DOI 10.7251/ZRSNG2525056S

Li-Fi Technology for Cybersecurity Solutions + SEON

Ljubinko Stojanović[1], Vesna Radojčić[1], Srđan Mitrović[2], Petar Spalević[1], Sinergija University[1], Bijeljina; Singidunum University[2], Belgrade

Abstract – In an epoch wherein the significance of cybersecurity has reached paramount importance, Li-Fi (Light Fidelity) emerges as a highly promising wireless communication paradigm that leverages visible light for the purpose of data transmission. In contrast to Wi-Fi, which is predicated on radio frequencies, Li-Fi utilizes the modulation of LED light to facilitate high-speed, secure, and interference-free connectivity. This manuscript investigates the operational principles of Li-Fi, its advantages, limitations, and prospective applications across diverse domains, including healthcare, transportation, and industrial settings. Notable advantages encompass augmented security, enhanced efficiency, and diminished electromagnetic interference, rendering Li-Fi a viable alternative in sensitive contexts such as medical facilities and aviation environments. Nonetheless, obstacles such as restricted range and reliance on light sources impede its extensive adoption. Furthermore, the manuscript addresses fraud prevention strategies in digital transactions, underscoring the pivotal role of SEON in the identification and alleviation of cyber threats. By amalgamating Li-Fi with advanced cybersecurity frameworks, the research accentuates innovative solutions for secure and efficient digital communication. The conclusions indicate that Li-Fi, in conjunction with robust cybersecurity infrastructures, has the potential to markedly improve the security and efficiency of data transmission within the continuously evolving digital milieu.

Keywords – Li-Fi (Light Fidelity); SEON; Cybersecurity; Fraud prevention; Risk Management

I. INTRODUCTION

In a contemporary epoch wherein the internet has become intricately woven into every dimension of our existence—encompassing business operations, personal communications, commerce, healthcare, and beyond—the significance of cybersecurity is increasingly paramount. The escalating prevalence of cyber threats, including but not limited to hacking, phishing, ransomware, and data breaches, presents considerable hazards to individuals, corporate entities, and governmental institutions.

Cybersecurity denotes the systematic endeavour to safeguard systems, networks, and information against digital incursions. Such incursions typically seek to illicitly access, modify, or obliterate sensitive data, extort financial resources from users, or disrupt the continuity of standard business functions. The fundamental objective of cybersecurity is to uphold the confidentiality, integrity, and availability of information. This entails that access to particular data should be restricted solely to authorized individuals, that the data must remain precise and unaltered except when permitted, and that the data should be accessible to authorized users at all requisite times.

Li-Fi (Light Fidelity) represents a novel wireless communication paradigm that utilizes visible light, infrared, or ultraviolet wavelengths for data transmission. In contrast to conventional Wi-Fi [1], which depends on radio frequency signals, Li-Fi utilizes the modulation of optical waves to disseminate information. Scholars contend that Li-Fi technologies will facilitate more dependable wireless communication by virtue of this modulation technique. This modulation entails the rapid oscillation of the luminosity of LED (Light Emitting Diode) [1], [2] light sources, thereby encoding information in binary form—comprising 1s and 0s—through these intensity variations. Li-Fi systems are composed of transmitters (predominantly LED bulbs [3]) and receivers (devices equipped with Li-Fi capabilities) that are furnished with photodetectors to decode the optical signals. By capitalizing on the inherent properties of light, Li-Fi presents the possibility of high-velocity data transfer, augmented by the benefits of enhanced security and diminished electromagnetic interference.

It is accurate to assert that light fidelity is an emerging technology that has not yet achieved widespread adoption; nevertheless, it has demonstrated itself to be an exceptional solution for wireless communication, offering advantages such as superior cybersecurity and elevated data transmission rates while possessing a bandwidth sufficiently expansive to meet the continually increasing demand for global connectivity. Through the innovative application of light beams for data transport, light fidelity can be seamlessly integrated into preexisting lighting infrastructures. Furthermore, the technology utilizes LED bulbs for data transmission, distinguishing itself from other alternative internet solutions by enabling wireless connectivity to attain unprecedented levels of environmental sustainability. Although Wi-Fi continues to dominate the domain of wireless connectivity, the exploration of wireless alternatives, including Li-Fi, can unveil opportunities for more rapid and clearer communication. In particularly specialized contexts where there is heightened demand for uninterrupted streaming, alternative internet technologies may vary from the high-speed, secure data transmission capabilities of Li-Fi to the extensive-range, low-power functionalities of LoRaWAN [4], [5], [6]. Each technological solution presents distinct advantages that can be harnessed to augment connectivity within everyday

applications, such as in healthcare, transportation, and personal sectors. As the landscape of wireless technology perpetually evolves, remaining cognizant of alternative internet solutions, including Li-Fi, ensures that the most robust options for office or home connectivity deliver uniquely swift communication, enhanced security [7], and efficient data transfer amidst an ever-expanding telecommunications ecosystem.

II. LI-FI TECHNOLOGY

Li-Fi technology is a wireless communication system based on the use of visible light between the violet (800 THz) and red (400 THz) [3], [8], [9]. Unlike Wi-Fi which uses the radio part of the electromagnetic spectrum, Li-Fi uses the optical spectrum i.e. Visible light part of the electromagnetic spectrum [6]. The principle of Li-Fi is based on sending data by amplitude modulation of the light source in a well-defined and standardized way. LEDs can be switched on and off faster than the human eyes can detect since the operating speed of LEDs is less than 1 microsecond. This invisible on-off activity enables data transmission using binary codes. If the LED is on, a digital 1 is transmitted and if the LED is off, a digital 0 is transmitted [2]. Also these LEDs can be switched on and off very quickly which gives us a very nice opportunity for transmitting data through LED lights, because there are no interfering light frequencies like that of the radio frequencies in Wi-Fi. Li-Fi is thought to be 80% more efficient, which means it can reach speeds of up to 1Gbps and even beyond [9]. Li-Fi differs from fibre optic because the Li-Fi protocol layers are suitable for wireless communication over short distances (up to 10 meters). This puts Li-Fi in a unique position of extremely fast wireless communication over short distances.

There are numerous applications of Li-Fi technology, from public Internet access through existing lighting (LED) to auto-piloted cars that communicate through their headlights (LED based). Applications of Li-Fi can extend in areas where the Wi-Fi technology lacks its presence like aircrafts and hospitals (operation theatres), power plants and various other areas [10], where electromagnetic (Radio) interference is of great concern for safety and security of equipments and people. Since Li-Fi uses just the light, it can be used safely in such locations or areas. In future with the Li-Fi enhancement all the street lamps can be transformed to Li-Fi connecting points to transfer data. As a result of it, it will be possible to access internet at any public place and street.

Li-Fi, which uses visible light to transmit signals wirelessly, is an emerging technology poised to compete with Wi-Fi. Also, Li-Fi removes the limitations that have been put on the user by the Radio wave transmission such as Wi-Fi. Advantages of Li-Fi technology include:

a) Efficiency [11]: Energy consumption can be minimised with the use of LED illumination which are already available in the home, offices and Mall etc. for lighting purpose. Hence the transmission of data requiring negligible additional power, which makes it very efficient in terms of costs as well as energy.

b) High speed: Combination of low interference, high bandwidths and high-intensity output, help Li-Fi provide high data rates [3] i.e. 1 Gbps or even beyond [12].

c) Availability [11]: Availability is not an issue as light sources are present everywhere. Wherever there is a light source, there can be Internet. Light bulbs are present everywhere – in homes, offices, shops, malls and even planes, which can be used as a medium for the data transmission [3].

d) Cheaper: Li-Fi not only requires fewer components for its working, but also uses only a negligible additional power for the data transmission.

e) Security [11]: One main advantage of Li-Fi is security. Since light cannot pass through opaque structures, Li-Fi internet is available only to the users within a confined area and cannot be intercepted and misused, outside the area under operation [13].

f) Li-Fi technology has a great scope in future. The extensive growth in the use of LEDs for illumination indeed provides the opportunity to integrate the technology into a plethora of environments and applications.

Some of the major limitations of Li-Fi are:

- Internet cannot be accessed without a light source. This could limit the locations and situations in which Li-Fi could be used.
- It requires a near or perfect line-of-sight to transmit data
- Opaque obstacles on pathways can affect data transmission
- Natural light, sunlight, and normal electric light can affect the data transmission speed
- Light waves do not penetrate through walls and so Li-Fi has a much shorter range than Wi-Fi
- High initial installation cost, if used to set up a full-fledged data network.
- Yet to be developed for mass scale adoption[14].

Some of the future applications of Li-Fi could be as follows:

a) Education systems: Li-Fi is the latest technology that can provide fastest speed for Internet access. So, it can augment/replace Wi-Fi at educational institutions and at companies so that the people there can make use of Li-Fi with the high speed.

b) Medical Applications: Operation theatres (OTs) do not allow Wi-Fi due to radiation concerns. Usage of Wi-Fi at hospitals interferes/blocks the signals for monitoring equipments. So, it may have hazardous effect to the patient's health, due to improper working of medical apparatus. To overcome this and to make OT tech savvy Li-Fi can be used to access internet and also to control medical equipments. This will be beneficial for conducting robotic surgeries and other automated procedures [9].

c) Cheaper Internet in Aircrafts: The passengers travelling in aircrafts get access to low speed Internet that too at a very high price. Also Wi-Fi is not used because it may interfere with the navigational systems of the pilots. In aircrafts Li-Fi

can be used for data transmission. Li-Fi can easily provide high speed Internet via every light source such as overhead reading bulb, etc. present inside the airplane [10], [15].

d) Underwater applications[16]: Underwater ROVs (Remotely Operated Vehicles) operate from large cables that supply their power and allow them to receive signals from their pilots above. But the tether used in ROVs is not long enough to allow them to explore larger areas. If their wires were replaced with light — say from a submerged, highpowered lamp — then they would be much freer to explore. They could also use their headlamps to communicate with each other, processing data autonomously and sending their findings periodically back to the surface. Li-Fi can even work underwater where Wi-Fi fails completely, thereby throwing open endless opportunities for military underwater operations [17].

e) Disaster management: Li-Fi can be used as a powerful means of communication in times of disaster such as earthquake or hurricanes. The average people may not know the protocols during such disasters. Subway stations and tunnels, common dead zones for most emergency communications, pose no obstruction for Li-Fi [13].

f) Applications in sensitive areas: Power plants need fast, inter-connected data systems so that demand, grid integrity and core temperature (in case of nuclear power plants) can be monitored. The Radio communication interference is considered to be bad for such sensitive areas surrounding these power plants. Li-Fi can offer safe, abundant connectivity for all areas of these sensitive locations. Also, the pressure on a power plant‘s own reserves (power consumption for Radio communications deployments) will be lessened.

g) Traffic management [18]: In traffic signals Li-Fi can be used to communicate with passing vehicles (through the LED lights of the cars etc) which can help in managing the traffic in a better manner resulting into smooth flow of traffic and reduction in accident numbers. Also, LED car lights can alert drivers when other vehicles are too close.

h) Mobile Interconnectivity: Personal devices such as smartphones, laptops, and tablets can seamlessly establish connections among themselves [19]. The short-range network facilitated by Li-Fi can provide remarkably high data transmission rates coupled with enhanced security features.

i) Replacement for other technologies: Li-Fi does not work using radio waves. So, it can be easily used in the places where Bluetooth, infrared, Wi-Fi, etc. are banned. Furthermore, LED automotive lighting systems can serve as a warning mechanism for drivers when other vehicles are in close proximity.

III. SEON

SEON represents a platform dedicated to fraud prevention and risk management, with a particular focus on verifying digital identities and monitoring transactions within the realm of online commerce.

In the modern digital marketplace, payment gateways have become an integral aspect of the infrastructure that supports online transactions. Their essential role involves serving as intermediaries between e-commerce vendors and financial institutions, thereby authorizing and facilitating the secure movement of funds from consumers to merchants. In contrast to payment processors, which are primarily concerned with the transmission of transaction data between acquiring and issuing banks, payment gateways undertake an additional security role by authenticating transactions in real time. They utilize encryption protocols, tokenization, and 3D Secure (3DS2) authentication to mitigate risks associated with card-not-present (CNP) transactions.

Feature	Description
Digital Footprint	Enriches data by analyzing email, phone, and IP addresses to assess user legitimacy.
Velocity Rules	Limits rapid attempts at logins, sign-ups, and payments that may indicate bots or automated attacks.
Custom Risk Scoring	Tailors fraud detection rules for different industries and risk profiles.
Consortium Data	Uses anonymized data from SEON’s network to detect global fraud patterns.
Real-Time Transaction Monitoring	Detects suspicious transactions as they occur.

Table 1. Key Features of SEON

Payment gateways scrutinize transaction data, including cardholder authentication, billing address validation, and device fingerprinting, to detect potentially fraudulent activities prior to the authorization of payments. Moreover, gateways such as Stripe, Worldpay, and PayPal incorporate fraud scoring engines that harness machine learning algorithms to categorize transactions according to their risk profiles [3].

The dependence on SSL encryption guarantees that sensitive data—such as primary account numbers (PANs) and Card Verification Values (CVVs)—is encrypted during transmission, thereby diminishing the probability of data interception [20]. Tokenization further bolsters security by replacing sensitive card information with a unique token that lacks utility if compromised. Nevertheless, in spite of these protective provisions, payment gateways continue to be targets for cybercriminals who exploit vulnerabilities through identity theft, BIN attacks, account takeovers, and card testing.

Fraudsters utilize a range of techniques to infiltrate payment gateways. Comprehending these typologies is vital for devising effective countermeasures. Identity theft entails the unauthorized acquisition and utilization of another individual’s personal and financial information to execute fraudulent transactions. Criminals frequently employ phishing, malware, and social engineering tactics to harvest sensitive information from unsuspecting individuals. Once this data is obtained, fraudsters can circumvent standard authentication protocols and finalize illicit transactions. Advanced fraud detection instruments utilizing multi-factor

authentication (MFA), biometric verification, and behavioural analytics can significantly mitigate the risks associated with identity theft [20]. A Bank Identification Number (BIN) attack involves generating a plethora of valid card numbers by exploiting the initial six digits, which denote the issuing bank and card type. Fraudsters employ automated scripts or bots to systematically test these numbers on merchant websites, seeking out active card numbers. These card numbers are subsequently sold on the dark web or utilized in future fraudulent transactions. Card testing, a related technique, employs similar automated methods to validate the authenticity of compromised card data by executing minor transactions on unsuspecting merchant platforms. Account Takeover (ATO) transpires when cybercriminals gain unauthorized access to legitimate user accounts on e-commerce platforms. Such takeovers typically result from credential stuffing or phishing attacks, wherein fraudsters exploit poor password practices or compromised databases. Once access is secured, fraudsters may make purchases using stored payment information, deplete loyalty points, or resell account access. Behavioural biometrics, IP geolocation analysis, and device fingerprinting are crucial in identifying anomalies that indicate an ATO attempt.

Friendly fraud manifests when a cardholder contests a transaction even though the card in question has not been misappropriated. In contrast to authentic card-not-present (CNP) fraud, where nefarious individuals exploit stolen card information for illicit purchases, friendly fraud implicates the bona fide cardholder. This phenomenon can present itself in various manifestations, such as “family fraud,” wherein a relative, such as a minor, utilizes the card without authorization—illustratively, executing app purchases through a parent’s account. Another variant, frequently referred to as “first-party fraud,” transpires when a cardholder inadvertently initiates a chargeback, potentially due to forgetfulness regarding the original purchase. In certain instances, friendly fraud is premeditated, with the cardholder deceitfully asserting that a legitimate transaction was unauthorized to obtain a reimbursement. Irrespective of the context, friendly fraud poses significant challenges for businesses seeking to contest such claims. Establishing whether a transaction was executed with intent, constituted an honest error, or was unauthorized by an individual closely associated with the cardholder can be an intricate and resource-demanding undertaking.

Bonus abuse, frequently discussed within the realms of online gaming or gambling, denotes the practice whereby individuals manipulate promotional incentives aimed at novice users, as offered by platforms, to derive unwarranted advantages or financial gains. This phenomenon represents a complex variant of fraud that exploits weaknesses inherent in operators [20] protocols, facilitating the misuse of promotional incentives specifically crafted for new participants. This unethical conduct, also known as promotional abuse, multi-accounting, or bonus hunting, specifically targets an array of bonus offerings, including additional funds, new user sign-ups, complimentary spins, no-deposit bonuses, and other incentives aimed at enticing new users or rewarding loyal clientele.

Individuals engaged in bonus abuse adeptly navigate these promotions through methodologies such as the establishment of multiple user accounts, collusion with others, or the application of betting patterns that mitigate risk while maximizing the advantages derived from these bonuses. Such actions contravene the stipulated terms and conditions of the platforms and may result in penalties such as account suspension, the forfeiture of winnings, and, in extreme instances, legal repercussions. Fundamentally, bonus abuse subverts the intended essence of promotional offers, engendering an imbalanced competitive landscape and potentially inflicting financial and reputational harm upon the service providers.

Seven Types of Popular Bonus Offers Bonus offerings constitute a conventional strategy employed by operators to attract and retain participants. Presented here are the seven predominant types of bonus offerings that are frequently targeted:

- Sign-Up Bonuses,
- No-Deposit Bonuses,
- Deposit Match Bonuses,
- Free Spin Bonuses,
- Refer-a-Friend Bonuses,
- Loyalty Bonuses,
- High-Roller Bonuses.

Strategies for Bonus Abuse Prevention and Detection Operators are compelled to implement innovative strategies to combat the fraudulent phenomenon of bonus abuse, thereby ensuring a secure and equitable environment for players. By harnessing advanced analytics and machine learning techniques, operators can identify and preempt fraudulent behaviours by recognizing patterns characteristic of abuse.

Collaboration within the industry can further augment these initiatives, establishing a formidable defense against fraud through the exchange of insights and best practices. Equally imperative is the education of players regarding the risks and indicators of bonus abuse, transforming them into informed participants capable of assisting in the identification of dubious activities [20]. By integrating technological innovations, fostering industry collaboration, and enhancing player awareness, operators can cultivate a healthy gaming ecosystem.

Effective fraud detection within payment gateways necessitates the implementation of multi-tiered security measures, integrating real-time data analytics, artificial intelligence-driven models, and risk assessment frameworks. Below is an elucidation of pivotal technologies employed in contemporary fraud detection architectures. Device fingerprinting entails the accumulation of a detailed profile of an individual’s hardware and software ecosystem, encompassing browser versions, installed extensions, operating system specifications, and IP address. Each unique amalgamation of these attributes generates a distinct

device identifier, which facilitates the identification and monitoring of fraudulent activities.

```
Step 1: User Registration / Login
     ↓
Step 2: Data Enrichment
     - IP Analysis
     - Device Fingerprint
     - Digital Footprint (Email / Phone Social Media Check)
     ↓
Step 3: Risk Scoring Engine
     - Custom Rules
     - Machine Learning Models (Whitebox & Blackbox)
     ↓
Step 4: Decision Engine
     - Approve
     - Flag for Manual Review
     - Reject
```

Figure 1. SEON's Fraud Detection Workflow

Use case: Fraud perpetrators frequently utilize multiple identities across various accounts; however, they often operate from the same device. Device fingerprinting possesses the capability to correlate ostensibly unrelated transactions, revealing multi-accounting networks and organized fraud enterprises. IP analysis ascertains whether a user's IP address is authentic or dubious. Through the examination of connection metadata, systems can identify the employment of virtual private networks (VPNs), proxies, or Tor networks, which are frequently suggestive of fraudulent intent [20]. Geolocation verification guarantees that transactions emanate from anticipated geographical locales. Velocity assessments—which scrutinize the frequency and rapidity of login attempts or financial transactions—further assist in the identification of questionable actions. Digital footprinting consolidates behavioural and historical data across online platforms to authenticate user identities. SEON's Digital Footprint solution investigates social media profiles, email registries, and telecommunications data to evaluate whether an individual's digital persona corresponds to their transactional activity. The lack of a credible online presence frequently triggers alarms within fraud detection systems. Fraud prevention platforms deploy machine learning (ML) algorithms that are trained on extensive datasets of historical transaction information [20]. These algorithms continuously enhance their predictive capabilities, discerning patterns that are indicative of fraudulent behaviour. Whitebox models, which are transparent and yield interpretable decision trees, and Blackbox models, which are non-transparent yet highly adaptable, are routinely utilized to classify transactions in real time.

Integrated fraud prevention systems are embedded directly within payment gateway interfaces. For instance:
Stripe Radar evaluates transactional information throughout its network, harnessing collective intelligence from millions of global merchants. Worldpay's FraudSight offers comparable functionalities, employing real-time data streams and rule-based methodologies. These systems are particularly effective for small to medium-sized enterprises due to their user-friendly nature, low maintenance demands, and minimal configuration prerequisites [20]. They are ideally suited for organizations that lack dedicated fraud management teams. Nonetheless, these systems are not without their limitations. They frequently depend on inflexible, generalized regulations and do not provide the same level of customization or detailed control as third-party solutions. Moreover, merchants may face the risk of becoming entrenched within a specific ecosystem, complicating the migration of their fraud prevention strategies across diverse gateways [20].

Third-party providers present independent fraud prevention platforms that integrate seamlessly with multiple payment gateways [20]. SEON, for instance, offers a modular, API-driven solution that augments existing systems. These platforms provide customizable risk assessment models, machine learning functionalities, and data enrichment modules to enhance detection precision.

Criteria	Built-In Tools (e.g., Stripe Radar)	Third-Party Providers (e.g., SEON)
Customization	Limited to predefined rules	Fully customizable rules and risk scoring
Data Sources	Internal transaction data only	Multi-source data enrichment (social, telecom, IP, device)
Integration	Seamless (already built-in)	Requires API integration
Pricing	Often bundled with transaction fees	Transparent pricing, modular solutions
Flexibility	Tied to one gateway ecosystem	Works across multiple gateways and systems
Accuracy	Generic machine learning models	Industry-tailored machine learning models
Manual Review Tools	Basic	Advanced queue management and case review

Table 2. Comparison of Built-In Fraud Tools vs. Third-Party Providers [20]

Third-party tools also furnish cross-platform insights, which are vital for enterprises that operate across multiple geographical regions and utilize various payment service providers. They additionally facilitate adaptability in risk management, enabling businesses to refine fraud thresholds in response to evolving threat landscapes.

```
User Action
     ↓
API Request Sent to SEON Platform
     ↓
Core Modules
     - Device Fingerprint
     - IP Intelligence
     - Digital Footprint
     ↓
Data Enrichment Layer
     - External Data Sources (Social, Telecom, Email Repositories)
     ↓
Risk Score Output
     ↓
Client Dashboard
     - Approve / Reject / Manual Review
```

Figure 2. SEON's Technology Stack Integration

IV. CONCLUSION

Li-Fi technology constitutes a revolutionary paradigm in wireless communication, providing enhanced velocity, security, and efficiency in comparison to conventional Wi-Fi. Its utilization spans a multitude of sectors, including healthcare institutions, autonomous transportation, and emergency response systems. Notwithstanding its merits, obstacles such as signal interference, constrained operational range, and significant initial expenditures hinder its widespread adoption. The resolution of these challenges through progressive technological innovations will be pivotal in determining the future acceptance of Li-Fi. Furthermore, within the domain of digital security, fraud detection and mitigation systems, exemplified by SEON, play an essential role in alleviating risks linked to cyber threats. The integration of Li-Fi with sophisticated cybersecurity protocols can yield a fortified communication framework, thereby diminishing vulnerabilities inherent in data transmission. As the digital ecosystem perpetually evolves, the allocation of resources towards Li-Fi research and fraud deterrence technologies is crucial for realizing a more secure, efficient, and interconnected global society. Future investigations should prioritize the resolution of technical impediments and the enhancement of Li-Fi's versatility to ascertain its significance within next-generation communication infrastructures.

REFERENCES

[1] Haihong, Sheng & Sun, Junchang & Li, Hang & Xiaodong, Liu & Qiu, Chen & Safari, Majid & Al-Dhahir, N. & Li, Shiyin. (2024). Feasibility Conditions for Mobile LiFi. IEEE Transactions on Wireless Communications. pp. 1-2.

[2] Monzon Baeza, Victor & Arellano García, Rafael. (2023). LiFi Technology Overview: taxonomy, and future directions. pp. 2.

[3] Zad, Omkar & Rawool, Pragalbha & Bhavarthe, Dr & Makwana, Viral & Sawant, Tejas. (2023). Image and Text Transmission using Li-Fi Technology. International Journal of Advanced Research in Science, Communication and Technology. pp. 1996-1997.

[4] Cuozzo, Giampaolo & Marini, Riccardo & Buratti, Chiara & Mikhaylov, Konstantin. (2024). On the Support of the 2.4 GHz Band in the LoRaWAN Standard. IEEE Internet of Things Magazine. pp. 1-6.

[5] Balyan, Vipin. (2024). Priority-based resource allocation in layering LoRaWAN. International Journal on Smart Sensing and Intelligent Systems. pp. 1-3.

[6] Kumar, B. (2024). Revolutionizing Highway Navigation: Exploring the Potential of LIFI Technology. Communications on Applied Nonlinear Analysis. 32. pp. 598-603.

[7] Fesenko, Herman & Illiashenko, Oleg & Kharchenko, Vyacheslav & Leichenko, Kyrylo & Sachenko, Anatoliy & Scislo, Lukasz. (2024). Methods and Software Tools for Reliable Operation of Flying LiFi Networks in Destruction Conditions. Sensors. pp. 4-5.

[8] Hernández-Oregón, Gerardo & Rivero-Angeles, Mario & Chimal, Juan Carlos & Coyac-Torres, Jorge. (2023). Performance Analysis of P2P Networks with Light Communication Links: The Static Managed Case. Applied Sciences. 13. pp. 9.

[9] Shen, Yansen. (2024). LiFi Technology Application and Prospect in the Field of Medical. Highlights in Science, Engineering and Technology. pp. 79-81.

[10] Younis, Manal & Alwan, Zainab & Tareq, Zahraa. (2020): Data Transmission Using Li-Fi Technique. pp. 7368- 7369.

[11] Ganesan, Devi & Jayanthi, N. & Rahul, S. & Karthick, M. & Srinivasan, Gokul & Anand, M.. (2023). A critical review on Li-Fi technology and its future applications. AIP Conference Proceedings. pp. 6-7.

[12] Jurczak, Christophe. (2017). Review of LiFi visible light communications : research and use cases. pp. 11.

[13] Fesenko, Herman & Illiashenko, Oleg & Kharchenko, Vyacheslav & Leichenko, Kyrylo & Sachenko, Anatoliy & Scislo, Lukasz. (2024). Methods and Software Tools for Reliable Operation of Flying LiFi Networks in Destruction Conditions. Sensors. 24. 5707. pp. 5-8.

[14] Murad, Sallar & Badeel, Rozin & Ahmed, Reham. (2024). Is LiFi Technology Ready for Manufacturing and Adoption? An End-user questionnaire-based study. Applied Data Science and Analysis. 2024. pp. 99-105.

[15] R. Badeel, S. K. Subramaniam, Z. M. Hanapi, and A. Muhammed. (2021):A Review on LiFi Network Research: Open Issues, Applications and Future Directions, Appl. Sci., vol. 11, no. 23, pp. 11118.

[16] Muhammad, Aman & Qiao, Gang & Muzzammil, Muhammmad. (2021). Design and Analysis of Li-fi Underwater Wireless Communication System. pp. 1100-1101.

[17] Pavaloiu, Alice. (2016): The Impact of Artificial Intelligence on Global Trends. pp. 13-14.

[18] Sahy, Seba & Jaaz, Zahraa & Abdulshaheed, Haider. (2021). Traffic Management with Deployment of Li-Fi Technology. Journal of Physics Conference Series. pp. 2-3.

[19] Swami, Nitin & Sirsat, Narayan & Holambe, Prabhakar. (2016). Light Fidelity (Li-Fi): In Mobile Communication and Ubiquitous Computing Applications. pp. 89-81.

[20] SEON. (2024). Fraud Prevention Solutions for E-Commerce. Retrieved from https://docs.seon.io.