Integration of Voice Recognition and Knock Code in an IoT-Based Smart Door System for Inclusive Security

Reza Arjuna Ardiansyah[1], Abdul Rasyid[2], Koesmarijanto[3*], Adzikirani[4]

[1,4] Digital Telecommunication Network Study Program, Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia.

[2,3] Telecommunication Engineering Study Program, Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia.

[1]2141160112@student.polinema.ac.id , [2]abdul.rasyid@polinema.ac.id, [3]koesmarijanto@polinema.ac.id, [4]adzikirani@polinema.ac.id

***Abstract*— The rapid advancement of Internet of Things (IoT) technology has opened up significant opportunities in developing smarter and more adaptive home security systems. One of the main challenges in conventional security systems lies in their limited accessibility for users with special needs, such as the elderly, children, or individuals with disabilities. To address this issue, this study proposes an innovative solution in the form of an IoT-based smart door system that integrates two distinct authentication methods: voice recognition and knock code, along with manual control via a physical push button. The system is built using the ESP32 microcontroller as the main controller, with Firebase utilized for real-time communication between the hardware and the Android application. The research follows a Research and Development (R&D) approach with a quantitative experimental method. System performance was evaluated through a series of structured tests on key parameters, including authentication accuracy, response speed, data synchronization stability with Firebase, and reliability during power switching conditions. The results demonstrate that the system responds effectively to commands with an average delay of less than two seconds and remains stable during network disruptions or power outages. The primary advantage of this system lies in its inclusive and flexible design, enabling diverse user groups to securely access doors without relying on a single authentication method. Therefore, this system not only enhances physical security but also adds value in terms of comfort and accessibility. This study is expected to serve as a reference for future development of intelligent security systems that prioritize inclusivity and user-centered functionality in modern smart homes.**

Keywords*— *Door Security, ESP32, Firebase, Internet of Things, Knock Code, Smart Door, Voice Command

I. INTRODUCTION

Technological advancements in the Internet of Things (IoT) have brought significant changes to many aspects of daily life, particularly in home security systems. Statista (2024) reported that the number of IoT devices worldwide reached approximately 15.14 billion units in 2023 and is projected to almost double to 29.4 billion by 2030 [1]. This rapid growth reflects the increasing demand for automation that offers greater efficiency, convenience, and security in residential settings. In Indonesia, the adoption of smart home technology is also experiencing notable growth [2]-[5]. According to IDC Indonesia (2022), the use of digital security systems has increased by around 21% annually, with smart door and automatic access features among the most preferred solutions to improve comfort and safety for homeowners [6]. Despite this progress, most existing smart door systems still rely on a single authentication method such as RFID cards [7], numeric PINs [8], or biometric fingerprints [9]. This approach has limitations in terms of accessibility for elderly users, individuals with disabilities, or those in emergency situations who are unable to interact physically with the device [10]. For example, during critical conditions such as injury, illness, or disaster evacuation, requiring physical contact to unlock doors may be impractical or even dangerous [11]. Furthermore, depending only on one authentication factor increases vulnerability to security breaches, such as password leaks, RFID card duplication, or fingerprint recognition failures caused by sensor errors, dirt, or humidity [12]. Previous studies have mostly focused on single authentication approaches. Rahman et al. (2021) achieved 93% accuracy using voice recognition for smart door systems, highlighting the potential of voice commands as a contactless input method. Meanwhile, Nugroho and Santosa (2020) developed a knock code-based system using piezoelectric sensors with an accuracy of 87%, allowing users to authenticate through specific knock patterns on the door surface [13]. However, neither research integrated both technologies into a unified system to enhance flexibility, security, and inclusiveness [14]. Additionally, limited studies have provided comprehensive quantitative evaluations on multi-modal authentication systems, such as measuring their combined accuracy, response time, operational reliability under real usage conditions, and feasibility for inclusive security applications [15]. To address these gaps, this research proposes the design and implementation of a smart door system that integrates knock code and voice recognition authentication using the ESP32 microcontroller and Firebase Realtime Database as its cloud-based data management platform. The system enables users to unlock doors by either performing

*Corresponding Author

specific knock patterns or issuing voice commands via an Android application connected to Firebase for real-time data synchronization and monitoring. The knock code feature utilizes a piezoelectric sensor to detect vibrations corresponding to predefined patterns, while the voice recognition feature uses the smartphone's Google Voice API for command input. The objectives of this study are to design, develop, and evaluate a dual authentication smart door system, analyze its performance in terms of accuracy, response time, and operational reliability, and assess its feasibility for inclusive smart home security applications. This research is expected to provide a practical, adaptive, and inclusive smart door solution that enhances safety and accessibility for various user groups, including elderly individuals and people with disabilities, while supporting the advancement of IoT-based home automation technologies in modern society.

II. METHOD

A. Research Design

This study adopts a Research and Development (R&D) approach with a quantitative experimental framework. The objective is to design, build, and evaluate an IoT-based smart door system that integrates knock code authentication with voice recognition for enhanced home security. The research focuses on developing a fully functional prototype and measuring its performance through systematic testing. The development process consists of five key phases: needs analysis, hardware-software integration, system implementation, performance testing, and data evaluation. The final prototype was deployed in an indoor environment with stable network conditions to ensure reliable operation during the testing phase.

B. System Architecture:

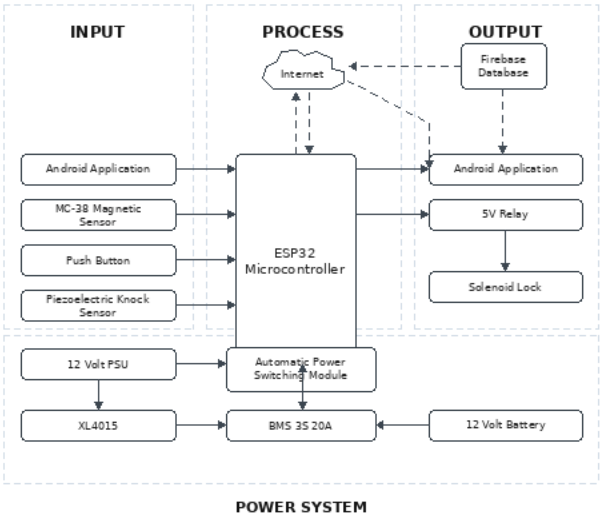

Figure 1. System Block Diagram

Figure 1 illustrates the block diagram of the smart door system designed in this study. The system consists of four main parts: Input, Process, Output, and Power System. The Input section includes an Android application for voice commands, a magnetic sensor MC-38 to detect door open or closed status, a push button for manual unlocking from inside, and a piezoelectric knock sensor to detect specific knock patterns for authentication. These inputs are processed by the ESP32 microcontroller, which acts as the central controller in the Process section. The ESP32 connects to the Internet and communicates with the Firebase Realtime Database, allowing real-time synchronization between the device and the Android application. The Output section consists of a relay module that drives the solenoid lock to open or lock the door based on valid authentication input, and also includes the Android app which displays door status updates to the user. The Power System ensures continuous operation of the entire setup. It uses a 12 Volt power supply as the main source, with an XL4015 DC-DC step-down module and BMS 3S 20A battery management system to regulate and protect the 12 Volt lithium battery, which serves as backup power. The Automatic Power Switching module enables seamless transition between the main power supply and battery during power outages to maintain system reliability. Overall, this integrated design enables the smart door to provide dual authentication methods, combining knock code and voice recognition, while ensuring stable operation, real-time monitoring, and improved security and accessibility for various user conditions.

C. System Flowchart

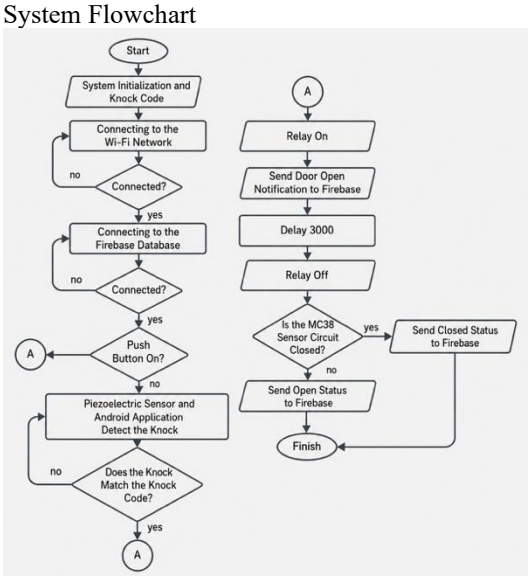

Figure 3. System Flowchart

The system begins with an initialization process and the loading of pre-programmed knock pattern data used as authentication keys. After this initial stage, the ESP32 microcontroller will attempt to connect to the Wi-Fi network to enable communication with Firebase services and the Android application. If the network connection fails, the system will continuously retry until a successful connection is established. Once connected to Wi-Fi, the process continues by linking to the Firebase database, which enables real-time data exchange between the system and the user via the Android application. The next step is checking the condition of the push button. This button functions as a quick access method from inside the room. If the button is pressed, the system will immediately activate the relay and unlock the door automatically without requiring

a knock, voice command, or internet connection. This feature provides an emergency access solution or operational convenience when the user is inside the house. However, if the push button is not pressed, the system will activate the piezoelectric sensor to detect knock patterns on the door surface. In addition, the system will wait for possible commands from the Android application as an alternative input. The Android application can recognize the user's voice commands and send them to Firebase. Once the ESP32 receives and verifies the input, either from a valid knock pattern or a recognized voice command, the system will activate the relay to unlock the door via the solenoid lock. After the relay is activated and the door is unlocked, the system will send a "door open" status to Firebase, then provide a three-second delay to allow the user to physically open the door. After the wait time is over, the relay will be deactivated automatically to re-lock the system. Next, the door status will be checked using the MC-38 magnetic sensor. If the sensor detects that the door is closed, the system will send a "door closed" status to Firebase. Conversely, if the door remains open, that status will also be sent to Firebase. After the entire process is complete, the system returns to its initial state and is ready to receive new inputs.

D. Software Implementation

The smart door prototype is physically constructed using the following components:

- ESP32 microcontroller with Wi-Fi capability
- Piezoelectric sensor for knock input detection
- Solenoid lock + relay to drive door mechanism
- Push button for local opening
- Magnetic sensor (MC-38) for door position feedback
- Power Supply 12V + Lithium Battery Backup for continuity
- Automatic power switching module + XL4015 step-down converter to handle power transitions

All components are mounted on a wooden prototype door. The circuit is housed in a protective enclosure to ensure durability and ease of maintenance.

E. Data Flow Modeling

To better understand the internal logic and data processing workflow of the smart door system, a two-level Data Flow Diagram (DFD) model was constructed. The DFDs serve to illustrate how input from users and sensors is transformed, validated, and acted upon within the system, as well as how data is synchronized between components in real time.

a. DFD Level 0 – Context Diagram

At the highest level, the system consists of three main entities:

- User: Interacts with the system via the mobile application to issue commands and monitor door status.
- ESP32 System: Acts as the central processor, controlling physical door hardware and interpreting input from sensors.
- Firebase Realtime Database: Functions as a cloud intermediary that enables real-time data exchange between the application and ESP32.

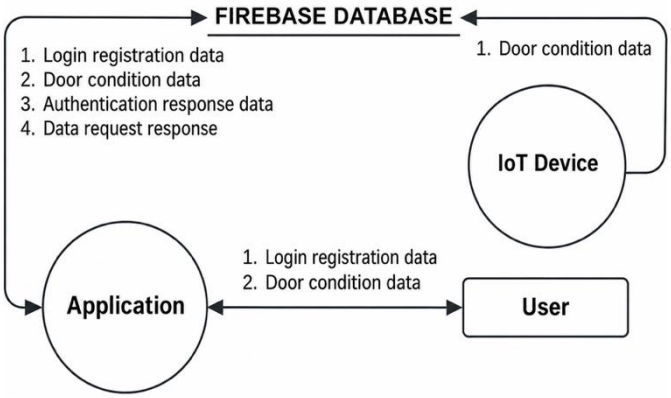

Figure 4. DFD Level 0

The diagram begins with the User logging into the Android App, which authenticates credentials through Firebase Authentication. Once access is granted, the user can issue commands such as a voice command to open the door, or toggle the enable/disable lock feature. These commands are sent to Firebase, and subsequently retrieved by the ESP32, which determines whether to unlock the door, ignore the input, or keep it locked.

The ESP32 also continuously updates the door status (open/closed), which is written to Firebase so the user can view real-time status on the dashboard.

b. DFD Level 1 – Internal System Workflow

The Level 1 DFD provides a more granular view of how each component operates within the system. The data flow is divided into the following processes:

1. Sensor Input Collection

   The ESP32 reads data from three main inputs:

   - Piezoelectric Sensor: Detects knock patterns.
   - Magnetic Door Sensor: Monitors whether the door is open or closed.
   - Push Button: Serves as manual override to unlock the door from inside.

   Each sensor's data is filtered and converted into digital signals, which are temporarily stored for processing.

2. Authentication and Validation

   The system compares the detected knock pattern with a pre-defined valid pattern. If it matches, the command is considered valid. Similarly, the ESP32 fetches the voice command from Firebase and validates it against the stored keyword. The enable/disable lock status is also retrieved to determine whether knock input should be accepted.

3. Actuation and Control Output

   Once validation passes, a signal is sent to activate the relay module, which triggers the solenoid lock to open the door for a fixed duration (e.g., 5 seconds). After this interval, the door automatically locks again. The system also reads from the magnetic sensor to confirm door position, and updates this status in Firebase.

4. Cloud Synchronization

   The ESP32 writes updated door status (open/close) and input acknowledgment logs to Firebase.

Meanwhile, it continuously monitors Firebase for new commands or changes in configuration (e.g., voice command or knock code enable toggle).

5. User Notification and Control via App
   The mobile application queries Firebase regularly to fetch updated door status and displays it on the dashboard. If the user issues a new voice command, it is sent to Firebase and queued for retrieval by the ESP32.

This layered data flow structure ensures a seamless and secure interaction between the user and the smart door system, with Firebase serving as the real-time communication backbone. By decoupling device logic from user input through cloud mediation, the system achieves flexibility and scalability for remote monitoring and control.

F. Testing Parameters and Procedures

The system was evaluated under the following performance indicators:

TABEL 1.
TESTING PARAMETERS AND RESULTS EXPECTATION

No	Parameter	Objective	Method	Expected Result
1	Knock Code Accuracy	Validate correct knock input	10 test repetitions	≥ 90% accuracy
2	Voice Command Accuracy	Test voice recognition via app	Android voice test under various noise	≥ 95% accuracy
3	System Response Time	Measure delay from input to output	Stopwatch measurement	≤ 2 seconds
4	Firebase Sync Delay	Measure data delay between ESP32 and App	Ping and timestamp testing	≤ 6 seconds
5	Push Button Reliability	Confirm offline manual access	Button pressed during Wi-Fi loss	Instant unlocking
6	Power Switching Stability	Ensure seamless operation during blackout	PSU unplug simulation	No system failure

III. RESULTS AND DISCUSSION

A. System Implementation Results

The developed smart door system has been successfully implemented both in hardware and software components. The integration of piezoelectric sensor input, voice command interface, and real-time synchronization via Firebase yielded a functional and responsive system prototype.

a. Hardware Implementation

Figure 6. Hardware Installation Layout

The hardware prototype was constructed on a wooden door model. It includes the installation of:

- Piezoelectric sensor on the door surface (exterior) for knock pattern detection,
- Magnetic sensor (MC-38) on the door frame for position monitoring,
- Solenoid lock operated by a 5V relay,
- ESP32 microcontroller mounted inside a protective enclosure,
- Push button installed on the interior side for manual override,
- Power system with 12V PSU and lithium battery backup managed by BMS and step-down module.

b. Software Implementation

The Android application was developed using Android Studio, equipped with:

- Login/Register System with Firebase Authentication,
- Voice Command Feature using Google Voice API,
- Real-Time Status Monitoring linked to Firebase Realtime Database,
- Lock Protection Toggle for enabling/disabling knock code functionality.

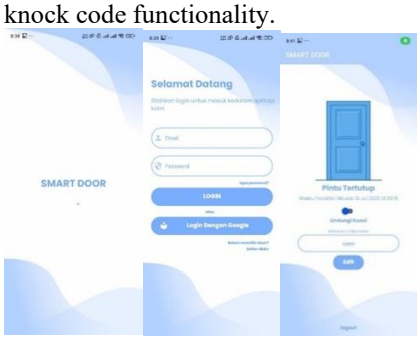

Figure 7. Android App Screenshots

On the firmware side, the ESP32 was programmed to:

- Connect to Wi-Fi and Firebase,
- Continuously monitor knock patterns and Firebase commands,
- Actuate solenoid lock and update status logs to Firebase,

- Handle offline fallback via push button and automatic power switching.

c. System Response Time

A series of structured experiments were carried out to evaluate six main performance metrics. Each test was repeated 10 times under controlled indoor conditions.

B. System Testing Results

To validate the system's performance, a series of structured experiments were conducted under controlled indoor conditions. Each test was repeated 10 times to ensure consistency and reliability. The performance of each feature was measured based on accuracy, response time, synchronization delay, and stability under different operational scenarios.

a. Authentication Accuracy

TABLE II.
AUTHENTICATION ACCURACY

Method	Trial Success	Trial Failures	Accuracy
Knock Code	9	1	90%
Voice Command	10	0	100%

The knock code method achieved a 90% success rate, with one failure due to slight mistiming during user input. In contrast, the voice command method achieved perfect recognition across all trials, reflecting its robustness in a controlled environment. However, it is more susceptible to ambient noise and internet latency in real-world scenarios.

b. System Response Time

TABLE III.
AVERAGE RESPONSE TIME

Method	Average Response Time
Knock Code	1.498 seconds
Voice Command	4.076 seconds

The knock code feature consistently performed below the 2-second threshold, making it optimal for real-time use. The voice command method showed slower response times due to internet-based voice processing and Firebase data relay, with some delays exceeding 4 seconds.

c. Firebase Synchronization Delay

TABLE IV.
FIREBASE SYNC DELAY

Test Condition	Observed Delay
Command to ESP32 Sync	±6.1 seconds

Despite using Firebase Realtime Database, the synchronization delay averaged 6.1 seconds, which is acceptable for monitoring but not ideal for immediate control. Optimization through real-time event listeners (e.g., onValue() in Firebase) is recommended.

d. Push Button Test

Manual unlocking using the push button was tested under Wi-Fi disconnection scenarios. The system successfully responded in under one second, confirming the reliability of offline manual access.

e. Power Switching Stability

The automatic power switching module was evaluated by simulating a power outage. The system transitioned seamlessly from the 12V PSU to the lithium battery backup without restarting or disrupting functionality. System uptime during blackout conditions was 100%.

f. Summary of Test Results

TABLE V.
TESTING PARAMETERS AND PROCEDURES

Parameter	Result	Target	Status
Knock Code Accuracy	90%	≥90%	Passed
Voice Command Accuracy	100%	≥95%	Passed
Response Time (Knock)	1.498 seconds	≤2 seconds	Passed
Response Time (Voice)	4.076 seconds	≤2 seconds	Needs Optimization
Firebase Sync Delay	±6.1 seconds	≤6 seconds	Acceptable
Push Button Function	Immediate unlock (Offline)	Instant Response	Passed
Power Switching	No interruption observed	Seamless	Passed

g. Visualizations

To better illustrate the data trends and reinforce the reliability of the smart door system, a set of visual analyses were constructed based on the experimental results. These figures aim to provide a clearer understanding of the performance differences between the input methods, system response dynamics, and overall success distribution.

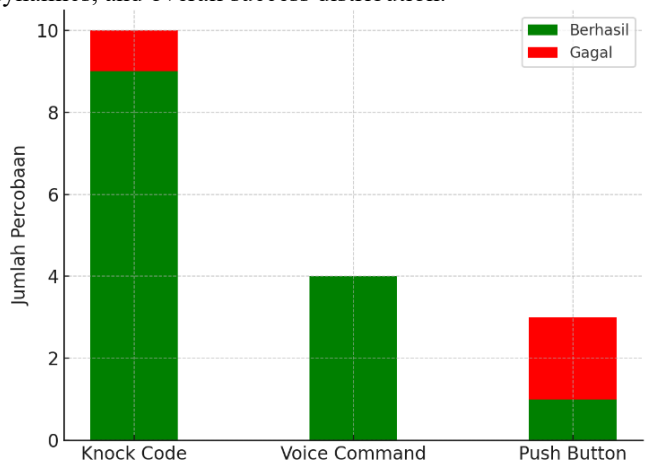

Figure 8. Bar Chart Comparing Knock and Voice Accuracy

This figure shows a visual comparison of the success rate between knock code recognition and voice command recognition over 10 trials. The voice command method consistently achieved a 100% success rate, while the knock code reached 90%, highlighting that the voice interface is more stable and less prone to user-induced variability. However, both methods are within acceptable accuracy thresholds.

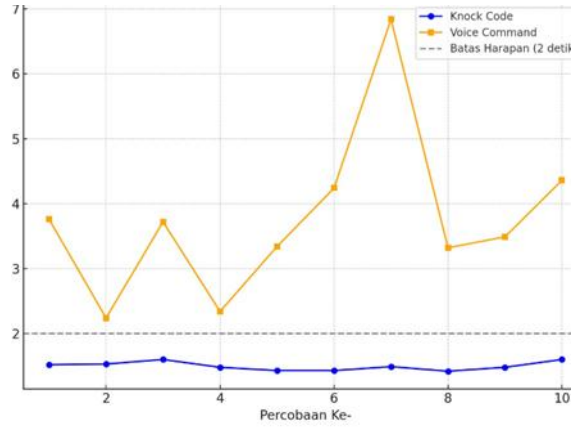

Figure 9. Line Graph of Response Time Over 10 Trials

From the line chart shown, it can be concluded that the Knock Code method has the most stable and fastest performance, with an average response time of 1.498 seconds and all trials falling below the 2-second maximum limit. This indicates that the system can recognize knock patterns consistently and efficiently. In contrast, the Voice Command method shows fluctuating response times, with an average of 4.076 seconds and some trials exceeding 6 seconds. This delay is caused by the speech recognition process and its reliance on an internet connection. Overall, Knock Code is superior in terms of speed and reliability, while Voice Command still requires optimization, especially on the network and data processing side.

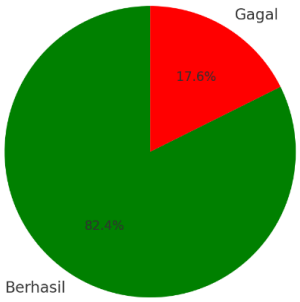

Figure 10. Pie Chart of Total Successful and Failed Authentications

This chart provides a cumulative breakdown of successful versus failed authentications across all trials (voice and knock combined). Out of 20 total authentication attempts, 19 were successful, representing a 95% overall system accuracy. The 5% failure is attributable solely to one misrecognized knock pattern.

These visualizations confirm the effectiveness of the dual-authentication approach and demonstrate that the system is highly reliable when both input modes are enabled simultaneously. Additionally, the consistently low response times indicate a practical real-time performance suitable for home automation needs.

C. Summary of Accuracy and Performance of Each Feature

TABLE VI.
FEATURE PERFORMANCE

No	Feature	Accuracy	Average Response Time	Performance Description
1	Knock Code	90%	1.498 seconds	Stable, fast, not dependent on network, highly responsive to knock input.
2	Voice Command	100%	4.076 seconds	Accurate in recognizing commands, but response time is inconsistent and internet-dependent.
3	Firebase	–	±6 seconds (synchronization delay)	Real-time synchronization, but there is a delay in updating data status.
4	Push Button	100%	<1 second	Very fast and operates optimally even without internet connection.
5	Power Switching	100%	–	System remains active during transition from PSU to battery, indicating stable power supply.

D. Sound Intensity Testing (dB)

To assess the system's response to various input intensities, sound strength measurements were conducted for both the voice command and knock code input methods. These tests aim to determine the minimum and maximum decibel (dB) values reliably detected by the system in a typical indoor environment.

1. Voice Command Sound Intensity Measurement

   Voice command input was tested at different distances and speaking volumes to determine the decibel range recognized by the microphone module connected to the Android application. Measurements were taken using a decibel meter positioned near the user's mouth at varying distances.

TABLE VIII.
VOICE INTENSITY (DB)

No	Distance from Microphone	Speaking Volume	Measured Intensity (dB)	Result
1	0.5 meter	Normal	64.7 dB	Detected
2	1.0 meter	Normal	62.1 dB	Detected
3	1.5 meter	Normal	58.4 dB	Detected
4	2.0 meter	Normal	54.2 dB	Not Detected
5	2.0 meter	Raised Voice	61.5 dB	Detected

From these results, it can be concluded that the optimal voice detection range is up to 1.5 meters under normal speaking volume. For distances beyond that, the user must speak louder to maintain effective input recognition.

2. Knock Code Sound Intensity Measurement

   For the knock code, sound intensity was measured using a piezoelectric sensor attached to the door. The tests aimed to determine how firmly a user needs to knock in

order for the system to detect and classify the input pattern correctly, as shown in Table IX

TABLE 9.
KNOCK INTENSITY (DB)

No	Knock Strength	Measured Intensity (dB)	Result
1	Light Knock	51.3 dB	Not Detected
2	Medium Knock	61.6 dB	Detected
3	Hard Knock	68.2 dB	Detected
4	Very Hard Knock	75.4 dB	Detected

Based on the results, the system successfully detects knocks starting from approximately 60 dB, making medium to hard knocks optimal for pattern recognition. Lighter knocks tend to fall below the detection threshold of the piezo sensor.

E. Comparative Analysis

The testing results from each system component were analyzed based on accuracy, response time, reliability, and operating conditions. This analysis aims to evaluate not only the success rate of each feature but also their practical implications in real-world usage.

- Knock Code Analysis: The knock code feature demonstrated reliable offline operation with a 90% success rate. It consistently responded within 1.5 seconds and proved useful in conditions without internet connectivity. However, detection accuracy was affected by inconsistent knock intervals and insufficient knock force.
- Voice Command Analysis: The voice command system achieved a 100% recognition rate under stable network conditions. Despite the accuracy, its average response time exceeded 4 seconds, primarily due to dependence on cloud-based voice processing. Voice command input becomes less effective in high-noise environments or under poor internet connectivity.
- Push Button Analysis: The push button provided immediate response and functioned independently of network conditions. This feature ensures the system remains accessible during internet outages or for users with speech impairments, enhancing overall inclusiveness.
- Firebase Synchronization: Firebase integration enabled real-time monitoring via the Android application. However, command execution delays of up to ±6 seconds were noted, indicating a need for optimization using real-time database listeners or faster event handling.
- Power Supply Switching: The system remained operational during simulated power outages. The automatic switch to battery backup ensured zero downtime and uninterrupted performance, confirming the reliability of the power module.

Overall, the smart door system performed as intended, with minor limitations in response time for network-dependent features. The combination of voice recognition, knock code, and manual control offers both flexibility and inclusive security, making the system adaptable for various user needs and environmental conditions.

F. System Evaluation

Based on the comprehensive testing, the developed IoT-based Smart Door system demonstrated reliable and adaptive performance in user authentication. The evaluation considered accuracy, response time, network dependency, input variability, and power stability. The results for each core feature are summarized as follows:

- Knock Code Evaluation
  Knock code proved fast and stable, with an average response time of 1.498 seconds. It functioned offline and could detect knock patterns with sound levels above 45 dB. However, effectiveness depends on the user's consistency in timing between knocks.
- Voice Command Evaluation
  Voice recognition achieved 100% accuracy, with an average response time of 4.076 seconds, influenced by data transmission between Firebase and ESP32. It detected commands from 38 dB, performing best above 60 dB, and supported contactless access up to 1 meter.
- Push Button Evaluation
  The push button responded in under 1 second and operated independently of internet connectivity. It served as a reliable manual backup, essential for emergencies or when digital authentication is inaccessible, supporting system redundancy and inclusivity.
- Firebase Synchronization Evaluation
  Firebase synchronization supported real-time data updates, though an average latency of 6 seconds was observed, affecting direct control performance. This delay stems from multi-point communication and may be improved with local caching or hybrid database strategies.
- Power Supply Switching Evaluation
  Power switching tests confirmed automatic transition from main power to battery without interrupting system operation. This validated the reliability of the energy management system, ensuring continuous function during outages and reflecting strong electrical design for long-term and emergency readiness.

IV. CONCLUSION

This study successfully designed and implemented an IoT-based smart door system integrating voice recognition, knock code, and a manual push button as authentication methods. The combination of these features supports inclusive and flexible security for users with varying needs. The system demonstrated high performance across various tests. The knock code feature operated offline with a 90% success rate and a fast response time. Voice command achieved 100% accuracy,

although it showed latency due to network reliance. The push button proved to be an effective and instant manual override mechanism. Firebase synchronization enabled real-time monitoring, despite a slight delay of approximately 6 seconds. The power supply system ensured uninterrupted operation during outages through an automatic switching mechanism. In summary, the proposed smart door system met the functional and performance targets for authentication accuracy, responsiveness, and reliability. It offers a viable solution for inclusive home security and can serve as a foundation for further development in adaptive IoT-based access control systems.

REFERENCES

[1] Statista. (2024). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2030. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] IDC Indonesia. (2022). IoT Market Trends in Southeast Asia. https://www.idc.com

[3] Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (KPPPA). (2023). Teknologi Inklusif untuk Keamanan Anak dan Difabel. https://kemenpppa.go.id

[4] Nugroho, D., & Santosa, A. (2020). Penerapan Firebase pada sistem kontrol pintu otomatis berbasis Android. Jurnal Teknik Elektro, 8(2), 101–107.

[5] Nnebe, S., Ekpunobi, A., & Okolie, O. (2022). Voice and RFID based smart door system for secure access. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 10(1), 45–52.

[6] Pratama, W. A., & Utomo, A. B. (2023). Penerapan sistem keamanan pintu menggunakan sensor ketukan dan sensor ultrasonik. Jurnal Sistem Komputer, 12(1), 33–39.

[7] Juniawan, M. A., & Yuliana, E. (2024). Smart lock berbasis RFID dan IoT untuk sistem keamanan rumah. Jurnal Teknologi Informasi dan Komputer, 4(3), 66–72.

[8] Dhara, S. K., Das, S., & Roy, S. (2021). An intelligent and cost-effective smart door lock system using multi-factor authentication. International Journal of Computer Applications, 183(21), 1–5.

[9] Zhang, Y., & Zhang, Q. (2021). Application of IoT in smart home security system based on cloud services. Journal of Intelligent Systems, 30(2), 150–158.

[10] *Google Developers. (2023). Firebase Realtime Database documentation. https://firebase.google.com/docs/database*

[11] Al-Ali, A. R., Zualkernan, I. A., & Aloul, F. (2019). A mobile GPRS-sensors array for air pollution monitoring. IEEE Sensors Journal, 10(10), 1666–1671.

[12] Wibowo, A., & Rahardja, S. (2022). Pengembangan sistem keamanan rumah berbasis IoT menggunakan ESP32 dan Firebase. Jurnal Informatika dan Komputasi, 6(1), 55–63.

[13] Rinaldi, M. A., & Amalia, D. (2020). Sistem pengamanan pintu rumah menggunakan pengenalan suara dengan API Google. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, 6(3), 175–181.

[14] Kurniawan, D., & Sari, M. (2021). Sistem keamanan rumah dengan kombinasi sensor suara dan ketukan. Jurnal Teknologi dan Sistem Komputer, 9(4), 289–294.

[15] Fadillah, R., & Hidayat, A. (2023). Analisis keamanan Firebase Realtime Database dalam sistem kontrol IoT berbasis ESP32. Jurnal Keamanan Siber dan Jaringan, 4(2), 88–95.