Revista Colombiana de Computación
Vol. 26, No.2. July – December 2025, pp. 44-52
e-ISSN: 2539-2115, https://doi.org/10.29375/25392115.5525
Selected paper previously presented at the Latin America High Performance Computing Conference (CARLA 2023), an event held in Cartagena de Indias, Colombia, September 18-22, 2023.

REVISTA COLOMBIANA DE COMPUTACIÓN

Visible light communication using the flash of smartphone cameras for access control application

Comunicación por luz visible mediante el flash de las cámaras de los teléfonos inteligentes para aplicaciones de control de acceso

Fabio Vega[1], Yuri Cáceres[2], Astrid Ramos[2]

[1] Grupo de Optoelectrónica y Procesamiento de Señales – OPSE, Universidad Popular del Cesar, Valledupar, Colombia
[2] Universidad Popular del Cesar, Valledupar, Colombia

fabiovega@unicesar.edu.co, yalejandracaceres@unicesar.edu.co, acarolinaramos@unicesar.edu.co

(Received: 20 October 2025; accepted: 20 December 2025, published online: 31 December 2025)

Abstract. Computer security is delving into new fields, and short-distance communication by light is one of them due to its advantages over traditional means that use radio frequency. A few advantages are not reading from a close distance, operating only when the user requires it, and short-range communication that is ideal for security applications and access control. This paper presents the development of an access control prototype with smartphones using light communication. Diverse sensors and flash response speeds were evaluated with physical tests in several cell phones; the same minimum response frequency of 60 Hz was obtained for different devices, and depending on the device, a maximum response of 140 Hz was obtained. Using this information, an app was developed on the Flutter platform to send data frames implementing protocols like infrared, where the signal is encoded with the flash camera's pulse-width modulation. Using an embedded system known as the ESP8266 WeMos D1 Mini, data bytes could be sent, received, synchronized, and verified from the cell phone at a frequency of 30 Hz modulation per bit.

Keywords: optical communication, mobile phones, data security, access control.

Resumen. La seguridad informática está incursionando en nuevos campos, y la comunicación de corta distancia mediante luz es uno de ellos, debido a sus ventajas frente a los medios tradicionales que utilizan radiofrecuencia. Algunas de estas ventajas son que no puede leerse a distancia, que opera solo cuando el usuario lo requiere y que su corto alcance la hace ideal para aplicaciones de seguridad y control de acceso. Este artículo presenta el desarrollo de un prototipo de control de acceso con teléfonos inteligentes mediante comunicación por luz. Se evaluaron diversos sensores y la velocidad de respuesta del *flash* mediante pruebas físicas en varios teléfonos celulares. En todos los dispositivos se obtuvo la misma frecuencia mínima de respuesta, 60 Hz, y una respuesta máxima de hasta 140 Hz, según el dispositivo. Con esta información se desarrolló una aplicación en la plataforma *Flutter* que envía tramas de datos implementando protocolos similares a los infrarrojos, en los que la señal se codifica mediante la modulación por ancho de pulso del flash de la cámara. Con un sistema embebido, el ESP8266 WeMos D1 Mini, fue posible enviar, recibir, sincronizar y verificar bytes de datos desde el teléfono celular con una modulación de 30 Hz por bit.

Palabras clave: comunicación óptica, teléfonos móviles, seguridad de los datos, control de acceso.

©2025 Universidad Autónoma de Bucaramanga- UNAB. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA 4.0) license (https://creativecommons.org/licenses/by-nc-sa/4.0/)

1 Introduction

Technology continues to advance in the security field and in ways to circumvent it. A clear example is radio frequency identification, in which there are gadgets on the market that allow you to copy, clone, and reproduce the codes that come factory-programmed for less than $50 USD. Optical wireless communication or Light Fidelity – Li-Fi has gained increasing attention (Chow et al., 2015; Hu et al., 2019; Huang et al., 2016), owing to its contribution to security and speed in sending data over short distances. Visible Light Communication – VLC has had its most significant contribution in optical fibers, where applications of around 44.2 Terabits of data per second (Shaaban et al., 2021) have been developed, which drive internet communication worldwide. It has also had different applications, such as indoor positioning, intelligent vehicular transportation, satellite-to-satellite and device-to-device communication, LASER communication, VLC integrated with power line communication, high-speed laser diodes, indoor communication, access control, and multicolor systems (Amanor et al., 2018; Boubezari, 2018; Corcoran et al., 2020; Duque et al., 2018; Khan, 2017; Liu & Ma, 2021; Luo et al., 2017; Martínez-Ciro et al., 2019; Martínez-Ciro et al., 2020; Shaaban et al., 2021; Tanaka et al., 2003).

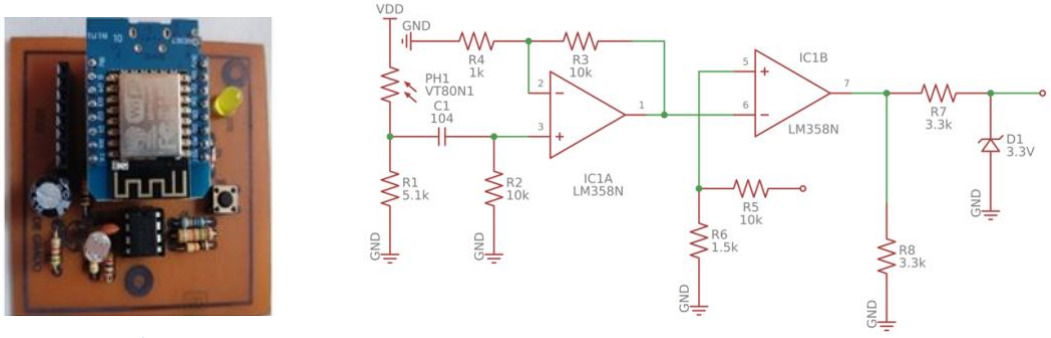
In the field of smartphones, studies have been conducted, such as Boubezari (2018), where a VLC communication was developed using the camera and flash considered in a thesis project; the study is insightful, but there are widespread technologies, such as Bluetooth, Quick Response – QR codes, and Wi-Fi to send data between mobile devices, and they do not apply the same to home automation.

In this study, we intend to develop access control systems using smartphone flash as an opening key linked to Internet of Things – IoT technology. In Martínez-Ciro et al. (2020), a Color Shift Keying – CSK system was developed using an embedded Red-Green-Blue – RGB color sensor for transmission; the system was implemented with a single low-cost Light Dependent Resistor – LDR sensor. Although data encryption is commonly considered a standard requirement in security-oriented systems, this work focuses specifically on the first stage of the process, namely the reliable transmission and reception of information. Data encryption strategies are therefore beyond the scope of this study and will be addressed in future works.

2 Materials and methods

2.1 Signal acquisition system design

Different sensors, such as phototransistors, Positive-Intrinsic-Negative – PIN diodes, and LDRs, were tested on a breadboard. The phototransistors did not work because their operating spectrum is in the infrared, and the camera flash is in the visible spectrum. The PIN diode was oversaturated with visible light; thus, it was always active. The LDR allowed the diode to obtain the best results in sensing. These sensors were selected due to their availability in the local Colombian market. Their design is shown in Figure 1.



a) b)

Figure 1. a) Implemented circuit. b) Light sensor design

For sensor signal conditioning, a voltage divider R1 and an Alternating Current – AC signal coupling capacitor C1 were used, which amplifies the time-varying signal with a resistor to ground on the positive

of the Operational Amplifier – OPAM, R2, to have a better ground reference. Next, a non-inverting amplification stage with a gain of 11 was entered; the general equation of the non-inverting amplifier is observed in Equation (1), and the calculation of the gain is shown in Equation (2).

$$V_0 = V_i\left(\frac{R_f}{R_g} + 1\right) = V_i\left(\frac{R_3}{R_4} + 1\right). \quad (1)$$

Replacing values from Figure 1.

$$V_0 = V_i\left(\frac{10\text{k}\Omega}{1\text{k}\Omega} + 1\right) = 11V_i. \quad (2)$$

The next step is to use a voltage comparator to generate the digital signal for the ESP WeMos D1 mini microcontroller system, which is placed as a reference for a voltage divider between R5 and R6, whose reference voltage value with Vdd = 5V is 0.65V, as calculated below:

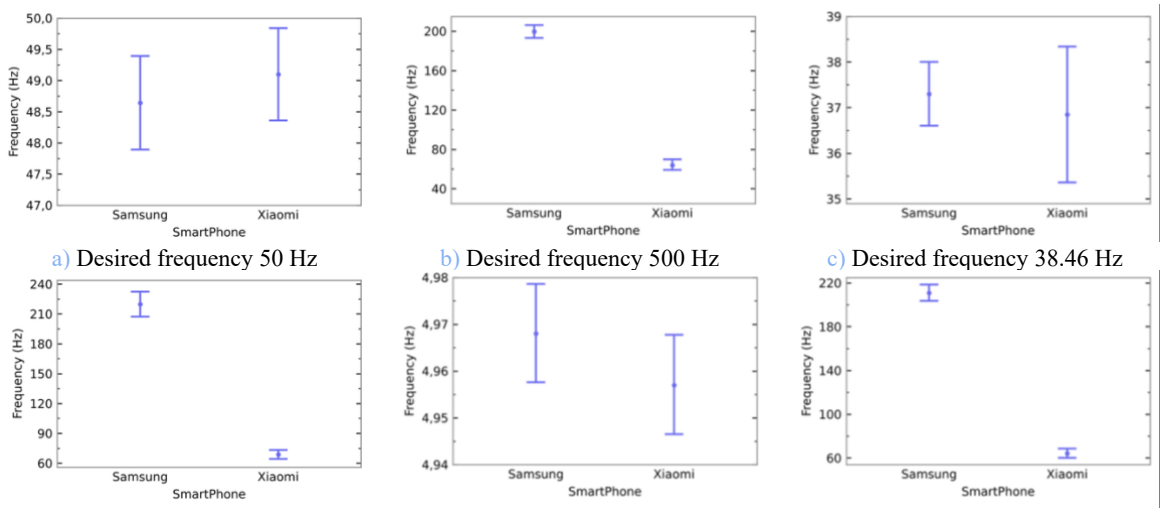
$$V_{ref} = V_{dd}\frac{R_6}{R_6+R_5} = 5\,V \cdot \frac{1.5\,k\Omega}{1.5\,k\Omega+10\,k\Omega} = 0.65\,V. \quad (3)$$

This comparison voltage, along with the gain of the OPAM in the previous stage, determined the maximum sensing distance of the circuit; for this reason, it was experimentally adjusted such that it works at a maximum distance between 4cm to 20cm from the Printed Circuit Board – PCB, avoiding interference from external light and the main voltage supply frequency. Finally, the output of the OPAM, a 3.3V Zener diode resistor, was added to condition the signal to the digital voltage supported by the ESP8266 Microcontroller Unit – MCU.

2.2 Response test with different smartphones

An app was designed to control the flash of the camera hardware, which was developed in Flutter, for which a test was conducted with various Android cell phones – because they are affordable and do not have iOS technology, which requires a PC with a Mac OS for its development – to determine the maximum response speed of the camera flash according to the brand of the cell phone. For each device, ten samples were implemented and measured at each operating frequency. This test was conducted because the circuit with the LDR has a response speed of around 1 kHz, according to results obtained from the web. The test devices were a Xiaomi 9S, 128 GB Random Access Memory – RAM, Android 11, and a Samsung J7, 16GB Android 8.1. Therefore, the Analysis of Variance – ANOVA was used to determine significant differences using the Least Significant Difference – LSD in a multiple range test. Fisher's LSD test is a multiple comparison test (Montgomery, 2017). The test helps compare the means of the t levels of a factor after having rejected the null hypothesis of equality of means employing the ANOVA technique. The frequencies generated vs. the measurements are observed in Figure 2.

Figure 2.a), 2.c), and 2.e) show an overlap of the blue bars, which indicates that the desired and measured frequencies are not significantly different. This means that the two cell phones behave similarly to generate a frequency of 50 Hz. Figure 2.b) shows no overlap of the blue bars, which indicates that the frequencies are significantly different statistically. This means that the two cell phones behave differently; one is faster than the other. Furthermore, the Xiaomi cell phone achieved a maximum output frequency of 60 Hz out of the expected 500 Hz, and the Samsung cell phone achieved about 140 Hz out of 500 Hz. This implies that the latter will not be able to generate square signals, as the camera's flash is above 140 Hz. Figure 2.d) and 2.f) show the difference between the Samsung and Xiaomi cell phones; they cannot generate more than 500 Hz. A maximum of 215 Hz is achieved for the Samsung, and 60 Hz for the Xiaomi.



a) Desired frequency 50 Hz b) Desired frequency 500 Hz c) Desired frequency 38.46 Hz

d) Desired frequency 1 kHz e) Desired frequency 5 Hz f) Desired frequency 5 kHz

Figure 2. Desired frequencies and measurements on the sensor with Samsung and Xiaomi smartphones.

2.3 Microcontroller firmware development

The high and low times, in milliseconds, of the signal generated on pin 7 of the OPAM was measured employing code in the MCU. When it receives light from the flash, the pin goes to logical zero, and high when it does not receive light on the sensor from the camera flash. The data measured with measurement intervals of 1ms are summarized in Table 1.

When the circuit detects light, it generates a low voltage of approximately 6ms due to the capacitor C1, which only allows the AC signal to pass, and the signal stabilizes after a few milliseconds. Thus, the frequency of sending light frames was set to 30 Hz, approximately 33.33ms, since some cell phones do not support more than 30 Hz, while high-end cell phones reach up to 144 Hz.

Table 1. Data measured with intervals of 1ms

Time generated by App	Low Time – TB ms	High Time – TA ms	Period = TB + TA ms	Frequency
TB = 10 ms	6	16	26	43.46 Hz
TA = 10 ms				
TB = 1 ms	3	3	6	166.6 Hz
TA = 1 ms				
TB = 500 us	4	3	7	142.87 Hz
TA = 500 us				
TB = 10 us	3	4	7	142.87 Hz
TA = 10 us				
TB = 13 ms	6	23	29	34.48 Hz
TA = 13 ms				
TB = 100 ms	6	190	196	5.1 Hz
TA = 100 ms				

2.4 Design of sending data by the flash of the camera

Based on the preliminary tests, the following protocol, modeled on the frame structure used in infrared remote-control communication, was adopted. Each frame consists of a start bit followed by two bytes, each transmitted most significant bit – MSB first. Every bit begins with the flash turned on for 10 ms, and the bit is identified by the duration of the off period that follows, pulse-distance encoding: the start bit is followed by 30 ms off, a logical 1 by 25 ms off, and a logical 0 by 20 ms off, as shown in Figure 3.

The start bit, whose off period is longer than that of any data bit, allows the system to identify the beginning of each frame. It is followed by the first byte and then the second byte, both starting with the MSB, after which the frame is transmitted again. Since the user may place the phone on the sensor at any moment, possibly in the middle of a frame, the frame is repeated continuously for approximately 3 s. Each frame lasts between 520 and 600 ms, so this interval contains about five complete frames and ensures that at least one is received correctly without requiring precise timing from the user.

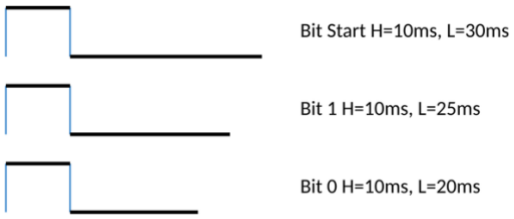


Figure 3. Graphical representation: Bit Start, logical 1, and logical 0.

In commercial communication systems, byte transmission commonly consists of synchronization bytes, payload data, and trailing Cyclic Redundancy Check – CRC bytes for error detection. Furthermore, an encryption layer should be applied to the data payload to improve overall system security.

2.5 Obtaining Detection Thresholds

A program was developed to count at intervals of 250 us. The number of pulses that correspond to a logical one or zero for the following data was obtained experimentally using the variable items, as summarized in Table 2.

Table 2. Pulse count at 250 µsec intervals for different high and low states

H = 10 ms	L = 20 ms	H= 10 ms	L = 25 ms	H = 10 ms	L =30 ms
26	100	26	112	26	141
26	96	25	121	25	138
26	100	25	120	26	139

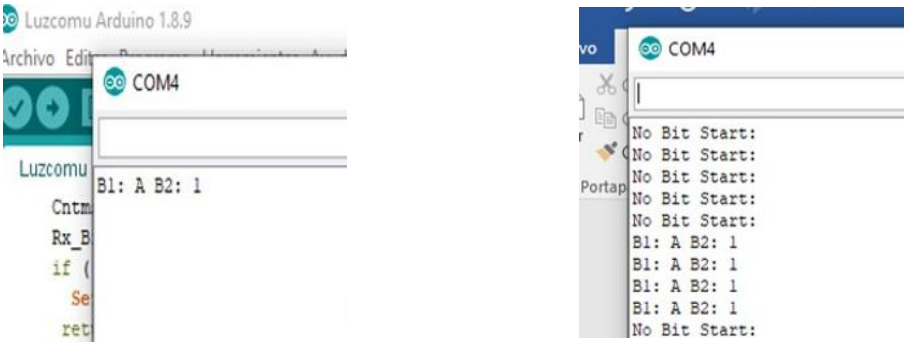
The threshold values listed in Table 3 were obtained.

Table 3. Thresholds for start bit, logical 1, and logical 0 detection.

Detected bit	Constant	Threshold
Start bit	$BitStart = 130$ $BitStartMax = 205$	$BitStart < Cntms$ $< BitStartMax$
Logical 1	$Bit1 = 125$	$Cntms \geq Bit0$
Logical 0	$Bit0 = 111025$	$Cntms \leq Bit0$

3 Data sending tests

Two bytes are sent from the app, and the received data are sent by a universal asynchronous receiver-transmitter to display them in the Arduino Integrated Development Environment – IDE serial monitor window; then, the frames are sent without being initially on the sensor, and whether they were synchronized was observed since the data was out of phase. The following data were received.



a) b)

Figure 4. Data test. a) Received data starting transmission directly to the sensor, the distance between 4 and 15cm. b) Received data, not started sending on the sensor to test synchronization, the distance between 4 and 15 cm.

4 Results and discussion

As illustrated in Figure 4.a), the circuit is synchronized with the camera signal, although it is not initially on the light sensor. The developed firmware turns on a Light Emitting Diode – LED after receiving the appropriate byte frame, indicating the correct signal decoding and demonstrating that our prototype complied with what was specified in the design. The field tests showed no interference from external light and the best results at a distance between 5 and 15 cm of direct exposure on the circuit sensor and a maximum distance of 35 cm. The sensing distance can be varied by adjusting the OPAM gain Eq. (1) and decreasing the comparison voltage Eq. (3). Among the several advantages of the developed system, some include short-distance communication by visible light, the easy generation of frame-width-encoded light data, as shown in Figure 3, the non-existence of a device that decodes these over long distances, the bytes of data sent can be encrypted to add an extra layer to communication, the use of ESP WeMos allows Wi-Fi connectivity, and the integration of the system to the IoT (Ceja y otros, 2017; Kodali & Mahesh, 2016; Madakam et al., 2015; Schwartz, 2016).

Although this work focuses on the first stage of the system, namely the reliable transmission and reception of data through VLC, the processing unit can incorporate standard lightweight encryption mechanisms commonly adopted in IoT-based security systems. In this context, symmetric cryptographic schemes such as Advanced Encryption Standard – AES-128 and stream ciphers like ChaCha20 are widely reported in the literature due to their low computational overhead, reduced latency, and suitability for short data payloads in embedded platforms (Daemen & Rijmen, 2002; Nir & Langley, 2018). These encryption strategies, although not implemented in the present study, can be seamlessly integrated at the processing stage to enhance data confidentiality and integrity.

For the implementation of an access control system, the receiving ESP module should be connected to a remote server via Wi-Fi, preferably using the Transmission Control Protocol – TCP, thereby avoiding traditional wired infrastructure. The optical data received through the VLC channel is transmitted to the server, where authentication procedures are executed. Upon successful validation, the server sends a control command back to the ESP module to authorize and actuate the opening of the access point, such as a door or gate.

The server-side data and access credentials can be managed and updated through a master application connected to the server. This application must be administered exclusively by the system owners or authorized personnel, allowing dynamic modification of access permissions without physical intervention in the hardware. Typical application scenarios of the proposed architecture include access control to hotel

rooms, restricted laboratories within a university, secure entry to corporate offices, and controlled access to industrial or research facilities.

The low communication speeds observed in this work are mainly attributed to the fact that the system operates at the smartphone application layer. Within the Open Systems Interconnection – OSI reference model (Tanenbaum & Wetherall, 2011), this layer is abstracted from the hardware layer and interacts with it through the operating system and device-specific Application Programming Interfaces – APIs. This abstraction limits precise timing control and direct hardware access, thereby restricting the achievable data transfer rates. The communication speed can be easily increased up to the order of kHz, but a higher speed is required between the application layer and the hardware of the cell phones, which depends on the manufacturers. You can use the infrared LED that some cell phone brands have, such as Xiaomi, which would allow the use of different infrared protocols directly from a user interface; although this has been on the market for several years, very few cell phone distributors include an infrared LED. Therefore, the development of this work does not require specific hardware because most current smartphones have a flash. Implementing this work in devices with the iOS operating system is easy because the Flutter IDE allows easy compilation for this platform.

5 Conclusions

A low-cost visible light-controlled access control system can be developed and implemented for approximately $5 USD, with commercial elements connected to IoT technology through the ESP WeMos D1 microcontroller system. Its main advantages are the simple configuration of the sensing distance, the easy generation of light frames in the camera flash, and the migration to other mobile devices such as the iPhone because the app was developed in Flutter.

Using the camera's flash as a means of communication by light allows for the development of different applications such as access control and light- encoded keys where data security is crucial in communication.

Acknowledgments

We declare that we have no significant competing interests, including financial or non-financial, professional, or personal interests interfering with the full and objective presentation of the work described in this manuscript.

ORCID ID

Fabio Vega https://orcid.org/0000-0001-9982-0823
Yuri Cáceres https://orcid.org/0009-0005-8190-8380
Astrid Ramos https://orcid.org/0009-0003-6273-4069

References

Amanor, D. N., Edmonson, W. W., & Afghah, F. (2018). Intersatellite communication system based on visible light. *IEEE Transactions on Aerospace and Electronic Systems, 54*(6), 2888-2899. https://doi.org/10.1109/TAES.2018.2832938

Boubezari, R. (2018). *Smartphone to smartphone visible light communications.* Thesis, University of Northumbria at Newcastle, Newcastle upon Tyne. https://nrl.northumbria.ac.uk/id/eprint/36194

Ceja, J., Renteria, R., Ruelas, R., & Ochoa, G. (2017). Módulo ESP8266 y sus aplicaciones en el internet de las cosas. *Revista de Ingeniería Eléctrica, 1*(2), 24-36. https://nafcom.es/fotos_pdt/108.MD0696/111.MD0696-COSILLAS.pdf

Chow, C.-W., Chen, C.-Y., & Chen, S.-H. (2015). Visible light communication using mobile-phone camera with data rate higher than frame rate. *Optics Express, 23*(20), 26080-26085. https://doi.org/10.1364/OE.23.026080

Corcoran, B., Tan, M., Xu, X., Boes, A., Wu, J., Nguyen, T. G., Chu, S. T., Little, B. E., Morandotti, R., Mitchell, A., & Moss, D. J. (2020). Ultra-dense optical data transmission over standard fibre with a single chip source. *Nature Communications, 11*(1), 2568. https://doi.org/10.1038/s41467-020-16265-x

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES – The Advanced Encryption Standard.* Springer. https://doi.org/10.1007/978-3-662-04722-4

Duque, A., Stanica, R., Rivano, H., & Desportes, A. (2018). Decoding methods in LED-to-smartphone bidirectional communication for the IoT. *2018 Global LIFI Congress (GLC)* (pp. 1-6). IEEE. https://doi.org/10.23919/GLC.2018.8319118

Hu, P., Pathak, P. H., Zhang, H., Yang, Z., & Mohapatra, P. (2019). High speed LED-to-camera communication using color shift keying with flicker mitigation. *IEEE Transactions on Mobile Computing, 19*(7), 1603-1617. https://doi.org/10.1109/TMC.2019.2913832

Huang, W., Tian, P., & Xu, Z. (2016). Design and implementation of a real-time CIM-MIMO optical camera communication system. *Optics Express, 24*(21), 24567-24579. https://doi.org/10.1364/OE.24.024567

Khan, L. U. (2017). Visible light communication: Applications, architecture, standardization and research challenges. *Digital Communications and Networks, 3*(2), 78-88. https://doi.org/10.1016/j.dcan.2016.07.004

Kodali, R. K., & Mahesh, K. S. (2016). A low cost implementation of MQTT using ESP8266. *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 404-408). IEEE. https://doi.org/10.1109/IC3I.2016.7917998

Liu, H., & Ma, F. (2021). Design of visible light communication transceiver system based on intelligent terminal. *2021 IEEE 6th Optoelectronics Global Conference (OGC)* (pp. 77-81). IEEE. https://doi.org/10.1109/OGC52961.2021.9654303

Luo, J., Fan, L., & Li, H. (2017). Indoor positioning systems based on visible light communication: State of the art. *IEEE Communications Surveys & Tutorials, 19*(4), 2871-2893. https://doi.org/10.1109/COMST.2017.2743228

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications, 3*(5), 164-173. https://doi.org/10.4236/jcc.2015.35021

Martínez-Ciro, R. A., López-Giraldo, F. E., Betancur-Perez, A. F., & Luna-Rivera, J. M. (2019). Design and implementation of a multi-colour visible light communication system based on a light-to-frequency receiver. *Photonics, 6*, 42. https://doi.org/10.3390/photonics6020042

Martínez-Ciro, R., Morales-Morales, D., López-Giraldo, F., & Rojas-Usuga, J. (2020). Visible light communication channel with a smartphone screen as a transmitter and color shift keying modulation for access control applications. *Journal of Physics: Conference Series, 1547*, 012002. https://doi.org/10.1088/1742-6596/1547/1/012002

Montgomery, D. C. (2017). *Design and analysis of experiments* (9 ed.). John Wiley & Sons. https://books.google.com.co/books?id=xJBEDwAAQBAJ

Nir, Y., & Langley, A. (2018). *ChaCha20 and Poly1305 for IETF protocols.* Internet Research Task Force. https://doi.org/10.17487/RFC8439

Schwartz, M. (2016). *Internet of Things with ESP8266.* Packt Publishing. https://books.google.com.co/books?id=M7A7vgAACAAJ

Shaaban, K., Shamim, M. H., & Abdur-Rouf, K. (2021). Visible light communication for intelligent transportation systems: A review of the latest technologies. *Journal of Traffic and Transportation Engineering (English Edition), 8*(4), 483-492. https://doi.org/10.1016/j.jtte.2021.04.005

Tanaka, Y., Komine, T., Haruyama, S., & Nakagawa, M. (2003). Indoor visible light data transmission system utilizing white LED lights. *IEICE Transactions on Communications, 86*(8), 2440-2454. https://globals.ieice.org/en_transactions/communications/10.1587/e86-b_8_2440/_p

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5 ed.). Pearson Education. https://books.google.com.co/books?id=I764bwAACAAJ

Tsai, C.-T., Cheng, C.-H., Kuo, H.-C., & Lin, G.-R. (2019). Toward high-speed visible laser lighting based optical wireless communications. *Progress in Quantum Electronics, 67*, 100225. https://doi.org/10.1016/j.pquantelec.2019.100225

Vappangi, S., & Mani, V. (2022). A survey on the integration of visible light communication with power line communication: Conception, applications and research challenges. *Optik, 266*, 169582. https://doi.org/10.1016/j.ijleo.2022.169582

Watson, S., Tan, M., Najda, S. P., Perlin, P., Leszczynski, M., Targowski, G., Grzanka, S., & Kelly, A. E. (2013). Visible light communications using a directly modulated 422 nm GaN laser diode. *Optics Letters, 38*(19), 3792-3794. https://doi.org/10.1364/OL.38.003792