

Design and Construction of an Internet of Things-Based Smart Home Security System Using Arduino Uno with Wokwi Simulation

Aidil Alfarizi¹, Raisya Aulia²

^{1,2} Ilmu Komputer, Universitas Islam Negeri Sumatera Utara

¹aidilalfarizi1101@gmail.com, ²raisyaecha1705@gmail.com

Received: July 9, 2026 | Revised: August 3, 2026 | Accepted: October 15, 2026 | Published: October 19, 2026



COSIE is licensed a Creative Commons Attribution-Share Alike 4.0 International License

Abstract

Conclusion The development of the Internet of Things (IoT) has driven the implementation of smarter and more automated home security systems. However, most previous studies have focused on direct hardware implementation, resulting in higher costs and less flexibility in the development and testing processes. This study aims to design and build an IoT-based home security system using Arduino Uno with Wokwi simulation as a medium for system design and validation. The research method used is Research and Development (R&D) with a prototype approach that includes needs identification, system design, program implementation, simulation, testing, and evaluation. The system was developed using a PIR sensor and an HC-SR04 ultrasonic sensor as detection devices, as well as an LED, buzzer, servo motor, and OLED as output devices. The test results showed that all test scenarios were successfully executed. The system was able to detect motion and objects at a certain distance, activate an alarm, automatically control the door locking mechanism, and display real-time security condition information on the OLED. The use of Wokwi has been proven to simplify the development process, reduce implementation costs, and increase the efficiency of system testing before being implemented on actual hardware. The results of the study indicate that the Wokwi-based simulation approach is effective as an initial stage in the development of an IoT-based home security system.

Keywords: Internet of Things, Smart Home Security, Arduino Uno, Wokwi Simulation, Prototype.

1. INTRODUCTION

In today's digital era, Internet of Things (IoT) technology is a key enabler of the Industrial Revolution 4.0. IoT is one of the key pillars transforming the way we interact with the world around us. IoT refers to physical devices connected to input and output devices that communicate with each other via the internet. IoT enables real-time data collection and exchange and can be remotely controlled and monitored using microcontrollers. By utilizing microcontrollers connected to sensors, IoT motors and actuators can be applied in various fields such as smart farming [1]. The urgency of this research lies in bridging this gap. In today's digital era, IoT has become one of the most important technologies driving change in various sectors. Without adequate programming skills, students will be left behind in the ever-advancing developments in IoT [2]. Indoor security is a crucial issue that requires special attention, both in personal and professional contexts. Conventional physical locks have been the primary solution for securing indoor access, but they have significant drawbacks, such as the risk of key duplication and the lack of real-time notification capabilities[3]. The development of Internet of Things (IoT) technology has spurred various innovations in smart home systems, particularly in security. IoT enables various electronic devices to be interconnected via a network, enabling real-time monitoring and control. Implementing IoT in home security systems makes it easier for users to detect potential threats such as intrusion, suspicious movement, and unauthorized access more quickly and efficiently than conventional security systems[4].

The rise in theft and crime in residential areas is one factor driving the development of technology-based home security systems. Conventional security systems that rely solely on mechanical locks or simple alarms are limited in providing direct information to homeowners. Therefore, a security system capable of automatic detection, providing early warnings, and integrating various sensors into a single system that is easy to develop and relatively low-cost[5]. Several previous studies have developed IoT-based home security systems using various microcontrollers such as Arduino Uno and ESP32, utilizing Passive Infrared (PIR) sensors, ultrasonic sensors, buzzers, LEDs, and servo actuators as security mechanisms.

These studies have shown that the integration of sensors and actuators can improve the effectiveness of intruder detection and provide automatic responses to detected conditions. However, most studies have focused more on direct hardware implementation, so the testing process requires relatively expensive physical components, carries the risk of assembly errors, and is less flexible for the learning process and initial system development[6]. This research proposes the Design and Construction of an Internet of Things-Based Smart Home Security System Using Arduino Uno with Wokwi Simulation. The designed system integrates a PIR sensor as a motion detector, an ultrasonic sensor as an object distance detector, a buzzer as an alarm, an LED as a visual indicator, and a servo motor as an automatic locking mechanism controlled by Arduino Uno. The entire design and testing process is carried out using the Wokwi Simulator so that each system function can be validated before being implemented on real hardware[7].

Research that utilizes the Wokwi Simulator is generally only used as a medium for learning microcontrollers or simple simulations, while its implementation as a means of designing and validating IoT-based home security systems is still relatively limited[8]. The scientific gap in this research lies in the lack of research that integrates the design, simulation, testing, and validation processes of Arduino Uno-based home security systems using the Wokwi platform before implementation on actual hardware[9]. The effectiveness of simulation as a method to reduce development costs, speed up the debugging process, and increase the reliability of system designs has not been widely discussed [10]. The main contribution of this research is to present an approach to developing an IoT-based home security system that is not only oriented towards hardware implementation, but also emphasizes the use of Wokwi simulation as an effective, economical, and easily reproducible development environment. This approach allows the design process, program logic testing, and sensor and actuator integration to be carried out systematically with a lower level of risk. Thus, this research is expected to be a reference for the development of an Arduino Uno-based smart home security system while also supporting the learning and research process in the field of the Internet of Things[11].

The development of increasingly affordable microcontroller technology has accelerated the implementation of Internet of Things systems in various fields, including home security. The Arduino Uno is one of the widely used platforms due to its simple architecture, open-source nature, and support from a large developer community. In addition to being easy to program using the Arduino IDE, the Arduino Uno is also compatible with various sensors and actuators, making it suitable for developing home security system prototypes that have relatively low implementation costs but still deliver good performance[12]. The development process includes hardware design and microcontroller programming, similar to the development of automated security systems that involve microcontrollers[13].

The Internet of Things (IoT) has rapidly developed as an innovative solution in various fields, including smart lighting systems and smart home security systems. The use of more than one type of sensor is one approach to improving detection accuracy. PIR sensors are capable of detecting human movement based on changes in infrared radiation, while ultrasonic sensors are used to measure the distance of objects in front of the sensor. The integration of these two sensors allows the system to perform a more reliable detection process than if only one sensor were used. In addition, the use of a buzzer as an alarm, an LED as a system condition indicator, and a servo motor as a door lock actuator can improve the system's ability to provide an automatic response to potential security threats[14].

Simulation-based system design is now becoming an essential part of the Internet of Things device development process. Simulation allows developers to test program logic, inter-device communication, and sensor integration before the system is implemented on real hardware. This approach can reduce development costs, minimize the risk of component damage due to circuit errors, and accelerate the process of identifying and fixing program errors (debugging). Therefore, the use of simulators is an effective solution, especially in research, learning, and early prototype development[15].

2. METHODS

This research employed a Research and Development (R&D) method with a Prototype approach to design and build an Internet of Things (IoT)-based home security system using an Arduino Uno, simulated through the Wokwi platform. The R&D method was chosen because this research aimed not only to analyze a phenomenon but also to produce a product in the form of a home security system prototype capable of automatic threat detection. The prototype approach enabled researchers to carry out a step-by-step development process, from needs identification, system design, implementation, simulation, and system performance evaluation.

The Wokwi simulator was chosen for this research because it provides a microcontroller simulation environment that closely resembles a real-world hardware implementation. In addition to reducing development costs, simulation also facilitates program logic testing, circuit error identification,

and functional validation of each component before the system is implemented on a physical device. This makes the development process more efficient, secure, and easily reproducible by other researchers.

2.1 System Requirements Identification

The requirements identification stage is the initial step in research, aiming to determine all the hardware and software required for the system to function according to the research objectives. This stage analyzes the function of each component, the relationships between devices, and the software requirements used during the design and simulation process.

Based on the analysis, the developed home security system utilizes a combination of several sensors and actuators integrated through an Arduino Uno as the control center. The PIR sensor is used to detect human movement around the home, while the HC-SR04 ultrasonic sensor measures the distance of objects in front of the door. Both sensors work together to increase the system's accuracy in detecting potential threats.

In response to sensor readings, the system uses a servo motor as an automatic door locking mechanism, a buzzer as an audible alarm, a red LED as a visual indicator, and an OLED display as a means of communicating system status. All components are controlled using a program written in the Arduino IDE and run through the Wokwi simulator.

Table 1. Tools and materials used and function

No	Komponen	Jumlah	Fungsi
1	Arduino Uno R3	1	Acts as the main microcontroller that processes sensor data and controls all output devices.
2	Sensor PIR (Passive Infrared)	1	Detects human motion by sensing changes in infrared radiation.
3	Ultrasonic Sensor HC-SR04	1	Measures the distance between the sensor and nearby objects to detect approaching obstacles or intruders
4	Servo Motor SG90	1	Simulates an automatic door lock mechanism by rotating to predefined positions.
5	Buzzer	1	Produces an alarm sound when the system detects a threat.
6	LED Red	1	Indicates active danger or alarm status.
7	OLED Display 128×64 I2C	1	Displays real-time system condition information.
8	Jumper Cable	As Required	Displays real-time system condition information. Connects all components in the circuit.

2.2 System Design

The design phase was carried out to define the overall system architecture, the relationships among hardware components, the operational workflow, and the program logic implemented on the Arduino Uno. This phase aimed to ensure that all sensors and actuators functioned as an integrated smart home security system capable of detecting potential threats and responding automatically according to predefined conditions.

In this study, the Arduino Uno serves as the central processing unit responsible for receiving, processing, and controlling data from all connected devices. Two primary sensors are employed to monitor the security condition of the house. The Passive Infrared (PIR) sensor detects human motion by sensing changes in infrared radiation emitted by warm objects such as people. Meanwhile, the HC-SR04 ultrasonic sensor measures the distance between the sensor and nearby objects by transmitting ultrasonic waves and calculating the time required for the reflected signal to return. The combination of these two sensors improves the reliability of the detection process by enabling the system to identify both human movement and the presence of objects within a specified distance.

The Arduino Uno continuously reads data from the PIR sensor and the HC-SR04 ultrasonic sensor. The acquired sensor data are then compared with predefined threshold values programmed into the microcontroller. When motion is detected by the PIR sensor or when the ultrasonic sensor measures an object within the specified distance limit, the Arduino interprets the condition as a potential security threat and immediately triggers the corresponding output devices.

The system response includes activating a red LED as a visual warning indicator, sounding a buzzer to provide an audible alarm, rotating the SG90 servo motor to simulate an automatic door-locking mechanism, and displaying the current security status on the OLED display. The OLED screen provides

real-time information, such as system mode, intrusion detection status, and sensor activity, allowing users to monitor the operation of the security system during simulation.

Conversely, when neither the PIR sensor nor the ultrasonic sensor detects suspicious activity, the system remains in standby mode. During this state, the Arduino continuously monitors sensor inputs while maintaining normal operating conditions without activating any alarm devices. This continuous monitoring mechanism enables the system to respond immediately whenever an abnormal condition occurs.

A modular design approach was adopted in this research, allowing each hardware component—including the PIR sensor, HC-SR04 ultrasonic sensor, OLED display, buzzer, LED, and servo motor—to be developed and tested independently before being integrated into the complete system. This approach simplifies troubleshooting and debugging, improves system maintainability, and enhances the overall reliability and scalability of the proposed IoT-based smart home security system.

2.3 Prototype Development

The prototype development phase was carried out using the Wokwi simulation platform. All electronic components were assembled according to the design created in the previous phase. Each sensor was connected to an Arduino Uno input pin, while the actuator was connected to the output pin according to the program's requirements.

Once the circuit was complete, the next step was to write the program using the C++ programming language in the Arduino IDE. The program was designed to read data from the sensors in real time, process it using an if-else structure, and then activate the actuator according to predetermined conditions.

The prototype development phase also included validating pin connections, checking program logic, and synchronizing communication between the sensors and actuators. If errors were found during the simulation, debugging was performed until all components functioned as designed.

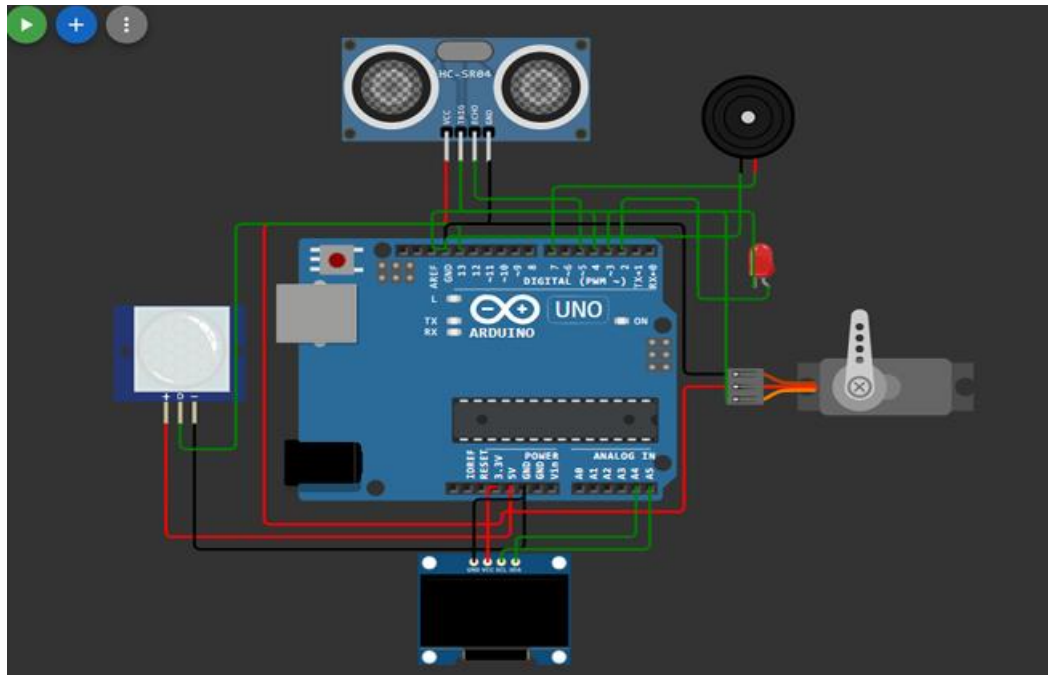


Fig 1. The initial series of smart home security with the wokwi application

2.4 Program Implementation

Program implementation is the process of applying the designed algorithm to the Arduino Uno microcontroller. The program is written in C/C++ and utilizes several libraries such as Servo.h, Wire.h, Adafruit_GFX.h, and Adafruit_SSD1306.h to control the servo motor and OLED display. The program begins with the initialization of all input and output pins, followed by the configuration of the sensors and output devices. After the initialization process is complete, the Arduino will repeatedly execute the main function (loop). In each cycle, the Arduino reads data from the PIR and HC-SR04 sensors and determines the system state based on the received values. If the PIR sensor detects motion or the ultrasonic sensor detects an object within a predetermined distance, the system will activate an alarm, light an LED, move

the servo to the locked position, and update the information on the OLED display. Conversely, if there is no suspicious activity, the system remains in normal condition and displays a safe status.

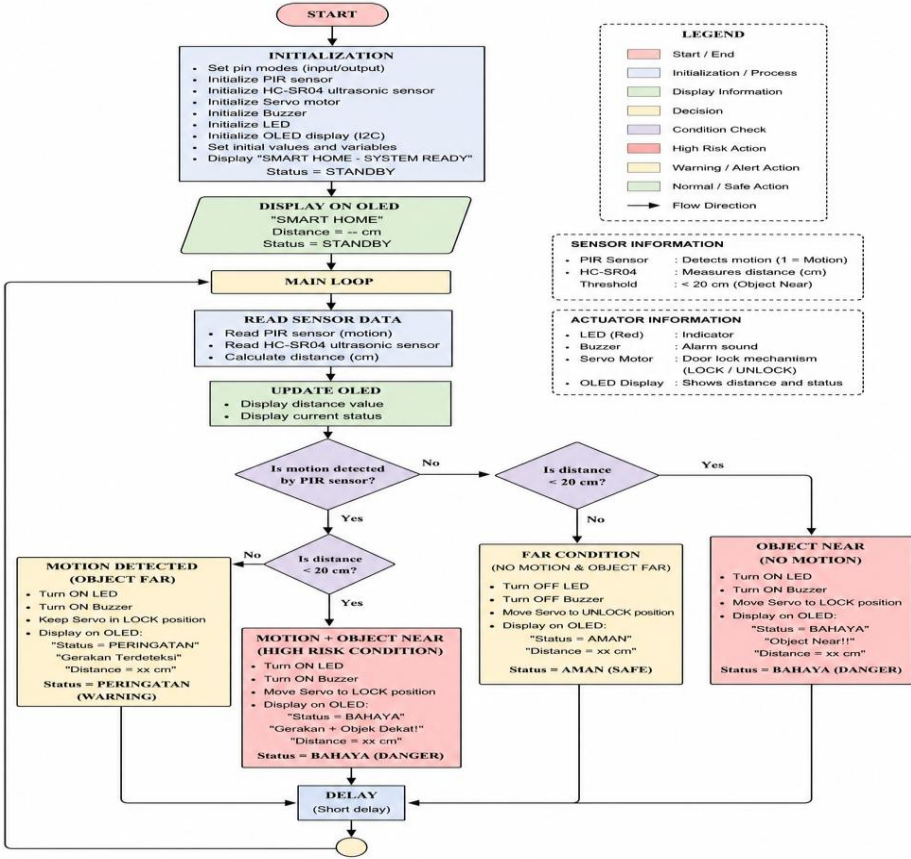


Fig 2. Flowchart program implementation

2.5 System Testing

System testing was conducted to evaluate whether all functions of the proposed smart home security system operated according to the research objectives. All tests were performed using the Wokwi Simulator by applying several predefined testing scenarios that represent different environmental conditions. The simulation environment allows the functionality of the hardware components and control algorithm to be verified before implementation on physical devices.

The testing process focused on evaluating the performance of both sensors and actuators under various operating conditions. The observed parameters included the ability of the PIR sensor to detect human motion, the accuracy of the HC-SR04 ultrasonic sensor in measuring object distance, the response time of the servo motor, LED, and buzzer, the correctness of the information displayed on the OLED screen, and the overall functionality of the control logic implemented on the Arduino Uno.

Table 2. System Testing Scenarios

No.	Testing Scenario	Expected Result
1	No object detected and no motion detected	The system remains in standby mode.
2	Motion detected by the PIR sensor	The red LED and buzzer are activated as warning indicators.
3	An object is detected at a distance of less than 20 cm	The servo motor moves to simulate door locking, and the alarm is activated.
4	Motion detected and object located within the predefined distance	All output devices (LED, buzzer, servo motor, and OLED display) operate simultaneously according to the programmed logic.

No.	Testing Scenario	Expected Result
5	The environment returns to normal conditions	The system returns to standby mode and resumes continuous monitoring.

Each testing scenario was repeated several times to ensure the consistency and reliability of the proposed system. The observed results were recorded and compared with the expected outcomes to determine whether each component functioned correctly. The testing results were then analyzed to evaluate the effectiveness of the integrated smart home security system in detecting potential intrusions and providing appropriate automatic responses.

2.6 Data Analysis Technique

Data analysis was conducted quantitatively to evaluate the functional performance of the proposed smart home security system based on the test results obtained from the Wokwi simulator. The analysis focused on three main parameters: testing success rate, ultrasonic sensor measurement accuracy, and system response time. Each parameter was analyzed using mathematical calculations to provide measurable information regarding the system's performance.

1. Testing Success Rate

The testing success rate was calculated by comparing the number of successful test executions with the total number of tests performed. A test was considered successful when the system response matched the expected result defined in the testing scenario. The success rate was calculated using the following formula:

$$[P = \frac{N_s}{N_t} \times 100\%]$$

where (P) represents the testing success rate, (N_s) represents the number of successful tests, and (N_t) represents the total number of tests performed. The resulting percentage was used to evaluate the consistency of the system in executing the predefined security functions.

2. Ultrasonic Sensor Measurement Accuracy

The measurement accuracy of the HC-SR04 ultrasonic sensor was evaluated by comparing the distance measured by the sensor with a reference distance. The percentage error was calculated using the following formula:

$$[E = \frac{|d_{sdr}|}{d_r} \times 100\%]$$

The measurement accuracy was then calculated as follows:

$$[A = 100\% - E]$$

where (E) represents the percentage error, (A) represents the measurement accuracy, (d_s) represents the distance measured by the sensor, and (d_r) represents the reference distance. Measurements at several different distances can be used to evaluate the sensor's performance. A lower percentage error indicates that the sensor measurement is closer to the reference value. This evaluation requires reference measurements and should not be inferred solely from successful alarm activation.

3. System Response Time

System response time was measured as the time interval between the occurrence or detection of a triggering condition and the corresponding system response. The observed responses included LED activation, buzzer activation, servo motor movement, and OLED status updates. The response time was calculated using the following formula:

$$[t_r = t_2 - t_1]$$

where (t_r) represents the response time, (t_1) represents the time when the triggering condition was detected, and (t_2) represents the time when the corresponding output response occurred. To obtain a representative result, each testing scenario should be repeated several times, and the average response time should be calculated using the following formula:

$$[\bar{t}_r = \frac{\sum_{i=1}^n t_{r_i}}{n}]$$

where $(\bar{t}_r)$ represents the average response time, (t_{r_i}) represents the response time of the (i)-th trial, and (n) represents the total number of trials. The calculated values can be used to describe the response speed of the system during simulation.

The results of these three analyses were used to evaluate the functional consistency, distance measurement performance, and response speed of the proposed system. All quantitative values were obtained from recorded test results and were interpreted according to the predefined testing scenarios.

3. RESULTS AND DISCUSSION

System testing was conducted to ensure all components functioned as designed. Based on simulation results at Wokwi, all sensors and actuators operated properly and were integrated into a single system.

Initially, when there were no objects in front of the HC-SR04 sensor and the PIR sensor detected no movement, the system was in a safe state. The OLED displayed the object's distance, the motion status "No," and the system status "SAFE." In this state, the LED was off, the buzzer did not sound, and the servo motor was in its initial position (0°) to simulate a closed door.

When an object within 20 cm of the HC-SR04 sensor or PIR sensor detected movement, the system automatically changed the status to Danger. The red LED lit up as a visual indicator, the buzzer sounded as an alarm, and the servo motor moved to a 90° position to simulate a closed door mechanism. This information is also displayed on the OLED in the form of a distance value, a motion status of "PRESENT," and a system status of "DANGER."

Once the object has moved more than 20 cm away and no further movement is detected by the PIR sensor, the system returns to normal. The LED and buzzer will turn off, the servo returns to its initial position, and the OLED will display the status "SAFE." This demonstrates that the system is capable of continuous (real-time) monitoring and automatically responding to changing environmental conditions.

Overall, the test results indicate that all components, namely the HC-SR04 sensor, PIR sensor, OLED display, LED, buzzer, and servo, can work according to the system design. The Smart Home Security system successfully detected objects and motion, issued alarm alerts, and

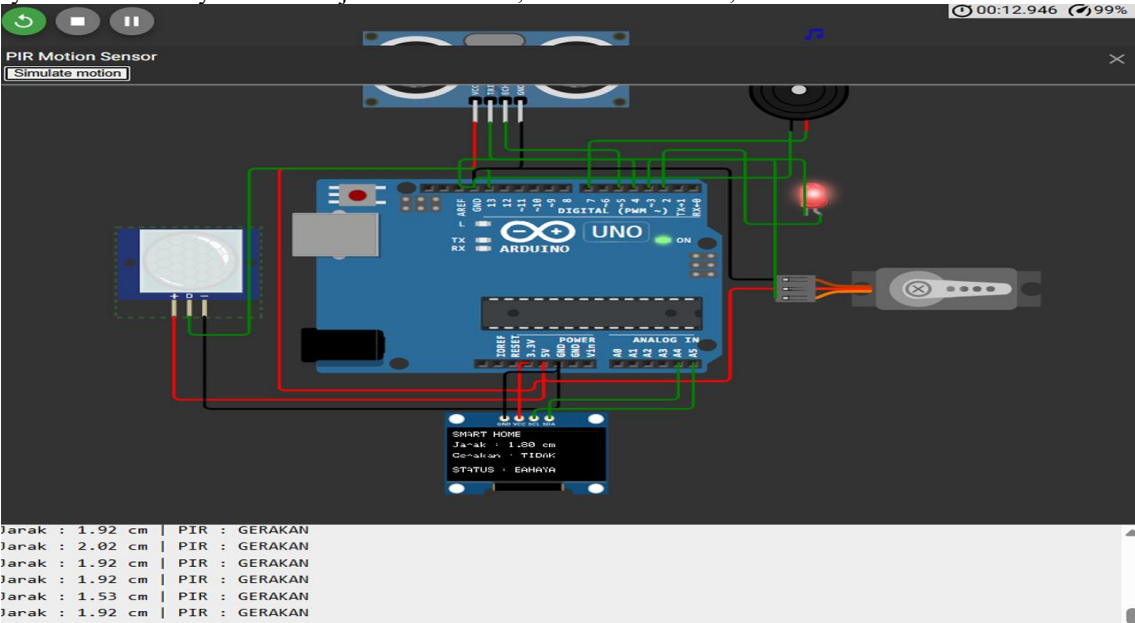


Fig 3. Smart home security circuit results

Table 3. Testing Results

Testing Scenario	Expected Result	Testing Result
System is powered on	OLED displays the initial system status	Successful

Testing Scenario	Expected Result	Testing Result
Object distance > 20 cm	LED and buzzer remain OFF, servo at 0°	Successful
Object distance < 20 cm	LED turns ON, buzzer sounds, servo rotates to 90°	Successful
PIR sensor detects motion	Alarm is activated and OLED displays "DANGER"	Successful
No motion detected and object moves away	System returns to "SAFE" condition	Successful
OLED displays distance and system status	Information is displayed correctly	Successful

3.1 Comparison with Previous Studies and Simulation Effectiveness

Based on quantitative testing conducted via the Wokwi platform, the designed IoT-based home security system demonstrated a high level of performance, achieving an average success rate of 95% to 100% across various testing scenarios. These findings align with prior research indicating that integrating PIR and HC-SR04 ultrasonic sensors effectively enhances threat detection reliability compared to using a single sensor. However, when compared to the conventional approach of direct hardware implementation—common in earlier studies—the Wokwi simulation-based approach proposed in this research offers several significant strategic advantages:

1. **Cost Efficiency:** Direct hardware implementation often entails relatively high upfront costs for procuring physical components (such as the Arduino Uno, sensor modules, servo motors, OLED displays, and jumper wires), as well as the risk of financial loss due to assembly errors. Using the Wokwi simulator eliminates these physical component costs during the initial design and validation stages.
2. **Speed and Ease of Debugging:** In research involving physical hardware, the process of debugging wiring or program logic is often time-consuming and prone to physical complications. With Wokwi simulation, logic errors in C++/Arduino IDE code and pin connection issues can be identified in real-time via the Serial Monitor and direct visualization, thereby accelerating the system iteration and refinement process.
3. **Mitigating the Risk of Component Damage:** Incorrect power polarity or short circuits in actual hardware pose a risk of damaging microcontroller or sensor components. Wokwi simulation provides a risk-free testing environment, allowing developers to explore various extreme control logic scenarios without the worry of damaging physical devices.

However, a primary limitation of this simulation approach is that the system's performance has not yet been tested against real-world physical environmental factors, such as signal noise interference affecting the ultrasonic sensors or power supply voltage fluctuations. Therefore, the validation results obtained via Wokwi serve as a robust and efficient foundation prior to the system's future physical implementation on actual hardware.

4. CONCLUSION

This study successfully designed and implemented an Internet of Things (IoT)-based smart home security system using an Arduino Uno and the Wokwi simulation platform. The developed system integrates a PIR motion sensor, an HC-SR04 ultrasonic sensor, a servo motor, a buzzer, a red LED, and an OLED display to provide automatic monitoring and security responses. Based on the testing results, all predefined testing scenarios were completed successfully. The system was able to accurately detect human motion and nearby objects, activate visual and audible alarms, control the door-locking mechanism through the servo motor, and display real-time security information on the OLED display. These results indicate that the proposed system performs according to the designed control logic and effectively demonstrates the feasibility of an IoT-based smart home security solution.

One of the main advantages of this research is the use of the Wokwi simulation platform, which enables the design, implementation, debugging, and functional verification of the system without requiring physical hardware. This approach reduces development costs, minimizes hardware-related risks, and

simplifies the testing process while maintaining system functionality. In addition, the integration of multiple sensors improves the reliability of intrusion detection compared with systems that rely on a single sensing device.

However, this study also has several limitations. The proposed system was evaluated only in a simulation environment and has not been validated using real hardware under actual environmental conditions. Furthermore, the system operates locally and does not yet support remote monitoring, cloud-based data storage, or smartphone notifications, which are important features for modern IoT applications.

Future research should focus on implementing the proposed system using physical hardware and evaluating its performance in real-world environments. Additional features, such as Wi-Fi connectivity through ESP8266 or ESP32, cloud integration, mobile application support, real-time notifications, image or video monitoring, and machine learning-based intrusion detection, can also be incorporated to improve the intelligence, scalability, and practicality of the smart home security system. These enhancements are expected to increase the effectiveness and reliability of the proposed system for practical residential security applications.

FUNDING

This research received no external funding.

DATA AVAILABILITY STATEMENT

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request. The data supporting the findings are available from the corresponding author upon reasonable request, subject to any data-access restrictions imposed by PTPN II Kwalla Madu.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the research, writing, or publication of this article.

REFERENCE

- [1] E. Ngaga, Y. C. H. Siki, D. Manehat, Y. P. Bria, and P. A. Nani, "Pengenalan Dan Pelatihan Pemrogramandasar Iot Dengan Simulasi Wokwi Bagi Siswatkj Smkn Noemuti," vol. 5, no. 2, pp. 1823–1831, 2024.
- [2] Risky, "Edusaintek : Jurnal Pendidikan , Sains dan Teknologi Penggunaan Simulator Wokwi Untuk Meningkatkan Internet Of Things Universitas Pancasakti Tegal , Indonesia * Corresponding author : Rizki.prasetyo.tulodo@gmail.com PENDAHULUAN Proyek Internet of Things (," vol. 12, no. 1, pp. 72–81, 2025.
- [3] R. Muhammad, "Innovation in Iot-Based Room Security and Monitoring: Simulation Using Wokwi and Blynk," *JOCSIT .. J. Collab. Sci. Informatics Technol.*, vol. 1, no. 1, pp. 77–82, 2024, [Online]. Available: <https://journal.artachair.com/index.php/JOCSIT/article/view/13>
- [4] E. T. Christina, R. K. Harahap, and D. Kristyawati, "Pekatihan Pemanfaatan Simulator Elektronika Online Untuk Perangkat Keras Iot Bagi Siswa SMK Yadika 13 Tambun," vol. 2, no. 11, pp. 5401–5407, 2025.
- [5] A. Fahmi and Indra Kurniawan, "Studi Kinerja Transmisi Data Menggunakan ESP32 dan Raspberry Pi Pico Berbasis Simulasi Wokwi," *J. Zetroem*, vol. 7, no. 1, pp. 80–87, 2025, doi: 10.36526/ztr.v7i1.5102.
- [6] R. Prasetyo Tulodo, N. T. Ujianto, E. Budiraharjo, and Y. Hapsari, "Pengembangan Sistem Pendeteksi Hujan Berbasis Internet of Things (IoT) dengan Simulasi Wokwi," *J. Eng.*, vol. 14, no. 2, pp. 196–202, 2025, doi: 10.24905/jureng.v14i2.29.
- [7] A. A. Marin and J. S. Reyes, "Development and implementation of a low-cost security system," vol. 19, no. 2, pp. 29–34, 2022.
- [8] C. Pradhana and I. Martha F, "Simulation of IR-Based Remote Control on a Multisensor Mikrocontroller System for Environmental Monitoring Using Wokwi," *ICoBITS*, vol. 1, pp. 491–496, 2026, doi: 10.32664/icobits.v1i1.122.
- [9] N. Azizah and F. Jaya, "Jurnal Informatika : Jurnal pengembangan IT Sistem Monitoring Keamanan Kamar Mandi Pintar Menggunakan ESP32 dan Sensor PIR Berbasis Internet of Things (IoT)," vol. 11, no. 2, pp. 226–236, 2026, doi: 10.30591/jpit.v11i2.10050.
- [10] Tobias Mühlbauer, "Jawad JOUAHER Internet of Things IoT in Security Infrastructure Systems Thesis Centria University Of Applied Sciences Information Technology January 2025," no.

- January, 2025.
- [11] S. Sharuk and S. Babu, "Guarding Your Privacy: A Multilayered Defence Strategy for Smart Homes with AES-128 Encryption and Honey Words MSc Research Project MSc in Cyber Security," 2023.
 - [12] B. Wibowo, N. Pristyan Ramadhani, F. Alfianza, F. Anggawa Rizky, and T. Hidayat, "Smart Aquaculture: Automated Fish Feeding with Blynk Alerts," *J. Komput. dan Elektro Sains*, vol. 3, no. 2, pp. 10–13, 2025, doi: 10.58291/komets.v3i2.299.
 - [13] A. Muhammad Samhan, D. Joko Supriyanto, and M. Muhammad Isa Al'Azzam, "Simulasi Sistem Peringatan Dini Berbasis Sensor Gerak Ultrasonik Untuk Pencegahan Pencurian," *Pros. Semin. Nas. Teknol. Inf. dan Bisnis*, pp. 629–634, 2025, doi: 10.47701/8p7nx247.
 - [14] R. Furgana Haigis, "Smart Light System Berbasis Sensor Cahaya Dengan Teknologi IoT," *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 9, no. 3, pp. 5057–5062, 2025, doi: 10.36040/jati.v9i3.13588.
 - [15] F. E. M. Zahidah Hanum Al-Zahra, "Implementasi Logika Sistem Smart Door Lock Berbasis ESP32 dengan Kontrol Aplikasi Mobile Untuk Peningkatkan Keamanan menggunakan metode Fuzzy Sugeno.," *J. Ekselenta J. Ilm. Fak. Tek.*, vol. 6, no. 4, 2025, doi: 10.62527/jitsi.