RESSTECH

Vol. 3, No. 2, pp. 40-50, 2026

RESEARCH ON INSTRUMENTATION

https://rin.resstech.org/

Development of An Iot-Based Smart Home Security System Using Laser Beams and LDR Sensors

Reza Oskarino*

Department of Physics, Faculty of Mathematics and Natural Sciences, University, Padang, INDONESIA

**Corresponding author: rezaoskarino1@gmail.com*

ARTICLE INFO

Article history:
Received October 13, 2026
Revised November 2, 2026
Accepted November 11, 2026
Available online November 11, 2026

Keywords:
Smart home; Arduino Uno; Laser Beam; LDR Sensor; RFID; Internet of Things

ABSTRACT

This study to analyze the design and performance evaluation of an Internet of Things (IoT) based home security prototype combining RFID access authentication with laser light dependent resistor (LDR) intrusion detection. The prototype employed an Arduino Uno, RFID RC522, laser emitter, LDR voltage divider, relay-controlled solenoid door lock, buzzer, and ESP32-CAM for image acquisition and Telegram notifications. Engineering research involved system design, prototype construction, and subsystem and integrated testing. Across 13 alarm test observations, LDR analog-to-digital converter readings ranged from 56 to 1004, a threshold of 850 distinguished the nine interrupted-beam observations from four uninterrupted-beam observations under the tested lighting conditions. RFID card were detected at distances of 1–6 cm but not at 7–9 cm. Registered credentials activated the door lock, whereas unregistered credentials were rejected. In 30 response-time tests, the buzzer responded in 120.87 ± 4.25 ms (mean ± standard deviation); Telegram transmission required 2290 ± 75.20 ms. The results demonstrate the functional integration of local authentication, beam-interruption detection, actuation, image capture, and remote notification. The findings apply to the tested prototype and environmental and network conditions.

This is an open-access article under the CC BY-SA license.
Copyright © 2024 by Author. Published by Researchers Society of Science and Technology.

1. INTRODUCTION

Previous studies have investigated various approaches to residential security, including RFID-based door access control [8], [9], camera-based monitoring and Telegram notifications [2], and IoT-based smarthome applications [11]. Although these studies demonstrate the potential of individual security technologies, the integration and experimental evaluation of door access authentication, indoor laser-based intrusion detection, local alarm activation, and remote image notification remain relevant aspects for further investigation. Accordingly, this study addresses the need for a prototype that combines these security functions within a single system. The research focuses on two main questions: (1) how can RFID authentication, laser–LDR sensing, and ESP32-CAM monitoring be integrated into an IoT-based smarthome security prototype? and (2) how does the developed system perform in terms of sensor response, RFID recognition distance, actuator operation, intrusion detection, and local and remote notification response times? To address these questions, this study develops and experimentally evaluates an applied smarthome security prototype using Arduino Uno, RFID RC522, laser–LDR sensors, a buzzer, a solenoid door lock, and ESP32-CAM. The primary contribution of this work is the implementation and quantitative evaluation of these integrated security functions under laboratory testing conditions rather than the introduction of a new sensing or authentication technology.

Previous studies primarily focused on RFID-based access control systems, in which security mechanisms were limited to authenticating authorized users at entry points without providing additional protection against unauthorized activities occurring inside the secured area. Consequently, these systems were unable to detect potential intrusions or suspicious movements within the protected environment after access had been granted.

To address this limitation, this work designed and evaluated a prototype integrating Arduino Uno, RFID RC522, laser–LDR sensing, a buzzer, relay, solenoid door lock, and ESP32-CAM. Unlike conventional RFID-based security systems, the proposed prototype combines access authentication with an additional intrusion detection mechanism using laser beams and LDR sensors to monitor a protected area. The research objectives were to specify the hardware and operational design and to assess beam-interruption classification, RFID recognition distance, access decisions, actuator behavior, and local and remote response times. The experimental observations and numerical results reported here were taken from the underlying thesis.

The contribution is a prototype-level evaluation of complementary access-control and intrusion-detection pathways. RFID governs entry authorization; a separate laser–LDR pathway monitors interruption, the buzzer supplies local feedback and ESP32-CAM and Telegram provide image-based remote reporting. This evaluation does not claim field-deployment reliability or robustness beyond the tested conditions.

Security and privacy remain important considerations in the development of Internet of Things (IoT)-based systems, particularly when connected devices are used for access control and remote monitoring [18]. Previous research has also identified security vulnerabilities in certain RFID technologies, including MIFARE Classic, highlighting the importance of considering authentication security when developing RFID-based applications [17]. In addition to access authentication, optical intrusion detection provides another approach to monitoring protected areas. Hashim and Hussain [19] demonstrated the application of laser beams and light-dependent resistors (LDRs) in a security alarm system, where changes in received illumination were used to identify interruptions in the monitored beam. Meanwhile, studies on IoT communication protocols have shown that communication performance is influenced by the selected protocol and network configuration [20], [21]. These findings provide a foundation for the present study, which integrates RFID-based door access control, laser–LDR intrusion detection, a local buzzer alarm, and ESP32-CAM image notifications through Telegram.

2. MATERIAL AND METHODS

2.1 Research Design

Engineering research was carried out at the Electronics and Instrumentation Laboratory, Department of Physics, Universitas Negeri Padang, beginning in April 2025. The workflow consisted of idea development, conceptual design, identification of system functions, detailed circuit design, prototype assembly, and testing. The system was evaluated through controlled functional trials and quantitative timing measurements rather than a household field deployment.

The main manipulated conditions were illumination at the LDR and the laser-beam state; RFID card identity and card–reader distance were varied in access tests. The recorded responses included ADC output, alarm state, authorization outcome, actuator response, image and message delivery, and response time. Ambient illumination and laser alignment are therefore important conditions when interpreting the observations.

2.2 System Design and Operation

To provide a clear overview of the proposed system, a block diagram is presented to illustrate the workflow and interactions between system components, from the input stage to the resulting output, including the processes involved. The block diagram is shown in Figure 8.



Figure 1. Block Diagram System

Figure 1 illustrates the block diagram of the proposed IoT-based smarthome security system, which integrates access control, intrusion detection, and remote monitoring functions. The system utilizes an Arduino Uno as the main controller to coordinate the operation of the RFID RC522 module, laser–LDR sensor, buzzer, relay, solenoid door lock, and ESP32-CAM module. The RFID module serves as an authentication mechanism to distinguish between registered and unregistered users, while the laser–LDR sensor functions as an intrusion

detection mechanism by monitoring interruptions in the laser beam. When a registered RFID card is detected, the Arduino activates the relay to unlock the solenoid door lock, allowing authorized access. Conversely, an unregistered RFID card is rejected, and the system generates a warning. When the laser beam is interrupted, the LDR detects a change in light intensity, causing the Arduino to activate the buzzer and trigger the ESP32-CAM to capture an image. The captured image is subsequently transmitted through the Telegram application, enabling users to receive remote notifications of potential security disturbances.

After all circuits were implemented, the components were integrated into a complete smarthome security system. The overall circuit integration of the proposed system is illustrated in Figure 2.

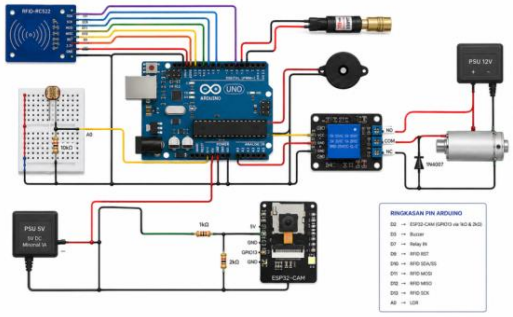


Figure 2. Complete Circuit Configuration

Figure 2 presents the complete circuit configuration of the proposed smarthome security prototype, illustrating the electrical connections between the main controller, input sensors, output actuators, and communication module. The Arduino Uno serves as the central processing unit and receives input signals from the RFID RC522 module and the laser–LDR sensing circuit. The LDR is connected to the Arduino analog input through a voltage-divider circuit consisting of an LDR and a 10 kΩ resistor, allowing changes in light intensity to be converted into analog voltage readings. The Arduino processes these signals based on a predefined threshold of 850 ADC counts to determine whether the laser beam is interrupted. The relay module controls the solenoid door lock using a separate 12 V power supply, while the buzzer provides audible warnings according to the detected security conditions. Additionally, the ESP32-CAM module is connected to the Arduino to receive intrusion detection triggers and transmit captured images through Wi-Fi to Telegram. This integrated hardware configuration enables the prototype to perform local authentication, intrusion detection, door-lock control, audible alarm activation, and remote security monitoring within a single system.

The LDR and a 10 kΩ resistor formed a voltage divider connected to Arduino analog input A0. A threshold of 850 ADC counts was implemented in the controller software. The solenoid was powered by a separate 12 V supply through a relay, with a 1N4007 flyback diode across the inductive load. The Arduino provided a trigger to ESP32-CAM through a voltage-divider interface, while the camera module used Wi-Fi and Telegram to deliver images and event notifications. The hardware design follows the component roles documented in the thesis [12–14].

2.3 Data Collection and Analysis

Data collection was conducted through experimental testing of the developed IoT-based smarthome security prototype. The evaluation covered the relationship between light intensity and LDR resistance, RFID card recognition distance and authorization, laser beam interruption detection under different lighting conditions, relay and solenoid door lock operation, buzzer activation, ESP32-CAM image acquisition, and Telegram notification delivery. The testing instruments consisted of an Arduino Uno, RFID RC522 module, laser transmitter, LDR sensor, relay module, solenoid door lock, buzzer, and ESP32-CAM module. The laser–LDR intrusion detection test comprised 13 recorded observations, including nine interrupted-beam conditions and

four uninterrupted-beam conditions. In addition, the buzzer response time and Telegram notification delivery time were each evaluated through 30 experimental trials.

Response time was defined as the elapsed time between the detection of a triggering event and the corresponding system response. Local alarm response time referred to the interval between event detection and buzzer activation, whereas remote notification response time referred to the interval between event detection and Telegram notification delivery. The remote notification process required an active Wi-Fi connection to transmit information from the ESP32-CAM to Telegram. The collected data were analyzed using descriptive statistical methods. The mean and standard deviation were calculated for buzzer response time and Telegram notification delivery time to evaluate their average performance and variability. Other experimental results were analyzed descriptively by comparing sensor readings, RFID detection distances, and observed system responses under the specified testing conditions.

2.4 Performance Criteria

Table 1. Performance indicators used for system evaluation

Parameter	Success indicator
Laser and LDR	Distinguish normal beam reception from interrupted beam
RFID	Distinguish registered and unregistered cards
Relay / solenoid	Operate according to Arduino access command
Buzzer	Provide the intended indication for each condition
ESP32-CAM	Receive trigger and capture image
Telegram	Receive notification and image
Overall system	All subsystems operate according to the design

3. RESULTS AND DISCUSSION

3.1 Design Specification

The developed smarthome security prototype integrates RFID-based access authentication, laser–LDR intrusion detection, local alarm activation, electronic door locking, and remote image notification. As illustrated in Figure 1, the Arduino Uno functions as the main controller, receiving input signals from the RFID RC522 module and the laser–LDR sensing circuit. The controller processes these signals to determine the appropriate system response, including relay activation, solenoid door lock operation, and buzzer activation. The ESP32-CAM module provides image acquisition and Wi-Fi communication capabilities for transmitting security notifications through Telegram. The complete circuit configuration is presented in Figure 2, illustrating the integration of the input sensors, processing unit, output actuators, and communication module. The solenoid door lock operates using a 12 V power supply controlled through a relay module, while the LDR sensing circuit uses a voltage-divider configuration with a 10 kΩ resistor. This configuration enables the system to combine access control and indoor intrusion detection within a single prototype.

3.2 LDR Characteristics

Table 2. Relationship between light intensity and LDR resistance

No.	Light intensity (lux)	LDR resistance (kΩ)
1	20	14.071

2	40	8.702
3	60	7.699
4	100	5.060
5	150	4.449
6	250	3.015
7	400	2.121
8	650	1.341
9	900	1.036
10	1100	0.860

The characteristics of the Light Dependent Resistor (LDR) were evaluated by measuring its resistance under different illumination levels. The experimental results indicate an inverse relationship between light intensity and LDR resistance, where increasing illumination produces a decrease in sensor resistance. As presented in Table X, the LDR resistance decreased from 14.071 kΩ at 20 lux to 2.121 kΩ at 400 lux. This behavior demonstrates the sensitivity of the LDR to changes in incident light intensity and supports its application as a sensing component in the proposed laser-based intrusion detection system. The relationship between light intensity and resistance was further examined using a power regression model, as illustrated in the corresponding graph.

The resistance curve is nonlinear, with a larger absolute change at low illuminance and a progressively smaller change at higher illuminance. Consequently, the LDR should be treated as a light-sensitive element whose output requires calibration for a given voltage-divider arrangement, rather than as a direct linear measure of illuminance. The subsequent alarm tests assess the actual ADC decision threshold in the assembled prototype.

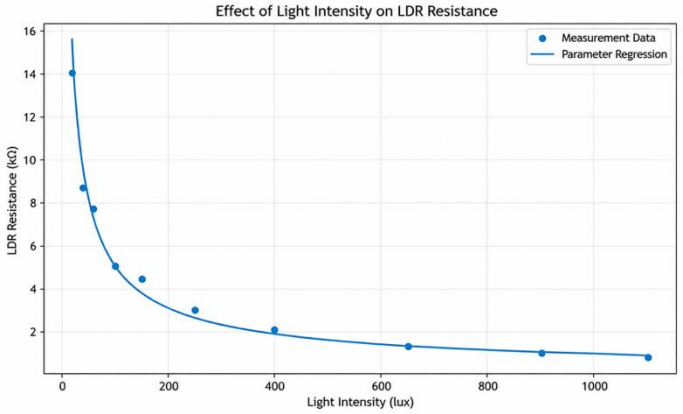


Figure 3. Characteristics of the LDR sensor

Figure 1 presents the decrease in resistance with increasing light intensity. The same trend is visible in the measurements in Table 2. In the prototype, this characteristic was used indirectly: the Arduino monitored voltage-divider ADC values to distinguish the laser-received state from interruption. The resistance measurements and the alarm ADC measurements are different quantities and should not be conflated.

3.3 RFID Reading Distance

Table 3. RFID RC522 reading-distance test.

Distance	Reading result
1 cm	Detected
2 cm	Detected
3 cm	Detected
4 cm	Detected
5 cm	Detected
6 cm	Detected
7 cm	Not detected
8 cm	Not detected
9 cm	Not detected

The RC522 detected the test card at every examined distance from 1 to 6 cm and failed to detect it at 7, 8, and 9 cm (Table 3). Accordingly, 6 cm is the largest successful reading distance observed in this setup, not a guaranteed maximum range for all cards, reader orientations, or installations. This result helps define the practical presentation distance for the prototype access point.

3.4 Intrusion Detection and Alarm

Table 4. Alarm test under different illumination conditions

Laser condition	Environment	LDR value	Alarm
Interrupted	Dark room (3 trials)	56–57	Active
Interrupted	Room illumination (3 trials)	396–405	Active
Interrupted	Phone flashlight (3 trials)	784	Active
Uninterrupted	Laser received (4 trials)	1000–1004	Inactive

Table 4 summarizes the 13 recorded alarm observations by illumination condition. The nine blocked-beam readings were 56–57 in darkness, 396–405 under room illumination, and 784 with a phone flashlight; the four unblocked readings were 1000–1004. The chosen 850-count threshold separated these groups in this dataset, producing the intended alarm state for all 13 observations. This is an observed classification result, not a validated false-alarm rate across all possible ambient-light conditions.

3.5 Access, Door Lock, and Buzzer

Table 5. Relay and solenoid door-lock test

Condition	System response	Result
Registered RFID	Relay active, solenoid opens	Successful
After access	Relay returns, solenoid locks	Successful
Unregistered RFID	Access rejected, door remains locked	Successful

Registered RFID	Relay active, solenoid opens	Successful
After access	Relay returns, solenoid locks	Successful
Unregistered RFID	Access rejected, door remains locked	Successful
Registered RFID	Relay active, solenoid opens	Successful
After access	Relay returns, solenoid locks	Successful
Unregistered RFID	Access rejected, door remains locked	Successful
Registered RFID	Relay active, solenoid opens	Successful
After access	Relay returns, solenoid locks	Successful
Unregistered RFID	Access rejected, door remains locked	Successful

Table 6. Buzzer response test

Condition	Buzzer response	Result
Registered RFID	Two beeps	Successful
Unregistered RFID	Alarm for 5 s	Successful
Laser Interrupted	Alarm active	Successfull
Registered RFID	Two beeps	Successful
Unregistered RFID	Alarm for 5 s	Successful
Laser Interrupted	Alarm active	Successfull
Registered RFID	Two beeps	Successful
Unregistered RFID	Alarm for 5 s	Successful
Laser Interrupted	Alarm active	Successfull
Registered RFID	Two beeps	Successful
Unregistered RFID	Alarm for 5 s	Successful
Laser interrupted	Alarm active	Successful

For a registered RFID UID, the relay energized and the solenoid opened; after access, the relay returned to its locking state. For an unregistered UID, access was rejected and the door remained locked (Table 5). The buzzer produced two beeps for registered access, a five-second warning for rejected access, and an active alarm when the laser beam was interrupted (Table 6). Together, these outcomes show that authorization and intrusion events can generate distinct local responses.

3.6 IoT Function and Response Time

Table 7. ESP32-CAM and Telegram test

Event	ESP32-CAM / Telegram response	Result
Laser interrupted	Capture image; image received	Successful

Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful
Laser interrupted	Capture image; image received	Successful
Unregistered RFID	Send notification; message received	Successful

Table 8. Buzzer Response-time statistics

Parameter	Result
Buzzer tests	30
Buzzer minimum	115 ms
Buzzer maximum	130 ms
Buzzer mean	120.87 ms
Buzzer standard deviation	±4.25 ms

Table 9.Telegram Response-time statistics

Telegram tests	30
Telegram minimum	2165 ms
Telegram maximum	2450 ms
Telegram mean	2290 ms (2.29 s)
Telegram standard deviation	±75.20 ms

The response times of the local buzzer and Telegram notification system were evaluated through 30 trials for each function. This number of trials was selected to provide repeated observations for estimating the average response time and its variability under the experimental conditions. The selection of 30 trials was a practical experimental decision rather than a sample size determined through a formal statistical power analysis. The buzzer exhibited a mean response time of 120.87 ms with a standard deviation of 4.25 ms, whereas the Telegram

notification system showed a mean response time of 2290 ms with a standard deviation of 75.20 ms. To assess the precision of these estimates, 95% confidence intervals were calculated using Student's t-distribution. The resulting intervals were 119.28–122.46 ms for the buzzer and 2261.92–2318.08 ms for Telegram notifications. These results indicate that the local alarm responded substantially faster than the remote notification mechanism under the tested conditions. However, the confidence intervals describe the uncertainty of the estimated mean response times and do not establish system reliability under different network or environmental conditions.

3.7 System Robustness Evaluation

The robustness of the proposed smarthome security system was examined by considering changes in light intensity, Wi-Fi connectivity interruptions, and laser beam misalignment. The LDR characterization results demonstrated that the sensor resistance decreased as the incident light intensity increased, indicating its sensitivity to variations in illumination. During Wi-Fi connectivity interruptions, the system was unable to transmit security notifications through Telegram. However, the local buzzer alarm remained operational when an alarm condition was triggered, indicating that the local warning mechanism could function independently of internet connectivity. Furthermore, slight laser beam misalignment did not immediately trigger the alarm as long as part of the laser beam continued to illuminate the LDR sensor sufficiently for the system to recognize the beam. When the laser beam was completely displaced from the LDR sensor, the system detected the loss of illumination and activated the buzzer alarm. These observations indicate that the prototype can maintain its local alarm functionality during network interruptions, although remote notification capabilities depend on Wi-Fi availability. Additionally, laser alignment remains an important factor in maintaining reliable intrusion detection, as complete misalignment may trigger an alarm without an actual intrusion.

3.8 Overall System Performance

Table 10. Overall system test

Scenario	System response	Result
Registered RFID	Access granted	Successful
RFID scanned again	System deactivated	Successful
Unregistered RFID	Access rejected; buzzer active	Successful
Laser interrupted	Buzzer active	Successful
Laser interrupted	ESP32-CAM captures image	Successful
Intrusion detected	Image sent to Telegram	Successful
Unregistered RFID	Telegram notification sent	Successful
Laser returns to normal	System returns to normal	Successful

Integrated tests demonstrated registered-card authorization, unregistered-card rejection, laser interruption warning, ESP32-CAM image acquisition, and Telegram delivery (Table 9). The results establish that the subsystems could operate together in the tested prototype. The alarm dataset and response-time statistics provide quantitative evidence for selected functions, whereas several other functions were assessed through categorical success observations.

The evaluation has several limitations. Although the LDR characteristics were examined under different illumination levels, the reliability of the complete intrusion detection system under prolonged exposure to varying environmental conditions has not been fully established. Observations during Wi-Fi interruptions indicated that the local buzzer remained operational, whereas Telegram notifications could not be delivered without network connectivity. Furthermore, complete laser beam misalignment triggered the alarm because the LDR no longer received sufficient illumination, indicating a potential source of false alarms. These

observations were limited to the prototype testing conditions, and no extended outdoor deployment, long-term reliability assessment, or backup power supply evaluation was conducted. Further testing is therefore required to assess the system's performance under prolonged environmental disturbances and power supply interruptions.

4. CONCLUSION

An IoT-enabled smart home security prototype integrating RFID authentication, laser–LDR beam-interruption sensing, solenoid locking, buzzer warning, and ESP32-CAM/Telegram reporting was designed and tested. The architecture combines local access control and interruption detection with remote event communication. The observed LDR ADC range was 56–1004, and the programmed threshold of 850 correctly separated the 13 reported blocked and unblocked observations. RFID reading was successful through 6 cm in the tested arrangement. The mean buzzer response was 120.87 ms (SD 4.25 ms), compared with 2290 ms (SD 75.20 ms) for Telegram transmission, based on 30 trials for each metric. These results support prototype functionality under the stated experimental conditions. Further research should examine adaptive or recalibrated optical thresholds, multiple sensing locations, stronger image documentation, backup power, network outages, and extended field testing. Quantitative tests of false positives, missed detections, and end-to-end notification reliability would strengthen the performance evidence.

ACKNOWLEDGMENTS

The authors thank the Department of Physics, Faculty of Mathematics and Natural Sciences, Universitas Negeri Padang, and the laboratory staff for supporting the experimental work. The first author acknowledges the academic guidance received during the underlying undergraduate research.

REFERENCES

[1] B. T. Kusuma, F. A. Pratama, H. D. P. Anugrah, S. Y. Distianto, and R. Susanto, “Sistem Keamanan Keris Menggunakan Laser Security Berbasis Arduino Uno,” Prosiding Seminar Nasional Teknologi Informasi dan Bisnis, 2024.

[2] H. A. Kusuma, S. B. Wijaya, and D. Nusyirwan, “Sistem Keamanan Rumah Berbasis ESP32-CAM Dan Telegram Sebagai Notifikasi,” Infotronik: Jurnal Teknologi Informasi dan Elektronika, vol. 8, no. 1, p. 30, 2023, doi: 10.32897/infotronik.2023.8.1.229.

[3] A. Rozaq, D. Irawan, and Y. A. Surya, “Sistem Keamanan Rumah Menggunakan RFID dan Keypad Matrix Dengan One Time Pad,” vol. 5, no. 1, 2023.

[4] S. E. Prasetyo et al., “Sistem Smart home menggunakan IoT,” Telcomatics, vol. 7, no. 1, p. 24, 2022, doi: 10.37253/telcomatics.v7i1.6763.

[5] Y. Kurniawan et al., “Desain Dan Implementasi Smart home Berbasis IoT Dengan Memanfaatkan Aplikasi Cisco Packet Tracer,” 2024, pp. 1279–1293.

[6] A. Fandidarma et al., “Rancang Bangun Mobil Remote Control Pemantau Area berbasis IoT menggunakan ESP32-CAM,” vol. 2, no. 1, pp. 31–38, 2021.

[7] M. Y. Kholifudin, “Sinar Laser Mainan Sebagai Alternatif Sumber Cahaya Monokromatik Praktikum Kisi Difraksi Cahaya,” Jurnal Penelitian Pembelajaran Fisika, vol. 8, no. 2, pp. 129–134, 2017, doi: 10.26877/jp2f.v8i2.1641.

[8] F. Sudarto et al., “Perancangan Sistem Smartcard Sebagai Pengaman Pintu Menggunakan RFID Berbasis Arduino,” CCIT Journal, vol. 10, no. 2, pp. 239–254, 2017, doi: 10.33050/ccit.v10i2.544.

[9] R. Suwartika and G. Sembada, “Perancangan Sistem Keamanan Menggunakan Solenoid Door Lock Berbasis Arduino Uno pada Pintu Laboratorium di PT. XYZ,” Jurnal E-Komtek (Elektro-Komputer-Teknik), vol. 4, no. 1, pp. 62–74, 2020, doi: 10.37339/e-komtek.v4i1.217.

[10] A. Setiawan and I. Purnamasari, “Pengembangan Passive Infrared Sensor (PIR) HC-SR501 dengan Microcontrollers ESP32-CAM Berbasiskan Internet of Things (IoT) dan Smart home sebagai Deteksi Gerak untuk Keamanan Perumahan,” Prosiding Seminar Nasional SISFOTEK, vol. 3, no. 1, pp. 148–154, 2019.

[11] S. Siswanto et al., “Prototype Smart home Dengan Konsep IoT (Internet of Thing) Berbasis NodeMCU Dan Telegram,”

Jurnal Sistem Informasi dan Informatika (Simika), vol. 3, no. 1, pp. 85–93, 2020, doi: 10.47080/simika.v3i1.850.

[12] NXP Semiconductors, “MFRC522 Standard Performance MIFARE and NTAG Frontend: Product Data Sheet, Rev. 3.9,” NXP Semiconductors, 2016.

[13] Espressif Systems, “ESP32 Series Datasheet,” Espressif Systems, 2025.

[14] Arduino, “Arduino UNO Rev3 Technical Specifications,” Arduino Documentation, 2026.

[15] V. A. Suoth et al., “Rancang bangun alat pendeteksi intensitas cahaya berbasis Sensor Light Dependent Resistance (LDR),” Jurnal MIPA, vol. 7, no. 1, p. 47, 2018, doi: 10.35799/jm.7.1.2018.19609.

[16] S. Sahara, “Studi Kesalahan Pada Sensor LDR Sebagai Alat Ukur,” Prosiding Seminar Nasional SISFOTEK, vol. 2, no. 1 pp. 8–15, 2024.

[17] F. D. Garcia et al., “Dismantling MIFARE Classic,” in *Computer Security – ESORICS 2008*, Lecture Notes in Computer Science, vol. 5283. Berlin, Germany: Springer, 2008, pp. 97–114, doi: 10.1007/978-3-540-88313-5_7.

[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in Internet-of-Things,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.

[19] H. M. B. Hashim and D. M. A. Hussain, “Security system via LDR,” *Journal of Applied Engineering & Technology*, vol. 2, no. 2, pp. 20–30, 2018, doi: 10.55447/jaet.02.02.10.

[20] S. Mijovic, E. Shehu, and C. Buratti, “Comparing application layer protocols for the Internet of Things via experimentation,” in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow (RTSI)*, 2016, doi: 10.1109/RTSI.2016.7740559.

[21] L. Năstase, I. E. Sandu, and N. Popescu, “An experimental evaluation of application layer protocols for the Internet of Things,” *Studies in Informatics and Control*, vol. 26, no. 4, pp. 403–412, 2017, doi: 10.24846/v26i4y201704.