WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Li-Fi Enabled Smart Door Lock System: A Secure and Innovative Approach to Access Control

Yogesh K. Kirange [a] , Dr. Shailaja A. Patil [b], Anjali S. Marathe [c], Rutuja S. Mali [d*], Dipali D. Potdar [e], Arati B. Patil [f], Bhumika P. Mali [g]

[a,b] Assistant Professor, Department of Electrical Engineering, R. C. Patel Institute of Technology, Shahada Road, Nimzari Naka, Shirpur and 425405
[c,d*,e,f,g] UG Students, Department of Electrical Engineering, R. C. Patel Institute of Technology, Shahada Road, Nimzari Naka, Shirpur and 425405

A B S T R A C T

Recent advancements in wireless communication and security technologies have spurred the development of innovative access control systems. Among various Arduino-based door lock projects, popular access methods include keypad entry, RFID cards, biometric devices, Wi-Fi, and Bluetooth. This paper presents a novel Li-Fi-based door lock system that enables access in an unconventional way - using a smartphone's flashlight. In this system, a password is first entered in a dedicated app, after which the information is transmitted via the smartphone flashlight, with no direct entry option on the lock itself. By combining Li-Fi technology with tamper detection, this approach enhances smart lock security by leveraging the speed and protection offered by visible light communication, while also providing real-time tampering alerts to ensure physical security. The proposed system offers a cost-effective, scalable, and secure alternative to traditional Wi-Fi or Bluetooth-based locking mechanisms, with potential applications in residential, commercial, and industrial access control. The expected outcome is a fully functional prototype that demonstrates the effectiveness of Li-Fi for secure communication and door control. This project aims to expand the practical understanding of wireless communication technologies and their application within security systems.

Keywords: Li-Fi-based door lock, Visible light communication (VLC), Smart access control system, Tamper detection, Wireless security technology.

1. Introduction

With the rapid advancements in wireless communication technologies, there is growing interest in exploring new methods for secure and efficient data transmission [1]. Currently, technologies such as Wi-Fi and Bluetooth rely on radio signals to transfer data [2]. However, there is a continuous push towards innovation and technical improvements that offer greater benefits and ease of use. This pursuit has led to the development of Li-Fi technology, which presents several advantages over traditional methods. Researchers continue to study Li-Fi to overcome its limitations and address gaps, aiming for widespread, large-scale implementation [3]. Li-Fi, introduced by Professor Harald Haas during a 2011 TED Global talk [4], is a wireless communication technology that uses light for data transmission, offering high-speed and secure communication capabilities [1]. Operating at speeds up to 100 times faster than Wi-Fi, Li-Fi leverages the visible light spectrum, providing a broad bandwidth range and enhanced data transmission potential [2].

2. Literature Survey

Most of the latest smart lock systems use RFID, Bluetooth, or Wi-Fi as their modes of connection, making them relatively convenient but vulnerable in terms of network vulnerabilities and the potential for remote hacking. One alternative, more recently prominent as a possible answer, is Li-Fi or Light Fidelity, focusing instead on using light waves instead of radio frequencies, providing a more secure communication, especially for it has limited range as well as requires light, which is mainly very convenient for situations where security comes to be an important point of concern because it limits the scope of interception because of the range. Li-Fi is a novel technology that uses visible light to transmit data and achieve a much higher speed in mobile and networked communication. For this, Li-Fi is known to be bidirectional because visible light can be used as an uplink whereas infrared can be used as downlink. Moreover, full duplex communication is also the feature through which data transfer can take place simultaneously in receiving and sending resulting in a faster user experience [4]. The invention will be replaced by Wi-Fi, which transmits at the range of 500Mbps. This technology uses all kind of light spectrum like white light, infrared. The Li-Fi is not limited to LED or Laser technologies or to a particular receiving technique. Li-Fi is a framework for all of these providing new capabilities to current and future services, applications and end users [6]. In this study, a system based on Li-Fi technology was designed and physically implemented. Experimental results obtained were a complete success. Unlike the case with other studies, this application opted to use a smartphone's flashlight as the source of Li-Fi transmission, which is a significant deviation from conventional approaches. While many other studies utilized the common conventional LED lights or Li-Fi dedicated transmitters, a novel approach to Li-Fi transmission was exploited using the most ubiquitous smartphone flashlight [3]. It is an open-source microcontroller board that integrates sets of digital and analogue I/O

pins which are capable of interfacing with various boards and circuits [4]. Various security systems have been implemented with different techniques and various performances. For instance, the system which based on the Zegbee technology used the processor of the personal computer. This limits the area in which one can work around the system to be about 10-20 meters. However, there is a chance to improve that by using a system which depends on the properties of the mobile phone which can be controlled by the Arduino technology. Arduino is just one combined system of software and hardware, involving the physical programmable circuit board with a corresponding software program that can be used, known as Integrate Development Environment (IDE), which is utilized by writing codes in a computer and then transmitted to the Arduino's physical board [7]. Tamper detection means a capacity of a device to detect the presence of any active attempt on compromising the device integrity or the data related with the device; the detection of the threat can enable the device to start proper defensive measures [8].Concurrently, the objective is towards business organizations, which depend on the analysis of large volumes of generated data to ensure and address the rise in the threat of attackers who mercilessly launch attacks and the challenges in protecting data confidentiality, integrity. By utilising accelerometers, vibration sensors, gyroscopes, and more, tampering detection enhances the resilience of the security solution and raises its effectiveness to a level that makes it a necessary element in applications like access control, IoT security, and data protection [8].

3.Methodology

Li-Fi provides enhanced security by limiting signal transmission to line-of-sight, reducing the risk of remote hacking. Additionally, tamper detection features—using sensors like an accelerometer and light-dependent resistor (LDR)—monitor the system for unauthorized physical manipulation. If tampering is detected, an alert is triggered via a buzzer. This design offers a robust solution for secure access control, suitable for environments where data privacy and physical security are critical. The system involves the components like Arduino nano, LDR, relay SPDT 12v, accelerometer, dc supply, resistors, RGB led module. The circuit is designed to create a reliable, secure and user friendly interface.

3.1 Selection of hardware

The System requires a carefully selected set of components to ensure reliable, secure operation. At its core, the Arduino Nano is chosen for its compact size and sufficient processing power, making it ideal for controlling lock mechanisms, processing Li-Fi data, and managing tamper detection features. For secure communication, a high-speed LED is used as the Li-Fi transmitter to send data through modulated light signals, while a photo detector or LDR sensor serves as the receiver, allowing the system to decode signals and control the lock based on verified access credentials. This light-based, line-of-sight communication reduces the risk of remote hacking, enhancing security. To address physical tampering, an accelerometer is incorporated to detect unauthorized movement, vibration, or tilt. This sensor activates an alert if any tampering attempts are detected, such as prying or forceful movement, providing an extra layer of security. The buzzer functions as an audible alarm, immediately alerting users or security personnel of tampering attempts. Finally, a stable power supply*is essential to ensure consistent functionality of all components. Together, this thoughtful component selection achieves a robust, secure, and efficient Li-Fi-based door lock system with real-time tamper detection capabilities, making it suitable for environments that prioritize data privacy and physical security.

3.2 System Architecture and Design

The circuit schematic of Li-fi door locking system uses Arduino with tampering detection incorporates many elements that assist in enhancing the access security control and tamper alert features. All components are connected to the digital and analog pins of Arduino making it compact and efficient suitable for secure applications. Ultimately, this project will develop a compact, affordable solution combining secured wireless links with proactive alerts when tampering occurs. This will allow for application in homes, businesses, or secure plant areas in which data privacy and physical security are of utmost importance. Ultimately, we believe this project will demonstrate the applicability of Li-Fi powered devices to enhance access control systems both in terms of their security and their functionality. The Data Collection Process includes repeatedly testing system functions and recording key performance metrics. First, determine Li-Fi signal response time by triggering a legitimate access attempt and measuring how quickly the lock mechanism responds. Second, simulate tampering by moving or shaking the system, and log tamper detection accuracy, noting any false positives or missed counts. Finally, assess signal reliability by testing Li-Fi communication in varying lighting and distance conditions, recording any interruptions and lags. Each test is repeated to take into account variability, and results are noted down for statistical analysis and future enhancement purposes. The new door locking system, using LiFi, employs visual light communication technology, also referred to as Visible Light Communication, VLC. This offers additional security along with some convenience in access control systems. The current project integrates novel modes of communication with the traditional locking mechanisms to enhance and secure the locking process.

Figure 1 indicates the block diagram of the suggested system of Li-Fi technology-based door lock system. Basically, this figures represents the research work flow of the system. It shows the communication happening in between the components.

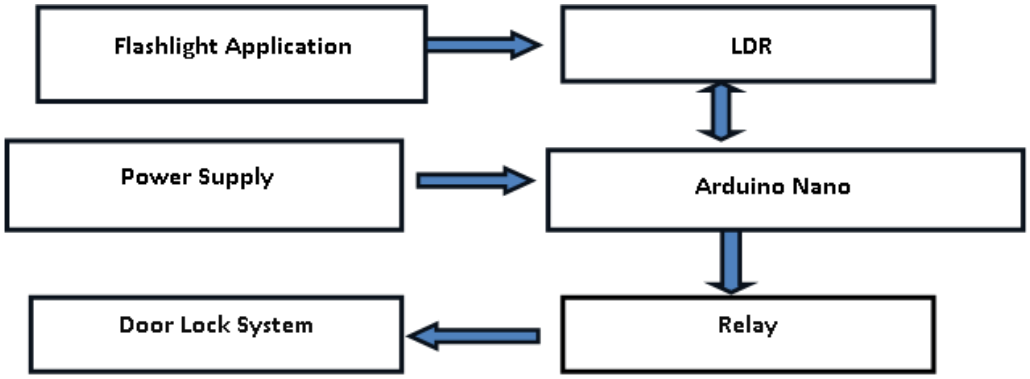

Fig. 1 - Block diagram of the proposed system of Li-Fi technology based door lock system

4. Implementation and Experimental Setup

This Li-Fi-based door lock system provide a secure and innovative access method by using visible light communication through a smartphone flashlight. The hardware assembly includes an LDR (light-dependent resistor) as a light signal detector, connected to an Arduino Nano, which processes these signals to control the door lock. A MOSFET switch and relay enable the locking and unlocking mechanism, while LEDs indicate the door's lock status, protected by resistors to prevent overload. Additionally, a tampering detection sensor continuously monitors for unauthorized access attempts, enhancing security.

4.1 Hardware Assembly

In First Stage light signal changes are detected via the use of an LDR which is an electronic component that acts as a photo detector in this case as a receiver of the Li-Fi signal. Whenever the LDR is exposed to a source of light which can be a Li-Fi signal, the light intensity variation is picked by the LDR and acknowledged to be sent as an analog signal to the Arduino going to the serial monitor. The next stage is Signal Processing. In this stage, Arduino Nano is utilized to gather the input from the LDR. The first step is reaching LDR in search of the Li-Fi signal light source. However, not all of them meet every requirement; that is when the Arduino regards it as an order to either lock or unlock the door.

The third stage is Lock/Unlock Action. When the LDR sends its signal, followed by the number of seconds in between the signals, the Arduino functions via a MOSFET (IRF730) arm switch. It corresponds to the door's resistor which works through the relay, allowing a moving mechanism. To make matters clear, if the need arises to unlock the door, such a situation is achieved when the relay feels an intensity of the light which triggers energy flow through the Arduino to the door lock allowing it to unlock. When locking the door however, it is needed to cut off energy to the lock cell and activate the relay which is the opposite of the lock signal. There are two types of possible door/latch positions and this is marked by LEDs as well. The defender LED will turn green for an arbitrary door opening, while the same LED will light red which means the door is tightly shut. To protect the LEDs from getting burnt out, 470 Ohm resistors are incorporated in the design as a current limiting device with the LEDs.

The tampering detection sensor (could be a vibration sensor, tilt sensor, or additional LDR placed in a specific spot) operates over time looking for unauthorized intervention or tampering. If abnormal conditions have been caused and measured by the tampering sensor, a signal shall be

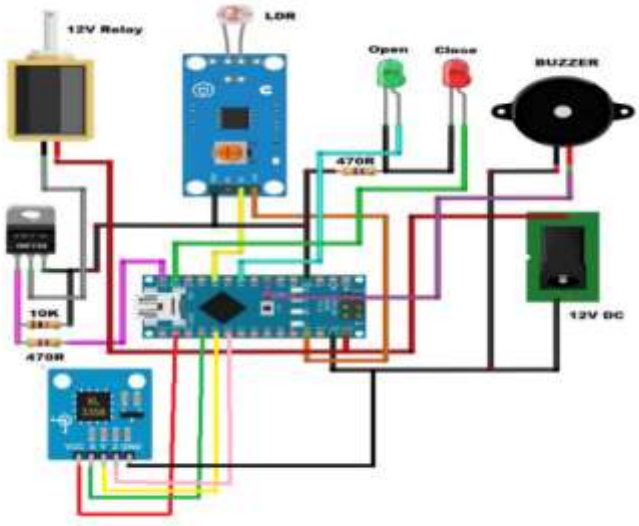

Fig. 2 - Circuit diagram of the proposed system of Li-Fi technology based door lock system

4.2 Software Touch

The software touch, involves an algorithm programmed on the Arduino Nano to manage the door's lock function based on received light patterns. The system initializes by defining key components such as the solenoid for locking, LEDs for status indication, and the buzzer for audio alerts. The Arduino continually monitors the LDR for specific light patterns, unlocking the door when the correct sequence is detected and resetting otherwise. A flowchart outlines the full system operation, ensuring both functionality and security through pattern recognition and tamper alerts.

4.2.1 Algorithm Flow

The algorithm starts by defining and setting up pins for essential components, including the solenoid, LDR, LEDs, and buzzer. In the main loop, the Arduino continuously monitors the LDR for specific light patterns. When the correct unlock pattern (such as "0001") is detected, it activates the solenoid to unlock the door for a brief period, then relocks it automatically.

Step 1 Define and Setup pins: First define and setup the given pins such as Solenoid (that controls the lock mechanism), LDR (that detects the light signals), Buzzers, Green colour LED which shows the unlocked state, Red colour LED which indicates the locked state Start by opening the serial monitor Click the Red LED to ON to shows that the door is locked in the normal position.

Step 2 Function to Open Door: Command the Solenoid to unlock the lock mechanism. Then turn the Green LED and Buzzer ON. Allow the door to be unlocked for 3s. Then after 3s switch off the solenoid so that it relocks the door. Turn off the green LED and buster and switch on the red LED.

Step 3 Main Loop: Continuously check LDR sensor in order to detect any light signals, if light is detected then: Start the light pattern and monitor the values in duration If the pattern '0001' (the signal for unlocking) is received then call the 'Open-door ()' function so as to unlock the door. If there is no specific pattern, the longest duration is automatically reset and the monitoring ceases Obtain Pattern-011. Then Check and Obtain Correct Pattern, in search for obtaining the correct light signal pattern which will trigger the unlock.

4.2.2 Flowchart:

The flowchart represents the whole process of the working of the li-fi door lock system using Arduino with tampering detection and alerts. The flowchart consist of all the main highlighted steps of the system.

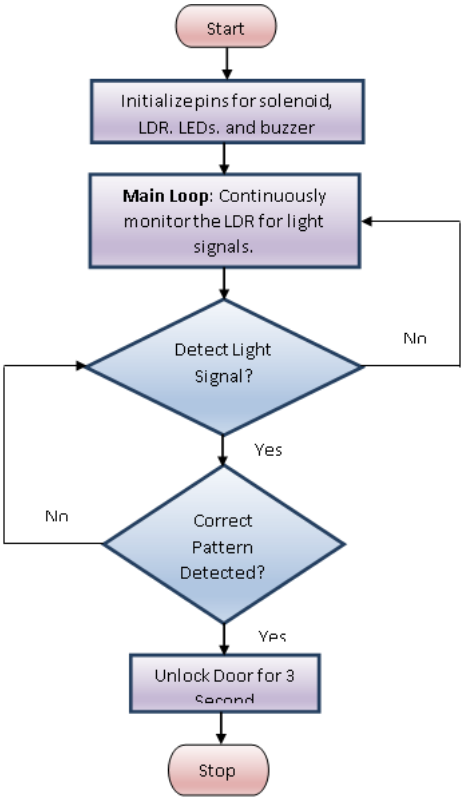

Fig. 2 – Flowchart of li-fi door lock System

5. Tasks and Solutions:

i. Signal Interference and Noise Control

ii. Limited Range and Line-of-Sight Requirement

iii. Power Consumption and Reliability of the Device

iv. Environmental Sensitivity of LDR

v. Hardware Limitations of Arduino

vi. Audible Alarm and False Alerts

vii. Physical Security of Components to Protect from temperature or moister.

viii. Latency in Signal Processing

ix. Complexity in Signal Pattern Recognition.

Advantages of a Li-Fi Door Lock System

1. Limited Range: Since Li-Fi signals cannot go through walls, it is more secure by default. It is also a limitation that implies that eavesdroppers from outside the base area find it difficult to intercept the signal.

2. Directional Communication: Li-Fi is capable of being directed through light focused on a particular beam. This focused method minimizes the chances of interception since, only those devices that are in the beam, can access the data.

3. Higher Data Rate and Capacity: Li-Fi is faster than Wi-Fi, hence can be a more efficient means of communication. Such a capability can accommodate higher encryption security systems that necessitate larger bandwidth.

4. Decreased Interference and Congestion: Li-Fi works on a different spectrum from that of Wi-Fi hence interference is significantly low enabling clearer communication channels. This reduction increases security and integrity of the data.

6. Increased Privacy: Higher speeds and bandwidth of Li-Fi allow users to take further steps such as data encoding and applying more than one security layers. This guarantees more security that even when data is captured within the given space, it remains encrypted.

Limitations of a Li-Fi Door Lock System

1. Environmental Susceptibility: Other luminous sources, including sunlight or fluorescent light, may interfere with the transmission of the signal, hence limiting the effectiveness of Li-Fi systems. Such susceptibility may result in erratic performance in environments with fluctuating lighting conditions. Also, for outdoor use, environmental conditions like rain, fog, or snow, will impede the light signals and thus affect the performance of the system. This renders Li-Fi somewhat inappropriate for outside door locks unless different protective measures are put in place.

2. Challenges in Scaling: The deployment of a Li-Fi door lock may be dependent on changes to the existing infrastructure Li-Fi requires certain lighting systems (egg: LED) to be installed in order to facilitate data transmission. This does mean higher upfront costs and complexity for the big circuits.

Future Enhancements

1. Mobile Integration:

i. Development of Mobile Apps: Devise a specific application for the purpose of controlling the access of users remotely, providing them notifications and managing them.

ii. Bluetooth Backup: Blue toothing coexists with LiFi where there is no reach of connectivity for LiFi ensuring connectivity is never the problem.

iii. User Authentication: The application will utilize biometric features such as fingerprints and facial recognition for ensuring security on the application.

2. Enhanced Tamper Detection:

i. Sophisticated Sensors: Employ accelerometers, gyroscopes and barometric pressure to detect and report instances of tampering or forced entry.

ii. Instant Alerts: Create a mechanism that alerts the users and the relevant authorities whenever tampering is detected.

iii. Geofencing: Modify lock access services so that an alert will be triggered whenever the lock is accessed from an unknown location.

6. Result and Performance Analysis

1. Testing Procedures: Check if the door can be locked or unlocked via the paired device using Li-Fi transmission (smartphone). The customer should check whether the device works correctly at different distances from the light source. Check the system's responsiveness in unlocking and locking a door after the command is received by the system.

i. Receiver not aligned with the Transmitter: Move or tilt the Li-Fi receiver or try any other simple manipulation to the light source. If the communication is interrupted, then the system should flag it as a tampering alert or that there has been an attempt at interfering from an unauthorized device.

ii. Unilateral Forcing of Manipulation to the Locking Mechanism: An attempt to insert oneself onto the locking machine, hence attempting to forcibly manipulate the real lock. This should not be allowed because it violates the system; mechanisms should then be in place to detect any aberrant mechanical behavior, which would involve, for instance rapid determination of an opposed state between the concerned lock's current position and its target position triggering of an alarm or alert from the system to the end user.

iii. Signal Jamming: Assume an active attacker that tries jamming the communication link to get into the lock through magic by creating a false signal. Signals that are not authorized such as those issues by the communication spoofing, should be turned away; we should not allow access to such signals.

iv. Unauthorized Device Connection: This tests the strength of the system in identifying, hence blocking access by any unauthorized devices.

7. Data Collection and Analysis:

The system asks the user to transmit the key through a mobile application, which uses the flash light of the smartphone to establish secure transmission of the key. The Arduino board makes use of LDR module to receive the key from the smartphone. Arduino board verifies the received key against prerecorded key set during the setup. If the key matches then the system will unlock either the door or the mechanism of electronic lock. So, the system stores its keys in a secure position so that no unauthorized can easily access them. A message is sent for every opened door and informs the owner about it. This helps in tracking and limiting and can take swift action in cases of suspicious activity. It is achieved through a dedicated mobile application. The entire efficacy of Li-Fi based wireless locking system would rely upon the extent of security measure and reliability of hardware as well as software components. Testing and Validation : It needs to be strictly tested and validated to validate its efficiency and robustness [1]

Performance Evaluation: It relates to the millisecond precision that is required for unlocking a door with a light flash. It does not recognize a pattern of light, but rather specific flashing lights in a precise manner down to milliseconds. In this respect, the sequence of the light flashes in combination with the millisecond time intervals makes the light flash highly impossible to be imitated without the proper sequence and timing. That's why it's a safe feature [2]. A Li-Fi door lock system generally operates with a success rate of more than 95% if the conditions are ideal, including direct line of sight and stable lighting. However, this may be degraded by some form of blockage, poor installation, or uneven lighting. Proper setup, when combined with proper interaction between a user and a Li-Fi door lock system, retains its high reliability. The sensitivity of tamper detection in a Li-Fi door lock system, therefore, is the ability to recognize attempts at access/interference. Some of the considerations include; Signal Monitoring: Always monitor the Li-Fi signals for anomalies. Threshold levels: Setting the sensitivities that will separate normal activity from suspicious activity. Mechanisms for quick detection and notification to minimize security risks. Environmental Adaptation: The ability to adapt to a changing light source or physical obstruction.

References

1. *Dr Shilpa KC, Kshama Mohammed Anas, Pradeep Hegde, Shivanand Chabbi "LI-FI BASED DOOR LOCK SYSTEM "International journal of creative research thoughts Volume 12, Issue 7 July 2024 | ISSN: 2320-2882*
2. *Raza, Asjad, Haider Mehdi, Zakir Hussain, Muhammad Arif, and Shabbir Hussain. "Visible light communication (Li-Fi technology)." In 2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), pp. 1-6. IEEE, 2021.*
3. *Hakan Aydin, Gülsüm Zeynep Gürkaş Aydın, Muhammed Ali Aydın." The potential of light fidelity in smart home automation".Bulletin of Electrical Engineering and Informatics. Vol 13, No 5 October 2024 pp.3135-3166.*
4. *Roy, Stuti, Shalini Siddhi, and Shweta Pandit. "Li-Fi based Home Navigation." (2023).*
5. *Mongwewarona, Winnie, Sajid M. Sheikh, and Benjamin C. Molefhi. "Survey on Li-Fi communication networks and deployment." African J Eng Res 8, no. 1 (2020): 1-9.*
6. *Bhavya, R., and M. R. Lokesh. "A Survey on Li-Fi Technology." An International Journal of Engineering & Technology 3, no. 1 (2016).*
7. *Albak, Lubab H., Arwa Hamed, and Raid Rafi Omar Al-Nima. "Design security system based on arduino." In TEST Engineering & Management, vol. 82, pp. 3341-3346. The Mattingley Publishing Co., Inc., 2020.*
8. *Caddy , T(Zoll) Tamper Detection . Springer ,Boston.*
9. *Shrivastava, Rajesh Kumar, Sanket Mishra, V. E. Archana, and Chittaranjan Hota. "Preventing data tampering in IoT networks." In 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6. IEEE, 2019.*
10. *Wadhwani, Siddharth, Uday Singh, Prakarsh Singh, and Shraddha Dwivedi. "Smart home automation and security system using Arduino and IOT." International Research Journal of Engineering and Technology (IRJET) 5, no. 2 (2018): 1357-1359.*

11. *Mocrii, Dragos, Yuxiang Chen, and Petr Musilek. "IoT-based smart homes: A review of system architecture, software, communications, privacy and security." Internet of Things 1 (2018): 81-98.*

12. *Kamweru Paul Kuria , Owino Ochieng Robinson , Mutinda Mutava Gabriel "Monitoring Temperature and Humidity using Arduino Nano and Module-DHT11 Sensor with Real Time DS3231 Data Logger and LCD Display". Volume 09, Issue 12 (December 2020).*

13. *By Richard Elliot "Arduino & Li-Fi: A New Era of Secure Door Lock Technology"(News) 10th January 2024*