Design And Development Of A Smart Door Security System Prototype Using Passcode And Voice Authentication Based On Arduino Uno Microcontroller In Integration Lab Of Civil Aviation Polytechnic of Surabaya

Dwi Angger Lailatul Rif'a[1], Nyaris Pambudiyatno[2], Yudhis Thiro Kabul Yunior[3]

[1,2,3)] *Civil Aviation Polytechnic of Surabaya*
[*]*Corresponding author. Email: anggerlailatul@gmail.com*

ABSTRACT

This study aims to develop and test a prototype smart door security system based on the Arduino Uno microcontroller with dual authentication that combines a Personal Identification Number (PIN) and voice recognition, referring to the modern security consensus that multi-factor authentication can significantly improve protection against illegal access compared to single methods. The PIN is used as knowledge-based verification, while voice recognition serves as biometric verification that is difficult to forge. This study also identifies the needs of users in educational laboratories for an efficient and user-friendly modern security system, designs a prototype with a user-friendly interface, and measures performance through testing of PIN accuracy, voice recognition accuracy, as well as tolerance for input variations and repetition. The method used was the prototype method, starting with needs identification (89.6% of respondents stated they needed this system), system design with components such as Arduino Uno, 4x4 Keypad, Voice Recognition Module V3, 16x2 LCD, relay module, and solenoid door lock, prototype creation using Arduino IDE, functional testing, and validation of feasibility by two experts who scored it at 95.83%. Test results showed 100% PIN accuracy and 72% voice recognition accuracy, consistent with previous research indicating accuracy levels of 65–80% on low-cost devices. The system also proved tolerant to input variations and repetitions without performance degradation. Overall, this study demonstrates that an Arduino Uno-based dual authentication system can serve as a low-cost, effective, and easily integrable security solution for laboratories or other confined spaces in educational environments.

Keywords: *Door security system, password, voice authentication, prototype*

1. INTRODUCTION

The development of security technology over the past ten years has undergone significant changes, particularly in access and room control systems. Mechanical keys, which were previously the standard, are now being replaced by electronic and digital security systems that offer a higher level of protection. This change has been driven by an increase in cases of lost keys, illegal duplication, and increasingly sophisticated break-in techniques. In the education sector, particularly in laboratories housing high-value equipment and sensitive data, the need for modern and effective security systems has become increasingly urgent. One global trend that has been widely adopted is multi-factor authentication, which combines knowledge-based methods such as Personal Identification Numbers (PIN) with biometric methods like voice recognition or fingerprint scanning. This integration is believed to provide a higher level of protection compared to using a single method [1].

Based on initial observations at the Surabaya Aviation Polytechnic Integration Laboratory, the security system used still relies on manual keys. Although practical, this system has a number of weaknesses, such as the risk of losing keys, the potential for unauthorized access by outsiders, and the lack of records of the time and identity of users who open the door. This condition is even more vulnerable given the large number of laboratory users, ranging from cadets, lecturers, to technicians. The high frequency of people coming in and out of the lab increases the risk of equipment loss,

damage, and misuse of facilities. This situation is the main reason for developing a more adaptive and layered security system.

Laboratory security is not only related to the physical protection of equipment, but also to maintaining the continuity of teaching and learning processes and research. PIN-based systems provide a layer of protection through knowledge-based verification, while voice recognition adds a layer of biometric verification that is difficult to forge [2]. The combination of the two has the potential to reduce security gaps while increasing user comfort. The use of the Arduino Uno microcontroller enables the creation of a cost-effective, flexible system that can be easily integrated with various additional devices.

Issues identified in the field include: (1) weak security of manual key systems that are vulnerable to being broken into or duplicated, (2) the absence of layered verification mechanisms to restrict access, (3) the lack of digital recording of room entry and exit activities, and (4) the limited application of modern technology in campus security systems. These four issues have direct implications for laboratory security and the potential for losses in the event of unauthorized access. As a solution, this study proposes the design of an Arduino Uno-based smart door prototype that uses dual authentication in the form of a PIN and voice recognition [3]. This system was developed using the prototype method, which allows for gradual development and testing at each stage, so that the final result meets user needs. With two stages of verification, the system is expected to close the security gaps that exist in the single method.

Based on the existing problems, this study aims to: (1) develop a prototype of a smart door security system with dual authentication based on Arduino Uno, (2) test the accuracy of PIN, voice recognition accuracy, and system tolerance to input variations, and (3) validate the feasibility of the system through expert testing in an educational laboratory environment.

The expected benefits of this research include the availability of an affordable, effective, and easily integrated security system alternative for laboratories or other restricted spaces; increased awareness of the importance of multi-factor security systems in educational environments; and the availability of references for future research and development of microcontroller-based security systems. Additionally, this research is expected to serve as a foundation for the development of security systems integrated with the Internet of Things (IoT) and remote control, in line with current trends in security technology [4].

The benefits of this research include providing a more modern and effective alternative solution for room security, which is easy to operate by users from various backgrounds, and can be used as a reference or basis for the development of other security systems. By utilizing the Arduino Uno microcontroller, this research also shows that the application of technology does not always require high costs, but can be adapted to existing needs and resources.

With a dual authentication approach, the system is designed not only to enhance security, but also to provide ease and convenience in everyday use. Users simply enter their registered PIN, then give a voice command to open the door, without the need for a physical key. This approach is ideal for modern campus environments that require a secure, efficient, and flexible access system..

2. METHODS

This research uses the prototype method because its main focus is to design and test a prototype of a smart door security system based on the Arduino Uno microcontroller that combines two authentication methods: a passcode (PIN) and voice recognition. This approach allows for an iterative development process, where the initial design is tested, evaluated, and then improved based on feedback until a system that meets user needs is obtained [5]. The prototype method was chosen to minimize the risk of design errors from the outset and to ensure that the final result aligns with real-world operational conditions in a laboratory environment. The stages of the prototype research method include: 1) identification of needs, 2) prototype design, 3) prototype creation, 4) evaluation, 5) system testing.

1. Identification of needs

The initial stage began with identifying user needs through the distribution of questionnaires to cadets at the Surabaya Aviation Polytechnic Integration Laboratory. The aim was to determine the urgency of implementing a smart door security system with dual authentication. Respondents were asked to assess the need for security features, ease of use, and system reliability. The analysis results showed a need level of 89.6%, falling into the “highly necessary” category. This information serves as the foundation for system design, ensuring that the developed solution aligns with field conditions and user expectations, while also guiding the technical specifications that must be met during the design phase [6].

2. Prototype Design

Based on the results of the needs assessment, an initial design was created for a system that combines two authentication methods: a PIN code and voice recognition. The design includes a system block diagram, workflow, and selection of key components such as a 4x4 keypad, V3 voice recognition module, 16x2 LCD, relay, and solenoid door lock. At this stage, the operational algorithm was also determined, starting from PIN input,

voice verification, to the automatic door opening mechanism. The design considers ease of hardware integration, programming efficiency on the Arduino IDE, and component availability to ensure the prototype can be realized at an affordable cost while remaining reliable.

3. Prototype Creation

This stage involves turning the design into a physical prototype using the specified components. A 4x4 keypad is installed as the initial PIN input, while a voice recognition module is used for voice authentication. The Arduino Uno acts as the control center, processing inputs and sending signals to the relay to activate the solenoid door lock. The 16x2 LCD is programmed to display system status such as “Enter Password,” “Enter Voice,” or “Access Denied.” The circuit is assembled on a PCB using jumper cables to facilitate assembly and maintenance. The prototype is internally tested to ensure all components are properly connected and function according to the initial design [7].

4. Evaluation

Once the prototype was complete, an initial evaluation was conducted with a limited number of users to test the system. Users were asked to operate the device from the PIN input stage to voice authentication. The feedback provided was used to improve the system's functionality or appearance. The evaluation covered ease of use, response speed, and verification success rate. If issues such as voice module sensitivity or response delays were identified, improvements were made to the hardware or programming [8]. This stage ensured that the system was close to the expected specifications before proceeding to more in-depth testing.

5. System Testing.

Testing was conducted to measure the performance and accuracy of the system. The keypad feature was tested with various combinations of correct and incorrect PINs, resulting in 100% accuracy in recognizing registered PIN. The voice recognition feature was tested 50 times, achieving 72% accuracy in relatively quiet conditions, falling into the “acceptable” category. User usability validation testing was conducted using 12 evaluation criteria, achieving a score of 95.83% (classified as “highly acceptable”). These results indicate that the system functions effectively, though voice recognition performance could still be improved. Testing marks the final stage before the system is ready for implementation in a laboratory environment.

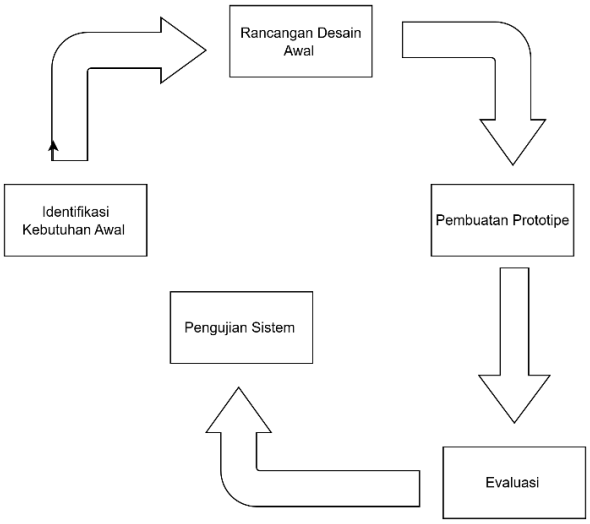

Figure1 Prototipe Method

3. RESULTS AND DISCUSSION

This section presents the results of the development of a smart door security system prototype using PIN code and voice authentication based on Arduino Uno microcontroller, as well as a discussion of its performance and validation [9]. The development process follows the stages of the Prototype Method (Identify Needs, Prototipe design, Prototype Creation, Evaluate, Test).

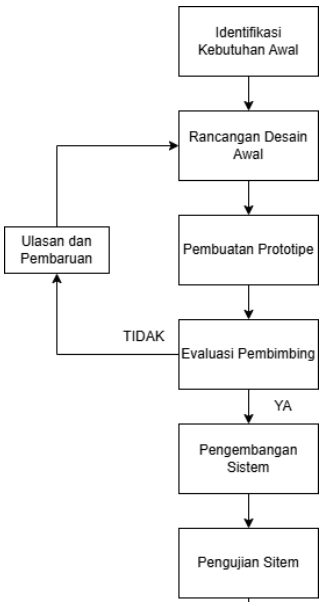

Figure2 flowchart

1. Identification of needs

The needs identification stage is the main foundation in the development of a smart door security system based on PIN and voice authentication. This process is carried

out to gain an in-depth understanding of the problems in the field and to ensure that the designed solution is relevant and meets user expectations. Data collection was conducted through the distribution of questionnaires to 10 respondents who are cadets at the Surabaya Aviation Polytechnic Integration Laboratory. The questionnaire questions were designed to measure the urgency of implementing the system, preferences for authentication methods, and expectations regarding system performance. Respondents were asked to evaluate aspects of security, ease of use, access speed, and potential technical obstacles. The results showed a need level of 89.6%, including the "highly necessary" category, indicating that the current conventional security system is no longer considered adequate [10]. Additionally, brief interviews were conducted to enrich the qualitative data, revealing that the risks of losing physical keys, unauthorized duplication, and illegal access are the primary concerns of users. This information was used to establish system specifications, such as the use of two-factor authentication to enhance security, integration of responsive components, and a design that is easy to operate by all users. With this approach, the needs identification phase is not only an initial process but also a foundation guiding the entire design and development stages of the prototype until it is ready for testing in a real-world environment.

2. Prototype Design

The initial design stage is an important step after user requirements have been clearly identified. At this stage, all data from the needs identification process is converted into technical specifications and system design plans for the system to be built. The smart door security system is designed to combine two authentication methods: PIN verification via a 4x4 keypad and voice authentication using the Voice Recognition Module V3. The Arduino Uno was chosen as the control center due to its ability to integrate various inputs and outputs with flexible programming through the Arduino IDE [11]. The initial design includes the creation of a block diagram illustrating the data flow from PIN input, voice verification, to relay activation and solenoid door lock activation. Additionally, a flowchart was created detailing the sequence of processes, from system initialization, input detection, data validation, to access granting. A 16x2 LCD was included in the design to provide real-time status information to the user, such as "Enter Password," "Enter Voice," "Access Denied," or "Access Granted, Open Door." Component selection considered market availability, ease of integration, power consumption, and cost efficiency. The design also prioritized ergonomic factors and component placement to ensure ease of operation and protection against physical damage. With a structured and detailed initial design, the prototype development process can proceed more efficiently, minimize assembly errors, and facilitate evaluation in subsequent stages.

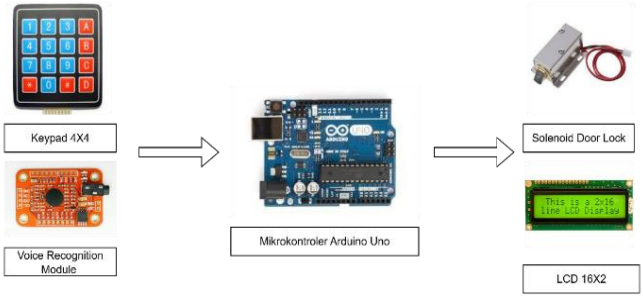

Figure3 System block diagram

3. Prototype Creation

The prototype development stage is the physical realization of the initial design that has been developed. All components selected in the previous stage, such as the 4x4 keypad, Voice Recognition Module V3, Arduino Uno, 16x2 LCD, relay, and solenoid door lock, are assembled according to the block diagram and circuit diagram. The Arduino Uno functions as the control center, processing input from the keypad and voice module, then sending commands to the relay to activate the solenoid as the door locking mechanism. The 16x2 LCD is programmed to display the authentication process status, guiding the user from the initial stage to the final decision on access granting.

Assembly was done using jumper cables and a breadboard to facilitate initial testing, then refined with a PCB board to make the circuit more robust and neat. Programming in the Arduino IDE includes PIN verification algorithms, voice recognition, and relay control logic and LCD display. At this stage, the sensitivity parameters of the sound module were also adjusted to accurately recognize voice passwords. The entire system was internally tested to ensure that all components were properly connected, there were no connection errors, and the device could operate according to the planned workflow. The creation of this prototype serves as an important bridge to the evaluation stage, as it allows for direct testing of the system's performance in a form resembling the final product [12].

Figure3 physical form of the system

4. Evaluation

The prototype evaluation stage aims to assess the extent to which the system that has been created can work according to the initial design and meet user needs. The evaluation process was carried out by involving a number of users to try the system directly at the Surabaya Aviation Polytechnic Integration Laboratory. Users were asked to carry out procedures ranging from entering a PIN on the keypad, voice verification through the Voice Recognition module, to the process of opening or denying door access. During the evaluation, aspects such as system response speed, ease of operation, clarity of information on the LCD, and stability of connections between components are observed. User feedback was recorded in detail, including challenges encountered such as voice recognition inaccuracies due to variations in intonation or speaking distance. The initial evaluation results were used to make adjustments to both hardware and software, such as recalibrating the sensitivity of the voice module, fixing the program code in the Arduino IDE, or adjusting the component mounting position for better ergonomics [13]. Additionally, the evaluation helps ensure that the system operates consistently without recurring errors, both during PIN authentication and voice recognition. With systematic evaluation, the prototype can be refined before entering formal testing, thereby increasing the likelihood of success when tested in real-world conditions and minimizing the risk of failure.

5. System Testing.

1. Keypad Testing

Keypad testing aims to ensure that the PIN input function works as designed and can distinguish between correct and incorrect PINs. The test is conducted with 20 trials, consisting of valid and invalid PIN combinations. The process begins with the user pressing the buttons on the 4x4 keypad to enter the PIN. The system then processes the input and matches it with the PIN data stored in the Arduino memory. If it matches, the LCD displays the message “Input voice” and the relay activates the solenoid door lock if not, the message “Access denied” appears without opening the door. The test results showed a 100% success rate in recognizing the correct PIN and rejecting the incorrect PIN. The real-time response time indicates that the system is highly responsive. This reliability ensures that PIN authentication can be used as the primary security layer. The evaluation of this stage showed no button reading errors or processing delays, so the keypad feature is ready for use without significant improvements.

2. Voice Recognition Testing

Voice recognition module testing was conducted to measure the system's accuracy in recognizing user voice passwords. A total of 50 trials were conducted using voice passwords previously recorded in the Voice Recognition V3 module. The test environment was kept relatively quiet to minimize noise. The system successfully recognized the voice correctly 45 times, resulting in an accuracy of 72%. The 5 failed trials were generally caused by differences in intonation, speaking speed, or the user's distance from the microphone. When the voice is recognized correctly, the LCD displays “Access granted, door open,” and the door opens. Conversely, if the system fails, it remains on “Voice Input.” These results indicate that while voice recognition can be used as an additional security layer, its accuracy can still be improved through optimization of training data or adjustment of module sensitivity. With an accuracy rate above 70%, this feature is still viable for use in an internal laboratory setting.

3. User Acceptance Testing

The acceptance testing phase is conducted to assess user acceptance of the system in terms of ease of use, security, and comfort. The testing method uses a questionnaire based on 12 evaluation indicators covering aspects of functionality, speed, design, and system reliability. Respondents consist of students from the Integration Laboratory who previously interacted directly with the prototype [14]. The summary results show an average score of 95.83%, falling into the “Highly Feasible” category. Respondents rated the system as easy to operate, providing a greater sense of security than conventional keys, and having a fast response. However, some suggestions were made, such as improving voice recognition sensitivity and providing a backup method if one authentication fails. These findings indicate that the system already meets the needs of the majority of users and is suitable for implementation, although further development could enhance overall satisfaction and reliability.

Table1 Tool Testing Results

No.	Components	Success Indicators	Test Results	System Accuracy Results
1.	Keypad 4x4	The system can accept the correct password input.	The system successfully reads the password input accurately. Users can enter their PIN according to the program.	The accuracy results from 15 users and the system responding accordingly produced a value of 100%.
2.	Modul Voice Recognition	Detect and match recorded user voices	The module successfully recognized the user's voice in normal speech and clearly recognized the word “open.”	The accuracy results from 25 users and the system responding accordingly produced a value of 72%.
3.	Solenoid Door Lock	Opens automatically after both authentications are successful	The solenoid automatically unlocks and relocks after a specified time delay.	The accuracy results from 15 users and the system responding accordingly produced a value of 100%.
4.	LCD 16x2	Displaying the authentication process status and notification results to users	The LCD can clearly display instruction messages, process status, and authentication results.	The accuracy results from 15 users and the system responding accordingly produced a value of 100%.

4. CONCLUSION

This study successfully designed and built a prototype of a smart door security system based on Arduino Uno with two authentication methods, namely PIN and voice recognition. The test results showed that PIN authentication had 100% accuracy, while voice recognition achieved 72% accuracy in relatively quiet laboratory conditions. The usability test yielded a score of 95.83% (category “Very Usable”), indicating that the system is easy to use, responsive, and provides a higher sense of security compared to conventional keys. The dual security layer implemented minimizes the risk of unauthorized access. Although voice recognition accuracy is already satisfactory, performance improvements are still needed, such as using more sensitive modules or optimizing the voice recognition algorithm. This system has met the research objectives

and is ready for implementation in a laboratory environment, with potential for further development with additional features like backup authentication to enable broader application, including in homes or public facilities.

REFERENCES

[1] M. R. Auzan, U. Syafitri, and M. Fadillah, "Rancang bangun pintu otomatis dengan sistem voice recognition berbasis Android dan solenoid lock," *J. Teknol. Dan Sistem Informasi*, vol. 10, no. 1, pp. 32–38, 2022.

[2] P. E. S. Dita, A. Al Fahrezi, P. Prasetyawan, and L. B. Ratu, "Sistem keamanan pintu menggunakan sensor sidik jari berbasis mikrokontroler Arduino UNO R3," *J. Teknologi Dan Sistem Komputer (JTIKOM)*, vol. 2, no. 1, 2021.

[3] A. Hanafie, A. Haslindah, B. Suradi, S. Baco, and S. Bahali, *Perancangan Alat Pengering Helm Berbasis Arduino*, Universitas Islam Makasar, 2021.

[4] R. Hidayat, *Pemrograman Arduino dan Pemanfaatan Modul Sensor dalam Proyek Mikrokontroler*, Andi Publisher, 2020.

[5] M. A. Mazidi, J. G. Mazidi, and R. D. McKinlay, *The 8051 Microcontroller and Embedded Systems: Using Assembly and C*, 2nd ed., Pearson Education, 2012.

[6] S. Monk, *Programming Arduino: Getting Started with Sketches*, 2nd ed., McGraw-Hill Education, 2016.

[7] M. Nafarin, *Belajar Sendiri Mikrokontroler Arduino dan ESP8266*, Andi Publisher, 2021.

[8] B. Novianti, T. Rismawan, and S. Bahri, "Prototype sistem keamanan pintu menggunakan radio frequency identification (RFID) dengan kata sandi berbasis mikrokontroler," *Coding: Jurnal Komputer Dan Aplikasi*, vol. 4, no. 3, 2016.

[9] D. Pratama and D. Wahyudi, "Implementasi sistem pengenalan suara untuk kontrol akses pintu berbasis Arduino," *J. Teknik Elektro Dan Komputer (JTEK)*, vol. 10, no. 2, pp. 45–51, 2021.

[10] L. Rohmatillah, "Implementasi LCD dalam sistem mikrokontroler menggunakan Arduino," *J. Teknologi Elektro Dan Komputer*, vol. 10, no. 1, pp. 45–52, 2021.

[11] Z. N. Saputri, "Aplikasi pengenalan suara sebagai pengendali peralatan listrik berbasis Arduino Uno," Universitas Brawijaya, 2014.

[12] R. Wahyuningrum and L. Febrianto, "Rancang bangun prototype sistem kontrol kunci pintu berbasis voice recognition Arduino Uno & sensor Bluetooth," *J. Esensi Infokom: J. Esensi Sistem Informasi Dan Sistem Komputer*, vol. 7, no. 2, pp. 78–85, 2023.

[13] Y. Suprapto, R. Z. Widyananda, R. Indrianto Sudjoko, and L. Moonlight Lady, "Prototype design of clean water distribution control system based on proportional integral derivative (PID) and Android Article History," *Appissode Journal (Application, Information System and Software Development Journal)*, vol. 2, no. 3, pp. 29–35, 2024.

[14] Z. Zulkarnaen and A. K. Al Koriah, "Rancang bangun sistem keamanan pintu rumah dengan voice recognition dan RFID gelang berbasis IoT," in *Teknimedia: Teknologi Informasi dan Multimedia*, vol. 5, no. 2, 2024, doi: 10.46764/teknimedia.v5i2.241.