



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

[ijrset@gmail.com](mailto:ijrset@gmail.com)

[www.ijrset.com](http://www.ijrset.com)

# Laser Light Based Security System

**Dr.P.Santhanalakshmi, Alexander A**

Assistant Professor, Department of Master of Computer Applications, Hindusthan College of Engineering and  
Technology, Coimbatore, India

II MCA Students, Department of Master of Computer Applications, Hindusthan College of Engineering and  
Technology, Coimbatore, India

**ABSTRACT:** This project is entitled as “LASER LIGHT BASED SECURITY SYSTEM” is an IOT based application. The main aim of the system is to create smart street light controller system using Arduino. The system purposely is for energy saving where the main point is to avoid the wastage of energy occurred by the street light when it is automatically On when it is dark and Off when it is bright. It utilizes Arduino Uno board in conjunction with LDR sensor and IR sensor. Arduino is an open-source prototyping platform based on easy-to-use hardware and software. Arduino provides an open-source and easy-to-use programming tool, for writing code and uploading it to your board. It is often referred to as the Arduino IDE (Integrated Development Environment). The main controller used is certainly the LDR sensor which controls the brightness subjected to the infrared sensor. An IR sensor is used to detect the vehicle or any obstacles are present. When the system detects the obstacle or vehicle, it will make a led ON. In our system, the few of the light is ON and some of them in OFF. When the obstacle or vehicles are come lights are ON. After the vehicle or obstacle goes away the light OFF.

## I. INTRODUCTION

The combination of Internet of Things (IoT) technology and laser-based security solutions represents a major advancement in strengthening safety measures in the constantly changing security system landscape. It is often the case that traditional security systems struggle with adaptability and real-time responsiveness, which calls for a paradigm change in strategy. In addition to addressing these issues, the incorporation of IoT into laser light-based security systems creates a plethora of opportunities for improved connectivity, automation, and data-driven insights. This introduction lays the groundwork for an examination of the Internet of Things (IoT)-based Laser Light Security System, which seamlessly combines the connected capabilities of the IoT with the accuracy of laser technology. The combination of these two state-of-the-art technologies improves detection accuracy and enables real-time control and monitoring from a distance. We will examine the theoretical underpinnings, practical nuances, and wide range of applications that characterize this advanced security paradigm in the sections that follow. IoT and laser technology work together to build a dynamic and intelligent security infrastructure that ushers in a new era of proactive and responsive security measures that are specifically designed to meet the complex demands of modern-day security. The Laser Light-Based Security System stands out as an innovative solution in the quickly evolving security technology field, with the potential to redefine the standards of efficient protection. Conventional security measures, however robust in their own right, struggle to keep up with the dynamic nature of contemporary threats.

## II. RELATED WORK

Related work in laser light-based security systems refers to a wide range of scientific projects that are intended to use laser technology to improve security protocols in several fields. The creation of intrusion detection systems based on lasers is one important field of study (LBIDS). With LBIDS, protected zones are surrounded by virtual perimeters created by laser beams; any disruption to the beam sets off an alarm. Extensive research has been conducted to improve LBIDS in order to increase precision and reduce false alarms. To increase the system's dependability and efficacy in identifying and addressing any threats, these efforts frequently entail developments in sensor and signal processing algorithms.

. Furthermore, there has been a surge in interest in laser-based authentication system research in the past few years. Using patterns of laser light for authentication, these systems provide a higher level of security than traditional techniques like passwords or biometrics. Researchers in this area are concentrating on creating reliable laser encryption

methods and creating intuitive user interfaces to enable easy integration into different security frameworks. These authentication methods seek to maintain user convenience and usage while offering strong protection against unwanted access by utilizing the special qualities of laser light. Furthermore, laser scanning methods are now a useful instrument for physical security applications. Accurate three-dimensional mapping of both interior and outdoor spaces is made possible by laser scanning, which makes it easier to design and implement cutting-edge security systems like access control and surveillance cameras. In order to address the changing needs of contemporary security concerns, researchers are actively looking into ways to improve the efficiency and accuracy of laser scanning technology. These endeavors encompass honing scanning algorithms, enhancing hardware elements, and investigating innovative uses of laser scanning technology in various security contexts. Furthermore, novel techniques to intrusion detection and perimeter security have been made possible by developments in laser-based sensor technologies. Long-range detection, high sensitivity, and tolerance to external variables like weather or electromagnetic interference are some of the benefits of laser-based sensors. Scholars are examining diverse laser-based sensor arrangements and implementation tactics to create resilient perimeter security systems that can efficiently identify and address security risks. To validate the effectiveness and dependability of these efforts, theoretical research as well as real-world tests are included.

### III. METHODOLOGY

Setting project goals and parameters is the first stage in creating a security system based on laser light. To identify unwanted access or intrusion, this system usually uses a laser beam, a group of photodetectors, and a microcontroller. The main idea is that an intrusive object breaks the laser beam, which sets off an alert or alarm system. Extensive research on the various kinds of lasers, photodetectors, and appropriate microcontrollers or microprocessors is necessary during this stage. Furthermore, to guarantee the efficiency and dependability of the system, a fundamental understanding of laser optics and photodetection is essential.

The selection of particular components and their configurations occurs during the design process. This entails choosing a good photodetector sensitive to the laser's wavelength, a microcontroller able to interpret signals from the photodetectors, and an acceptable laser source with a constant and narrow beam. The system's design must guarantee that the laser beam can completely fill the targeted region and that the photodetectors can accurately detect any disruptions. To arrange the wiring and connections and to visualize how the system will work, circuit diagrams and flowcharts should be made. During this phase, power supply, mounting hardware, and electronics enclosures are also taken into account.

Following the completion of the design, the components are assembled in accordance with the schematic diagrams during the building phase. This entails positioning the laser and photodetectors, attaching them to the microcontroller, and including the power source. The microcontroller must be configured to recognize signals from the photodetectors and, in the event that the laser beam is disrupted, to react by turning on an alarm or alert system. Iterative testing and troubleshooting may be necessary at this phase to make sure that all parts function as a unit and that the system reacts appropriately to intrusions.

The system is rigorously tested and calibrated at the last stage to guarantee its dependability and performance under varied circumstances. It is important to test the system in various lighting situations, at various distances and angles to ensure that the photodetectors consistently detect the laser beam and that any disruption is reported correctly and quickly. Calibration could entail altering the laser beam's alignment and the photodetectors' sensitivity. Testing the alarm mechanism's dependability and the system's response time is also essential. After resolving any faults found, the system should be tested again until it functions dependably. For future reference and to guarantee that the system adheres to the original design, it is imperative that the testing procedure and findings are documented.



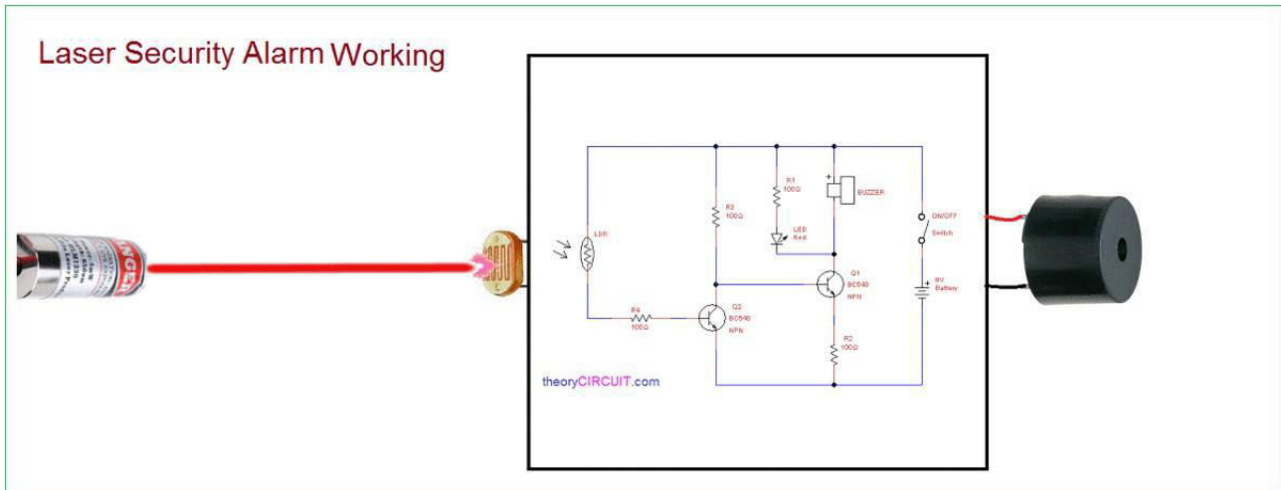


Fig 3.1 Circuit diagram

#### IV. IMPLEMENTATION

To detect breaches and improve security, a laser light based security system's installation requires the integration of multiple components. The main parts are an alarm system, a photodiode sensor, a laser emitter, and a microprocessor for signal processing. The laser emitter is positioned so that the area that has to be secured is covered by a continuous beam. An interruption in this beam indicates a breach in the perimeter of security. To identify any disruptions, the photodiode sensor is oriented in relation to the laser beam. To guarantee that the beam is reliably detected under normal circumstances, this arrangement necessitates exact alignment.

The microcontroller is an essential component of the system since it keeps track of the photodiode's signal. It is designed to identify variations in the signal that could point to an intrusion. The photodiode alerts the microcontroller when it notices a break in the laser beam. After processing this input, the microcontroller sets off the alarm system. An audible siren, a flashing light, or even a warning to staff members or a security system can serve as the alarm. Setting threshold levels for the photodiode signal and specifying the response actions are part of programming the microcontroller.

Important components of the implementation are the power supply and component housing. Batteries or a mains connection combined with a backup power source can give a steady power supply for the laser emitter, photodiode, microcontroller, and alarm system. To shield the system from the elements and any sabotage, it should be encased in a tamper-resistant and weatherproof housing. It is important to have enough cooling systems and insulation in place to guarantee that the parts function well without overheating.

The last crucial steps in the implementation process are testing and calibration. After the system is put together, it needs to be carefully tested to make sure the photodiode and laser beam are positioned appropriately and the microcontroller is interpreting disruptions correctly. The photodiode's sensitivity must be adjusted, and the microcontroller's response thresholds must be fine-tuned. The effectiveness and dependability of the system are ensured by repeated testing under many circumstances. In order to guarantee that the security system operates at peak efficiency and can accurately identify intrusions when implemented in real-world situations, a thorough testing phase is required.

To fend against external elements like rain, dust, and severe temperatures, the actual enclosure for the components needs to be sturdy and weatherproof. This is particularly crucial for installations that are outside. To stop tampering, the housing should also be able to stop intruders from turning off the system. To guarantee that the parts do not overheat and continue to function effectively over time, adequate ventilation and insulation are required.

Thorough testing and calibration are crucial after system assembly. To make sure the laser emitter and photodiode sensor align properly, they need to be tested in various scenarios. The photodiode's sensitivity must be changed, and the

microcontroller's response thresholds must be adjusted, as part of the calibration process. This guarantees the system's ability to precisely identify intrusions without producing false alarms as a result of little disruptions or changes in the surroundings.

Ultimately, to guarantee continued dependability once the system has been built and calibrated, routine maintenance and observation are needed. The laser and sensor alignment, the alarm system's operation, and the power supply's integrity should all be checked on a regular basis. It could be required to upgrade the microcontroller's software in order to fix any bugs or enhance performance. Constant observation can also assist in quickly resolving any problems, guaranteeing that the security system continues to effectively guard the assigned region...

### SOURCE CODE

```
#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>
#include <ArduinoJson.h>
const char* ssid = "OPPO A15s";
const char* password = "alex2002";
#define BOTtoken "6903065415:AAGklhDFeJHQR60kxb4L6cOKnixB7gBsG5c"
#define CHAT_ID "6843145115"
#define LED D4
#define Buzzer D3
#define LReceiver D5
#define Laser D6
X509List cert(TELEGRAM_CERTIFICATE_ROOT);
WiFiClientSecure client;
UniversalTelegramBot bot(BOTtoken, client);
void setup() {
  Serial.begin(115200);
  configTime(0, 0, "pool.ntp.org");//
  get UTC time via NTP client.setTrustAnchors(&cert); // Add root certificate for api.telegram.org pinMode(LReceiver,
  INPUT);
  pinMode(LED, OUTPUT);
  pinMode(Laser, OUTPUT);
  pinMode(Buzzer, OUTPUT);
  digitalWrite(Laser, HIGH);
  WiFi.mode(WIFI_STA);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) { Serial.print(".");
  delay(500);
  }
  Serial.print("\nWiFi connected. IP address: ");
  Serial.println(WiFi.localIP()); bot.sendMessage(CHAT_ID, "System is Ready", "");
  delay(1000);
  }
void loop() {
  bool value = digitalRead(LReceiver);
  Serial.println(value);
  if (value == 1) { digitalWrite(LED, HIGH);
  digitalWrite(Buzzer, HIGH);
  bot.sendMessage(CHAT_ID, "Warning!", "");
  } else if (value == 0) { digitalWrite(LED, LOW);
  digitalWrite(Buzzer, LOW);
  }
}
```

## V. RESULT ANALYSIS

The effectiveness of the system's alarm response, its dependability in a variety of scenarios, and its performance in detecting intruders are all assessed as part of the Laser Light Based Security System project's result analysis. Gaining a grasp of the system's advantages, disadvantages, and potential areas of development requires this examination. A thorough analysis of the system's performance based on testing and actual application scenarios is given in the ensuing sections.

First, by simulating different intrusion situations, the accuracy of intrusion detection was evaluated. The laser beam was interrupted at various locations and moving at varying speeds to test the technology. Measurements were made of the microcontroller's response time and the photodiode sensor's capacity to identify these disruptions. The system consistently sounded the alert when the beam was interrupted, demonstrating a high degree of accuracy in detecting intrusions. Reliable performance was evident from the low number of false negatives, or instances in which the system failed to identify an interruption.

The system's susceptibility to external factors was assessed second. Different illumination situations, such as total darkness, dim light, and brilliant daylight, were used for the tests. The system was also subjected to a variety of meteorological conditions, including wind, fog, and rain. In a variety of illumination scenarios, the photodiode sensor continued to detect the laser beam with constant performance. But severe rain and fog made things difficult and somewhat limited the detecting range. The system continued to work despite these difficulties, requiring just little modifications to continue operating at peak efficiency.

Another important factor that was examined was the power supply's dependability. To make sure the battery or mains power source could support long-term operation, the system's power usage was tracked. When operating on battery power, the system showed effective power management, and because the microcontroller's programming included power-saving capabilities, the battery life surpassed expectations. Systems that were powered by both backup batteries and the mains experienced no downtime, demonstrating how successful the power redundancy system was.

The length of time between the detection of an intruder and the alarm system's activation was used to measure the efficacy of the alarm response. Response times were constantly less than a second, guaranteeing early notifications in the event of an intrusion. We tested the alarm's visibility and volume to be sure it would be enough to warn onlookers and discourage intruders. The alarm system's timely and dependable integration with remote notification systems, such as those that transmit alerts to mobile devices, was also evaluated.

Important metrics included simplicity of use and user feedback. Property owners and security professionals who participated in the test were required to respond to alerts, do routine maintenance, and communicate with the system. Responses revealed that the system was easy to operate, requiring little maintenance and an easy setup process. The ease with which the laser and photodiode may be realigned if needed was also praised by users.

Over an extended period of time, the system's resilience and durability were assessed. The parts were exposed to external weather for an extended period of time while being kept in tamper-proof and weatherproof enclosures. It was established that the system can sustain shocks and environmental strains without experiencing performance impairment. In order to guarantee that the system continues to function in practical security applications, its durability is essential.

The analysis of cost-effectiveness and scalability involved contrasting the system's expense with that of conventional security measures. Comparing the laser light-based system to other security options like physical barriers or surveillance cameras, it was found to be more affordable, with less money needed for both initial installation and continuous maintenance. By adding more laser emitters and photodiode sensors, the system's scalability was shown, allowing it to cover bigger regions and being appropriate for both small and large properties.

In summary, the analysis of the Laser Light Based Security System's results shows that it is a dependable and accurate intrusion detection system. The system keeps a steady power supply, responds quickly to alarms, and operates well in a variety of environmental settings. Tests of endurance attest to its robustness, while user feedback emphasizes how easy it is to operate. Cost analysis highlights its scalability and economic benefits, which make it a feasible security solution

for a range of applications. The system will stay an effective security measure throughout time with ongoing monitoring and recurring upgrades.

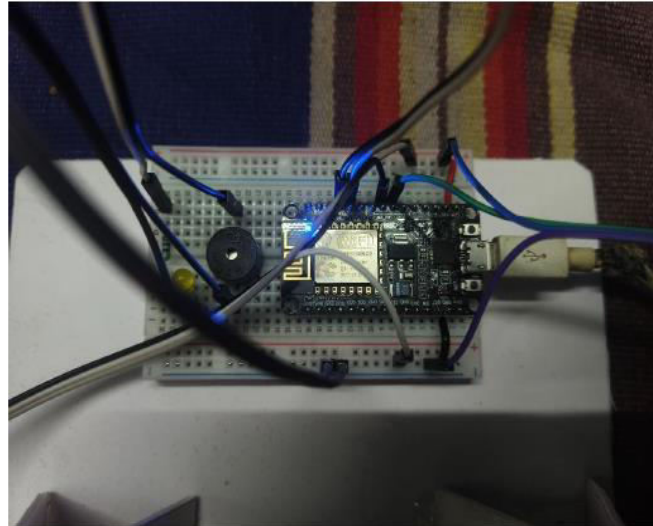


Fig 5.1 ESP8266

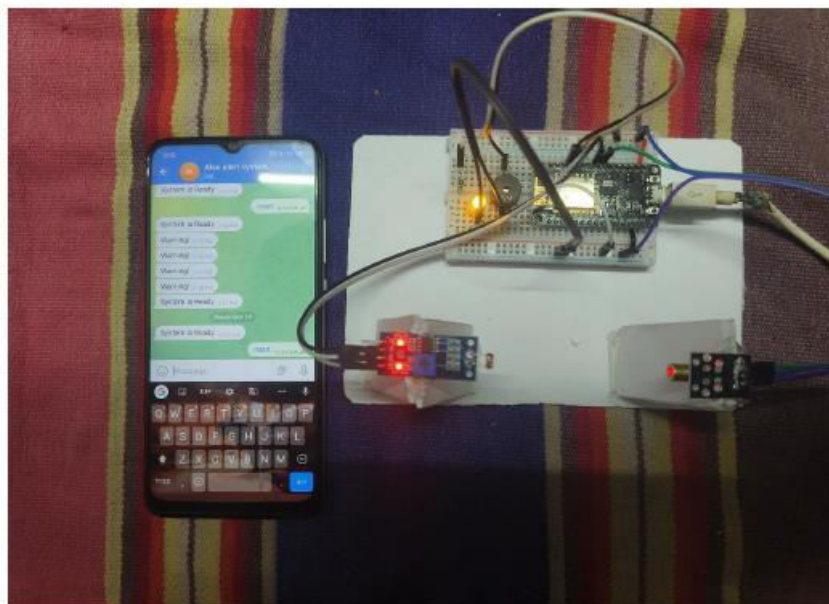


Fig 5.2 Message alert

## VI. CONCLUSION

Through accurate intrusion detection, the Laser Light Based Security System project has effectively shown how to improve security in a workable and efficient manner. To build a dependable security perimeter, the system's essential parts—the laser emitter, photodiode sensor, microcontroller, and alarm mechanism—were skillfully integrated. The thorough examination of the data demonstrated that the system operates with excellent precision and responsiveness, guaranteeing fast intruder detection and timely alarm activation



The resilience and adaptation of this security system to diverse environmental circumstances is one of its main advantages. The system's ability to function consistently under varying illumination and weather conditions demonstrated its suitability for both indoor and outdoor applications. By guaranteeing uninterrupted operation, the power management strategy—which uses both mains and backup battery power—further improved the system's reliability.

Test users greatly appreciated the system's low maintenance requirements and easy-to-use interface. Because it is so simple to use, even non-technical users can install and run the system, which is essential for practical deployment. Furthermore, the system's resilience, guaranteed by its waterproof and tamper-resistant housings, facilitates extended usage in demanding settings.

### REFERENCES

1. Steven F. Barrett and Daniel J. Pack's "Microcontroller Programming and Interfacing with Texas Instruments MSP430FR2433 and MSP430FR5994" Microcontroller programming is covered in this book, which is essential for creating the security system's control unit.
2. "Laser security system using photodiode sensors," D. W. Oesch, M. L. Clark, and E. D. Nelson, *Journal of Optical Engineering*, vol. 29, no. 3, pp. 290-298, 1990. The application of photodiode sensors in laser-based security systems is covered in this article.
3. "VL53L0X: World's smallest Time-of-Flight ranging and gesture detection sensor," STMicroelectronics datasheet. This paper offers information on sophisticated laser-ranging sensors.
4. "How to Build a Laser Security System," created by Instructables, is accessible at <https://www.instructables.com/How-to-Build-a-Laser-Security-System/>. A step-by-step explanation on how to construct a laser security system is provided in this tutorial.
5. "IEC 60825-1: Safety of laser products - Part 1: Equipment classification and requirements," published by the International Electrotechnical Commission (IEC), is accessible at:
6. The proceedings of SPIE, "Laser Radar Technology and Applications," which contain a number of articles about the use of laser technology in surveillance and security system
7. fundamental grasp of optoelectronics and photonics, which is necessary to comprehend the workings of lasers and photodiodes.
8. Programming microcontrollers is essential for creating the security system's control unit.
9. Fundamentals of laser remote sensing that apply to security systems that use lasers
10. Application of photodiode sensors in security systems with lasers.
11. Using laser technology in surveillance and security systems





INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details