The potential of light fidelity in smart home automation

Hakan Aydin[1], Gülsüm Zeynep Gürkaş Aydin[2], Muhammed Ali Aydin[2]
[1]Department of Computer Engineering, Faculty of Engineering, İstanbul Topkapı University, İstanbul, Turkey
[2]Department of Computer Engineering, Faculty of Engineering, İstanbul University-Cerrahpasa, İstanbul, Turkey

Article Info

Article history:

Received Dec 31, 2023
Revised Mar 11, 2024
Accepted Mar 20, 2024

Keywords:

Internet of things
Light fidelity
Optical wireless communication
Smart home automation
Wireless communication

ABSTRACT

Light fidelity (Li-Fi) is a pioneering optical wireless communication (OWC) technology that utilizes visible light for wireless data transmission. Since its inception in a TED global talk by Professor Harald Haas in 2011, Li-Fi has captured significant attention in the research community. Smart home automation systems (SHAs) leverage internet of things (IoT) technology to remotely manage and automate various home devices and systems. Li-Fi technology has the potential to enable remote control of devices such as lighting, air conditioning, music systems, security cameras, and door locks within SHAs. This study presents Li-Fi-IoT, a Li-Fi-based system designed for efficient and secure IoT device management in SHAs. A series of experiments demonstrates the system's potential in IoT device control using Li-Fi technology. The research findings highlight the substantial improvement in data transfer speed, energy efficiency, and data security that Li-Fi technology can bring to SHAs.

Corresponding Author:

Hakan Aydin
İstanbul Topkapı University, Department of Computer Engineering, Faculty of Engineering
İstanbul, Turkey
Email: hakanaydin@topkapi.edu.tr

1. INTRODUCTION

Light fidelity (Li-Fi) was introduced by Professor Harald Haas in a 2011 TED global talk [1]. This innovative technology, which relies on visible light communication (VLC) for data transfer, distinguishes itself by its ability to function within predefined areas while eliminating electromagnetic interference [2]. Li-Fi offers several advantages compared to Wi-Fi and bluetooth, including swift data transfer, heightened security, and reduced electromagnetic interference. However, its implementation necessitates dedicated infrastructure and relies on direct light, a feature that could potentially conflict with existing lighting systems. Li-Fi has the potential for applications in a wide array of domains, ranging from smart lighting, medical devices, and vehicles to industrial systems, space exploration, and bridging connectivity gaps in the internet landscape [3]. Li-Fi is rapidly gaining ground as the future of communication technology, owing to its distinct advantages, which encompass an abundant spectrum, rapid data transfer rates, cost-effective implementation, and built-in beamforming capabilities [4]. In the realm of connecting smart devices, various wireless technologies come into play, such as internet protocol version 6 (IPv6), 6LoWPAN, ZigBee, bluetooth low energy (BLE), Z-Wave, and near field communication (NFC) [5]. Li-Fi, as a cutting-edge technology, offers short-range, secure, high-speed, and cost-effective internet access through visible light, in contrast to traditional radio wave-based approaches, positioning it as the next-generation communication technology [6]. Li-Fi offers various advantages over Wi-Fi, including a significantly broader spectrum, enhanced security due to its inability to penetrate obstacles like concrete, increased bandwidth, cost-effectiveness, energy efficiency, environmental friendliness, suitability for indoor communication with reliable security, potential applications in smart lighting and medical facilities, interference-free aviation usage, industrial suitability, underwater applications, faster data transfer for educational institutions, and improved traffic management through LED-based communication, addressing the limitations of traditional Wi-Fi systems [7]. Li-Fi harnesses the visible light spectrum (380-780 nm/384-789 THz) emitted by LED lamps, offering a two-way, high-speed wireless technology that emphasizes security and environmental friendliness [8]. Given the widespread use of LEDs in residential areas, industrial facilities, and outdoor lighting, Li-Fi can leverage the existing lighting infrastructure, resulting in cost-effective deployment [4]. In a direct comparison with Wi-Fi, Li-Fi shines with its superior data transfer speeds, enhanced security features, and reduced electromagnetic interference [9]. Nevertheless, Li-Fi does come with some limitations, including the need for specific infrastructure, data transfer restrictions to well-lit areas, and susceptibility to pre-existing light sources [1]. Li-Fi technology, despite offering high-bandwidth indoor communication, encounters challenges, including precise line-of-sight device alignment, dynamic transmitter settings, wavelength sensitivity, limited reliability at high data rates, highlighting the need for continued enhancements to overcome these limitations and ensure robust LOS connectivity [10], the decreasing equipment costs accompanying the emergence of this new technology underscore its tremendous potential within the realm of future wireless communication technology, signifying a significant shift on the horizon [11]. To provide a visual perspective, Figure 1 illustrates the global Li-Fi market size in 2017 and the projected size for 2028 based on application.

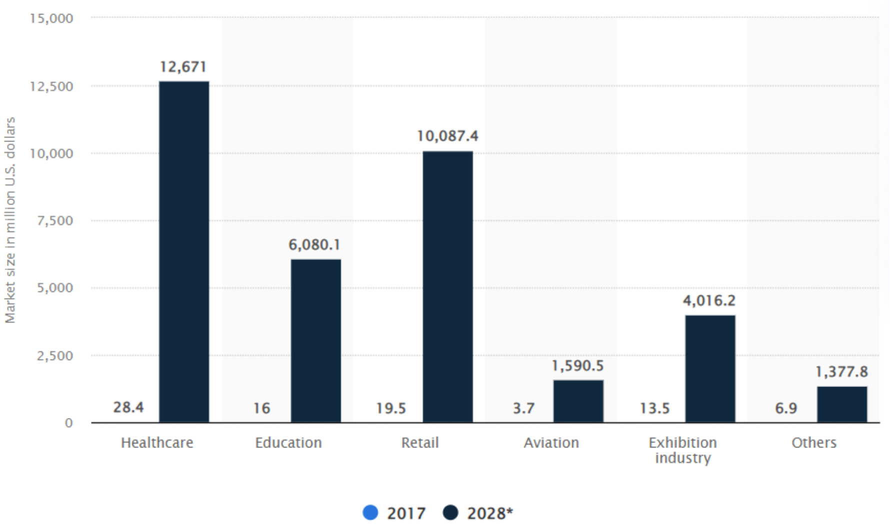

Figure 1. Li-Fi market revenue worldwide [12]

Smart home automation systems (SHAs), commonly referred to as home automation, streamline household chores by utilizing advanced technology and intelligent systems [13]. These systems integrate various devices, sensors, and networks to oversee and regulate household appliances and systems [14]. SHAs harness the power of the internet of things (IoT), wireless communication, and artificial intelligence to efficiently manage tasks related to appliances, energy, security, and more [15]. In addition to traditional Wi-Fi, other wireless technologies are also integral to the functionality of SHAs. Wi-Fi, as one of the primary wireless technologies, enables the seamless connectivity of various devices within a smart home ecosystem. It serves as the backbone for interconnecting smart appliances, such as thermostats, security cameras, and voice-controlled assistants, facilitating their control and management through a central hub or a smartphone application. This wireless connectivity is instrumental in creating a cohesive and responsive smart home environment. Besides Wi-Fi, there are other wireless technologies like ZigBee and Z-Wave that play essential roles in SHAs. ZigBee, for instance, is known for its low power consumption and ability to create robust mesh networks, making it suitable for connecting numerous low-energy devices like sensors and smart lighting. Z-Wave, on the other hand, is designed for interoperability and reliability in home automation, making it a preferred choice for various smart home products. These wireless technologies, including Wi-Fi, ZigBee, and Z-Wave, form the foundation of SHAs, ensuring effective communication and control among the ever-expanding array of IoT devices.

As the number of IoT devices within SHAs continues to grow, the significance of reliable and secure wireless technology becomes increasingly critical. Li-Fi, with its exceptional speed and robust security, also holds promise in enhancing the management of IoT devices within SHAs. In the realm of SHAs, which are dependent on IoT technology for remote device management, Li-Fi emerges as a promising solution. It promises enhanced data speed, energy efficiency, and data security. Nevertheless, it faces obstacles related to its infrastructure requirements and line-of-sight limitations. This study aims to tackle these issues and investigates the potential of leveraging Li-Fi's performance for SHAs.

In previous research, several notable advancements have been made in the realm of smart home technology. An application integrating voice and text controls facilitated remote access to household appliances in [16]. Yasir *et al.* [17] introduced an indoor positioning system via visible light communication and accelerometers. Kodali *et al.* (2016) [18] explored IoT applications in home security and automation, offering remote control of lighting, heating, and more using sensors. Chinchawade and Sujatha (2016) [19] proposed Li-Fi-based home/office automation through LED lamps. Alaa *et al.* (2017) [20] emphasized IoT-based smart home benefits, including appliance control and energy efficiency. Malik and Bodwade (2017) [21] predicted broader smart home applications. Wu *et al.* (2017) [22] discussed a hybrid Li-Fi/Wi-Fi network. Šul'aj *et al.* (2018) [23] designed a Li-Fi-based home automation prototype. Albraheem *et al.* (2018) [24] devised an IoT architecture using Li-Fi. Shanmughasundaram *et al.* (2018) [25] proposed Li-Fi for traffic signal control. Arfan and Lakshminarayana (2018) [8] explored Li-Fi for underwater operations. Molla *et al.* (2018) [26] analyzed energy management. Sharma *et al.* (2018) [27] proposed a secure cloud framework. Agarwal *et al.* (2019) [28] reviewed IoT-based home automation. Ismail *et al.* (2020) [29] introduced a Li-Fi-based home automation system. Romdhane and Yuksel (2020) [30] addressed Li-Fi security. Mekuria *et al.* (2021) [31] reviewed smart home reasoning systems. Stolojescu-Crisan *et al.* [32] proposed a Li-Fi-based home automation system. Stolojescu-Crisan *et al.* [32] introduced an IoT-based smart home system. Thaljaoui *et al.* (2022) [33] presented a Li-Fi and infrared-based medical device monitoring system. Diambeki *et al.* (2022) [34] enhanced Li-Fi network security. Gupta *et al.* (2022) [35] developed a Li-Fi system for smart home appliances, addressing data transfer speeds and signal obstacles. Singh *et al.* (2018) [36] designed an IoT-based smart home automation system with sensor nodes for device control and monitoring. Table 1 presents a selection of pertinent studies reviewed in the literature research.

Table 1. The research and several relevant studies

Reference	Exp. name	Purpose
Šul'aj *et al.* (2018) [23]	Integrating Li-Fi technology into home automation	Crafting a Li-Fi-based smart home control application for data transfer.
Ismail *et al.* (2020) [29]	Implementing a home automation system with Li-Fi	Designing a Li-Fi-powered smart home appliance control app.
Singh *et al.* (2018) [36]	Building an IoT-enabled smart home automation system with sensor nodes	Creating an environmentally-responsive automatic device control system.
Gupta *et al.* (2022) [35]	Li-Fi-driven data transfer for smart home appliances	Emphasizing Li-Fi i's swift and secure communication in smart homes.

The studies examined in this research underscore the potential of Li-Fi technology, especially in the realm of home automation applications. They demonstrate the versatility of this technology in enabling remote control of household appliances, improving energy efficiency, enhancing home security, facilitating environmental monitoring, and enabling device programming. This study introduces Li-Fi-IoT, a Li-Fi-based system tailored for efficient and secure IoT device management within SHAs. The system utilizes smartphones' flashlights as Li-Fi transmitters, showcasing Li-Fi's practicality. To ensure data security, AES encryption is integrated. A series of experiments demonstrates Li-Fi's versatility in controlling devices, from basic LED lamps to complex servo motors. It also showcases wireless text message transmission to a computer, emphasizing data security through AES encryption. The research delves into the data transfer rate of the Li-Fi-IoT system and examines the relationship between light intensity, distance, and the angle of the light source. This study differentiates itself from previous research in several notable ways:

- Li-Fi-IoT system: in this study, a system based on Li-Fi technology was designed and physically implemented. The experimental results obtained were highly successful. Unlike other studies, the application utilized a smartphone's flashlight as the source of Li-Fi transmission, which represents a significant departure from conventional approaches. While other studies typically employed traditional LED light sources or dedicated Li-Fi transmitters, this research introduced a novel method of Li-Fi transmission using a readily available smartphone flashlight.
- AES encryption: this study introduced a Li-Fi-based system that enhances data security through the utilization of the AES encryption algorithm, marking a significant departure from other studies on Li-Fi technology for smart home applications (SHAs). This aspect highlights the potential of Li-Fi technology in enhancing security within SHAs. Unlike other studies, this research placed a strong emphasis on

cybersecurity. In the study a system for SHAs that is both secure and rapid, emphasizing data transfer and cybersecurity awareness was presented.

- Experiments conducted in this study: the experiments demonstrated that Li-Fi technology effectively controlled basic devices such as LED lamps and could also manage more complex devices like servo motors, showcasing its versatility. The transmission of wireless text messages to a computer was achieved using Li-Fi, underscoring its potential for data transfer in IoT applications. The implementation of AES encryption ensured data security within the system. The data transfer rate was measured at approximately 1.01 KB/s, with variations from prior studies likely stemming from different system configurations. Additionally, the relationship between light intensity and distance was investigated, revealing that encrypted messages could be decrypted beyond a specific distance, with the illumination range overlapping as the distance increased. Finally, the experiment examining the angle of the smartphone's light source on the receiver's brightness value highlighted the impact of the angle on received light intensity. These results collectively emphasize the promising role of Li-Fi technology in enabling secure and efficient communication within IoT systems, with potential applications in SHAs.

2. METHOD

2.1. Proposed method

This study proposes a fast and secure approach that explores the incorporation of Li-Fi technology to enhance SHAs. The Li-Fi-IoT system implemented in the study is presented in the Figure 2. The Li-Fi-IoT system is a comprehensive setup that encompasses several essential hardware components to facilitate efficient data transmission and device management. At its core, this system employs an arduino board equipped with Li-Fi modules, functioning as the central hub for data processing and communication. This arduino board establishes communication with a smartphone, serving as both a data source and a light transmitter via its flashlight. The flashlight emits modulated light signals, conveying data to a photodiode sensor, a critical element for receiving transmitted information. The sensor converts the received light signals back into data that can be processed by the arduino board. In addition, LED lamps are integrated into the system to exemplify the control of household devices, such as lighting, through Li-Fi technology. Crucially, data security during transmission and reception is ensured by the AES encryption module. In totality, these hardware components constitute the Li-Fi-IoT system, showcasing the integration of Li-Fi technology with IoT devices to enable efficient and secure data management within SHAs. In order to validate the potential of Li-Fi technology, a series of experiments were conducted. The diagram illustrating both the architecture of the Li-Fi-IoT system and the experiments is presented in Figure 3.

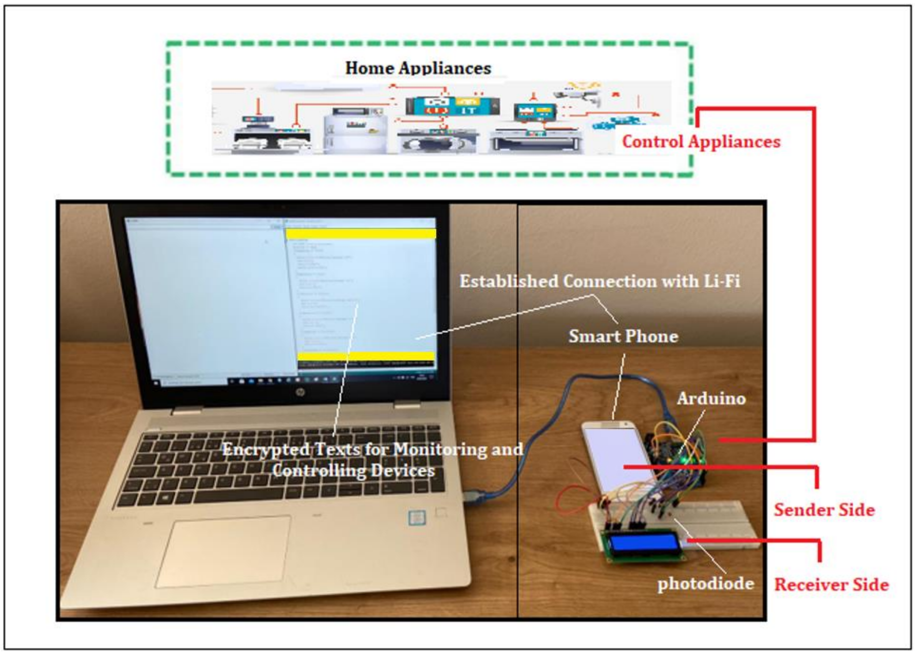
Home Appliances
Control Appliances
Established Connection with Li-Fi
Smart Phone
Arduino
Encrypted Texts for Monitoring and Controlling Devices
Sender Side
photodiode
Receiver Side

Figure 2. The implementation of the Li-Fi-IoT system

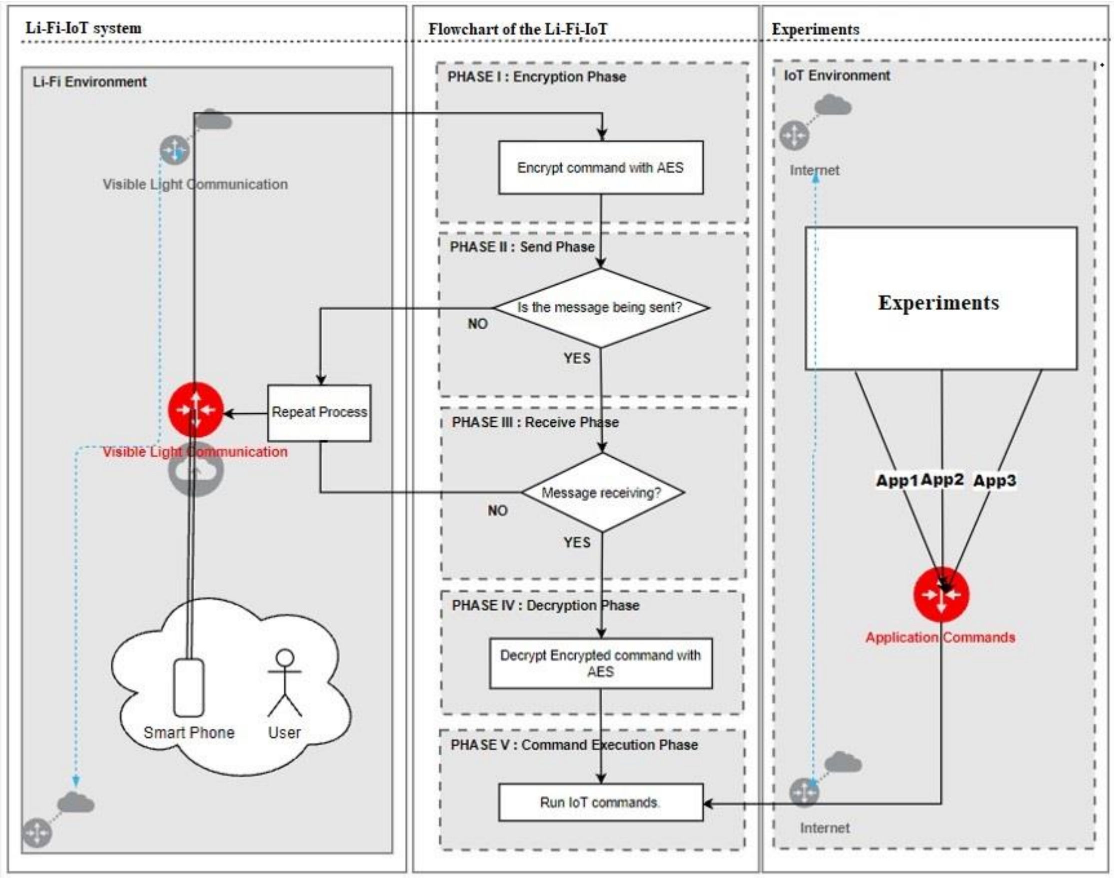
Li-Fi-IoT system
Li-Fi Environment
Visible Light Communication
Repeat Process
Visible Light Communication
Smart Phone
User
Flowchart of the Li-Fi-IoT
PHASE I : Encryption Phase
Encrypt command with AES
PHASE II : Send Phase
Is the message being sent?
NO
YES
PHASE III : Receive Phase
Message receiving?
NO
YES
PHASE IV : Decryption Phase
Decrypt Encrypted command with AES
PHASE V : Command Execution Phase
Run IoT commands.
Experiments
IoT Environment
Internet
Experiments
App1
App2
App3
Application Commands
Internet

Figure 3. Li-Fi-IoT architecture

These experiments encompassed activities such as using Li-Fi to control an LED lamp for data transfer, demonstrating Li-Fi's capacity to manage more complex devices by controlling a servo motor, and showcasing wireless text message transmission via Li-Fi. Additionally, the implementation of AES encryption was instrumental in bolstering data security for secure message transmission. The visual representation of the experiments conducted in the study is presented in Figure 4. In these experiments, the data transfer rate of the Li-Fi-IoT system was measured at approximately 1.01 KB/s. Furthermore, the study delved into investigating the relationship between light intensity and distance in the Li-Fi-IoT system, shedding light on the significance of the illumination range as distance increased. Moreover, the research scrutinized how the angle of the smartphone's light source impacted the receiver's brightness, offering invaluable insights for system design and performance enhancement. This research distinguishes itself by introducing the Li-Fi-IoT system, incorporating innovative features like AES encryption for robust data security, and harnessing a smartphone flashlight for Li-Fi transmission. The combined results of these experiments underscore the potential of Li-Fi technology in enhancing data transfer speed, energy efficiency, and data security in the realm of SHAs and IoT applications.

2.2. Experimental studies

In the experimental studies, the Li-Fi-IoT system was designed with both a sender and a receiver. The receiver unit converted incoming light into current using a photodiode, allowing users to control IoT devices through a smartphone application. Text commands were encrypted, transmitted via the smartphone's flashlight, and received by an arduino-based system, facilitating data transfer. The details and objectives of each experiment, along with their respective results, are provided in Table 1 and are further elaborated upon in the subsequent subsections. Table 2 outlines various experimental scenarios and objectives, demonstrating the versatility and potential of Li-Fi technology in controlling devices, transmitting data, ensuring security, and optimizing performance parameters in an IoT system.

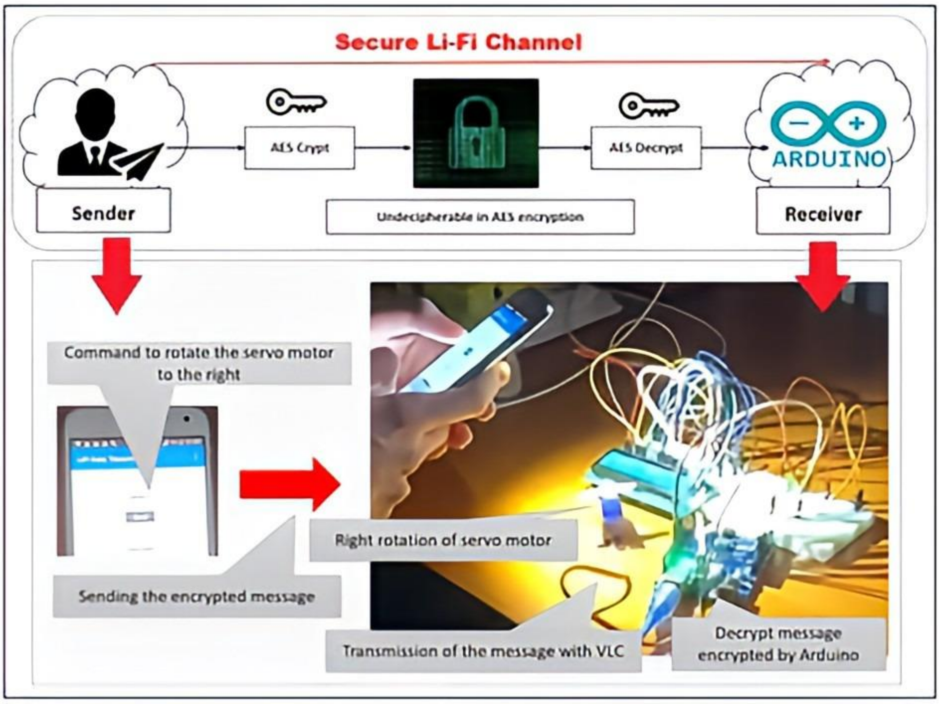
Secure Li-Fi Channel
AES Crypt
AES Decrypt
ARDUINO
Sender
Undecipherable in AES encryption
Receiver
Command to rotate the servo motor to the right
Right rotation of servo motor
Sending the encrypted message
Transmission of the message with VLC
Decrypt message encrypted by Arduino

Figure 4. Experiments carried out in the research

Table 2. Experimental scenarios and objectives

No.	Exp. name	Purpose
1.	Turning a led lamp on and off	To demonstrate that Li-Fi technology successfully turned an LED lamp on and off, transmitting commands via light for data transfer and highlighting the potential for controlling simple devices with Li-Fi.
2.	Controlling a servo motor	To prove that Li-Fi technology can precisely control a servo motor, which indicates its potential to control even more intricate devices for data transfer.
3.	Sending a text message to a PC	To transmit a text message wirelessly to a computer using Li-Fi technology, to demonstrate the potential of Li-Fi as an alternative for wireless data transmission.
4.	Ae’s encryption	To ensure data security using the AES encryption algorithm.
5.	Data transfer rate of Li-Fi-IoT system	To measure the data transfer rate of the proposed Li-Fi-IoT system.
6.	Minimum illumination threshold and range analysis	To analyze the relationship between light intensity and distance using the Li-Fi-IoT system.
7.	Angular brightness measurement	To measure the effect of the angle of the smartphone's light source on the brightness value at the receiver for the Li-Fi-IoT system.

2.2.1. Turning an LED lamp on and off with Li-Fi

The aim of this experiment was to demonstrate the feasibility of data transmission using Li-Fi technology to control the operation of an LED lamp. The experimental setup consisted of the Li-Fi IoT system along with a separate LED lamp. Specific instructions for switching the LED lamp on and off were recorded in a text file. These instructions were then sent from the computer to the Li-Fi transmitter module and subsequently relayed to the arduino board through the Li-Fi receiver module, resulting in the activation and deactivation of the LED lamp. The software used in this experiment was essential, with the Arduino integrated development environment (IDE) being used to interpret the instructions in the text file and supervise the operation of the LED lamp.

2.2.2. Controlling a servo motor with Li-Fi

The aim of this experiment was to control a servo motor and perform data transfer using Li-Fi technology. For the experiment, a servo motor and a Li-Fi transmitter were utilized. Once properly connected, the servo motor responded to commands sent via the transmitter. The transmitter converted the commands in the text file into a signal that the servo motor could interpret and act upon using Li-Fi technology. The necessary hardware included a servo motor, a Li-Fi transmitter, an Arduino, and a computer.

The Arduino converted text files into Li-Fi signals and managed the movement of the servo motor. Li-Fi software facilitated data communication between the transmitter and the receiver.

2.2.3. Sending a text message to a PC with Li-Fi

In this experiment, the primary objective was to showcase the capability of wirelessly transmitting a text message to a computer utilizing Li-Fi technology. This experiment aimed to validate the feasibility of sending data from the Li-Fi-IoT system to a PC through a secure and efficient method.

2.3.4. Data transfer rate

AES is an encryption algorithm that was standardized based on a proposal by Daemen and Rijmen [37]. The structure of this algorithm is depicted in Algorithm 1 [38]. According to this algorithm, the AES encryption function takes a 128-bit plaintext block (P) and a key (K) as input, resulting in the production of a 128-bit ciphertext block (C). The algorithm goes through several rounds, which include operations such as SubBytes, ShiftRows, and MixColumns (except in the final round), as well as key schedule to perform encryption. The ultimate outcome, C, represents the encrypted data. In this study, AES encryption was applied to enhance data security during transmission via Li-Fi. In the Li-Fi-IoT system, text data was encrypted using AES before being transmitted and exchanged between the sender and the receiver. AES encryption transformed the data into an encrypted format. As a result, end-to-end encrypted messages and contextual data transmitted via Li-Fi-IoT remained inaccessible to potential attackers. This was because neither individuals nor third parties possessed the encryption key necessary to access this data. The encrypted text remained indecipherable until it was decrypted with the appropriate encryption key.

Algorithm 1. The AES encryption function [38]

```
$\boldsymbol{Input}$: $The\ 128 - bit\ plaintext\ block\ P\ and\ key\ K.$
$\boldsymbol{Output}$: $The\ 128 - bit\ ciphertext\ block\ C.$
$X \leftarrow AddRoundKey(P, K)$
$for\ i \leftarrow 1\ to\ 10\ do$
    $X \leftarrow SubBytes(X)$
    $X \leftarrow ShiftRows(X)$
    $if\ i \neq 10\ then$
    $X \leftarrow MixColumns(X)$
    $end$
    $K \leftarrow KeySchedule(K, i)$
    $X \leftarrow AddRoundKey(X, K)$
$end$
$C \leftarrow X$
$return\ C$
```

2.2.5. Data transfer rate

In the study, the data transfer rate of the Li-Fi-IoT system was also measured. To achieve this, the transmission and reception time of a data packet sent from the smartphone, which was part of the system, and received by a photodiode sensor was precisely measured. Subsequently, the data transfer rate was calculated based on these measurements. It is important to note that the data transfer rate is contingent on both the size of the data packet and the time taken for transmission. Initially, the size of the data packet was determined. Following this, the total transmission time was calculated by meticulously measuring the transmission and reception time.

2.2.6. Minimum illumination threshold and range analysis

This experiment aimed to investigate the relationship between light intensity and distance in the Li-Fi-IoT system. The initial step involved analyzing ambient light to determine the minimum threshold at which the sensor would cease reading data. However, it was observed that complete prevention of environmental light interference was not attainable, and an ambient light intensity of 270 lux was measured. In the second stage of the experiment, the relationship between distance and the range of illumination when transmitting encrypted messages using the Li-Fi-IoT system was examined. It was observed that the decryption of encrypted Li-Fi messages only became possible beyond a specific distance, with the illumination ranges beginning to overlap as the distance between the sender and receiver increased. The experiment yielded a range of measured light brightness, which varied between 280 and 880 lux. In the third stage, the adaptability of Li-Fi-IoT by increasing the distance between the sender and receiver beyond 100 cm was assessed, conducting several experiments to determine the system's performance at extended distances.

2.2.7. Angular brightness measurement

In this experiment, the impact of the angle of the light source from the smartphone used in the Li-Fi-IoT system on the brightness value at the receiver was measured. The experiment involved assessing the brightness values received by the system's receiver while varying the orientation of the smartphone. Specifically, the smartphone was set to specific angles, including 45, 60, and 90 degrees, and the corresponding light intensity was measured at each of these angles. To perform these measurements, a lux meter was employed.

3. RESULTS AND DISCUSSION

3.1. Turning an LED lamp on and off with Li-Fi

The results of the experiment unequivocally demonstrated the successful capability of utilizing Li-Fi technology to switch the LED lamp on and off. Li-Fi technology capitalizes on light as the primary medium for data transmission, with the LED lamp serving as the light source in this particular experiment. Furthermore, the experiment conclusively established that instructions contained in the text file could be effectively transmitted through Li-Fi technology. Thus, this experiment provided compelling evidence of the potential of Li-Fi technology in controlling basic devices like LED lamps for data transfer. The experiment effectively affirmed the competency of Li-Fi technology in managing elementary devices such as LED lamps for data transmission, thereby validating the use of light as a medium for data transfer within the Li-Fi framework, with the LED lamp as the emissive light source.

3.2. Controlling a servo motor with Li-Fi

The experiment results demonstrated that the servo motor could be effectively controlled using Li-Fi technology. Li-Fi technology utilizes light directly for data transfer, and in this experiment, the servo motor served as the light source. The experiment illustrated that Li-Fi technology can handle more complex devices for data transfer. It effectively showcased the capabilities of Li-Fi technology in controlling a servo motor and enabling data transfer. These results validate the use of Li-Fi technology as a means to control intricate devices, expanding its potential applications beyond simple devices like LED lamps.

3.3. Sending a text message to a PC with Li-Fi

The experiment's results confirmed that the text message could be successfully received by the computer through the use of Li-Fi technology. Li-Fi technology directly employs light for data transfer, and in this experiment, the LED lamp served as the light source. This experiment effectively demonstrated that Li-Fi technology can be used for wireless data transfer.

2.3.4. Data transfer rate

The results of this experiment confirmed the successful implementation of AES encryption within the Li-Fi-IoT system, thereby ensuring a secure connection for message transmission and reception. The steps related to the AES encryption process for this experiment were depicted in Algorithm 2. Algorithm 2 outlines a process for securing communication within the Li-Fi-IoT system, where plain text is transformed into cipher text and vice versa using a shared encryption key. This ensures that IoT commands can be securely transmitted and executed, following a specific protocol. Overall, these experiments demonstrated the capabilities of Li-Fi technology in wireless data transfer and data security. The results showcased the potential application of Li-Fi in enabling secure and efficient communication within smart home automation systems.

Algorithm 2. Li-Fi-IoT encryption

```
Input: Plain Text
Output: Cipher Text / Plain Text
function GenerateEncryptionKey ();
if IoT Command (message) is ready then
        Encrypt the message using the shared key;
        Send the encrypted message with Li − Fi wireless network;
if encrypted message is taken then
Decrypt the IoT command (message) using the shared key;
        Run the IoT command.
```

2.2.5. Data transfer rate

The data transfer rate is obtained by dividing the size of the data packet by the transmission time. In this experiment, a simple text message was utilized, and the size of the data packet was measured to be approximately 100 bytes. The transmission time of this data packet with the Li-Fi-IoT system was measured as 99 milliseconds. Therefore, if the transmission time of a data packet with a size of 100 bytes is 99 milliseconds, the data transfer rate of the Li-Fi-IoT system can be calculated. Expressing the amount of transmitted data as 'M' and the transmission time as 'T,' the data transfer rate 'V' can be calculated using the following mathematical formula:

$$V = \frac{M}{T} \tag{1}$$

Here, "M" is expressed in units of bytes (B), and "T" is expressed in seconds (s). Therefore, the data transfer rate is calculated in bytes per second (B/s). M stands for 100 bytes, which is equivalent to 0.1 KB. T represents 99 milliseconds, which can be converted to 0.099 seconds. To calculate the value of V, the formula V=M/T was used, where M is 0.1 KB and T is 0.099 seconds. Plugging these values into the formula, V is equal to 1.01 KB/s. In this case, based on these experiments, the measured transmission time for a 100-byte data packet with Li-Fi-IoT was found to be approximately 99 milliseconds. This calculation resulted in a data transfer rate of approximately 1.01 KB/second. Notably, the data transfer rate reported in this study contrasts with the 1 Mbps data transfer rate stated in [30]. The variance between these results could be attributed to differences in the systems used or variations in test conditions. This experiment's results underscore that the data transfer rate of the Li-Fi-IoT system was approximately 1.01 KB/s, as calculated from the transmission of a 100-byte data packet in 99 milliseconds. It's worth noting that the data transfer rate of the system developed in [30] was reported as 1 Mbps, which contrasts with these findings of 1.01 KB/s, potentially due to differences in the systems or test conditions employed.

2.2.6. Minimum illumination threshold and range analysis

The results of this experiment are presented in Table 3. These findings indicate that the light intensity of messages transmitted through Li-Fi-IoT was inversely proportional to the distance

Table 3. Results of the experiment

Stage	Description	Results
1.	Analysis of ambient light to determine the minimum threshold for sensor data reading	Unable to completely prevent environmental light interference. Ambient light intensity measured: 270 lux.
2.	Investigation of relationship between distance and illumination range for transmitting encrypted messages	Encrypted Li-Fi messages deciphered after a certain distance. Illumination ranges overlapped as distance increased. Measured light brightness range: 280-880 lux.
3.	Testing the adaptability of Li-Fi-IoT by increasing distance beyond 100 cm	Conducted several experiments to assess adaptability.

The experimental results for light intensity as a function of distance are presented in Figure 5. According to the results obtained in this experiment, it was observed that encrypted Li-Fi messages could be decrypted beyond a specific distance, and the illumination range started to overlap as the distance between the sender and receiver increased. Furthermore, the measurements in these experiments suggest that the system can find practical applications, with the illumination range being a key consideration as the distance increases.

2.2.7. Angular brightness measurement

According to the experimental results, it was observed that brightness values changed in response to the angle of the smartphone. The highest brightness value, 880 lux, was recorded at a 45-degree angle. At a 60-degree angle, the brightness value measured 700 lux, and at a 90-degree angle, it measured 600 lux. The receiver could only attain the maximum brightness when the smartphone was directed towards it, resulting in the highest brightness value Figure 6. The findings of this experiment are also presented in Table 4.

These results indicate that the highest brightness value, 880 lux, was observed at a 45-degree angle, followed by 700 lux at a 60-degree angle, and 600 lux at a 90-degree angle. The receiver received the maximum brightness when the smartphone was directed towards it, resulting in the highest brightness value. This information can be valuable in the system's design and in enhancing its performance.

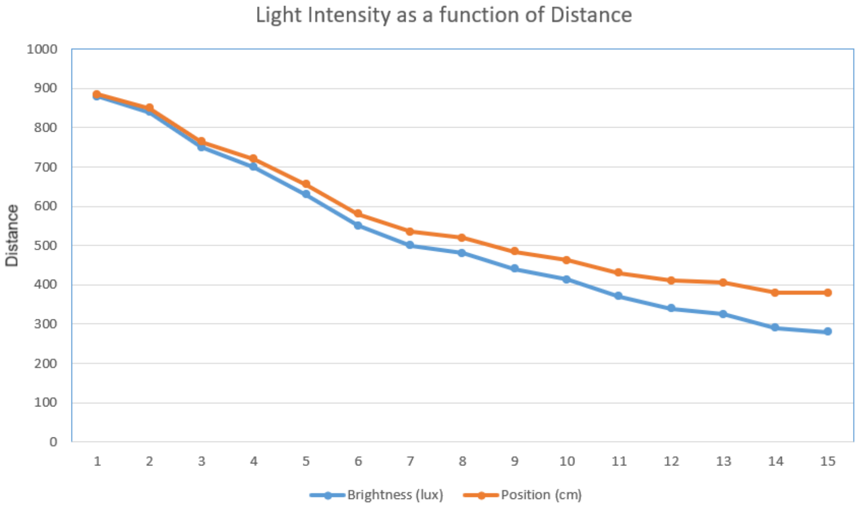

Figure 5. Light intensity as a function of distance

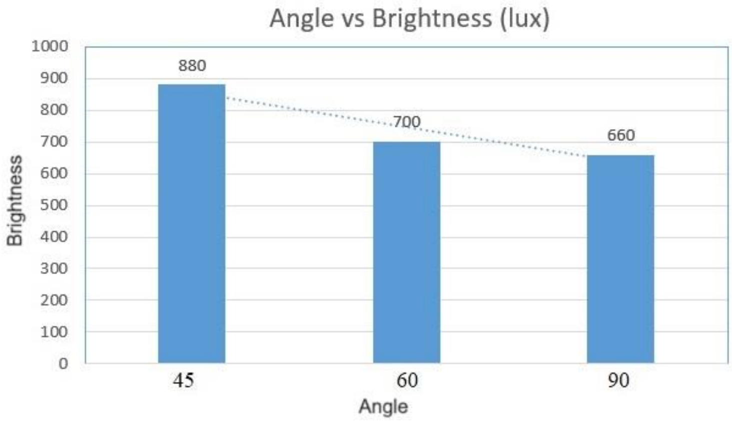

Figure 6. Light intensity as a function of angle

Table 4. Results of the experiment

Angle (degrees)	Brightness value (lux)
45	880
60	700
90	600

4. CONCLUSION

This study presented an integration of Li-Fi technology within SHAs, demonstrating its potential in efficient and secure data management. The Li-Fi-IoT system showcased Li-Fi's versatility. The implementation of AES encryption ensured data security, with a measured data transfer rate of approximately 1.01 KB/s. Experiments exploring light intensity, distance, and smartphone angle provided valuable insights for system design. These results highlight Li-Fi technology's promise in enhancing data transfer speed, energy efficiency, and data security in SHAs and IoT applications, positioning it as a viable solution for the future of wireless communication technology. In future research, the potential benefits of nanotechnology will be harnessed to enhance Li-Fi technology by extending its range and improving its performance in low light conditions. The objective is to explore innovative methods that utilize nanomaterials and nanometer-scale devices to increase the signal range and reduce reliance on light, thereby pushing the boundaries of Li-Fi technology for broader applications.

ACKNOWLEDGEMENTS

Within the scope of this study, we would like to express our gratitude to Batuhan Aydin, a Computer Engineering student at Atılım University, Ankara, Türkiye, for his valuable contributions to establishing the Li-Fi mechanism and conducting experiments on this system.

REFERENCES

[1] H. Haas, “Wireless data from every light bulb,” TED Talks Director, 2011, [Online]. Available: http://www.youtube.com/watch?v=NaoSp4NpkGg. (Accessed on March 8, 2024).

[2] C. Mercer, “What is Li-Fi? Everything you need to know,” Retrieved from https://wwwtechworldcom/data/what-is-li-fi-everything-you-need-know-3632764/, 2018. (Accessed on March 8, 2024).

[3] H. Haas, L. Yin, Y. Wang, and C. Chen, “What is LiFi?,” *Journal of Lightwave Technology*, vol. 34, no. 6, pp. 1533–1544, Mar. 2016, doi: 10.1109/JLT.2015.2510021.

[4] A. Petrosino, D. Striccoli, O. Romanov, G. Boggia, and L. A. Grieco, “Light Fidelity for Internet of Things: A survey,” *Optical Switching and Networking*, vol. 48, p. 100732, Mar. 2023, doi: 10.1016/j.osn.2023.100732.

[5] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of Things (IoT) communication protocols: Review,” in *2017 8th International Conference on Information Technology (ICIT)*, IEEE, May 2017, pp. 685–690, doi: 10.1109/ICITECH.2017.8079928.

[6] A. Z. Rabia, N. Ali, S. Ali, A. Sajid1, “A security review over wi-fi and li-fi,” *Information Management and Computer Science*, vol. 3, no. 1, pp. 01–09, Apr. 2020, doi: 10.26480/imcs.01.2020.01.09.

[7] M. Khan, A. Sajid, A. Hanif, M. Aqib, and A. Zafar, “A review on (wi-fi vs. li-fi) technology,” *Information Management and Computer Science*, vol. 3, no. 1, pp. 10–13, Mar. 2020, doi: 10.26480/imcs.01.2020.10.13.

[8] M. Arfan and C. Lakshminarayana, “VLC for Underwater Operations: Li-Fi Solution for Underwater Short Range Communication,” in *2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, IEEE, Dec. 2018, pp. 638–642, doi: 10.1109/ICEECCOT43722.2018.9001519.

[9] D. A. N. A. Sarkar and S. Agarwal, “Li-Fi Technology: Data Transmission through Visible Light,” *International Journal of Advance Research in Computer Science and Management Studies*, vol. 3, no. 6, 2015.

[10] F. Khair, F. Mustika, I. W. Zulherman, D. Hario, “Performance Analysis of Indoor Light Fidelity Technology Propagation Using Fixed and Movable LED Panels,” *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 2, pp. 1–13, Feb. 2023, doi: 10.22266/ijies2023.0430.01.

[11] D. G. Paspalaris, “Application and feasibility of Light Fidelity (LiFi) and power line communications (PLC) on U.S. Navy ships,” *(Doctoral dissertation, Monterey, California Naval Postgraduate School)*, 2019.

[12] Statista, “Light fidelity (Li-Fi) market revenue worldwide in 2017 and 2028,” by application. Available:: https://wwwstatistacom/statistics/965950/global-li-fi-market-by-application/. (Accessed on March 8, 2024).

[13] V. S. Gunge and P. S. Yalagi, “Smart Home Automation: A Literature Review,” *International Journal of Computer Applications*, 2016, doi: 10.5120/ijca2016911192.

[14] A. C. Jose and R. Malekian, “Smart Home Automation Security: A Literature Review,” *The Smart Computing Review*, vol. 5, no. 4, Aug. 2015, doi: 10.6029/smartcr.2015.04.004.

[15] A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smart home automation system,” *Future Generation Computer Systems*, vol. 56, pp. 719–733, Mar. 2016, doi: 10.1016/j.future.2015.09.003.

[16] S. Uma, R. Eswari, R. Bhuvanya, and G. S. Kumar, “IoT based Voice/Text Controlled Home Appliances,” *Procedia Computer Science*, vol. 165, pp. 232–238, 2019, doi: 10.1016/j.procs.2020.01.085.

[17] M. Yasir, S.-W. Ho, and B. N. Vellambi, “Indoor Positioning System Using Visible Light and Accelerometer,” *Journal of Lightwave Technology*, vol. 32, no. 19, pp. 3306–3316, Oct. 2014, doi: 10.1109/JLT.2014.2344772.

[18] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, “IoT based smart security and home automation system,” in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, IEEE, Apr. 2016, pp. 1286–1289, doi: 10.1109/CCAA.2016.7813916.

[19] A. J. Chinchawade and K. Sujatha, “Li-Fi Based Audio Transmission with Home/Office Automation System,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, no. 4, 2016, doi: 10.13140/RG.2.2.34531.25120.

[20] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, “A review of smart home applications based on Internet of Things,” *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, Nov. 2017, doi: 10.1016/j.jnca.2017.08.017.

[21] N. Malik and Y. Bodwade, “Literature Review on Home Automation System,” *IJARCCE*, vol. 6, no. 3, pp. 733–737, Mar. 2017, doi: 10.17148/IJARCCE.2017.63173.

[22] X. Wu, M. Safari and H. Haas, "Access Point Selection for Hybrid Li-Fi and Wi-Fi Networks," in *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5375-5385, Dec. 2017, doi: 10.1109/TCOMM.2017.2740211

[23] P. Šul'aj, R. Haluška, L. Ovseník, S. Marchevský, A. Firouzian and V. Kramar, "An Example of Li-Fi Technology Implementation for Home Automation," *2018 World Symposium on Digital Intelligence for Systems and Machines (DISA)*, Košice, Slovakia, 2018, pp. 183-187, doi: 10.1109/DISA.2018.8490607.

[24] L. I. Albraheem, L. H. Alhudaithy, A. A. Aljaser, M. R. Aldhafian, and G. M. Bahliwah, “Toward Designing a Li-Fi-Based Hierarchical IoT Architecture,” *IEEE Access*, vol. 6, pp. 40811–40825, 2018, doi: 10.1109/ACCESS.2018.2857627.

[25] R. Shanmughasundaram, S. P. Vadanan, and V. Dharmarajan, “Li-Fi Based Automatic Traffic Signal Control for Emergency Vehicles,” in *2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, IEEE, Feb. 2018, pp. 1–5, doi: 10.1109/ICAECC.2018.8479427.

[26] T. Molla, B. Khan, and P. Singh, “A comprehensive analysis of smart home energy management system optimization techniques,” *Journal of Autonomous Intelligence*, vol. 1, no. 1, p. 15, Oct. 2018, doi: 10.32629/jai.v1i1.14.

[27] P. K. Sharma, S. Rathore, and J. H. Park, “DistArch-SCNet: Blockchain-Based Distributed Architecture with Li-Fi Communication for a Scalable Smart City Network,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 55–64, Jul. 2018, doi: 10.1109/MCE.2018.2816745.

[28] K. Agarwal, A. Agarwal, and G. Misra, “Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT,” in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Dec. 2019, pp. 629–633, doi: 10.1109/I-SMAC47947.2019.9032629.

[29] S. Ismail, N. Ahmad, and I. D. Arshad, “Implementation of Li-Fi based home automation system,” *IOP Conference Series: Materials Science and Engineering*, vol. 767, no. 1, p. 012051, Feb. 2020, doi: 10.1088/1757-899X/767/1/012051.

[30] I. Romdhane and H. Yuksel, “A low-complexity security technique in physical layer for fixed LiFi communication systems,” *Journal of Information Security and Applications*, vol. 53, p. 102514, Aug. 2020, doi: 10.1016/j.jisa.2020.102514.

[31] D. N. Mekuria, P. Sernani, N. Falcionelli, and A. F. Dragoni, “Smart home reasoning systems: a systematic literature review,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 4, pp. 4485–4502, Apr. 2021, doi: 10.1007/s12652-019-01572-z.

[32] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, “An IoT-Based Smart Home Automation System,” *Sensors*, vol. 21, no. 11, p. 3784, May 2021, doi: 10.3390/s21113784.

[33] A. Thaljaoui, S. El Khediri, S. Zeadally, and A. Alourani, “Remote monitoring system using Light Fidelity and InfraRed technologies,” *Computers and Electrical Engineering*, vol. 101, p. 108073, Jul. 2022, doi: 10.1016/j.compeleceng.2022.108073.

[34] D. D. Diambeki, R. E. Mandiya, K. Kyamakya, and S. K. Kasereka, “Securing the light escaping in a Li-Fi network environment,” *Procedia Computer Science*, vol. 201, pp. 684–689, 2022, doi: 10.1016/j.procs.2022.03.091.

[35] S. Gupta, M. Sarkar, H. Kaur, M. Agrebi, and A. Roy, “An Efficient Data Transferring Through Li-Fi Technology: A Smart Home Appliance,” *Procedia Computer Science*, 2022, pp. 59–78, doi: 10.1007/978-981-19-0924-5_4.

[36] H. Singh, V. Pallagani, V. Khandelwal, and U. Venkanna, “IoT based smart home automation system using sensor node,” in *2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, IEEE, Mar. 2018, pp. 1–5, doi: 10.1109/RAIT.2018.8389037.

[37] J. Daemen and V. Rijmen, *The Design of Rijndael*. in Information Security and Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020, doi: 10.1007/978-3-662-60769-5.

[38] M. Tunstall, “Practical complexity differential cryptanalysis and fault analysis of AES,” *Journal of Cryptographic Engineering*, vol. 1, no. 3, pp. 219–230, Nov. 2011, doi: 10.1007/s13389-011-0018-7.

BIOGRAPHIES OF AUTHORS

Hakan Aydin obtained his undergraduate degree in Electrical and Electronics Engineering in 1993, followed by two Master’s degrees in Software Engineering in 2003 and International Relations in 2005, respectively. He earned his Ph.D. in Information Management from Hacettepe University in 2017. His research encompasses information security and cryptology, artificial intelligence, and computer software. He can be contacted at email: hakanaydin@topkapi.edu.tr.

Gülsüm Zeynep Gürkas Aydin completed her undergraduate degree in Computer Engineering at Istanbul University’s Faculty of Engineering in 2003. She received the M.Sc. degree in computer engineering from Istanbul University in 2005. She earned her first Ph.D. in Computer Engineering from Istanbul University’s Institute of Science in 2011 and her second Ph.D. in Informatique from Universit´e Pierre-et-Marie-Curie: Paris VI, France, in 2014. Her research covers a wide range of topics in computer science and engineering. She can be contacted at email: zeynepg@iuc.edu.tr.

Muhammed Ali Aydin completed his undergraduate degree in Computer Engineering at Istanbul University’s Faculty of Engineering in 2001. He earned his Master’s and Ph.D. degrees in Computer Engineering from Istanbul Technical University and Istanbul University, respectively. His research encompasses cybersecurity, software, internet of things, computer networks, and communications. He can be contacted at email: aydinali@iuc.edu.tr.