SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 1.1, (2026), pp. 4036-4052
Open Access. Online & Print

DOI: 10.5281/zenodo. 121126299

HYBRID LI-FI AND WI-FI SECURE TRANSMISSION MODEL FOR SMART COMMUNICATION SYSTEMS

Charanjit Kaur[1]*, Mithilesh Kumar Dubey[2], Sudha Dubey[3]

[1,2] Department of Computer Sciences and Engineering, Lovely Professional University, Phagwara, Punjab, India 144411.
[3] Department of Sociology,Lovely Professional University,Pagwara.Punjab,India 144411.

Received: 01/12/2025
Accepted: 02/01/2026

Corresponding author: Charanjit Kaur (kj169987@gmail.com)

ABSTRACT

The rapid growth of global internet users, surpassing 6 billion in 2025, alongside advancements in mobile and Wi-Fi connectivity, has underscored the need for innovative wireless communication technologies.This study investigates how Li-Fi and Wi-Fi can be combined in a hybrid network architecture, utilizing Wi-Fi's extensive infrastructure and Li-Fi's built-in security and high-speed capabilities.The proposed HCK algorithm enhances this hybrid system by implementing robust security measures, including RSA, AES, and ChaCha20 encryption, alongside authentication and non-repudiation protocols. Simulation results demonstrate the HCK algorithm's superior performance, achieving a throughput of 988.56, speed of 1468.68, bandwidth of 398.46, and a low packet drop rate of 0.018%, significantly outperforming existing algorithms. The hybrid network ensures scalability, energy efficiency, and security, addressing critical gaps in current systems, particularly for IoT applications. By combining Li-Fi's secure, interference-free transmission with Wi-Fi's mobility, this framework offers a scalable and reliable solution for modern connectivity demands.

KEYWORDS: Li-fi,Wi-fi,Text, Video, Image,Throughput,RSA

1. INTRODUCTION

Recent data reveals a more connected world than previously anticipated. The Cisco Visual Networking Index (CVNI) forecast of 5.3 billion internet users by 2023 has been surpassed. As of early 2024, there are 5.35 billion internet users, representing over 66% of the global population.By late 2025, the world had over 6 billion internet users, representing roughly 74% of the global population, Looking ahead,It is anticipated that the number of internet users will continue its upward trend, reaching an estimated 5.52 billion in 2024. This indicates a slightly faster growth trajectory than the 6% Compound Annual Growth Rate (CAGR) projected from 2018. [1]

The proliferation of mobile subscribers has also kept pace with predictions. According to the projection, by 2023, 71% of people on the planet would have mobile phone service. 69% of the world's population, or 5.6 billion people, had a mobile service subscription by the end of 2023. According to Ericsson's projections, there will be 8.51 billion mobile subscriptions globally in 2023, and by 2024, that number is predicted to rise to 8.66 billion. [2]

The growth of public Wi-Fi hotspots has been a key factor in expanding internet accessibility. While the initial forecast predicted a fourfold surge to nearly 628 million hotspots by 2023, the actual numbers show a varied landscape. In 2022, the global count of public Wi-Fi hotspots reached 549 million, a significant increase from 169 million in 2018. Market analysis indicates continued growth in the public Wi-Fi market, fueled by the growth of smart cities and the rising need for connectivity. [3]

Mobile network speeds have seen remarkable improvements, exceeding the projections for 2023. 43.9 Mbps is the anticipated average mobile network connection speed has been left behind. In 2023, mobile network speeds saw a significant leap, with the average overall download speed in some regions showing substantial increases. For instance, in the Asia Pacific (APAC) region, the average improvement was 5.2 Mbps, with countries like India seeing their average speeds more than triple due to rapid 5G rollout. By the end of 2023, South Korea's average download speed was a notable 140.2 Mbps. Data from early 2024 shows that the global median mobile download speed has continued to climb. In the US, for example, one major carrier's users saw average download speeds of 113.1Mbps in early 2024.

In a similar vein, Wi-Fi speeds have increased dramatically. The estimate for the typical Wi-Fi network connection speed to exceed 91.6 Mbps by 2023 appears to be on track, with some regions even surpassing this. The Asia Pacific region was correctly identified as a leader, with South Korea enjoying particularly high average mobile download speeds. For fixed broadband, which includes Wi-Fi, global median download speeds have also seen a dramatic rise. [4]

1.1. A Background Study on Li-Fi and Wi-Fi

Two technologies in the constantly growing field of wireless communication are Wi-Fi and Li-Fi, offer distinct approaches to data transmission. While Wi-Fi has become a ubiquitous standard, Li-Fi presents a compelling alternative, leveraging light to transmit information. This background study explores the fundamental principles, comparative advantages and disadvantages, and future trajectories of both technologies. [5]

Wi-Fi: The Established Standard of Radio-Based Connectivity

The wireless networking technology known as Wi-Fi, or Wireless Fidelity, uses radio waves to make it easier for devices to share data. Wi-Fi allows gadgets like smartphones, computers, and smart home appliances to connect to the internet and to one another via a wireless router or access point.2.4 GHz and 5 GHz are its main operating frequency ranges. Since its inception, the technology has come a long way, and new standards offer increased capacity, faster speeds, and improved efficiency. More recent models, like Wi-Fi 6 (802.11ax) and the soon-to-be released Wi-Fi 7 (802.11be), are designed to survive congested areas and bandwidth-demanding applications. [6]

1.2. Key Characteristics of Wi-Fi:

Mobility and Coverage: Wi-Fi's main benefit is its broad coverage, as radio waves can pass through barriers like walls. This makes it possible to move more freely within a specified area.

Established Infrastructure: Wi-Fi is currently a convenient and affordable alternative for the majority of consumers because of its extensive and easily accessible infrastructure, which has been the consequence of its global proliferation.

Device Compatibility: Smooth interoperability is ensured by a large network of devices with Wi-Fi capabilities.

Security: Protocols like WPA3 (Wi-Fi Protected Access 3) have improved Wi-Fi security by providing stronger defense against unwanted access.

1.3. Limitations of Wi-Fi:

Spectrum Congestion: Since the radio frequency spectrum is a limited resource, performance may be impacted by congestion and interference brought on by the growing number of Wi-Fi devices.

Security Vulnerabilities: Despite advancements, Wi-Fi networks remain susceptible to hacking, especially if not properly secured. The broadcast nature of radio waves means signals can be intercepted outside of the intended physical area.

Interference: Interference from other electronic devices using the same radio bands can reduce performance. [7]

1.4. Li-Fi: Using Light to Transmit Data at High Speed

A wireless communication technique called Li-Fi, or Light Fidelity, uses the visible light spectrum in addition to infrared and ultraviolet radiation to send data. LED light intensity is modulated by the technology at speeds that are invisible to the human eye.These flickers are interpreted as data by a photodetector on a receiving device. Professor Harald Haas came up with this novel idea in 2011, and it has several potential benefits over conventional radio-frequency-based systems. [8][9]

1.5. Key Characteristics of Li-Fi:

Speed and Bandwidth: The whole radio frequency spectrum that Wi-Fi uses is around 10,000 times smaller than the visible light spectrum. Theoretically, considerably faster data transfer speeds—possibly hundreds of gigabits per second—are made possible by this enormous capacity.

Enhanced Security: Li-Fi's intrinsic security is one of its main advantages. The visible light spectrum is approximately 10,000 times larger than the entire radio frequency band used by Wi-Fi. This massive capacity theoretically enables far quicker data transfer speeds, potentially reaching hundreds of gigabits per second. [10]

No Radio Frequency Interference: Li-Fi doesn't interfere with radio frequency communications because it uses light to function. This makes it perfect for places like hospitals, airplane cabins, and industrial settings where RF interference is an issue.

High Density: In densely populated areas, where Wi-Fi can suffer from congestion, each Li-Fi-enabled light source can act as a separate access point, offering a more robust and interference-free connection. [11]

1.6. Limitations of Li-Fi:

Line-of-Sight Requirement: Li-Fi's need on a direct line of sight between the light source and the receiving device is its biggest drawback. The signal may be blocked by any impediment. [12]

Limited Range: A single Li-Fi access point's effective range is restricted to the region that the light source illuminates. A dense network of Li-Fi-enabled lights would be required for widespread coverage.

Infrastructure and Compatibility: While Li-Fi can leverage existing LED lighting infrastructure, it requires specialized transmitters and receivers. The technology is still relatively new, and the ecosystem of compatible devices is limited compared to Wi-Fi.

Ambient Light Interference: Strong light sources, such as direct sunshine, may disrupt the Li-Fi signal. [13]

The Future Landscape: Coexistence and Integration

While Li-Fi offers compelling advantages in specific scenarios, it is unlikely to completely replace Wi-Fi will be available soon. Rather, a hybrid approach is probably what wireless communication will look like in the future, with Wi-Fi and Li-Fi enhancing each other's advantages. Wi-Fi is still evolving, with an emphasis on faster speeds, reduced latency, and more capacity to accommodate the expanding Internet of Things (IoT) ecosystem. For seamless connectivity in a variety of settings, Wi-Fi integration with 5G and upcoming 6G networks will be essential.

Li-Fi is poised for significant growth in niche applications where its unique benefits are paramount. Real-world trials and applications are already underway in various sectors:

Healthcare: Providing secure, interference-free connectivity for medical devices.

Aviation: Offering in-flight connectivity without RF interference.

Defense and Security: Ensuring highly secure data transmission in sensitive environments.

Smart Cities: Utilizing streetlights to provide public internet access.

Underwater Communication: Where radio waves are ineffective, light can be used for data transmission.

For widespread adoption, Li-Fi technology must overcome challenges related to standardization, manufacturing costs, and public awareness.The development of Li-Fi-enabled devices will also be critical for its integration into the mainstream market.[14]

1.7. Research Gap

Current hybrid network schemes, while achieving impressive handover efficiency with low latency, lack comprehensive security frameworks, particularly in implementing robust hybrid encryption (AES, RSA) and authentication protocols to protect Wi-Fi components from eavesdropping and data breaches. Additionally, energy efficiency considerations for Li-Fi access points integrated with lighting systems are underexplored, limiting sustainable deployment. Scalability issues for diverse IoT applications remain

unaddressed, as do Quality of Service (QoS) mechanisms for managing varied traffic types. Furthermore, the potential benefits of emerging technologies such as AI-driven optimization and advanced modulation techniques like DCO-OFDM have not been sufficiently integrated, leaving significant gaps in performance enhancement and network adaptability. Addressing these gaps is essential to develop secure, scalable, energy-efficient, and intelligent hybrid networks suitable for real-world applications. [15][16]

2. LITERATURE REVIEW

This study suggests a GPS and GSM-enabled Li-Fi-based V2V communication system for fleet management.LEDs transmit speed and direction data between vehicles at high speed, ensuring safe and energy-efficient operation.When Li-Fi communication is lost, GPS tracking and GSM alerts provide the vehicle's location to the leader and base station.The system uses a low-power TI MSP430F5529 microcontroller for efficient control and reduced operating costs. Results show improved reliability, eco-friendliness, and potential for scalable, real-time intelligent transportation.17

This paper proposes a secure Li-Fi communication system using a hybrid encryption approach that combines ChaCha20 for fast symmetric encryption and RSA for robust asymmetric key protection. The system design integrates Li-Fi with Free Space Optics (FSO) and fiber optic channels, employing simulation via OptiSystem and MATLAB to validate performance. The hybrid algorithm encrypts the data with ChaCha20 and secures the ChaCha20 key with RSA, achieving both speed and high security. Experimental results show extremely low bit error rates, high Q-factor, and rapid encryption/decryption time of 0.036 seconds. This approach strengthens Li-Fi's inherent security against cyber threats while ensuring reliability for high-speed, sensitive data transmission.18

By creating a hybrid encryption method that combines RSA for secure key exchange with ChaCha20 for quick data encryption, this work improves the security of Li-Fi connection..The system integrates Li-Fi with Free Space Optics and fiber optic channels, simulated using OptiSystem and MATLAB for performance validation. ChaCha20 encrypts the message while RSA secures the ChaCha20 key, ensuring confidentiality and integrity. Results show a very low bit error rate, high Q-factor, and an execution time of only 0.036 seconds. The approach significantly strengthens Li-Fi against cyber threats,making it appropriate for transmitting sensitive data at fast speeds.19

In order to address the growing cybersecurity threats in Industrial Control Systems (ICS), such as False Data Injection (FDI) attacks, this study suggests a novel Li-Fi technology-based solution. According to the authors' architectural model, Li-Fi is used to communicate the most crucial data links, such as those between the Interface between the Human and Machine (HMU) and the master terminal unit (MTU). The system incorporates a two-factor authentication procedure using specialized hardware dongles and IEEE 802.1X standards to increase security and ensure that only authorized devices and users may access the network. This method uses Li-Fi's built-in physical security to prevent common threats like MitM and eavesdropping because light signals are restricted to a physical area.In the end, the study shows that network forensics can be facilitated while ICS data security and integrity are preserved by utilizing a secured Li-Fi architecture.20

This study investigates the use of Light Fidelity (Li-Fi) as a safe and efficient alternative to Wi-Fi in Internet of Things applications to enhance audio data transfer. The researchers constructed a simple Li-Fi circuit that transforms audio into optical signals and uses solar cells to transmit them in order to show that it is feasible. The results demonstrated that Li-Fi performed better because it can withstand radio frequency interference, particularly in networks with high traffic. This study demonstrates how Li-Fi could improve audio quality and security as a proof-of-concept. Although more research is required to fully realize its potential, the study concludes that Li-Fi is a promising and practical approach for future IoT data transfer.21

This study investigates a safe and efficient Wi-Fi alternative for Internet of Things applications. Application of Light Fid The approach for handling the handover process in 5G networks with Visible Light Communications (VLC), commonly referred to as Li-Fi, is presented in this paper. Li-Fi has been suggested as a possible substitute when the radio frequency spectrum becomes more saturated as a result of the expansion of IoT and IoE. The project's goal is to guarantee users' uninterrupted connectivity and smooth mobility in an indoor setting.The proposed framework utilizes steerable Access Points (APs) to manage the handover process when a user moves between coverage areas. This work aims to enhance handover performance and minimize connection loss, thereby tackling a significant challenge for the practical deployment of Li-Fi in mobile settings.22

This paper investigates Li-Fi technology as a secure alternative to Wi-Fi for high-speed data transmission,

addressing the security vulnerabilities and spectrum limitations of traditional radio-frequency networks. The authors discuss the inherent security of Li-Fi, which stems from the line-of-sight nature of light, preventing data leakage through walls.The article compares LS and MMSE channel estimation techniques and examines the Bit-Error Rate (BER) performance using a simulation employing OFDM modulation.

The results demonstrate Li-Fi's potential for significantly higher data rates and improved security over Wi-Fi. The paper concludes that Li-Fi is a more secure and reliable communication method, summarizing its security advantage as simply "shutting the door" to external threats.23

This study presents Light-Fidelity (Li-Fi), a fast and safe substitute for traditional Wi-Fi in wireless data transfer.

It highlights the security weaknesses of Wi-Fi, which is susceptible to interception and attacks, and contrasts this with Li-Fi's inherent security due to its use of light waves that cannot penetrate walls. The study's objective is to showcase Li-Fi's capability to create highly secure network zones with significantly faster data transfer rates, proven by lab tests achieving speeds far exceeding Wi-Fi. It reviews Li-Fi's applications, particularly where security and RF interference are major concerns, such as in medical and military settings. The paper concludes that Li-Fi, using Visible Light Communication (VLC), offers a more reliable and secure architecture, effectively addressing the data leakage and hijacking risks associated with Wi-Fi.24

This paper details the implementation of a basic Li-Fi system to demonstrate Visible light is used to convey data between two computers. A silicon photodiode serves as the system's receiver, and a high-brightness LED serves as its transmitter., managed by a simple circuit. Data from the sending computer is converted into byte format, which then modulates the LED's light signals in rapid on-off patterns. The photodiode on the receiving end detects these light signals, and a reverse process retrieves the original data. This project successfully showcases the fundamental working principle of a simple, secure, line-of-sight Li-Fi communication system.25

Table 1: Comparative analysis

Ref.	Year	Author Name	Input Data Available		
			Text	Image	Video
28.	2022	Sanket Salvi et al.	☑	☑	☒
29.	2022	Hamis Hesham et. al	☑	☒	☒
30.	2020	K.MD et al.	☑	☒	☒
31.	2018	Pardeep Kumar et al.	☑	☑	☒
49.	2012	Min Xing et. al	☒	☒	☑
Proposed	2025	HCK Algo	☑	☑	☑

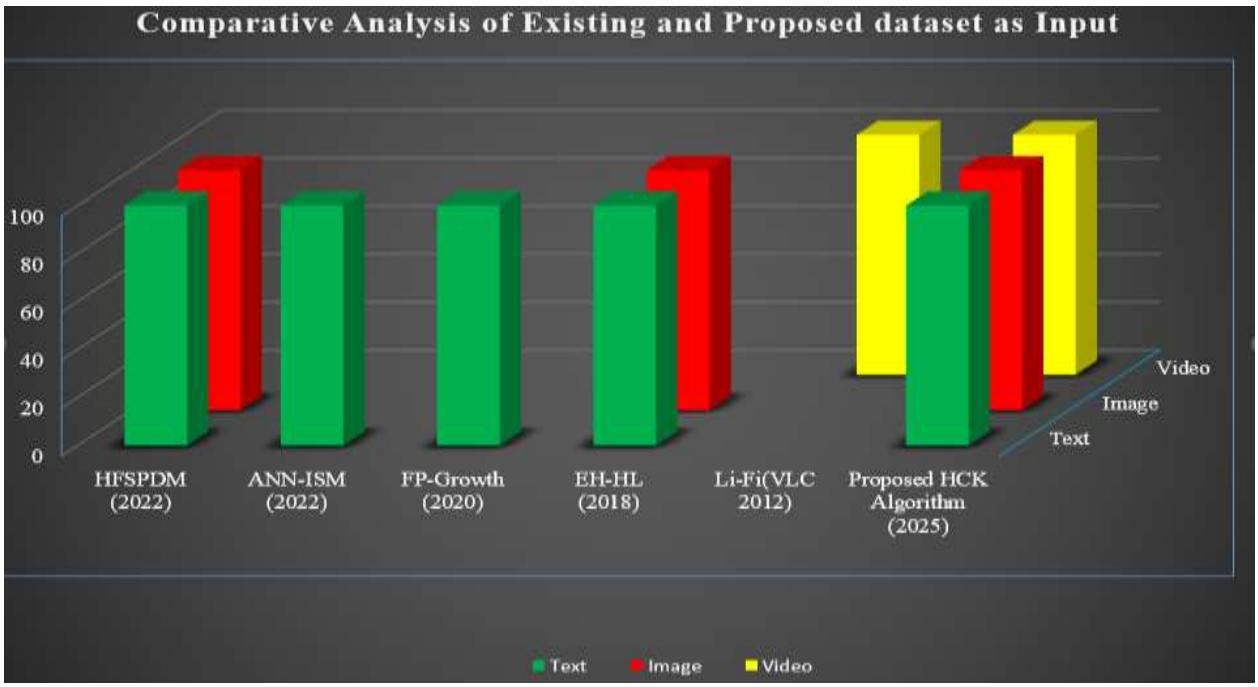

Figure 1: Comparative analysis of existing and proposed dataset as input

Table 2: Comparative Analysis: Li-Fi vs.Wi-Fi [26][27]

Feature	Li-Fi	Wi-Fi
Transmission Medium	Visible Light, Infrared, Ultraviolet	Radio Waves
Spectrum	Vast, unregulated visible light spectrum	Limited, regulated radio frequency spectrum (2.4GHz, 5GHz, 6GHz)
Speed	Theoretically much higher (up to 224 Gbps reported)[12]	Up to several Gbps with latest standards
Bandwidth	Very High	High, but susceptible to congestion
Security	High; signal confined by walls	Moderate to High; requires robust encryption, vulnerable to external interception
Interference	Immune to RF interference	Susceptible to interference from other RF devices
Range	Shorter; requires line-of-sight	Longer; penetrates walls and obstacles
Infrastructure	Requires LED lighting with Li-Fi transmitters and compatible devices	Widespread existing infrastructure of routers and compatible devices
Maturity	Emerging technology	Mature and widely adopted technology

2.1. Types of dataset

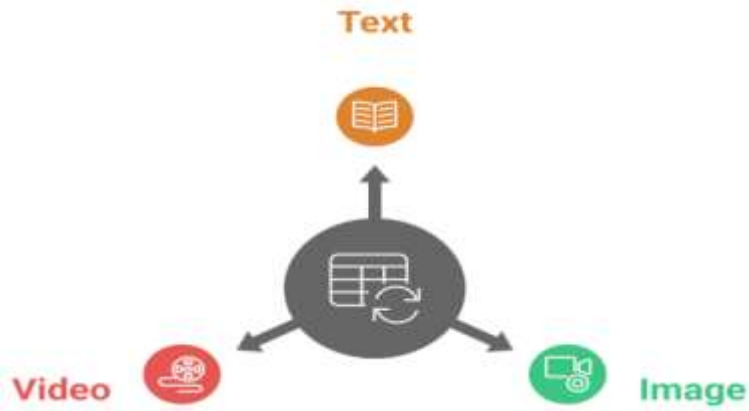

Figure 2: Types of Dataset

2.1.1. Text Dataset

The text dataset in the simulation represents structured or unstructured information transmitted across the hybrid Li-Fi and Wi-Fi network. Using this dataset, scenarios like transferring private documents, chat messages, or text logs produced by sensors are simulated. The RSA technique, which offers robust public-key encryption, non-repudiation, and resistance to brute-force attacks, is used to encrypt the text data in order to guarantee security.

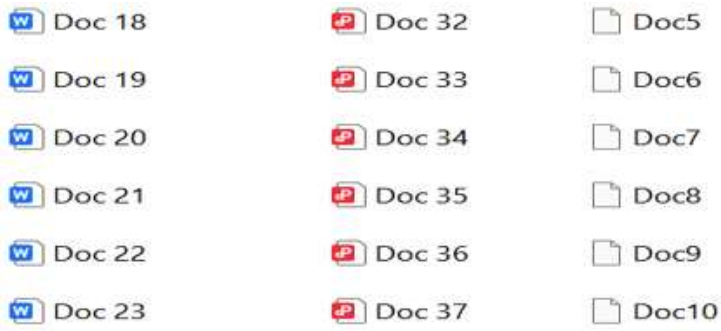

Figure 3: Text Dataset icons

The dataset helps assess how the framework manages sensitive textual communication in real time by enabling testing of network parameters such as speed, jitter, and packet delivery ratio under various encryption loads.

2.1.2. Image Dataset

The image dataset is made up of static visual data that is sent over a hybrid network, like pictures, security camera snapshots, or scans from medical equipment. The CSITA technique, which offers strong secrecy and integrity and guarantees little distortion during encryption and decryption, is used by the simulation to secure visual data. Analyzing the framework's capacity to manage big files and preserve quality after transmission is made easier with the help of this dataset.

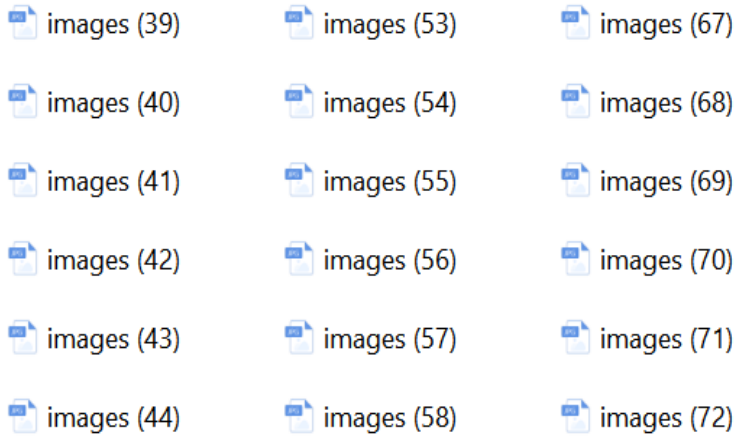

Figure 4: Image Dataset icons

When sending high-resolution images over Wi-Fi and Li-Fi channels, it makes it easier to assess throughput, error rate, and delay performance. [30]

2.1.3. Video Dataset

The video dataset includes continuous media streams, such as live conference feeds, security cameras, or multimedia content, that require high bandwidth and low latency. In the simulation, video data is protected using a hybrid AES + RSA encryption approach—AES ensures fast and efficient bulk encryption of large files, while RSA secures the encryption keys for additional protection.

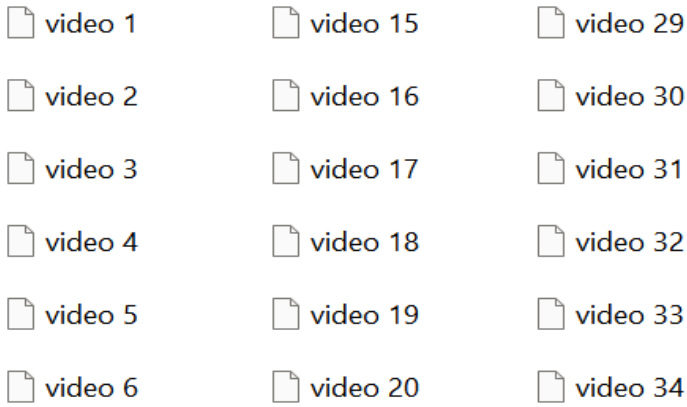

Figure 5: Video Dataset icons

This dataset is crucial for assessing the network's performance in handling time-sensitive and high-volume data, focusing on parameters such as frame drop ratio, playback smoothness, and encryption/decryption delay. [31]

3. METHOD

Hybrid Li-fi/Wi-fi Security: A hybrid Li-Fi and Wi-Fi system improves security by integrating the two technologies for data transfer, according to the document that was provided. In this system, the downlink data (from the network to the user) is typically provided through Li-Fi, while the uplink (from the user to the network) is supported by Wi-Fi. [32][33]

This method improves security by leveraging the inherent physical security of Li-Fi for receiving data; since light cannot pass through opaque surfaces like walls, it prevents eavesdropping from outside the room. While the uplink uses Wi-Fi, which is more susceptible to interception, the overall security of the system is increased by protecting the typically larger volume of downloaded data. To achieve high security in this hybrid model, the document suggests implementing several security methods in unison, such as encryption, O-OFDM or CSK, MAC address filtering, access control, and quantum cryptography. [34][35]

3.1. Proposed Methodology

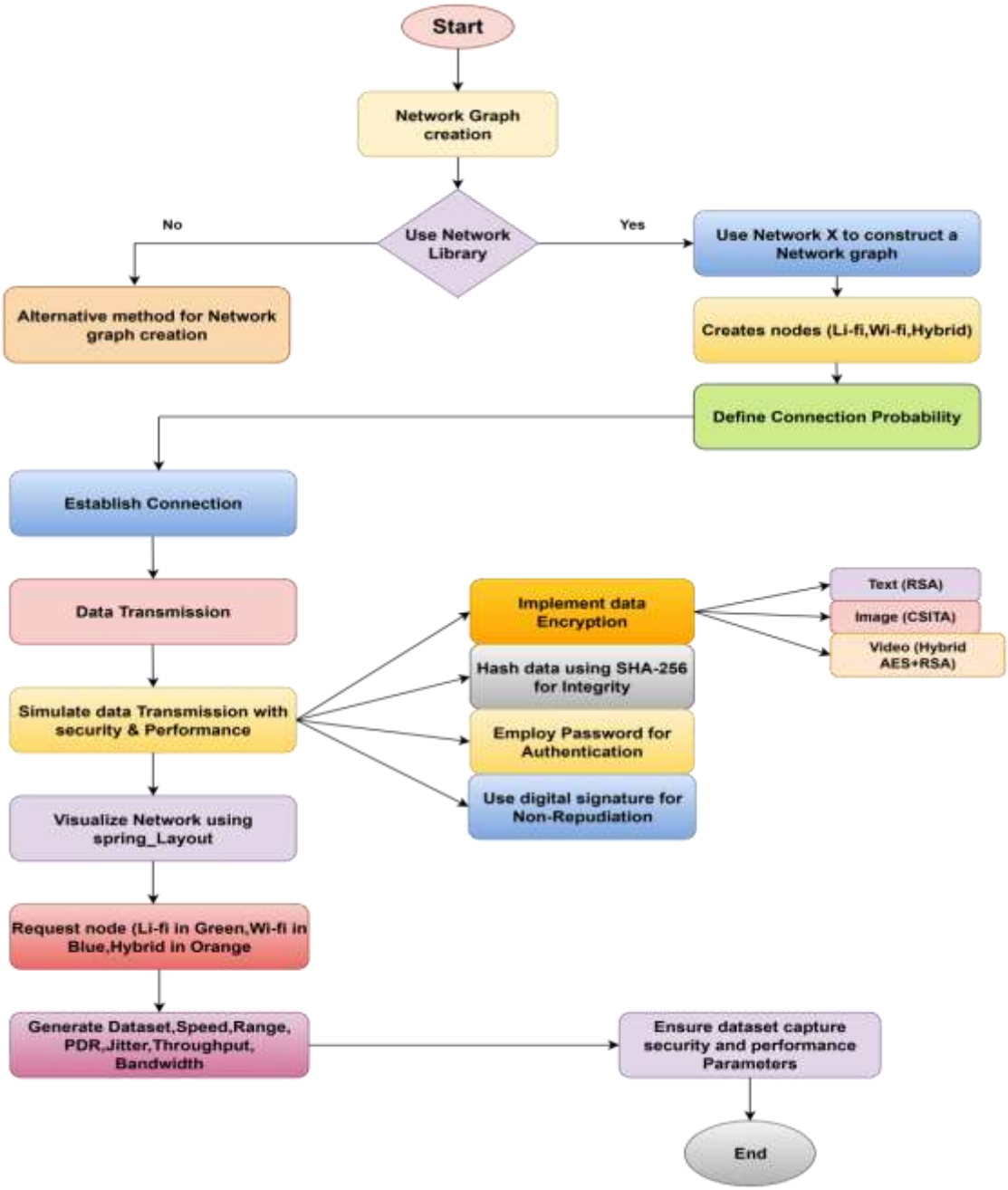

Figure 6: Proposed Methodology. [35][36][37][38]

Proposed Algorithm [39]

Algorithm : HCK(Hybrid Communication Key)
Step 1: Network Graph Creation Using NetworkX Library Node types: **LiFi**, **WiFi**, **Hybrid**. Create a Node with Attributes (device type, speed, range) Add the Node to the Graph G **Step 2: Connection Establishment** Define a connection ***probability*** conn_prob = base connection probability (0..1) used after distance check **Step 3: Data Transmission** **For** Each Data Transmission: **a. If** the Data Type is Text: Encrypt the Data Using RSA Algorithm **If** the Data Type is Image:

Encrypt Image Using Hash-LSB Technique.
If the Data Type is Video:
Use Hybrid AES+RSA Algorithm
b. Hash the Data Using SHA-256 for Integrity Checks
c. Use Passwords for Device Authentication
d. Apply Digital Signatures for Non-Repudiation
Step 4: Network Visualization
Visualize the Network Using a Spring Layout
Represent Li-Fi Nodes in Green and Wi-Fi Nodes in Blue,Hybrid Orange.
Step 5: Dataset Generation
Initialize an Empty Dataset
For each node in G:
Generate Attributes (speed, range, PDR, jitter, throughput,Bandwidth)
Add the Attributes to the Dataset
Dataset Captures Security and Performance Parameters apply.

3.2. Hybrid Framework Parameters

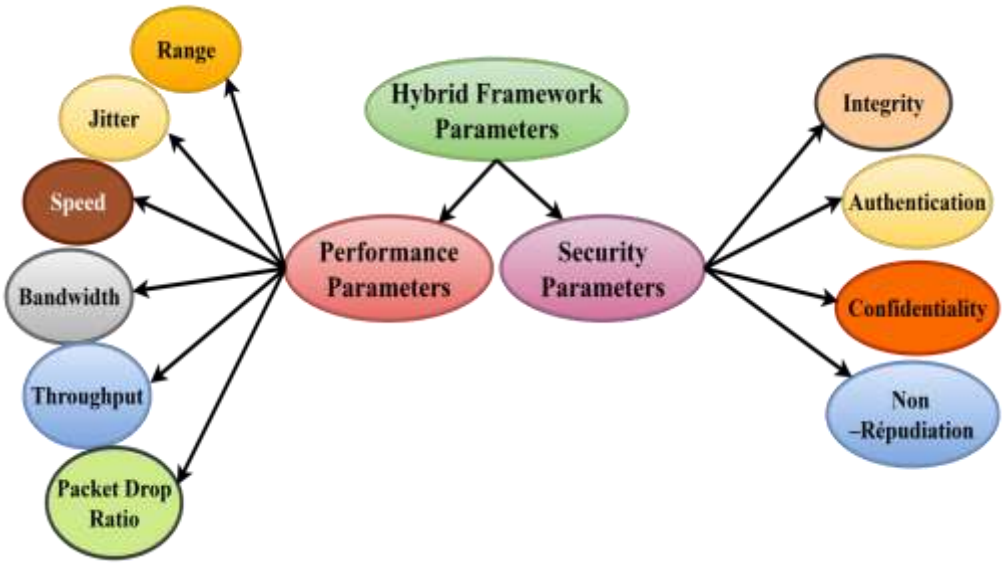

Figure 7: Performance Standards for hybrid Wi-Fi/Li-Fi networks. [39]

3.2.1. Performance Parameters

- **Range** – The maximum physical distance over which the network can transmit data effectively without significant loss in quality.
- **Jitter**-In real-time communications, such as sound or video, jitter—a variation in packet arrival times—can result in delays or uneven playing.
- **Speed-**Speed is the pace at which information is transferred; it is commonly expressed in Mbps or Gbps and shows how quickly information moves.
- **Bandwidth-** which is commonly expressed in bits per second, is the maximum amount of data that can be sent over a network link in a specific amount of time.
- **Throughput:** The actual amount of data that is successfully transmitted over the network in a given period of time is known as throughput; because to delays or losses, this amount is typically less than the maximum bandwidth.
- **Packet Drop Ratio**: The percentage of data packets lost or destroyed during transmission is known as the packet drop ratio, and it indicates problems with network reliability. [40]

3.2.2. Security Parameters

- **Confidentiality** is a basic information security principle that ensures data is safe from unwanted access or disclosure and available only to authorized users. It entails adopting strategies like encryption, access controls, and secure authentication to protect sensitive data, including financial, personal, and classified information. Confidentiality in communication systems preserves privacy and mutual trust by preventing eavesdroppers from deciphering intercepted messages. [40]
- **Integrity** is an essential information security principle that guarantees data accuracy,

consistency, and unalteredness when it is being processed, stored, or transmitted. It ensures that unauthorized parties cannot alter, remove, or tamper with information. Techniques such as cryptographic hash functions, checksums, and digital signatures are commonly used to verify integrity. Maintaining integrity ensures that the received data is exactly the same as the original, preserving reliability and trust in systems. [41]

- **Authentication** Before allowing access to resources or services, authentication is the process of confirming the identity of a user, device, or system. It guarantees that the organization making the access request is actually who or what it says it is. Passwords, PINs, digital certificates, security tokens, and biometric scans (facial recognition, fingerprint) are examples of common authentication techniques. Strong authentication is frequently the first step in creating secure communication, helps stop unwanted access, and safeguards sensitive data. [42]
- **Non-repudiation**: A security principle known as non-repudiation guarantees that a party to a communication or transaction cannot contest the legitimacy of their signature, message, or action later. It provides proof of origin and delivery, preventing either sender or receiver from falsely denying involvement. This is commonly achieved through cryptographic techniques like digital signatures and timestamps, which provide undeniable evidence of the transaction or communication. Non-repudiation is essential in legal, financial, and secure communication systems to maintain trust and accountability. [43]

Table 3: Simulation parameters [10]

Simulation Parameters	Value
Area needed for a transmission room	15m,15m,10m
Quantity of LED lights	40
The LED lamps' height	3 m
The device's height	1m
Power from LED emissions	55mW
View angle at the receiving end	750
Photodiode (l*b)	Approx1(cm*cm)

Simulation results based on the HCK (Hybrid Communication Key) algorithm

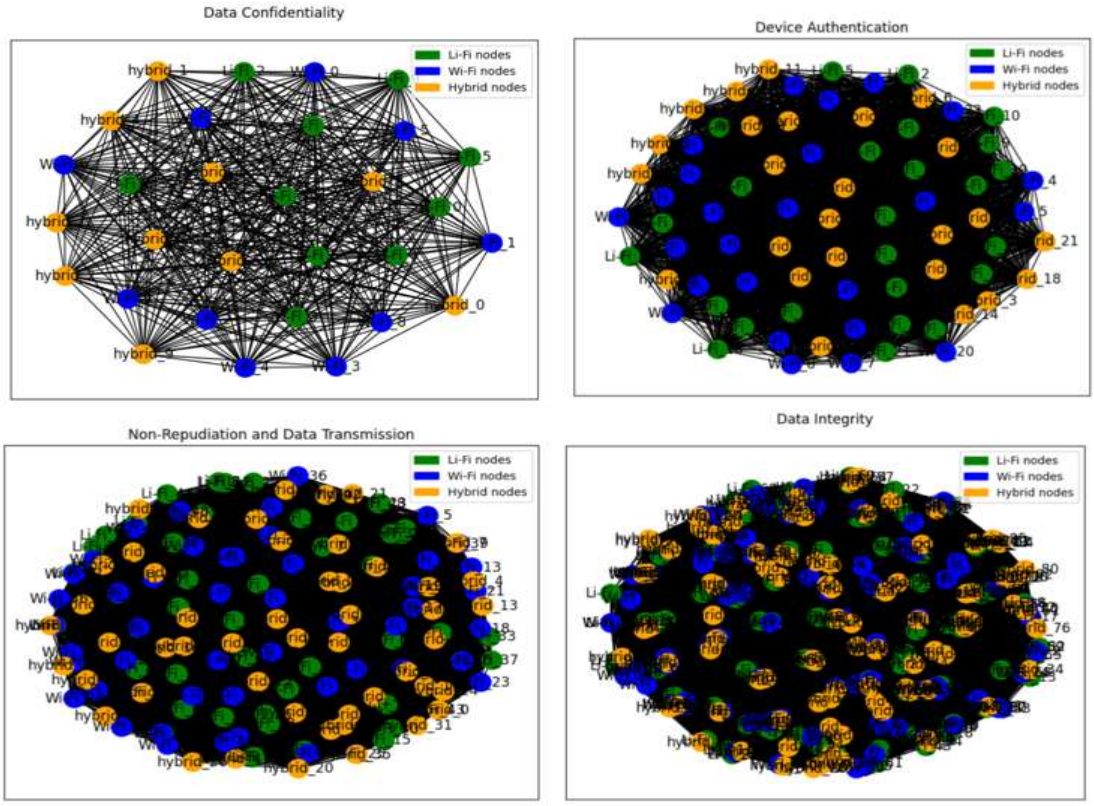

Figure 8: Data Confidentiality, Integrity, Device Authantication, Non-Repudiation

The above pictures present a number of simulations on a hybrid network made up of hybrid, Wi-Fi, and Li-Fi nodes, each of which focuses on a distinct core cybersecurity concept. The behavior and structure of the network are shown in these simulations as the number of connecting nodes rises, highlighting the growing difficulty of maintaining security in a diverse wireless setting. In order to guarantee that data is only available to authorized users, the first simulation, "Data Confidentiality," probably investigates ways to stop information from being disclosed without authorization. In order to prevent unwanted access, the second, "Device Authentication," focuses on confirming the identity of any node trying to join to the network.To prevent any node from disputing its involvement in a communication, the third simulation, "Non-Repudiation and Data Transmission," tackles the necessity of establishing a secure record of data transmission. In order to guarantee that the information supplied and received is identical, "Data Integrity" lastly looks at the safeguards put in place to prevent data from being changed or distorted during transmission. When taken as a whole, these simulations simulate the scalable security architecture of a network that combines Wi-Fi and Li-Fi, illustrating the difficulties and solutions involved in preserving a reliable and safe communication environment as the network expands in size and complexity.

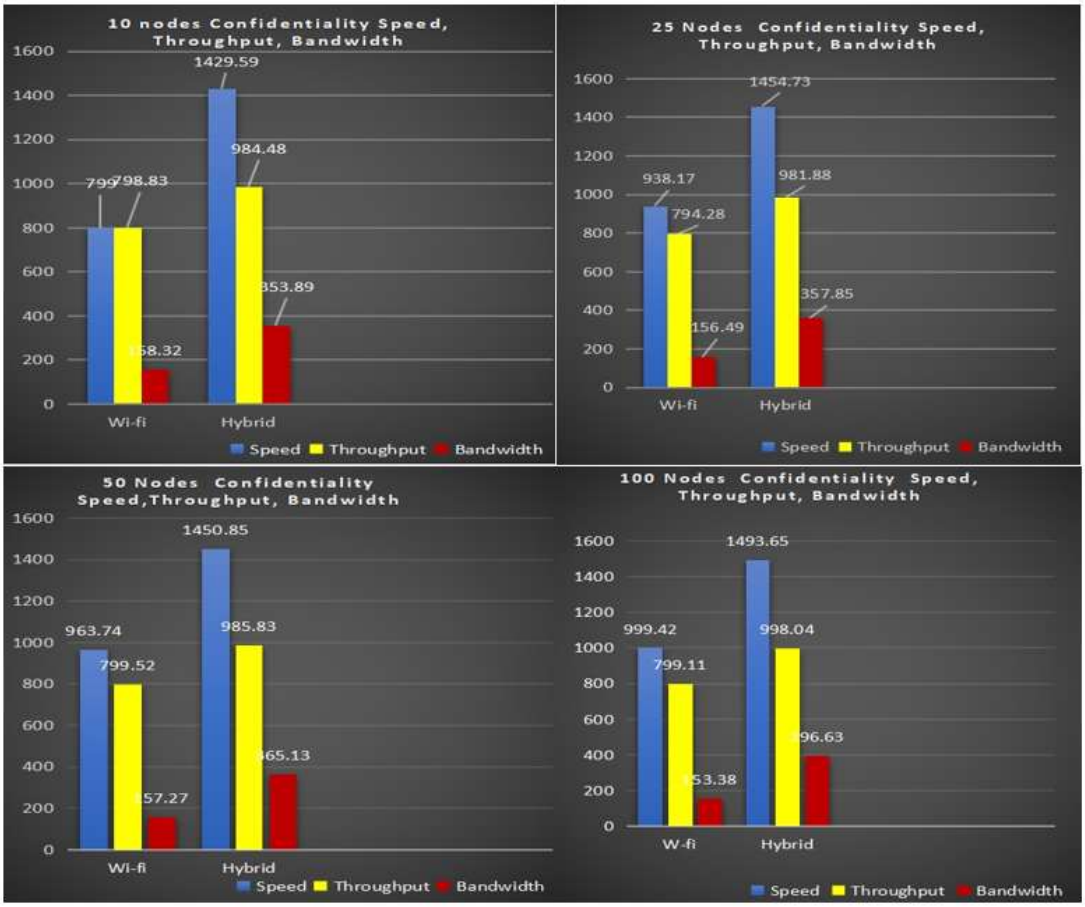

Figure 9: Data confidentiality,Speed,Throughput,Bandwidth flow graph

This series of bar charts illustrates a performance comparison between a standard "Wi-Fi" network and a "Hybrid" network under increasing loads of 10, 25, 50, and 100 nodes, focusing on confidentiality speed, throughput, and bandwidth. A consistent trend is evident across all four graphs: the Hybrid network architecture consistently and significantly outperforms the Wi-Fi network in all three metrics. As the number of nodes increases, the Hybrid system maintains its superior speed (around 1400-1500), high throughput (near 1000), and robust bandwidth (over 350), showcasing excellent scalability. In contrast, the Wi-Fi network delivers considerably lower performance that shows limited improvement with scale, particularly in its stagnant throughput and bandwidth figures. This visual data strongly suggests that the Hybrid network is a more capable and scalable solution for maintaining high-performance, confidential communications in increasingly dense network environments.

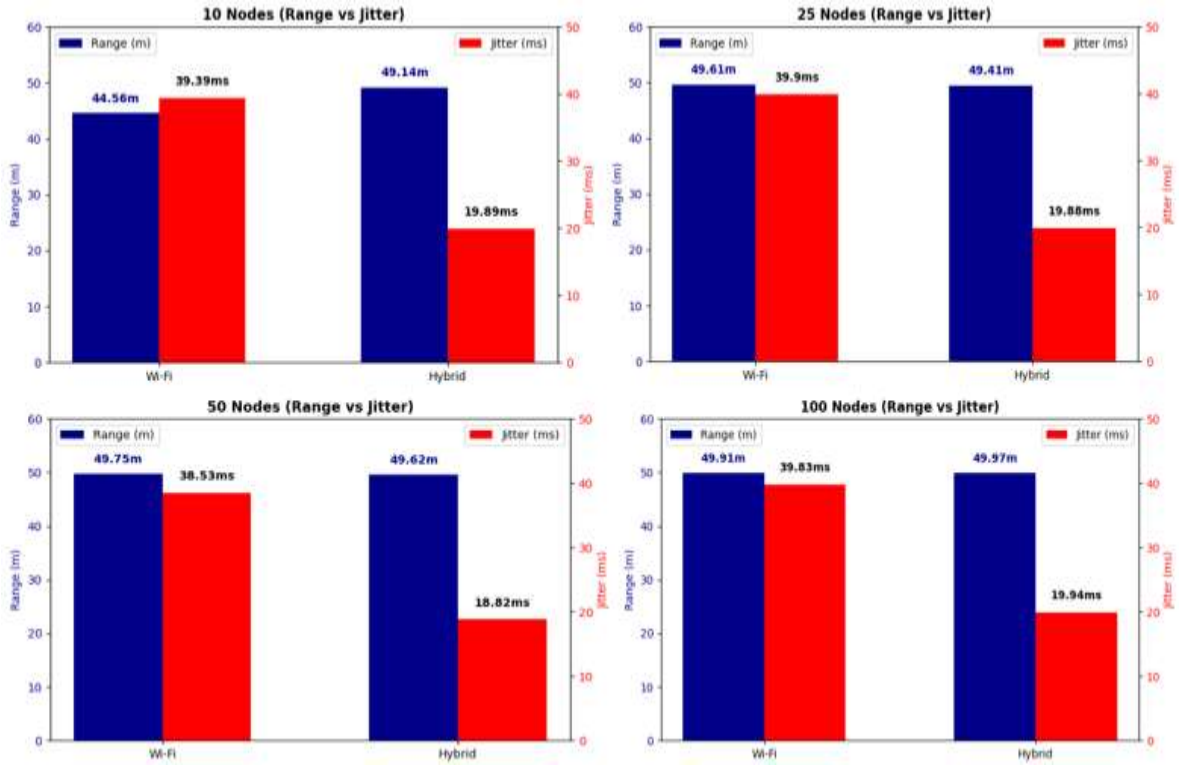

Figure 10: Output Number of Nodes Range and Jitter

Based on the data presented across the four graphs, a clear performance distinction emerges between the "Wi-Fi" and "Hybrid" systems as the network scales from 10 to 100 nodes. The "Hybrid" system continuously shows a notable advantage in terms of network reliability, even if both systems eventually reach a comparable maximum communication range of roughly 49 meters. Specifically, the jitter of the Hybrid system consistently remains low, averaging roughly 19 milliseconds across all node counts. The "Wi-Fi" system, on the other hand, has jitter that is consistently around 39 milliseconds, which is about twice as much as the Hybrid system. It is also much more variable. This implies that although the two technologies can travel a comparable physical distance, the hybrid system provides a far more dependable and stable connection, which is an essential feature for applications that are especially susceptible to delays and disruptions in the delivery of data packets.

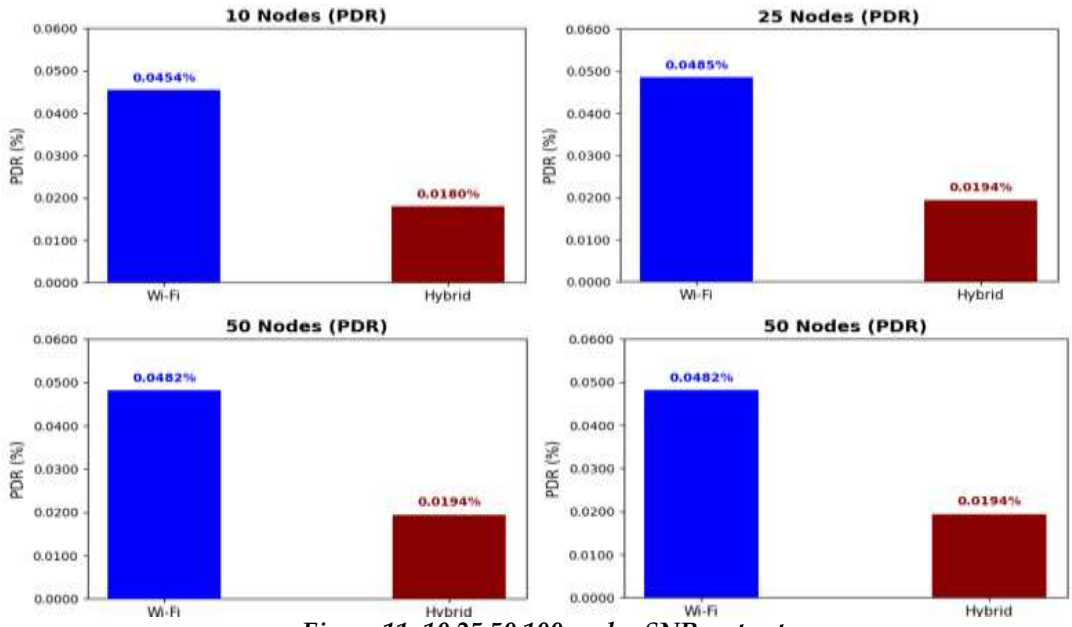

Figure 11: 10,25,50,100 nodes SNR output

When comparing the "Wi-Fi" and "Hybrid" systems across a range of network densities, the accompanying figures demonstrate a consistent trend in Packet Drop Rate (PDR). The hybrid system has a substantially lower PDR than the Wi-Fi system in all cases, ranging from 10 to 100 nodes. Specifically, as the number of nodes increases, the PDR for the Wi-Fi system shows a slight increase, ranging from 0.045% to 0.049%. In contrast, the hybrid system consistently maintains a much lower and more stable PDR, staying below 0.02% and ranging from 0.0180% to 0.0197%. This suggests that the Hybrid system is significantly more dependable than the Wi-Fi system, losing fewer data packets. This performance advantage is sustained as the network gets more congested.

4. DISCUSSION

An analysis of the provided data reveals that the proposed 2025 HCK (Hybrid Communication Key) algorithm represents a substantial advancement in performance compared to preceding algorithms developed between 2019 and 2022. The most striking improvement is in throughput, where the HCK algorithm achieves 988.56, significantly outperforming the next best algorithm, the 2022 PSO, which had a throughput of 725. Beyond this key metric, the HCK algorithm is distinguished by a more comprehensive performance evaluation, providing crucial data across several dimensions not detailed for the other methods.With a low Packet Drop Rate (PDR) of just 0.018%, it possesses remarkable reliability in addition to its high speed of 1468.68 and bandwidth of 398.46. It is also a reliable and efficient connectivity option, maintaining a 49.29-meter communication range with a low jitter of 19.89 ms. The HCK algorithm outperforms its predecessors in terms of speed, robustness, and comprehensiveness, as demonstrated by this intricate performance profile.

Table 4: performance comparison between the proposed hybrid system and hybrid systems from previous research. [44][45][46][47][48]

Year	Algorithm's	Throughput	Speed	Bandwidth	PDR	Range	Jitter
2019	**Optimized Algo**	**72**	-----	-----	----	-----	----
2020	**Fuzzy Logic**	**400**	-----	-----	----	-----	----
2020	**RL**	**175**	-----	-----	----	-----	----
2020	**RL Method**	**110.69**	-----	-----	----	-----	----
2022	**PSO Algo**	**725**	-----	-----	----	-----	----
Proposed Algorithm 2025	***HCK***	***988.56***	***1468.68***	***398.46***	***0.018***	***49.29***	***19.89***

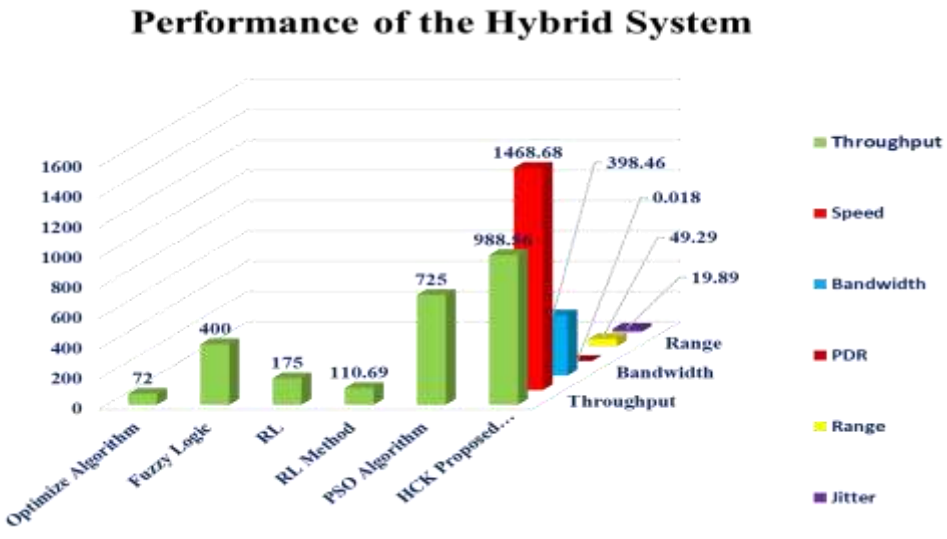

Figure 12: Comparison with Existing Algorithm

The performance of various algorithms, such as the "Optimize Algorithm," "Fuzzy Logic," "RL," "RL Method," and "PSO Algorithm," is contrasted in this 3D bar chart with a newly proposed "HCK Proposed" technique. The "HCK Proposed" approach beats all others with a throughput of 988.56, followed by the "PSO Algorithm" at 725. The main metric used to compare all methods is throughput. With its high speed of 1468.68, bandwidth of 398.46, range of 49.29, and jitter of 19.89, the graph further illustrates the "HCK Proposed" approach's overall performance.By outperforming the other algorithms in throughput

and demonstrating exceptional performance across a range of other crucial performance metrics, the graphic highlights the benefits of the "HCK Proposed" technique and positions it as a superior alternative.

4.1. Technical Explanation of the HCK Algorithm

The HCK encryption algorithm workflow is made by taking into account the size, type, and security needs of different types of data, such as text, images, and videos. Different cryptography methods are chosen to find the best balance between security strength and computational efficiency because one encryption method doesn't work well for all types of data.

RSA Algorithm: The RSA algorithm is used for text data. Text files are usually small, but they often have very sensitive information in them, like commands, authentication data, or private messages. RSA is an asymmetric cryptographer algorithm that uses public and private key pairs to provide strong security. It is especially good for managing keys and sending data securely. It keeps things private and stops people from getting in without permission, so it's good for protecting text-based datasets.

Hash-LSB Technique: The Hash-LSB (Least Significant Bit) method is used for image data. Image files have a lot of pixel data, and traditional encryption can be very expensive in terms of computing power. The Hash-LSB method puts encrypted hash values in the least significant bits of image pixels. This keeps the data private while keeping the quality and format of the image intact. This method cuts down on processing time and is great for sending images securely, especially when bandwidth is limited.

Hybrid AES+RSA Algorithm: A combination of AES and RSA encryption is used for video data. Video data consists of continuous, high-volume streams that need to be encrypted quickly and with little delay. AES is a symmetric encryption algorithm that works well for encrypting video because it is fast and doesn't need a lot of processing power. RSA is used to encrypt and securely send the AES secret key to solve the problem of distributing keys with symmetric encryption. This hybrid strategy uses the speed of AES and the strong key security of RSA to protect video data in real time.

4.2. Analyzing the Frequency of the Algorithm from Lower to Higher Output

This frequency chart uses a number of increasingly complex strategies to show the shift from "Lower Output" to "Higher Output," offering an intriguing visual narrative of algorithmic progress. A waveform that increases in complexity and volume along the horizontal axis is used to depict the performance. Starting with the "Optimized Algo," which produces a minimal and stable output, the waveform progressively becomes more dynamic through the "Fuzzy Logic," "RL Method," and "RL" stages, exhibiting continuous improvements. The "PSO Algo" significantly improves performance, as shown by the waveform's amplitude rapidly increasing. "HCK" Hybrid Communication Key algorithm, which displays the most powerful and complex waveform on the chart, marks the conclusion of the development and proves that it is the most effective algorithm in the series.

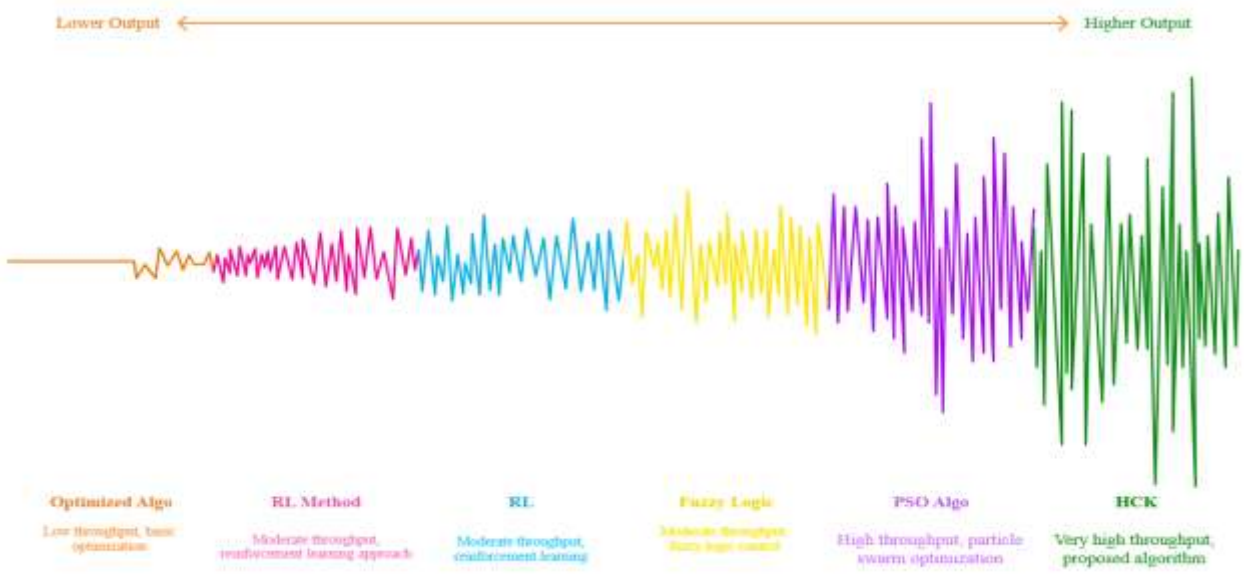

Figure 13: Algorithm's Frequency Evaluation

4.3. Comparative analysis between the Proposed Algorithm (blue) and Existing Algorithms

With a balancing scale metaphor, this info-graphic compares a "Proposed Algorithm" with "Existing Algorithms" in a simple and succinct manner, demonstrating superiority. The scale clearly tilts in the Proposed Algorithm's favor, demonstrating its improved performance on a number of important metrics. Each metric for the Proposed Algorithm, shown in blue on the left, is contrasted with its counterpart for Existing Algorithms, shown in green on the right. The Proposed Algorithm is depicted as having higher throughput (symbolized by a flowing river), faster speed (a cheetah), wider bandwidth (a multi-lane road), a longer range (a lighthouse), and lower jitter (calm water). In contrast, existing methods are associated with lower throughput, slower speed (a tortoise), narrower bandwidth, a shorter range (a desk lamp), and higher jitter (choppy water). The chart also indicates a "Lower PDR" (Packet Delivery Ratio) for the proposed algorithm, which, when paired with an icon of clear air versus a stormy cloud for higher PDR, suggests it represents a more favorable, lower packet drop or error rate. Collectively, the visual elements strongly convey that the Proposed Algorithm is a more robust and efficient solution.

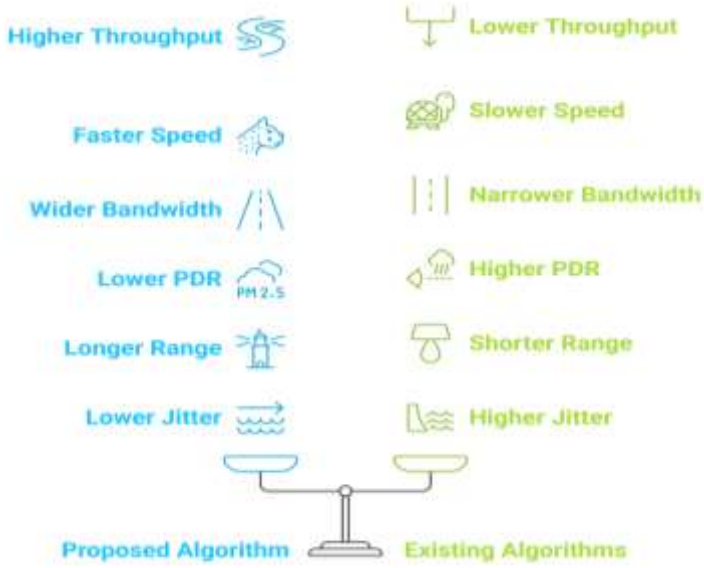

Figure 14: Algorithm Evaluation

5. CONCLUSIONS AND FUTURE WORK

With a throughput of 988.56, speed of 1468.68, bandwidth of 398.46, range of 49.29 meters, jitter of 19.89 ms, and a low packet drop rate of 0.018%, the hybrid Li-Fi and Wi-Fi network, driven by the HCK algorithm, is a major breakthrough in wireless communication. By combining the safe, fast, and interference-free transmission of Li-Fi with the widespread infrastructure and incorporating advanced encryption (RSA, AES) and security protocols, the system effectively addresses cybersecurity vulnerabilities and ensures scalability for IoT applications. Future work will focus on enhancing energy efficiency for Li-Fi access points, standardizing the technology, integrating AI-driven optimization and advanced modulation techniques like DCO-OFDM, and developing robust QoS mechanisms to manage diverse traffic types, ensuring scalable, secure, and intelligent hybrid networks for real-world deployment.

REFERENCES

Olalere OE, & Dorasamy, N. Perspectives On Digitization and Economic Growth in India. Journal of Namibian Studies: History Politics Culture. 2024; 40:464-99.

Ding L, Tian, Y., Liu, T., Wei, Z., & Zhang, X. Understanding commercial 5G and its implications to (Multipath) TCP. Computer Networks. 2021; 198:108401.

Mozaffariahrar E, Theoleyre, F., & Menth, M. A survey of Wi-Fi 6: Technologies, advances, and challenges. Future Internet. 2022;14(10):293.

Le DT, Tran, T. T., Dang, K. Q., Alkanhel, R., & Muthanna, A. Malware spreading model for routers in Wi-Fi networks. IEEE Access. 2022; 10:61873-91.

Toni Besjedica , Krešimir Fertalj , Vlatko Lipovac and Ivona Zakarija, Evolution of Hybrid LiFi–WiFi Networks:

A Survey. Sensors 2023, 23, 4252, pp1-28.
Szott S, Kosek-Szott, K., Gawłowicz, P., Gómez, J. T., Bellalta, B., Zubow, A., & Dressler, F. Wi-Fi meets ML: A survey on improving IEEE 802.11 performance with machine learning. IEEE Communications Surveys & Tutorials. 2022;24(3):1843-93.
Wang Y, Wu, X., & Haas, H. Fuzzy logic based dynamic handover scheme for indoor Li-Fi and RF hybrid network. In 2016 IEEE international conference on communications (ICC) 2016:1-6.
Waleed A. Ali M. H. Shaker Mona Shokair. Green underwater communication for ROVs: harnessing Li Fi.
Badeel R SS, Hanapi ZM, Muhammed A. A review on LiFi network research: Open issues, applications and future directions. Applied Sciences. 2021;11(23):11118.
Alfattani S. Review of LiFi technology and its future applications. Journal of Optical Communications. 2021;42(1):121-32.
Zeng Z, Soltani, M. D., Wang, Y., Wu, X., & Haas, H. Realistic indoor hybrid WiFi and OFDMA-based LiFi networks. IEEE Transactions on Communications. 2020;68(5):2978-91.
Bambang Winardi 1, Thiago Rocha, Tanwir. Light Sensing Technology Innovation (Li-Fi) as an Alternative Wireless. Communication Solution.Journal of Moeslim Research Technik, 2(2), 78–86.
Sanusi J, Idris, S., Adeshina, S., Aibinu, A. M., & Umar, I. Development of handover decision algorithms in hybrid Li-Fi and Wi-Fi networks. In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). 2020:1232-9.
Ma G, Parthiban, R., & Karmakar, N. An adaptive handover scheme for hybrid LiFi and WiFi networks. IEEE Access. 2022; 10:18955-65.
Zeena Mustafa.Enhancing Indoor Positioning Accuracy using a Hybrid Li-Fi/Wi-Fi System with Deep Learning Support Vol. 15, No. 2, 2025, 21575-21585.
Tsonev D, Chun, H., Rajbhandari, S., McKendry, J. J., Videv, S., Gu, E., ... & O'Brien, D. 3- Gb/s Single-LED OFDM-Based Wireless VLC Link Using a Gallium Nitride $\mu {\rm LED} $. IEEE photonics technology letters. 2014;26(7):637-40.
RAFIQ AHMAD KHAN 1, H. U. (January 2025). 5G Networks Security Mitigation Model: An. IEEE, 881-925.
Hamza1, Z. M. (2024). Enhancing Hybrid System Based on Reinforcement Learning. International Journal of Intelligent Engineering and Systems, 596-611.
Mohammed Zabeeulla a, *. (2023). Design and Modelling of hybrid network security method for increasing. Measurement: Sensors, 1-8.
Mohammed Majid Msallam1, 2. R. (2024). A Review of Security Methods in Light Fidelity Technology. Proceedings of Engineering and Technology Innovation, 01-17.
Mohan6, M. A. (2024). Mobility aware load balancing using Kho–Kho optimization algorithm. Wireless Networks, 5111-5125.
B. Anitha Vijayalakshmi1. (2024). Integrating Li Fi for enhanced security in MANET data. RESEARCH ARTICLE, 1-8.
B. W. (2025). Light Sensing Technology Innovation (Li-Fi) as an Alternative Wireless. Journal of Moeslim Research Technik, 78-86.
Ahmed, M. M. (2025). Cipher T Cipher Text t ext to Secur o Secure Li-Fi System Using Hybrid Encr e Li-Fi System Using Hybrid Encryption yption. IrIraqi Journal for Computer Science and Mathematics, 210-220.
Yadav, B. R. (2025). Enhancing Underwater Audio Transmission with Secure Li-Fi. AMERICAN Journal of Engineering, , 48-54.
Wu X, Soltani, M. D., Zhou, L., Safari, M., & Haas, H. Hybrid LiFi and WiFi networks: A survey. IEEE Communications Surveys & Tutorials. 2021;23(2):1398-420.
A Review of Security Methods in Light Fidelity Technology.Mohammed Majid Msallam1, Refik Samet.Proceedings of Engineering and Technology Innovation, vol. 27, 2024, pp. 01-1
Salvi S, & Vasantha, G. An optical camera communication using novel hybrid frequency shift and pulse width modulation technique for Li-Fi. Computation. 2022;10(7):110.
Riqaa FHMAD Khan, Habibullah Khan, Hathal Salamah Alwageed, Hussein Alhashimi, & Ismail Keshta. 5G Networks Security Mitigation Model: An ANN-ISM Hybrid Approach. Volume 6; 2025.
Khan KMS, Chaithra, S. V., Chandrasekhar, V. Y., & Vinay, B. Journal of Xi'an University of Architecture & Technology. 2020;7(4).
Sharma PK, Jeong, Y. S., & Park, J. H. EH-HL: Effective communication model by integrated EH-WSN and

hybrid LiFi/WiFi for IoT. IEEE Internet of Things Journal. 2018;5(3):1719-26.
Singh PR, Singh, V. K., Yadav, R., & Chaurasia, S. N. 6G networks for artificial intelligence- enabled smart cities applications: A scoping review. Telematics and Informatics Reports. 2023; 9:100044.
Zeena Mustafa, Ekhlas Kadhum Hamza. Enhancing Hybrid System Based on Reinforcement Learning.International Journal of Intelligent Engineering and Systems, Vol.17, No.1, 2024.
Bhutani M LB, Agrawal M. Optical wireless communications: research challenges for MAC layer. IEEE Access. 2022; 10:126969-89.
Lanza M, Sebastian, A., Lu, W. D., Le Gallo, M., Chang, M. F., Akinwande, D., & Roldan, J. B. Memristive technologies for data storage, computation, encryption, and radio-frequency communication. Science. 2022;376(6597): eabj9979.
Mohammed M. Ahmed, Satea H. Alnajjar. Cipher Text to Secure Li-Fi System Using Hybrid Encryption Algorithm.IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;6:210–220
Halder R, Sengupta, S., Ghosh, S., & Kundu, D. A secure image steganography based on rsa algorithm and hash-lsb technique. IOSR Journal of Computer Engineering (IOSR-JCE). 2016;18(1):39-43.
Meshal Alharbi1, S. Neelakandan, Sachi Gupta, R. Saravanakumar, Siripuri Kiran. A. Mohan.Mobility aware load balancing using Kho–Kho optimization algorithm for hybrid Li-Fi and Wi-Fi network.Wireless Networks (2024) 30:5111–5125
Mohammed Zabeeulla, Arjun singh, Sudhir Kumar Sharma, Sanjay Pratap Singh Chauhan. Design and Modelling of hybrid network security method for increasing security in vehicular ad-hoc network.Measurement: Sensors 29 (2023) 100878.
Zubow A, Gawłowicz, P., Brunn, C., Bober, K. L., Jungnickel, V., Habel, K., & Dressler, F. Hybrid-fidelity: Utilizing IEEE 802.11 MIMO for practical aggregation of LiFi and WiFi. IEEE Transactions on Mobile Computing. 2022;22(8): 4682-97.
Rabia NA, Ali, S., Sajid, A., & Zafar, A. A security review over wi-fi and li-fi. Information Management and Computer Science. 2020;3(1):01-9.
Mohammed Majid Msallam1, Refik Samet.A Review of Security Methods in Light Fidelity Technology.Proceedings of Engineering and Technology Innovation, vol. 27, 2024, pp. 01-17.
Fang W, Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. Digital signature scheme for information non-repudiation in blockchain: a state of the art review. EURASIP Journal on Wireless Communications and Networking. 2020; 2020:1-15.
Ahmad R, & Srivastava, A. Optimized user association for indoor hybrid Li-Fi Wi-Fi network. 21st International Conference on Transparent Optical Networks (ICTON). 2019:1-5.
Wu X, & Haas, H. Load balancing for hybrid LiFi and WiFi networks: To tackle user mobility and light-path blockage. IEEE Transactions on Communications. 2019;68(3):1675- 83.
Ahmad R, Soltani, M. D., Safari, M., & Srivastava, A. Load balancing of hybrid LiFi WiFi networks using reinforcement learning. In 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications. 2020:1-6.
Ahmad R, Soltani, M. D., Safari, M., Srivastava, A., & Das, A. Reinforcement learning based load balancing for hybrid LiFi WiFi networks. IEEE Access. 2020; 8:132273-84.
Ibraheem EK, & Hamza, E. K. Load Balancing Performance Optimization for LI-Fi/Wi-Fi HLR Access Points Using Particle Swarm Optimization and DL Algorithms. International Journal of Intelligent Engineering & Systems, 2022;15(6).
Min Xing, S. X. (2012). Rate Adaptation Strategy for Video Streaming over. University of Victoria, Victoria, BC, Canada: Wireless Networking Symposium.