol berfungsi sebagai lapisan keamanan sekunder. Sistem ini dievaluasi berdasarkan kinerja pengenalan suara pada jarak dan kondisi lingkungan yang berbeda, termasuk kondisi tenang, normal, dan hujan. Hasil eksperimen menunjukkan bahwa modul pengenalan suara dapat mendeteksi suara secara efektif pada jarak hingga 1.250 cm dalam kondisi tenang, 400 cm dalam lingkungan normal, dan 100 cm dalam kondisi bising atau hujan. Secara keseluruhan, prototipe ini berhasil menerapkan mekanisme akses keamanan ganda yang menggabungkan pengenalan suara dan otentikasi kata sandi, sekaligus menyediakan pemantauan keamanan real-time tambahan melalui sistem terintegrasi.

Kata kunci: Kunci Pintu Solenoida, Modul Pengenalan Suara, NodeMCU ESP32, Papan Tombol, Relai

1. Introduction

Smart home technology has improved residential security systems through automated access control [1], [2]. Conventional door locks still have limitations, such as the risk of loss, duplication, and unauthorized access [3]. Therefore, a multi-layered security system is needed to enhance door access protection [4]. Voice recognition technology enables users to interact with electronic systems through voice commands by converting audio signals into digital patterns and comparing them with stored commands. This technology has been applied in smart access systems to provide more flexible user interaction [5]. In addition to serving as an interaction method, voice can also be utilized as a biometric authentication mechanism because the characteristics of an individual's speech can be analyzed to verify or recognize the speaker. However, voice-based authentication must also consider security and privacy issues because voice biometric systems may be exposed to spoofing and other forms of attack [6].

Wardoyo designed a microcontroller-based smart home security system using fingerprint and password authentication with an emergency entry feature via the HC-05 Bluetooth module. The system utilizes the ZM-20 fingerprint sensor and a keypad, with data stored in the Arduino Mega's EEPROM. The research results showed that the system worked well; however, the 80.83% user success rate was influenced by users forgetting their passwords, so the inclusion of a password-reset feature and notifications via Telegram was recommended [7]. Gultom and Susanto developed an Internet of Things (IoT)-based smart lock using a piezoelectric sensor to detect knock sounds and the Blynk app as an alternative access method. The study achieved an 80% success rate with the Blynk app and less than 60% with the knock-sound method, so the use of voice recognition is recommended [8]. Mustaqin and Triandi designed an automatic door-locking system based on voice commands via the Arduino Voice Control app connected to an Arduino Uno via Bluetooth; however, the system requires a connection time before it can be used. Meanwhile [9], Okafor and Leonard developed a door access system using RFID and voice recognition equipped with a PIR sensor, LCD, and solenoid door lock to control user access, and suggested the use of a 4x4 matrix keypad as an additional security measure for the system [10].

More recent research has demonstrated the feasibility of integrating voice recognition directly into IoT-based door security systems. Syafrizal et al. developed a door-lock security system based on voice recognition and natural language processing using an ESP32 Dev Kit V1, MQTT communication, relay, and solenoid door lock. Their system was designed to recognize variations in voice commands for opening and closing the door, demonstrating the potential of voice recognition as a practical access-control mechanism in IoT-based home security [11]. Similarly, Ardiansyah et al. developed an IoT-based smart door system that combines voice recognition and knock code as two authentication methods, together with manual control using a physical push button. Their work highlights the potential of combining different access methods to improve accessibility and flexibility in smart door systems [12].

Although voice recognition provides convenient and contactless interaction, security considerations remain important. Voice authentication has also been investigated as a privacy-preserving security mechanism for connected and IoT devices. Alattar proposed a hands-free voice authentication system that incorporates speaker recognition and anti-spoofing mechanisms while protecting users' voice biometric information. These findings demonstrate the potential of voice authentication as an additional security factor for connected devices [13]. Furthermore, voice biometric systems may raise privacy and fairness concerns because speech contains sensitive speaker-related information. Previous research has shown that demographic information can influence the performance and privacy characteristics of voice biometric systems, highlighting the importance of considering these factors when implementing voice-based authentication [14]. Bonastre et al. reported that voice biometric systems require particular attention to security and privacy, including protection against spoofing attacks and the development of appropriate countermeasures. Their work also highlights the importance of benchmarking methods for evaluating the security of automatic speaker verification systems [6]. These findings indicate that relying on voice recognition alone may not provide sufficient protection for access-control applications, particularly when the system is intended to secure physical spaces. Unlike previous studies that relied on a single authentication method or external smartphone applications, the proposed system integrates trained voice-command recognition, keypad-based password verification, and real-time Telegram notifications in a single ESP32 platform. This integration provides a dual-layer authentication mechanism and real-time security monitoring, thereby improving both the practicality and security of smart door-access systems.

The objective of this study is to design and develop a NodeMCU ESP32-based smart door access system using trained voice-command recognition and password authentication. The main contribution of the proposed system is the integration of dual-layer authentication with automatic Telegram notifications after three consecutive incorrect password attempts. The system performance was evaluated based on voice-command recognition under different environmental conditions and distances, door access functionality, response time, and Telegram notification performance.

2. Method

2.1. Equipment and Materials

The equipment used in this study includes a laptop, a breadboard, a PCB, a soldering iron, a battery, a sound level meter and a battery box. Sound intensity levels were measured using a Hadabotest HT64 digital sound level meter. This sound level meter has a measurement range of 30–130 dB and an accuracy of ±1.5–5 dB, which is suitable for measuring sound intensity levels during speech recognition testing. The materials used in this study include a voice recognition DF2301Q V1.1 module, a relay, a solenoid door lock, a keypad, a NodeMCU ESP32, an LCD, and jumpers.

2.2. Hardware System Design and Testing

The voice recognition module is trained by recording predefined voice commands, and it stores these commands or fixed words within the module. The recorded voice patterns are stored in the module's internal memory as voice commands. During operation, the input voice is compared to the stored patterns to determine whether the command is recognized. The voice recognition module memorizes voice commands through a training process before system operation. During the training process, the user records a specific voice command, and the module extracts the voice pattern from the recorded signal. The extracted pattern is then stored in the internal memory of the voice recognition module with a specific command ID. During operation, the input voice command is processed and compared with the stored voice patterns. If the input matches the trained pattern, the module sends the corresponding command ID to the NodeMCU ESP32 for further processing [15].

The system begins by inputting a voice command, followed by entering a password via the keypad to unlock the door. If the voice input is successfully recognized by the system, the user can proceed to the password input stage, however, if the voice does not match the stored data, the password cannot be entered. To enhance security, the system limits password input attempts to three times. If the user enters the wrong password three times, the system will send a notification via Telegram to the registered user to confirm door access. If the access is indeed initiated by the user, the system will send the password; however, if it is not the registered user, the door will remain locked.

As shown in Figure 1, recorded audio is processed by the voice recognition module to match data stored on the NodeMCU ESP32, while the password entered via the keypad is processed by the NodeMCU ESP32. Once the verification process is complete, the system will unlock the door using the solenoid door lock if the access credentials are correct, and the LCD will display the message "door open." Conversely, if the access credentials do not match, the door remains locked. The system uses two power supplies because the solenoid door lock requires a 12 V voltage to operate optimally, while the NodeMCU ESP32 can only accept a maximum input voltage of 5 V.

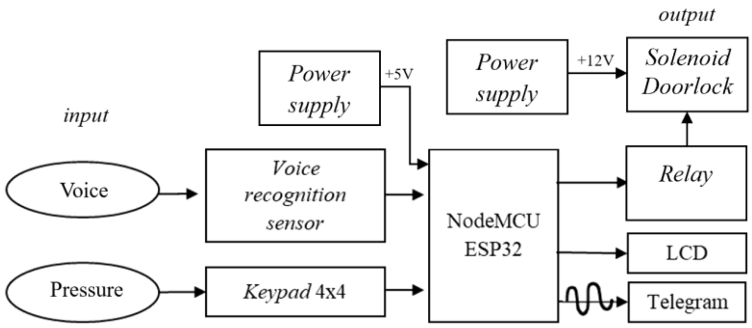

Figure 1. System block diagram.

Figure 2 shows the complete circuit for operating all components to allow access to the door. The keypad is connected to the NodeMCU ESP32 on pins 24 through 31 for password input, which will be displayed on the LCD. The NodeMCU ESP32's 3.3V pin is connected to the VCC of the relay, voice recognition module, and LCD. The NodeMCU ESP32's GND pin is connected to the GND of the relay, voice recognition module, and LCD. Pin 33 of the NodeMCU ESP32 is connected to the D/T pin on the voice recognition module and the SDA pin on the LCD. Pin 36 is connected to the C/R pin on the voice recognition module and the SCL pin on the LCD. Pin 31 is connected to the relay's IN pin. The door lock solenoid is connected to the relay's COM and NO pins, with the NO pin connected to a +12V power source, and the NodeMCU ESP32 is connected to a 5V power source.

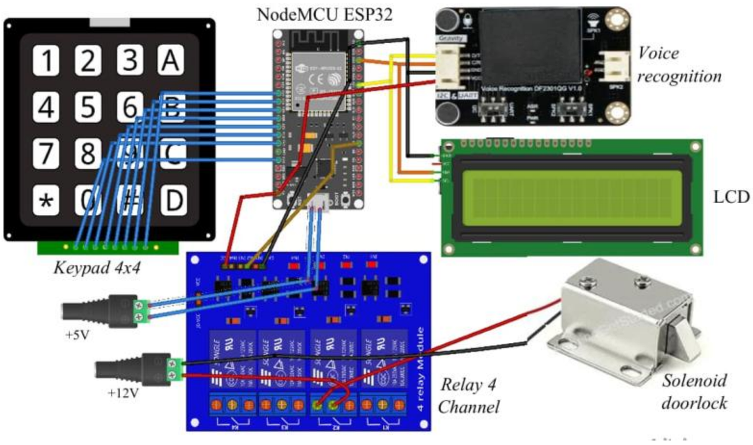

Figure 2. Overall system circuit.

The overall system circuit consists of a voice recognition module, a NodeMCU ESP32, a 4x4 keypad, an LCD, a solenoid door lock, a relay, and a Telegram bot for notifications. The circuit produces a voice-recognition and password-based home door security system that displays access status on the LCD and sends notifications to users via Telegram. The physical layout of the system is shown in Figure 3.

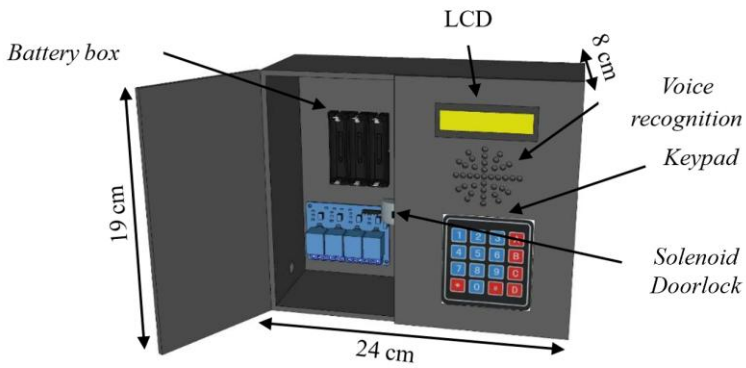

Figure 3. Physical design of the system.

2.3. Software System Design and Testing

The design of the door access system using voice recognition and a password is shown in Figure 4. In the flowchart, the LCD initially displays "Waiting for voice" and detects the voice input from the voice recognition module. If the spoken phrase is "open the door," the LCD displays "Enter PIN," and the process continues with entering the password. However, if the spoken command is incorrect, the LCD display remains unchanged. If the 'C' button is pressed, the password can be entered. Alternatively, the system can be accessed using a phrase previously learned by the module to directly activate the door solenoid, allowing the door to open without a password. The password is entered after the phrase "open the door," detected by the module, is successfully recognized. If the entered password is correct, the LCD displays "door opened" and the door lock solenoid activates; however, if the entered password is incorrect, the LCD displays "incorrect password, please try again," and the user must re-enter the password, with up to three attempts allowed. After three failed attempts, the LCD will display "Shutdown 30s," and the device will be disabled for 30 seconds. Afterward, the device will send the password and a notification via Telegram to registered users. Thus, if anyone other than a registered user attempts to access the door without knowing the password, the device remains locked and the door lock solenoid remains deactivated. When the door is successfully opened, if the command "close the door" is given, the device will deactivate the solenoid door lock; however, if no such command is given, the device will automatically close the door within 5 seconds.

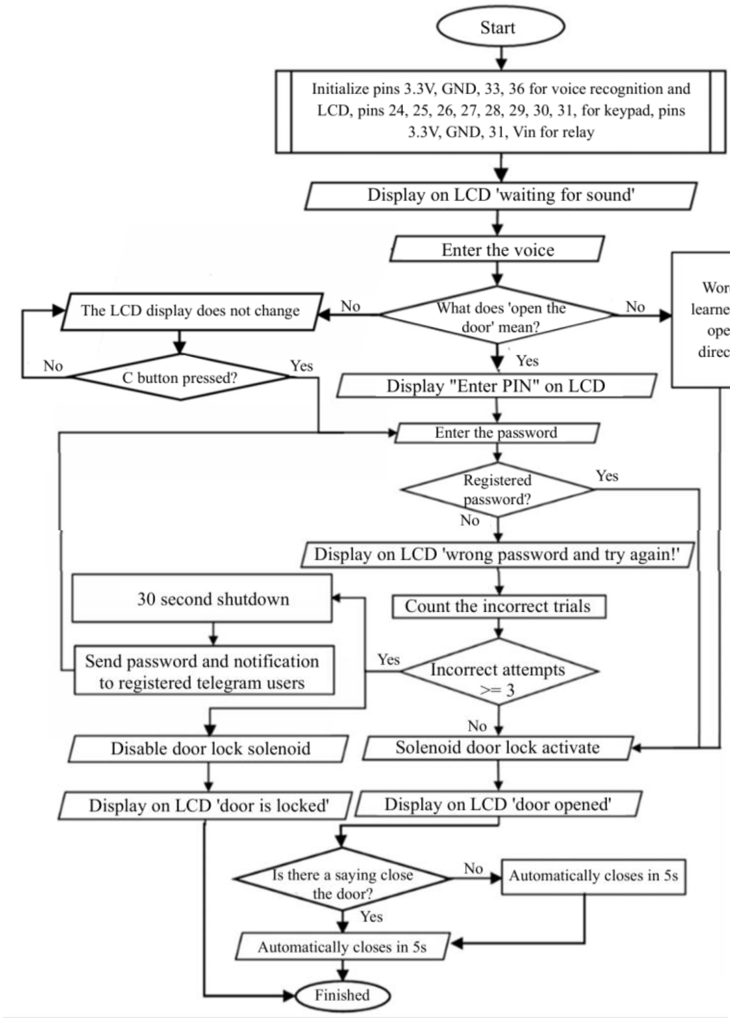

Figure 4. Software system flowchart.

The proposed system employs two-layer authentication. The user first speaks a previously trained voice command, which is verified by the voice recognition module. If the command is recognized, the ESP32 requests password entry through the keypad. The entered password is then verified before the relay activates the solenoid door lock. If three consecutive incorrect password attempts occur, the system temporarily disables access and sends a warning notification to the registered Telegram account. The Telegram Bot is used to provide real-time notifications regarding successful access, incorrect password attempts, and temporary system lockout after three consecutive failed password entries.

3. Results and Discussion

3.1. Voice Recognition Module Testing

Voice recognition performance using the ESP32 was tested under quiet, normal, and rainy conditions. Voice recognition performance under quiet conditions, with sound intensity levels ranging from 55 dB to 69 dB, was tested using the phrase “Hello Robot” five times as the wake-up word to activate the device. During the voice recognition test, the sound intensity level was measured at the sound source and near the voice recognition module. The measurement was performed by placing the sound level meter at the same position as the voice input direction. The measured values were recorded in dB for each testing distance and environmental condition. The sound intensity was measured at two different positions. S (Sound Source) denotes the sound intensity measured near the user while speaking the voice command, whereas T (Voice Recognition Module) denotes the sound intensity measured near the microphone of the voice recognition module. A digital sound level meter was placed alternately near the sound source and near the voice recognition module to record the sound intensity at each measurement point. The test results are shown in Table 1.

Table 1. Voice recognition test results in a quiet environment.

Distance (cm)	Sound Intensity Level (dB) at the Sound Source (S) and at the Receiver (T) for Module and Experiment No-									
	S	T-1	S	T-2	S	T-3	S	T-4	S	T-5
50	87	✓ (79)	89	✓ (83)	88	✓ (81)	85	✓ (79)	92	✓ (81)
250	97	✓ (74)	96	✓ (77)	98	✓ (77)	96	✓ (77)	98	✓ (76)
500	110	✓ (80)	107	✓ (79)	107	✓ (83)	109	X (82)	109	X (83)
750	110	X (78)	112	✓ (80)	109	✓ (83)	117	✓ (80)	113	✓ (79)
1,000	113	✓ (74)	110	✓ (72)	109	✓ (75)	110	✓ (74)	110	X (74)
1,250	113	X (75)	112	X (74)	112	X (70)	113	X (69)	115	X (71)
1,300	113	X (71)	116	X (71)	114	X (69)	115	X (69)	119	X (68)

Based on Table 1, in a quiet environment, the voice recognition system can detect (✓) and fail to detect (X) sounds up to a distance of 1,300 cm. The source sound intensity varies from 85 dB to 119 dB, and the received sound intensity ranges from 83 dB to 68 dB. As shown in Table 1, the source sound intensity (S) was measured using a sound level meter capable of detecting sound intensity. The received sound intensity (T) near the module decreases as the distance between the sound source and the sound level meter increases. The full detection range of the module is from 50 cm to 250 cm in five experiments the module detected all sounds within this range, because the voice signal received by the module was still strong and had minimal interference. At longer distances, a 1,250 cm the recognition success rate decreased because the received sound intensity decreased, causing the voice signal to become weaker and more difficult for the module to match with the stored voice pattern. This aligns with the inverse relationship between sound intensity and distance. Under normal conditions, the test results are shown in Table 2.

Table 2. Voice recognition test results under normal conditions (77 to 90 dB).

Distance (cm)	Sound Intensity Level (dB) at the Sound Source (S) and at the Receiver (T) for Module and Experiment No-									
	S	T-1	S	T-2	S	T-3	S	T-4	S	T-5
50	105	✓ (87)	107	X (88)	96	✓ (88)	98	✓ (89)	99	✓ (88)
150	108	✓ (87)	108	✓ (88)	108	✓ (88)	108	✓ (89)	100	✓ (89)
250	101	X (89)	107	✓ (88)	105	✓ (89)	107	✓ (88)	101	✓ (88)
350	102	X (85)	107	✓ (85)	100	X (85)	105	X (89)	99	✓ (88)
450	107	X (88)	110	X (88)	106	X (88)	110	X (88)	98	X (86)
500	109	X (89)	116	X (89)	113	X (88)	109	X (89)	105	X (89)

Based on Table 2, under normal conditions, the voice recognition system can detect (✓) or fail to detect (X) sounds from a distance of 50 cm to 500 cm. The module can receive sounds and activate the system up to 400 cm, with 3 out of 5 trials resulting in detection. The failure observed in the T-2 trial at 50 cm under normal conditions does not indicate that a shorter distance always provides better performance. The recognition result can also be affected by variations in voice pronunciation, speaking intensity, background noise, and the matching accuracy of the trained voice pattern. Therefore, occasional failures may occur even at closer distances. The received sound is not only the source sound but also includes noise or interference from the surroundings, therefore, under normal conditions, the module cannot recognize sounds beyond a quiet environment. Noise or sound interference can affect the source sound signal or wave, thereby reducing its quality.

Table 3. Results of voice recognition testing in rainy conditions.

Distance (cm)	Experiment No-				
	1	2	3	4	5
50	Success	Success	Success	Success	Success
100	Failure	Failure	Success	Failure	Failure
150	Failure	Failure	Failure	Failure	Failure

Based on Table 3, during rain the device cannot detect sounds from a distance; however, after testing, the device was able to detect sounds up to 100 cm away from the device. Therefore, during rain, the device cannot detect sounds from a distance. During rain or in noisy conditions, the received noise level is higher, which reduces the effective detection range of the module. The sound intensity level was not measured during rainy conditions because the test was conducted to evaluate the effect of environmental noise on voice recognition performance rather than to characterize the exact noise intensity. The rainy condition was considered a high-noise environment where the main observation parameter was the recognition success or failure of the module.

The performance of the proposed voice recognition system was compared with previous smart door access studies. Previous research by Mustaqin and Triandi developed a voice-controlled door locking system using Arduino and an Android-based voice control application; however, the system required a connection process between the application and the device before operation. Meanwhile, Gultom and Susanto implemented a smart lock system using sound detection, but the recognition success rate was limited under certain conditions. Previous studies have also demonstrated the use of voice authentication as a security mechanism for connected and IoT-based devices. Alattar et al. proposed a privacy-preserving hands-free voice authentication system that incorporates speaker recognition and anti-spoofing mechanisms, demonstrating the potential of voice authentication for secure connected-device applications. In addition, Chouchane et al. highlighted that voice biometric systems should consider privacy and fairness issues because speaker-related characteristics can affect biometric system performance. Bonastre et al. further emphasized the importance of security and privacy evaluation in voice biometric systems, particularly in relation to spoofing attacks and countermeasures. In this study, the voice recognition module stores trained voice commands directly in the module, allowing the system to recognize commands without relying on a smartphone connection. The test results show that the proposed system can recognize trained commands up to a certain distance, although the performance decreases under noisy conditions. This indicates that environmental noise remains a major factor affecting voice recognition performance.

3.2. Final System Testing

Final system testing was conducted to ensure that the device operates according to the customized program. The results of the door access testing can be seen in Table 4.

Table 4. Voice recognition test results in rainy conditions.

Voice Command	Voice Access	Password Access	Door Action	Response Time	Telegram Status
'Open the door'	Detected	Correct	Open	33s	"Access granted, door open"
'Open the door'	Detected	Incorrect	Closed	0s	"Incorrect PIN (1)"
'Close the door	Detected	-	Closed	9s	-
Learned Word	Detected	-	Open	9s	"Voice access granted"
'Password OK'	Not Detected	-	Closed	-	-
'*Keypad* active'	Not Detected	-	Closed	-	-
'Turn On prototype'	Not Detected	-	Closed	-	-
'Hello robot'	Detected	-	Closed	-	-
'Forget	Detected	-	Closed	-	-
'Clear Screen'	Detected	-	Closed	-	-

According to Table 4, the device can operate using voice commands and a passcode to unlock and lock the door after two access codes have been entered as programmed. An undetected voice is one not registered in the voice module, as voices must first be registered in the module; once registered, the device reads them as numbers in the command to identify them. Incorrect passwords entered are counted up to three times, after which Telegram sends a notification containing the correct password. The response time of the system varies depending on the access verification process. Based on Table 4, the longest response time occurs during successful access using voice recognition and password verification. This is because the system requires several processes, including voice command recognition, password validation, relay activation, and Telegram notification transmission. Meanwhile, a shorter response time occurs for incorrect password input or voice-only verification because fewer processes are executed. The response delay is also affected by the communication time between the ESP32 and Telegram server through the Wi-Fi connection. The implementation of password verification as a second authentication layer provides an additional security mechanism compared with systems that rely only on voice recognition. This approach is particularly relevant because previous studies have identified security and privacy considerations in voice biometric systems [11–13]. The combination of voice recognition and password authentication in the proposed system therefore reduces reliance on a single authentication method while maintaining the convenience of voice-based access. Notifications and the device's status can be viewed in the Telegram app, as shown in Figure 5.

Figure 5. Telegram interface.

Figure 5 shows the Telegram bot notification interface used in the proposed smart door access system. The system sends real-time notifications to users regarding door access activities, including successful PIN authentication, voice access verification, sound activation status, and emergency exit operations. In addition, the system provides security alerts when incorrect PIN entries are detected. After three consecutive incorrect PIN attempts, the system automatically sends a warning notification indicating suspicious access activity. This real-time notification mechanism provides an additional monitoring function by allowing users to receive information about access attempts without directly observing the door. Therefore, the Telegram integration complements the dual-layer authentication mechanism by providing remote security monitoring in addition to local access control. These notification features enhance user monitoring and improve the overall security of the smart home door access system.

4. Conclusion

Based on the testing and analysis result, the developed door security system successfully implements two access mode, voice command ("open the door") and keypad password entry. The system therefore provides a dual-layer access mechanism by combining voice recognition and keypad password authentication. The voice recognition module is capable of recognizing previously trained voice commands stored in its internal memory, although its performance is affected by environmental factors such as distance and background noise. Based on the experimental results, the voice recognition module can recognize commands at distances of up to 1,250 cm under quiet conditions, approximately 400 cm under normal conditions, and 100 cm under rainy conditions. In addition, the system can send real-time access code notification to the user's Telegram account when connected to a Wi-Fi network. The Telegram notification feature also enables users to monitor access attempts, including incorrect password attempts. Overall, the proposed system demonstrates the feasibility of integrating voice recognition, keypad password authentication, and Telegram-based monitoring into an ESP32 smart door security system.

Acknowledgments

The authors would like to thank the staff and colleagues at the Electronics and Instrumentation Laboratory at Andalas University for their contributions to the calibration and testing processes, as well as for the facilities and technical support provided during this research.

References

[1] M. Muslihudin, W. Renvilia, T. Taufiq, A. Andoyo, and F. Susanto, "Implementasi Aplikasi Rumah Pintar Berbasis Arduino dengan Arduino Mikrokontroller," *J. Keteknikan dan Sains*, vol. 1, pp. 23–31, 2018.

[2] N. A. Dewy, "Kontrol Akses Pintu Rumah Menerapkan Konsep OTP (One Time Password) untuk Meningkatkan Keamanan dengan Implementasi Iot (Internet of Things)," *J. Mahasiswa Teknik Informatika*, vol. 2, pp. 467–473, 2018.

[3] R. Suwartika and G. Sembada, "Perancangan Sistem Keamanan Menggunakan Solenoid Door Lock Berbasis Arduino Uno pada Pintu Laboratorium di PT. XYZ," *J. Elektro-Komputer Teknik (E-KOMTEK)*, vol. 4, pp. 62–74, 2020.

[4] W. Wiraditama, D. Candra, A. P. Nugraha, and S. Sulartopo, "Sistem Keamanan Rumah Menggunakan Sensor Passive Infrared," *Seminar Nasional Teknologi dan Multidisiplin Ilmu (SEMNASTEKMU)*, vol. 3, pp. 200–210, 2023.

[5] W. A. Vincent, I. P. Satwika, and A. A. A. P. Ardyanti, "Implementasi Speech Recognition dalam Melakukan Automasi pada Perangkat Elektronik Rumah Menggunakan ESP8266," *J. Ilmiah Komputer*, vol. 16, pp. 13–24, 2020.

[6] J.-F. Bonastre *et al.,* "Benchmarking and challenges in security and privacy for voice biometrics," *Prociding ISCA Symposium on Security and Privacy in Speech Communication*, pp. 52–56, 2021.

[7] J. Wardoyo, N. Hudallah, and A. B. Utomo, "Smart Home Security System Berbasis Mikrokontroller," *J. SIMETRIS*, vol. 10, pp. 367–374, 2019.

[8] D. Gultom and M. F. Susanto, "Studi Aplikasi Smartlock pada Pintu Rumah dengan Arduino Berbasis Iot dengan Sensor Suara," *Prosiding Indrustrial Research Workshop and National Seminar,* pp. 239–245, 2020.

[9] R. Mustaqin and B. Triandi, "Perancangan Alat Pengunci Pintu dengan Perintah Suara Melalui Android," *J. Info Digit*, vol. 2, pp. 501–513, 2024.

[10] C. Okafor and A. T. Leonard, "Door Access Control Using RFID and Voice recognition System," *International Journal For Research in Applied Science and Engineering Technology*, vol.10, pp.157–163, 2022.

[11] M. Syafrizal, V. Ikawati, A. Siswanto, and N. Lestari, "Sistem Keamanan Door Lock Berbasis Voice Recognition dengan Natural Language Processing," *Infotronik: Jurnal Teknologi Informasi dan Elektronika*, vol. 9, 2024.

[12] R. A. Ardiansyah, A. Rasyid, Koesmarijanto, and Adzikirani, "Integration of Voice Recognition and Knock Code in an IoT-Based Smart Door System for Inclusive Security," *JURNAL JARTEL: Jurnal Jaringan Telekomunikasi*, vol. 16, pp. 213–220, 2026.

[13] Z. S. Alattar, T. Abbes, and F. Zerai, "Privacy-preserving hands-free voice authentication leveraging edge technology," *Security and Privacy*, vol. 6, 2023.

[14] O. Chouchane, M. Panariello, C. Galdi, M. Todisco, and N. W. D. Evans, "Fairness and Privacy in Voice Biometrics: A Study of Gender Influences Using wav2vec 2.0," *Procedings of the 22nd International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–7, 2023.

[15] D. Al-Fraihat, F. Alzyoud, Y. Sharrab, and A. A. Maaita, "Speech Recognition Utilizing Deep Learning: A Systematic Review of The Latest Developments," Article in *Human-Centric Computing and Information Sciences*, 2024.