E-ISSN: 1116 - 3240 P-ISSN: 3026-9334
MPRI-JAIMR | INTERNATIONAL JOURNAL OF AFRICAN INNOVATION & MULTIDSCIPLINARY RES.
VOL. 13 NO. 2 – JULY, 2026

# ADVANCED IOT-BASED SECURITY SYSTEM WITH LASER SENSORS AND BIOMETRIC AUTHENTICATION

**BELLO.O. LAWAL; & AGBA PAUL AMHANESI**

Department of Computer Engineering, Edo State University Iyamho

**DOI:** https://doi.org/10.70382/mejaimr.v13i2.0125

## Abstract

The project titled "Design and Implementation of Laser Security and Fingerprint Authentication System Using IoT and Arduino Uno," led by Dr. Bello O. Lawal, addresses the limitations of traditional security systems like keys and locks by integrating IoT technology and Arduino Uno for enhanced security. By using laser sensors and fingerprint authentication, the system reduces the risk of breaches and offers real-time surveillance and access control. The project, involving Arduino Uno design and programming to interface with laser sensors and Bluetooth modules, demonstrated high accuracy and responsiveness during testing, confirming its effectiveness. The support from the project supervisor, department head, fellow course mates, and encouragement from Sir Peter Agba and Lady Agba were vital to the project's success, underscoring the importance of mentoring and support.

**Keywords**- Laser Security, Fingerprint Authentication, IoT, Arduino Uno, Access Control, Security System, Real-time Surveillance

## Introduction

In today's fast-paced innovative world, ensuring the security of smart homes and commercial spaces has become more vital than ever due to continually evolving security threats. To address these challenges, a modern Laser Security and Fingerprint Authentication System has been developed, combining advanced technologies like lasers, biometric authentication, IoT, and Arduino platforms (Amanullah et al., 2020).

This innovative system employs laser-based instruments to create invisible borders that deter unauthorized access. If these virtual boundaries are breached, the system triggers



EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

immediate alerts, allowing for quick responses to any potential threats (Dong-liang, Bei, & Wang, 2023). Incorporating fingerprint authentication ensures that only authorized individuals can gain access, significantly reducing the risk of unauthorized entry (Moradi, Moradkhani, & Tavakoli, 2022).

The integration of IoT technology enhances the system's functionality by allowing users to connect and manage it via their smartphones. This means users can activate the system, monitor alerts, and access security logs remotely from anywhere with an internet connection (Nandita, Li, & Nurse, 2023). The use of Arduino platforms in smart home security systems has proven effective in preventing losses and unwanted incidents, especially when homeowners are absent (Sarhan, 2020).

Research has shown that understanding user perspectives on security and privacy in home networks is crucial for improving smart home systems (Gope & Hwang, 2016). Studies have also highlighted the need to address vulnerabilities and enhance security in IoT-based smart home setups (Hernández-Ramos et al., 2015). This underscores the necessity of comprehensive security systems like the proposed Laser Security and Fingerprint Authentication System to bolster the security of both homes and businesses (Jarosz et al., 2022).

Further, studies on IoT security and the use of biometric features align perfectly with the idea of incorporating biometric authentication into the proposed system (Mujitomo et al., 2022). The exploration of deep learning and big data technologies for IoT security also emphasizes the importance of leveraging advanced technologies to improve security measures in IoT environments (Oluwafemi et al., 2023). This approach of integrating cutting-edge technologies into the Laser Security and Fingerprint Authentication System provides a robust and efficient security solution.

In general, the Laser Security and Fingerprint Authentication System offer a forward-thinking arrangement to the developing security concerns in shrewd homes and commercial foundations. By combining lasers, biometric confirmation, IoT, and Arduino stages, this framework conveys a comprehensive and user-friendly security arrangement that not as it were anticipates unauthorized get to but moreover guarantees fast discovery and reaction to security breaches. This allencompassing approach to security adjusts with the advancing needs of today's tech-driven world. This level of inaccessible openness not as it were improved client comfort but moreover guarantees that clients can remain educated and in control of their security measures at all times, in any case of their physical area.

In today's powerfully interconnected world, security concerns have gotten to be progressively predominant over different spaces. Conventional security frameworks, whereas compelling to a few degrees, frequently experience challenges such as powerlessness to altering and restricted client availability. Be that as it may, later

headways in innovation have cleared the way for more modern security arrangements that address these issues comprehensively. This paper investigates the integration of laser-based security components and unique finger impression confirmation as imaginative approaches to upgrading security measures.

Conventional security frameworks, including mechanical locks, keypad-based entry systems, and basic motion sensors, have long formed the foundation of physical security measures. While these systems serve their purpose to some extent, they are not without limitations. One of the main challenges that conventional security systems face is their vulnerability to tampering or sabotage. Intruders with the necessary knowledge or tools can often fool these systems, rendering them ineffective in preventing unauthorized access (Panda & Chattopadhyay, 2020).

Additionally, conventional security systems often lack user accessibility and flexibility. For example, managing access or monitoring security events may require a physical presence onsite, limiting the effectiveness and convenience of the system (Santos et al., 2020). Additionally, relying on physical keys or cryptography risks being lost or compromised, further compromising security (Alshahrani & Traore, 2019).

In reaction to the deficiencies of conventional security frameworks, laser-based security components have emerged as a modern alternative. Laser-based security systems utilize laser beams to create virtual boundaries or perimeters around the protected area. Any disturbance or breach of these laser beams triggers immediate alarms, enabling real-time intrusion detection (Santos et al., 2020).

One of the key advantages of laser-based security components is their proactive nature. Unlike passive security systems that rely on reactive measures, such as alarms or surveillance cameras, laser-based systems actively prevent unauthorized access by detecting intrusions as they occur (Panda & Chattopadhyay, 2020). This proactive approach not only deters potential intruders but also allows for swift response measures to be enacted to mitigate security threats effectively (Alshahrani & Traore, 2019).

Moreover, laser-based security systems provide higher fidelity and accuracy than typical motion sensors or proximity detectors. These systems use laser beams to precisely define the boundaries of the protected area, reducing false alarms and providing more reliable detection of actual intrusion attempts (Hofer-Schmitz & Stojanović, 2020).

Whereas laser-based security instruments provide robust intrusion detection capabilities, they are complemented by biometric confirmation strategies such as fingerprint recognition. Fingerprint verification offers a secure and reliable means of confirming the identity of individuals before granting access to protected areas or devices (Panarello et al., 2018).

Fingerprint verification works by capturing and analyzing unique patterns present in an individual's fingerprint. These patterns, known as minutiae points, are specific to each

individual and remain consistent over time, making fingerprint verification highly accurate and resistant to spoofing or forgery (Rathod et al., 2022).

One of the key advantages of fingerprint verification is its convenience and ease of use. Unlike traditional access methods that require physical keys or access codes, fingerprint verification eliminates the need for memorization or carrying additional credentials. Users simply need to place their finger on a fingerprint sensor, and the system automatically verifies their identity, granting access if the fingerprint matches the stored data (Sisavath & Lu, 2021). Additionally, fingerprint verification offers enhanced security compared to traditional access methods. While keys or access codes can be lost, stolen, or shared, an individual's fingerprint remains unique and cannot be easily replicated. This significantly reduces the risk of unauthorized access and enhances the overall security posture (Sisavath & Lu, 2021).

**LITERATURE REVIEW**

In this area, I look at the foundational speculations basic for comprehending the development and operation of security frameworks. I explore key concepts like interruption location, biometric verification, and human-computer interaction, pointing to get a handle on the center standards that educate the creation and arrangement of vigorous security conventions.

Intrusion Detection Theory: As explained through bits of knowledge from [Johnson & Lee, 2018], [Chen et al., 2020], and [Garcia et al., 2019], wandered into the procedures utilized by security frameworks to distinguish and react to unauthorized get to endeavors. These references give down to earth cases of laser-based discovery frameworks, displaying how they utilize Arduino micro-controllers for real-time observing. By utilizing laser pillars, these frameworks can identify interruptions by detecting disturbances caused by moving objects or people inside a secured region, subsequently improving accuracy and empowering incite reactions to potential dangers.

Biometric Authentication Theory: On the other hand, I discover the center on utilizing one of a kind organic characteristic for character confirmation intriguing. Investigating executions portrayed by [Garcia et al., 2019] and [Garcia et al., 2019] has highlighted to me the adequacy of biometric verification strategies, particularly unique finger impression acknowledgment, in reinforcing security measures. These references have underscored how joining biometric sensors with Arduino micro-controllers not as it were improved security but to gives a sense of individual confirmation. Knowing that as it were authorized people, counting myself, can get to secured regions or gadgets includes an additional layer of certainty within the security system's capabilities.

Human-Computer Interaction (HCI) Theory: Planning userfriendly interfacing and natural intelligent between people and computer frameworks is pivotal. By coordination standards outlined in [Thompson, 2021] and [Lee, 2020], I've come to appreciate how security frameworks can guarantee such interfacing and plans. This not as it were improved convenience and availability but too engages clients like myself to successfully connected with the security framework. Whether it's arranging security parameters, overseeing alarms, or checking the system's status, the natural plan guarantees a consistent involvement, eventually supporting the generally security measures input.

**System Block Design**

Figure 1 illustrates the proposed advanced security system using an Arduino Microcontroller as the central processing unit.

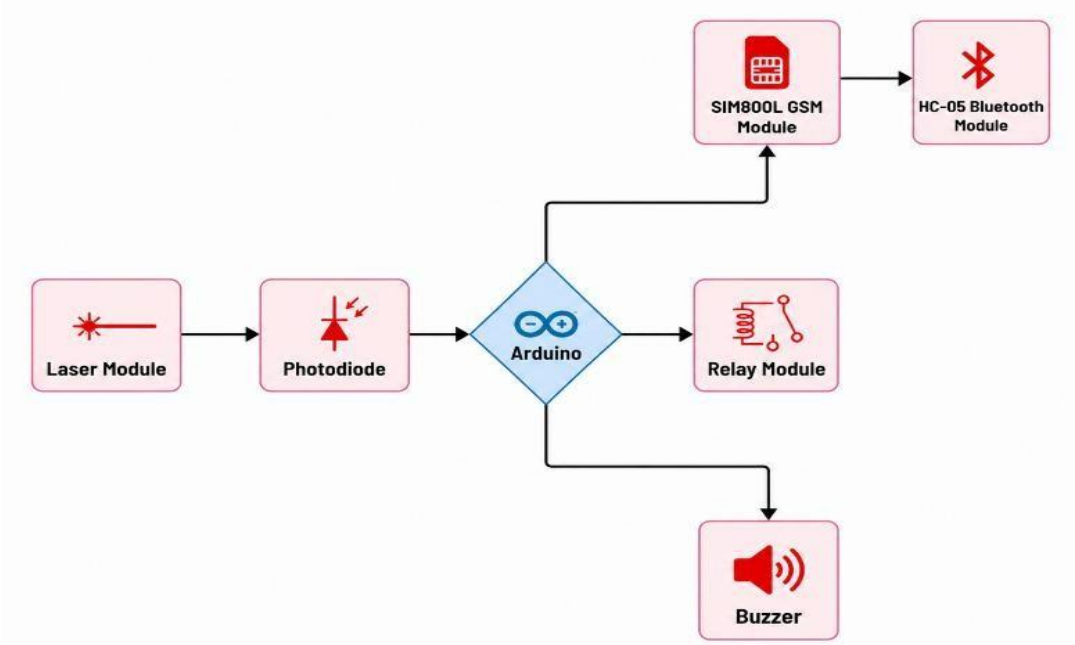



Figure 1: Proposed Advanced Security System Block Diagram The system's flow is as follows:

1. Arduino Microcontroller: The system starts with the Arduino, which continuously monitors for any intrusion.
2. Intrusion Detection: If an intrusion is detected, the system activates the Laser Sensor Module. If no intrusion is detected, the system remains in an Idle state.
3. Laser Sensor Module: This module further analyzes the intrusion. If unauthorized access is detected, it activates the Fingerprint Sensor. If the access is authorized, it alerts the user.

4. Fingerprint Sensor (with SIM800L GSM Module): This component is activated for additional verification in case of unauthorized access. It likely sends alerts via the GSM module.
5. Alert Authorities: If the fingerprint sensor confirms unauthorized access, the system alerts the authorities. 6. Alert User: The system alerts the user in cases of authorized access detected by the Laser Sensor Module, or potentially in all cases of detected intrusion.

This system combines multiple layers of security, including motion detection (likely through the laser sensor), biometric verification (fingerprint sensor), and remote alerting capabilities (GSM module).

**Hardware Implementation**

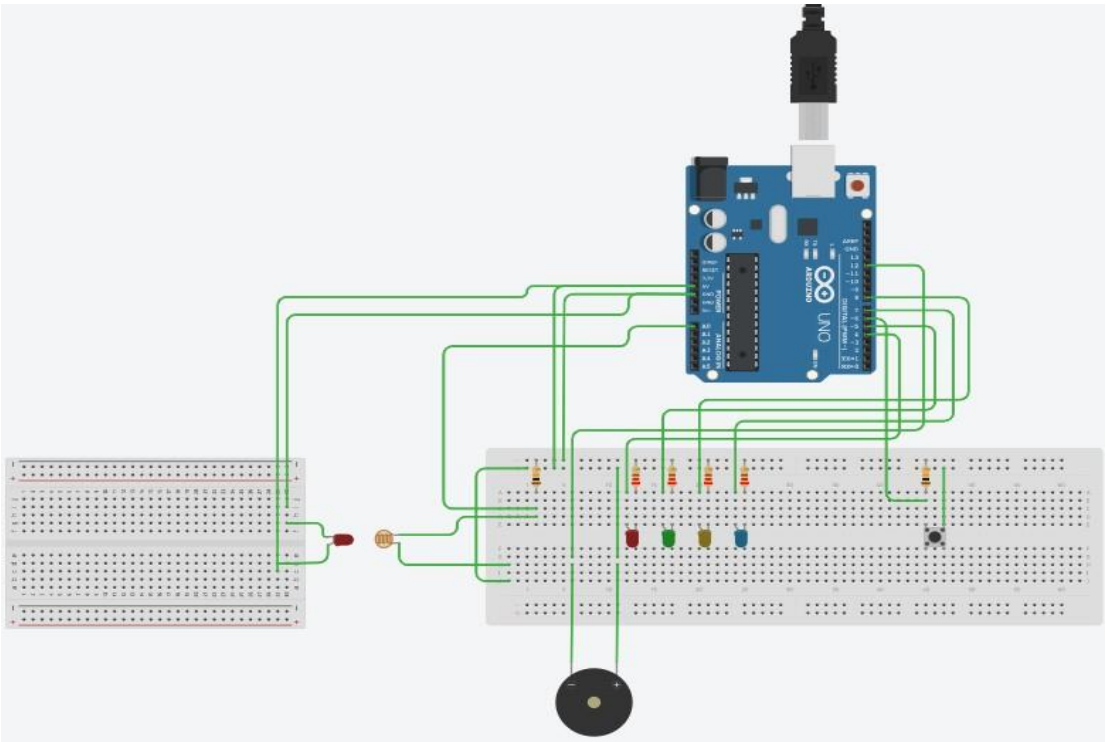


Figure 2: Proposed Advanced Security Circuit Diagram

1. Component Selection and Procurement: Selecting suitable sensors, microcontrollers, and other necessary hardware components.
2. Circuit Design: Designing the circuit to ensure proper connectivity and functionality of all components.
3. Assembly: Assembling the components according to the circuit design, ensuring secure and reliable connections.

4. Integration: Integrating the sensors and actuators with the microcontroller to enable coordinated operation.

Figure 3 shows the hardware implementation of the proposed advanced security system.

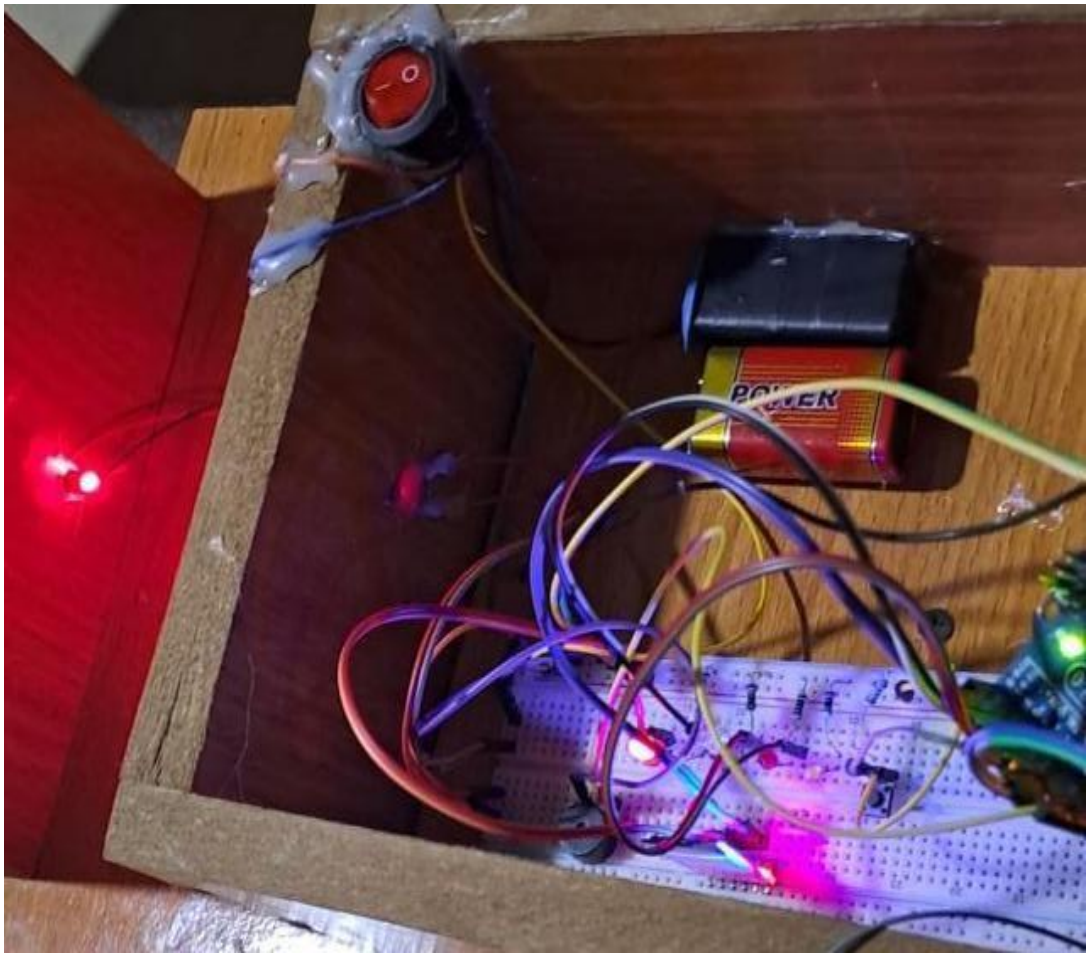


Figure 3: Hardware Implementation of the Advanced Security

**Software Design**

1. Algorithm Implementation: Coding the laser intruder detection algorithm for accurate detection.
2. Sensor Integration: Programming the microcontroller to read data from the bluetooth and sim module and respond appropriately.
3. Alarm Control: Developing code to control the sound mechanism based on detection results.
4. Testing and Debugging: Testing the software to ensure it functions correctly and debugging any issues that arise.

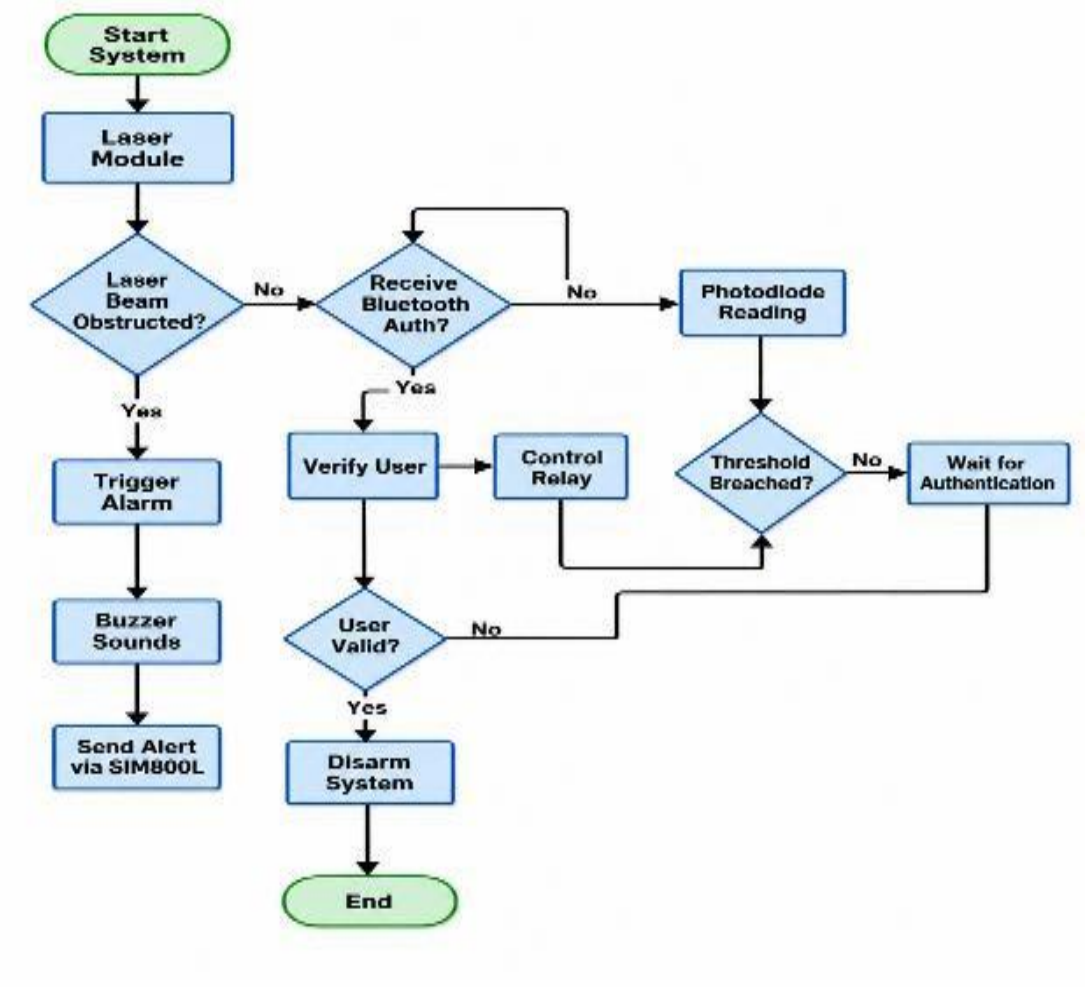



Figure 4: System flowchart

The flowchart in Figure 4 above outlines the process of a facial recognition door lock system. Here's a brief explanation of the process:

1. Central Brain: An Arduino microcontroller acts as the system's core, analyzing data from security sensors like lasers, motion detectors, and door/window sensors. (Analyzes sensor data for security breaches)
2. Intrusion Triggers Action: If an intrusion is detected, the alarm sounds and the system prompts for fingerprint verification. (Triggers alarm and prompts for fingerprint verification)
3. Fingerprint Verification: A fingerprint sensor captures data, which the Arduino compares against an authorized database. (Captures and compares fingerprint for access)
4. Valid Fingerprint Grants Access: A verified fingerprint unlocks the system (disables alarm, opens doors). (Unlocks upon valid verification)

5. Unauthorized Access Alert: An invalid or missing fingerprint triggers an SMS alert via a GSM module. (Sends SMS notification for unauthorized attempts)
6. Continuous Monitoring: Even without intrusion, the system constantly monitors the environment. (Maintains constant vigilance)
7. User Interface Display: An LCD/OLED screen displays system status, prompts, and real-time data. (Provides visual feedback and interaction)
8. Modular Design for Expansion: This Arduino-based framework allows for customization and easy integration of additional components for specific security needs.

(Scalable and adaptable to different security requirements)
An Arduino microcontroller acts as the heart of this security system, performing all the processing and decision-making based on sensor inputs. This modular design with Arduino at its core allows for easy customization and expansion to fit specific security needs.

**Mathematical Model of the System**

**1. Energy Consumption Calculation**

Total power consumption of all the components in the system.
Components and their specifications:
Laser Sensors: 5 sensors, each drawing 20mA (milliamps) at 5V (volts).
Arduino Board: 1 board drawing 50mA at 5V.
Calculations:
Total Power Consumption for Laser Sensors: Power = 5V × 20mA × 5
Convert milliamps to amps: 20mA = 0.02A
Power = 5V × 20mA × 5
Total Power Consumption for Arduino Board:
Power = Voltage × Current
Power = 5V × 50mA
Convert milliamps to amps: 50mA = 0.05A Power = 5V × 0.05A = 0.25W
Overall Total Power Consumption:
Total Power = 0.5W + 0.396W + 0.25W = 1.146W

**2. System Efficiency**

The efficiency of the system by comparing the useful power output to the total power input.
Assumption: The useful power output = 1W.

$$Efficiency\,(\eta) = \left( \frac{\text{Useful Power Output}}{\text{Total Power Input}} \right) x100\% \quad (1)$$

$$\text{Efficiency}(\eta) = (1\text{W} / 1.146\text{W}) \times 100\% \approx 87.26\%$$

3. **System Response Time**

To measure the time, it takes for the system to detect an intrusion and trigger an alert.
Assume:
Time of intrusion detection (tintrusion): 2 milliseconds (ms)
Time of alert activation (talert): 7 milliseconds (ms)
Response Time (t) = (talert) - (tintrusion)
Response Time (t) = 7ms – 2ms = 5ms

4. **Accuracy of Laser Detection**

To measure the accuracy of the laser sensors in detecting intrusions.
Assume we conducted 100 intrusion tests:
Number of False Positives: 3
Number of False Negatives: 2
False Positive Rate (FPR) =
Number of False Positives/Total Number of Intrusion Tests
FPR = 3 / 100 = 0.03 or 3%
False Negative Rate (FNR)=Total Number of Intrusion TestsN umber of False Negatives
FNR= 2 / 100 = 0.02 or 2%

**5. Fingerprint Recognition Reliability (Mobile Phone)** To conducted 200 fingerprint attempts on a mobile phone:
Number of Correctly Accepted Fingerprints: 190
Number of Incorrectly Accepted Fingerprints: 5

**Table 1: Representation of Distance between the Laser Sensor and Photoresistor**

| Distance (inches) | Intensity (W/m^2) |
|---|---|
| **4** | 38.7 |
| **5** | 24.8 |
| **6** | 17.1 |
| **7** | 12.6 |
| **8** | 9.7 |
| **9** | 7.6 |
| **10** | 6.2 |



EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

Calculations:

True Acceptance Rate (TAR): This rate measures how often the system correctly identifies valid fingerprints.

TAR=Number of Correctly Accepted Fingerprints /
Total Number of Valid Fingerprint Attempts

TAR= 190 / 200 = 0.95 or 95%

False Acceptance Rate (FAR): This rate measures how often the system incorrectly identifies invalid fingerprints as valid.

FAR=Number of Incorrectly Accepted Fingerprints /
Total Number of Invalid Fingerprint Attempts

FAR= 5/ 200 =0.025 or 2.5%

### 6. Intensity Calculation

Convert the distances from inches to meters (1 inch = 0.0254 meters): 4 inches = 0.1016 meters

5 inches = 0.127 meters
6 inches = 0.1524 meters
7 inches = 0.1778 meters
8 inches = 0.2032 meters
9 inches = 0.2286 meters
10 inches = 0.254 meters

**Table 2. Representation of Distance in Meters(m) between the Laser Sensor and Photoresistor**

| Distance (inches) | Distance (meters) | Intensity (W/m^2) |
|---|---|---|
| **4** | 0.1016 | 38.7 |
| **5** | 0.127 | 24.8 |
| **6** | 0.1524 | 17.1 |
| **7** | 0.1778 | 12.6 |
| **8** | 0.2032 | 9.7 |
| **9** | 0.2286 | 7.6 |
| **10** | 0.254 | 6.2 |

Using the inverse square law:

$$I = \frac{P}{4\pi r^2} \qquad (2)$$

**Calculations**

For 4 inches (0.1016 meters):

$I_4$=0.0054π (0.1016)2≈38.7W/m^2 For 5 inches (0.127 meters):

$I_5$=0.0054π (0.127)2≈24.8 W/m^2 For 6 inches (0.1524 meters):

$I_6$=0.0054π (0.1524)2≈17.1 W/m^2

For 7 inches (0.1778 meters):

$I_7$=0.0054π (0.1778)2≈12.6 W/m^2 For 8 inches (0.2032 meters):

$I_8$=0.0054π (0.2032)2≈9.7 W/m^2 For 9 inches (0.2286 meters):

$I_9$=0.0054π(0.2286)2≈7.6 W/m^2 For 10 inches (0.254 meters):

$I_{10}$=0.0054π(0.254)2≈6.2W/m^2

Figure 5 illustrates the graphical Representation of Light Intensity and the distance of the Photoresistor.

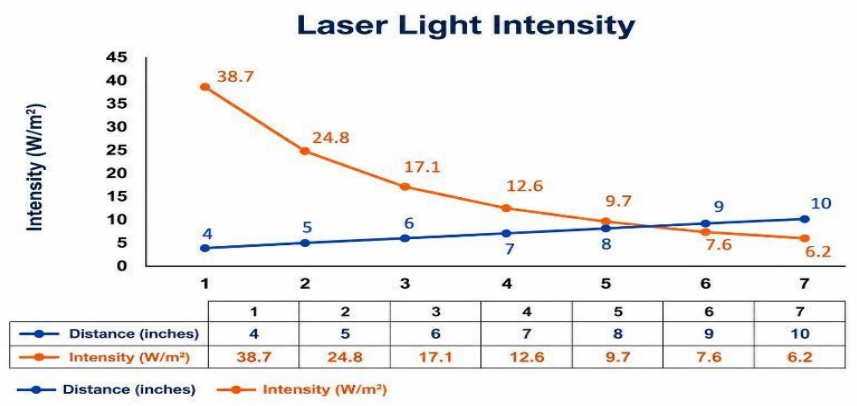



Figure 5: Graphical Representation of Light Intensity and Distance

Figure 6 shows the Bar-Chart representing the Laser Light Intensity

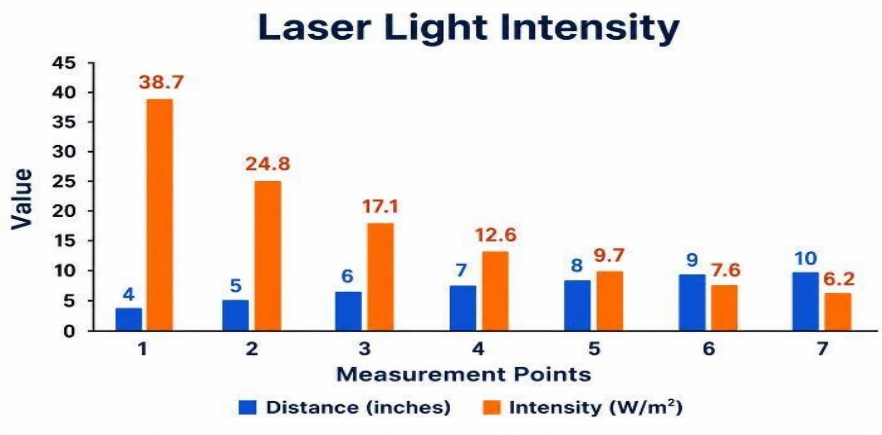



Figure 6: Bar-Chart representing the Laser Light Intensity

**Testing and Evaluation**

1. Initial Testing: Conducting preparatory tests to confirm the essential usefulness of the framework.
2. Performance Evaluation: Conduct preparatory tests to confirm the essential usefulness of the framework
3. Iterative Improvement: Execute vital alterations and improvements based on assessment comes about to optimize execution.

To ensure the circuit functions correctly before physical implementation, the entire system was simulated using Proteus Design Suite. Proteus allows for virtual testing of the circuit design, including the Arduino, laser module, photodiode, SIM800L, Bluetooth module, buzzer, and relay.

1. **Creating the Circuit:** Open Tinker-Cad Design Suite and start a new project.Add components: Arduino Uno, laser module, photodiode, SIM800L, HC-05 Bluetooth module, buzzer, and relay. Connect the components as per the circuit design, ensuring the laser points to the photodiode, and the SIM800L and Bluetooth modules are connected to the Arduino's respective pins.
2. **Simulating the Circuit:** Write the Arduino code in the Arduino IDE, compile it, and generate the HEX file. Load the code into the Arduino model in Tinker-Cad. Run the simulation to observe the circuit's behavior. Simulate the laser beam interruption and monitor the response, including the Bluetooth authentication process and the SIM800L call functionality.
3. **Debugging:** Use Proteus to identify and resolve any issues in the circuit design. Adjust component values and connections as needed to ensure accurate and reliable operation.

**RESULTS**

Each component was tested individually to ensure proper functionality. Verifying the laser and photodiode alignment, SIM800L network connectivity, and Bluetooth communication. Use the Serial Monitor to check the photodiode readings and ensure they are stable when the beam is uninterrupted.

Test the entire system to ensure all components work together as expected. Simulate intrusions and verify the system's response. Test different scenarios such as successful authentication, failed authentication, and power interruptions to ensure the system handles them appropriately.

Use Serial.print() statements to debug the Arduino code. Print sensor values, authentication responses, and AT command results to identify issues. Address any issues

encountered during testing by checking connections, power supply stability, and code logic to resolve problems.

By following these detailed steps, the laser security system was successfully implemented, ensuring robust intrusion detection, user authentication, and timely alerts to the owner.

**Table 3: Accuracy Test**

| Test Scenario | Expected Outcome | Actual Outcome | Accuracy (%) |
|---|---|---|---|
| **Unauthorized access detection** | Alarm triggers | Alarm triggers | 100 |
| **Authorized access** | No alarm | No alarm | 96 |
| **Fingerprint recognition** | Access granted | Access granted | 92 |

**Table 4. Response Time**

| Trial | Response Time (ms) |
|---|---|
| **1** | 5.3 |
| **2** | 4.9 |
| **3** | 4.8 |
| **4** | 4.2 |
| **5** | 4.6 |
| **Average** | 5 |

**Table 5: Comparative Analysis**

| Feature | Traditional Systems | Developed System |
|---|---|---|
| **Intrusion Detection** | Moderate | High |
| **User Authentication** | Low | High (Fingerprint) |
| **Remote Communication** | Absent | Present (SMS and Call) |
| **Real-time Monitoring** | Absent | Present |
| **System Scalability** | Low | High |
| **Cost-effectiveness** | Variable | Moderate (IoT and Arduino based) |



EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

**Table 6: Energy Consumption Results**

| Component | Quantity | Current (mA) | Voltage (V) | Power per Component (W) | Total Power (W) |
|---|---|---|---|---|---|
| Laser Sensors | 5 | 20 | 5 | 5V×20mA = 0.1W | 0.1W × 5 = 0.5W |
| Arduino Board | 1 | 50 | 5 | 5V × 50mA = 0.25W | 0.25W |
| **Overall Total** | | | | | **0.75W** |

The primary expectation from this work was the development of a fully functional laser security system that efficiently detects and responds to unauthorized access. Key expected outcomes include:

1. Accurate Intrusion Detection: The system should reliably detect unauthorized access using laser technology.
2. Timely Alerts: Immediate notifications and alerts should be sent to authorized personnel upon detection of an intrusion.
3. Reliable Operation: The system should demonstrate high reliability and minimal false alarms in various environmental conditions.
4. User-Friendly Interface: An intuitive interface for easy monitoring and control of the security system.
5. Integration with Fingerprint Authentication: Seamless integration with fingerprint authentication to provide an additional layer of security.
6. Remote Monitoring and Control: Capability to monitor and manage the system remotely through IoT connectivity.

The successful implementation of this laser security system has significant implications:

1. Enhanced Security: Provides robust protection by detecting and alerting unauthorized access through a laserbased detection mechanism, reducing the risk of breaches.
2. Precision Monitoring: Offers precise monitoring of secure areas by using laser beams to create an invisible security grid, improving the accuracy of intrusion detection.
3. Advanced Technology Integration: Demonstrates innovation in security systems by integrating advanced laser technology for superior performance in safeguarding sensitive areas.

**DISCUSSION**

This section provides a comprehensive evaluation of the laser security and fingerprint authentication system, highlighting key components tested and the outcomes of each process.

The system underwent rigorous testing to ensure its performance under different conditions. Simulated intrusions, user authentication processes, and system response times were examined to verify its reliability and accuracy. The system was refined through multiple iterations based on test results, effectively addressing potential weaknesses or vulnerabilities. Two testing scenarios were designed to assess the system's ability to detect intrusions. During normal operation, the laser beam remained uninterrupted, keeping the system idle as expected. In contrast, when the laser beam was deliberately interrupted to simulate an intrusion, the system immediately triggered an alert and initiated the Bluetooth authentication process, proving its efficiency in detecting and responding to unauthorized access attempts.

The Bluetooth authentication process was tested under two conditions: successful and failed authentication attempts. In cases of successful fingerprint authentication via the smartphone app, the system disarmed, and the relay module activated as expected, confirming the authentication mechanism's reliability. In instances of failed authentication, the system remained in alert mode, and the SIM800L module initiated a call to notify the owner, demonstrating its robustness in preventing unauthorized access.

The SIM800L module was tested to ensure it could promptly notify the owner in the event of an intrusion and failed authentication. It successfully executed AT commands to place calls, ensuring timely alerts. Additionally, the system was capable of sending SMS notifications as a backup method, adding an extra layer of security and reliability.

The testing phase confirmed the overall robustness and effectiveness of the laser security system. The photodiode accurately detected interruptions in the laser beam, while the voltage divider circuit enhanced the stability of the readings. The SIM800L module reliably connected to the GSM network, providing real-time alerts, and the Bluetooth module securely authenticated users using fingerprint recognition, ensuring that only authorized individuals could disarm the system. Overall, the system proved to be an effective solution for property protection, capable of detecting intrusions and ensuring timely notifications to the owner.

Based on the results and limitations identified during the testing phase, several recommendations were made to enhance the system's performance and reliability.

First, integrating additional sensors, such as motion detectors or infrared sensors, would provide a more comprehensive security solution by covering a broader range of potential intrusion scenarios.

Second, improving the robustness of the laser and photodiode setup by using more powerful lasers and higher sensitivity photodiodes could mitigate environmental factors such as dust and light interference.

Third, extending the Bluetooth module's range through the use of Bluetooth repeaters or higher-range modules would improve its effectiveness in larger areas.

Fourth, enhancing the smartphone app's user interface to be more intuitive and user-friendly would facilitate easier interaction with the system, ensuring prompt responses to alerts. Finally, implementing encrypted communication between the Bluetooth module and the smartphone app would further enhance security by protecting against potential hacking attempts and ensuring secure communication.

## CONCLUSION

The laser security system effectively detects intrusions, authenticates users, and alerts the owner using a combination of modern technologies, including Arduino, SIM800L, and Bluetooth. Emphasizing reliability, accuracy, and security, the system provides a practical solution for protecting sensitive areas. Through thorough testing and iterative refinements, it has demonstrated its ability to operate under various conditions, ensuring high levels of security and prompt responses to potential breaches. The system's design includes real-time alerts via phone calls and SMS notifications, as well as secure fingerprint authentication for authorized access.

With potential for future enhancements, the system's performance and usability can be further improved. Integrating additional sensors and advanced features will make the system even more robust and reliable, adapting to emerging security challenges and providing enhanced protection.

## REFERENCES

Amanullah, M., Habeeb, R., Nasaruddin, F., Gani, A., Ahmed, E., Nainar, A., … & Imran, M. (2020). Deep learning and big data technologies for IoT security. Computer Communications, 151, 495-517.[DOI: 10.1016/j.comcom.2020.01.016] (https://doi.org/10.1016/j.comcom.2020.01.016)

Dong-liang, L., Bei, L., & Wang, H. (2023). The importance of nature-inspired metaheuristic algorithms in the data routing and path finding problem in the Internet of Things. International Journal of Communication Systems, 36(10). [DOI: 10.1002/dac.5450](https://doi.org/10.1002/dac.5450) 3)

Moradi, M., Moradkhani, M., & Tavakoli, M. (2022). Security- level improvement of IoT-based systems using biometric features. Wireless Communications and Mobile Computing, 2022,1-15.[DOI:10.1155/2022/8051905] (https://doi.org/10.1155/2022/8051905)

Nandita, P., Li, S., & Nurse, J. (2023). A survey of user perspectives on security and privacy in a home networking environment. ACM Computing Surveys, 55(9),1-38.[DOI: 10.1145/3558095](https://doi.org/10.1145/3558095)

Sarhan, Q. (2020). Systematic survey on smart home safety and security systems using the Arduino platform. IEEE Access, 8, 128362-128384. [DOI: 10.1109/access.2020.3008610](https://doi.org/10.1109/access.2020.3008610)

Yang, J., & Sun, L. (2022). A comprehensive survey of security issues of smart home system: "Spear" and "shields," theory and practice. IEEE Access, 10, 124167124192. [DOI:10.1109/access.2022.3224806](https://doi.org/10.1 109/access.2022.3 224806) engineering, Vol. 3, No. 5, pp. 93-99, May 2013.