STM JOURNALS

Trends in
Opto-electro & Optical Communication

ISSN: 2231-0401 (Online)
ISSN: 2347-9957 (Print)
Volume 15, Issue 1, 2025
January–April
DOI (Journal): 10.37591/TOEOC

https://journals.stmjournals.com/toeoc

Review TOEOC

Quantum Key Distribution in Optical Fiber Communication: A Study

Kazi Sultanabanu Sayyad Liyakat[1,*], Kazi Kutubuddin Sayyad Liyakat[2]

Abstract

The relentless march of technological advancements, particularly in the realm of quantum computing, stances a noteworthy threat to security of existing cryptographic systems. Traditional encryption methods, like RSA and AES, trust on mathematical problems considered computationally hard for computers. However, sufficiently powerful quantum computers could render these systems vulnerable to attacks, jeopardizing the confidentiality of sensitive data transmitted over optical fiber networks. This looming threat has spurred significant research and development into alternative security paradigms, with Quantum Key Distribution (QKD) emerging as promising solution. QKD leverages the fundamental laws of quantum mechanics, specifically principles of Superposition and Entanglement, to generate and distribute cryptographic keys. Unlike classical cryptography that depends on mathematical complexity, QKD's security is rooted in Laws of Physics. Any effort by an observer to catch or measures quantum signals used to transmit the key will inevitably add detectable disturbances, notifying the legitimate parties and compromising the key. The most common QKD protocols, like BB84 and E91, utilize polarized photons to represent quantum bits (qubits). These photons are transmitted through optical fibers between two parties, usually referred to as Alice (the sender) and Bob (the receiver). Alice randomly encodes each photon with one of several possible polarization states, representing either a '0' or a '1' in different bases. Bob, on the receiving end, randomly processes polarization of each photon using detectors aligned with different bases.

Keywords: Optical fiber communication, quantum key distribution, photon, polarization, quantum

INTRODUCTION

Optical fiber communication has long been the backbone of our interconnected world, enabling high-speed data transmission across vast distances. However, the insatiable demand for bandwidth, driven by cloud computing, streaming services, and IoT, is pushing the limits of existing infrastructure. To meet these challenges, a wave of emerging technologies is reshaping the landscape of optical fiber communication, promising faster speeds, increased capacity, and improved efficiency [1–3].

One of the primary avenues for increasing bandwidth is to exploit new regions of the optical spectrum. Traditionally, optical communication has primarily utilized the C-band (1530–1565 nm). Emerging technologies are now exploring the L-band (1565–1625 nm) and even the O-band (1260–1360 nm) to unlock additional bandwidth potential. This expansion necessitates the development of new optical components and amplifiers optimized for these wavelengths.

***Author for Correspondence**
Kazi Sultanabanu Sayyad Liyakat
E-mail: rajasaheb.3617@gmail.com

[1]Assitant Professor, Department of General Science and Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India
[2]Professor and Head, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur Maharashtra, India

Received Date: February 17, 2025
Accepted Date: February 21, 2025
Published Date: March 03, 2025

Citation: Kazi Sultanabanu Sayyad Liyakat, Kazi Kutubuddin Sayyad Liyakat. Quantum Key Distribution in Optical Fiber Communication: A Study. Trends in Opto-electro & Optical Communication. 2025; 15(1): 30–40p.

Complementing wavelength expansion is advancements in modulation techniques. Higher-order modulation formats, like 64-QAM and beyond, pack more bits per symbol, effectively increasing the data transmission rate. However, these advanced modulation schemes are more susceptible to noise and impairments, requiring sophisticated signal processing techniques for mitigation [4–8].

Space-Division Multiplexing (SDM): A Multi-Lane Highway for Data

Space-Division Multiplexing (SDM) offers a revolutionary approach by utilizing multiple spatial channels within a single fiber. This can be achieved through various methods, including:

- *Multi-Core Fiber (MCF):* This technology incorporates multiple optical cores within a single fiber cladding, essentially creating multiple independent transmission pathways.
- *Few-Mode Fiber (FMF):* FMF supports a limited number of spatial modes, each carrying a separate data stream.
- *Mode-Division Multiplexing (MDM):* MDM leverages advanced signal processing to separate and combine different spatial modes within a fiber, allowing for simultaneous data transmission.

SDM holds immense potential for scaling fiber capacity exponentially, addressing the future bandwidth needs of data centers and long-haul networks.

Silicon Photonics: Integration and Efficiency

Silicon Photonics integrates optical components directly onto silicon chips, similar to the way microprocessors are manufactured. This approach offers several advantages, including:

- *Miniaturization:* Silicon photonic devices are significantly smaller than traditional discrete components, enabling denser integration and reducing footprint.
- *Cost Reduction:* Leveraging existing silicon manufacturing infrastructure leads to lower production costs.
- *Improved Performance:* Shorter signal paths reduce signal loss and improve energy efficiency.

Silicon photonics enable the development of compact, high-performance optical transceivers that are crucial for meeting the bandwidth demands of data centers and short-reach applications.

Quantum Key Distribution (QKD): Securing the Future of Communication

As data security becomes increasingly critical, QKD offers a revolutionary solution. QKD influences the principle of quantum mechanics to generate and distribute encryption keys with absolute security. Any effort to eavesdrop on the quantum channel will inevitably introduce disturbances, alerting communicating parties to intrusion.

While still in its early phases of utilization, QKD is composed of playing a vital role in securing critical infrastructure and protecting sensitive data in the future.

While these emerging technologies hold tremendous promise, several challenges remain:

- *Cost:* Implementing these advanced technologies can be expensive, requiring significant investment in research, development, and infrastructure upgrades.
- *Complexity:* Managing the complexity of advanced modulation formats, SDM schemes, and quantum systems require sophisticated control and management systems.
- *Standardization:* Establishing industry-wide standards is crucial for ensuring interoperability and promoting widespread acceptance.

Notwithstanding these challenges, opportunities are immense. By overcoming these hurdles, these emerging technologies can unlock unprecedented bandwidth capacity, improve energy efficiency, and enhance data security, paving the way for a future of seamless connectivity and transformative applications.

In conclusion, the field of optical fiber communication is undergoing a period of rapid innovation. Emerging technologies are pushing the boundaries of what is possible, promising a future where bandwidth is no longer a limiting factor. As we continue to explore these advancements, the potential to revolutionize industries and connect the world in unprecedented ways becomes increasingly apparent [9–14].

Quantum Key Distribution: Securing Communication in a Quantum World

In an era where data security is paramount, and cyberattacks are becoming progressively sophisticated, the need for unbreakable encryption methods is more serious than ever. Enter QKD, a revolutionary technology that promises to protected communication using fundamental laws of quantum physics [15–19].

Customary encryption means trust in complex mathematical algorithms and are often susceptible to brute-force attacks or breakthroughs in computing power. QKD, on the other hand, takes a different approach. It leverages the principles of quantum mechanics to produce and distribute encryption keys in a way that is inherently secure.

At its core, QKD involves two parties, traditionally called Alice and Bob, who wish to communicate securely. Here is a simplified overview of the process:

1. *Quantum Transmission:* Alice encodes information on individual photons, the fundamental particles of light. These photos are prepared in different polarization states, representing binary digits (0s and 1s).
2. *Transmission Channel:* These photons are transmitted through a quantum channel that could be fiber optic tow or free space.
3. *Measurement and Key Agreement:* Bob accepts photos and measures polarization states. He uses randomly chosen measurement bases to decode the information. Due to the probabilistic nature of quantum mechanics, Bob will not always guess the correct basis.
4. *Classical Reconciliation:* Alice and Bob then communicate on a public, classical channel (like the internet). They compare their measurement bases and discard results where they used dissimilar bases. This leaves them with a shared string of bits.
5. *Error Correction and Privacy Amplification:* Even with careful alignment, errors can occur during transmission. Alice and Bob use error correction techniques to identify and correct these errors. They then use privacy amplification techniques to eliminate any information that an eavesdropper (Eve) may have gleaned from channel [20–25].
6. *Secure Key Generation:* The remaining string of bits forms the secure encryption key, which Alice and Bob may use to encrypt and decrypt their messages using classical encryption algorithms.

The key advantage of QKD lies in its ability to detect eavesdropping. The act of observing a quantum system inherently disturbs it. If Eve attempts to intercept the photons to learn the key, she will inevitably alter their polarization states, introducing errors into the data. Alice and Bob can detect these errors and know that the key has been compromised. This allows them to discard the key and start the process again, ensuring absolute security.

Benefits of QKD are:

- *Unconditional Security:* QKD's security is based on physics laws, not on the complexity of mathematical algorithms. It remains secure even against adversaries with unlimited computing power, including potential quantum computers.
- *Eavesdropping Detection:* The ability to detect any attempt to intercept the key is a crucial advantage, providing real-time security awareness.
- *Future-Proof Security:* As quantum computers become reality, QKD offers a viable solution to protect sensitive data against attacks that could break current encryption methods.

Despite its potential, QKD faces several challenges:

- *Distance Limitations:* Photon loss in the quantum channel limits the distance over which QKD can be effectively implemented. Relay stations using trusted nodes are often required to extend the range, which can introduce vulnerabilities.
- *Cost:* Implementing QKD systems can be expensive, especially for large-scale deployments.
- *Practical Implementation:* Integrating QKD with existing network infrastructure presents technical challenges.

Despite these challenges, research and development efforts are focused on:

- *Developing Long-Distance QKD:* Exploring techniques like quantum repeaters and satellite-based QKD to extend the range.
- *Reducing Costs:* Developing more affordable and scalable QKD systems.
- *Improving Integration:* Simplifying the integration of QKD with existing network infrastructure.

QKD is finding applications in a variety of sectors where security is paramount:

- *Government and Military:* Protecting sensitive government communications and classified information.
- *Financial Institutions:* Securing financial transactions and protecting sensitive customer data.
- *Healthcare:* Safeguarding patient records and protecting medical research data.
- *Critical Infrastructure:* Securing power grids, communication networks, and other essential infrastructure.

QKD represents a paradigm shift in cybersecurity. By leveraging the fundamental laws of quantum physics, it offers a path towards unbreakable encryption and provides a vital defense against the growing threat of cyberattacks in a quantum-dominated future. While contests remain, continuing research and expansion are pavement ways for broader adoptions and a more secure digital landscape. As quantum computers continue to advance, QKD stands as a crucial technology for safeguarding our most sensitive information [26, 27].

QUANTUM KEY DISTRIBUTION (QKD) IN OPTICAL FIBER COMMUNICATION: SECURING THE FUTURE OF DATA TRANSMISSION

In a progressively interconnected world, security of data transmission is paramount. Customary encryption approaches, while effective, are vulnerable to evolving computational power and sophisticated hacking techniques. This vulnerability has spurred research into innovative security solutions, with QKD emerging as a leading candidate for securing the future of data communication, particularly in the realm of optical fiber networks [28, 29].

QKD is cryptographic protocol which leverages fundamental laws of quantum mechanics to begin a secret key between two events, often denoted as Alice and Bob. Unlike usual cryptography that trusts mathematical algorithms that can be potentially broken, QKD's security is founded on the laws of physics, making it fundamentally immune to eavesdropping.

The core principle lies in the transmission of individual photons, the smallest units of light, over a quantum channel. These photons are encoded with quantum states, like polarization, representing bits of information. Any effort to interrupt or measure these photos inevitably alters their state, notifying Alice and Bob of the presence of an eavesdropper, often referred to as Eve.

The most common QKD protocols, like BB84 and E91, utilize polarized photons to represent quantum bits (qubits). These photos are transmitted through optical fibers between Alice and Bob. Alice randomly encodes each photon with one of several possible polarization states, representing either a '0' or a '1' on different bases. Bob, on the receiving end, randomly processes polarization of each photon by detectors aligned with different bases.

After the transmission, Alice and Bob publicly compare a portion of their recorded bases. They discard the bits where they used different bases and keep the bits where their bases matched. This process generates a raw key. Critically, any eavesdropping attempts, often referred to as an intercept-resend attack, will lead to errors in shared key due to the disturbance of the quantum state of photons.

The final step involves error adjustment and privacy intensification to distill secure, secret key. Error correction protocols identify and correct the errors led during transmission, including those potentially caused by an eavesdropper. Privacy amplification then reduces the information an eavesdropper might have gained about the key through eavesdropping, resulting in a final key that is virtually impossible to compromise using classical or quantum computing techniques [30, 31].

Optical fiber provides a natural medium for transmitting photos, making it a well-suited platform for QKD. The process usually involves these key stages:

1. *Quantum Key Generation:* Alice generates random stream of quantum bits (qubits) and encodes them onto photons. She uses different polarization positions (e.g., horizontal, vertical, diagonal) to represent 0s and 1s.
2. *Quantum Transmission:* Alice transmits these photons through an optical fiber channel to Bob.
3. *Quantum Measurement:* Bob receives photons and measures polarization states. He randomly chooses different bases for measurement without knowing Alice's initial encoding.
4. *Sifting and Basis Reconciliation:* Alice and Bob publicly communicate (using a secure, but not necessarily quantum, channel) to compare bases they used for encoding and measuring. They discard the bits where their bases do not match, keeping only the bits where they used the same basis; this is called sifting.
5. *Error Correction and Privacy Amplification:* The sifted key may contain errors due to noise or the presence of an eavesdropper. Alice and Bob use classical error correction techniques to identify and correct these errors. Finally, privacy amplification is applied to reduce the information Eve might have gained, resulting in a highly secure, shared secret key.

Advantages of QKD in Optical Fiber:

- *Unconditional Security:* Quantum Key Distribution (QKD) offers information-theoretic security, meaning the security is guaranteed by the laws of physics, regardless of the computational power of any potential attacker. This makes QKD immune to advancements in computing, including potential threats from quantum computers.
- *Eavesdropping Detection:* Every effort to interrupt the quantum signal inevitably leaves a trace, permitting Alice and Bob to identify the presence of eavesdropper and abort the key exchange.
- *Future-Proof Security:* QKD is resistant to attacks from future quantum computers, which threaten security of many traditional cryptographic algorithms.

While QKD offers significant advantages, it also faces challenges:

- *Distance Limitations:* Signal degradation and photon loss in optical fiber limit the transmission distance of QKD. Repeaters are needed to extend the range, but these can introduce vulnerabilities. Research is ongoing to improve the efficiency of single-photon detectors and reduce fiber losses.
- *Cost and Complexity:* Implementing QKD systems can be expensive and complex, requiring specialized equipment and expertise.
- *Integration with Existing Infrastructure:* Integrating QKD with existing communication infrastructure can be challenging, requiring new protocols and interfaces.
- *Authentication:* QKD relies on a pre-shared secret or an authenticated classical channel for basis reconciliation and error correction. Protecting this channel is crucial for the overall security of the system.
- *Practical Security Considerations:* While theoretically secure, the practical implementation of QKD systems is vulnerable to side-channel attacks targeting imperfections in hardware and software. Ongoing research focuses on mitigating these vulnerabilities to ensure the overall security of QKD systems.

Despite the challenges, QKD is finding applications in various sectors:

- *Government and Military:* Protecting sensitive government and military communications from espionage.
- *Financial Institutions:* Securing financial transactions and protecting sensitive customer data.
- *Healthcare:* Protecting patient records and confidential medical information.
- *Critical Infrastructure:* Securing power grids, water supply systems, and other critical infrastructure from cyberattacks.
- *Data Centers:* Protecting data stored and transmitted within and between data centers.

QKD is still a relatively nascent technology, but it holds immense promise for securing the future of data communication. Current research efforts are focused on:

- Increasing the transmission distance of QKD systems.
- Reducing the cost and complexity of QKD implementations.
- Developing new QKD protocols that are more robust to noise and imperfections.
- Integrating QKD with existing communication infrastructure seamlessly.
- Developing trusted repeater solutions to overcome distance limitations without compromising security.

As these encounters are addressed, QKD is predictable to play an increasingly significant part in securing critical infrastructure, protecting sensitive data, and ensuring the confidentiality of communications in a world increasingly reliant on digital technologies. Its integration with optical fiber communication offers a powerful pathway to a future where data is fundamentally immune to eavesdropping, ensuring privacy and security of information for generations to come [32].

DESIGN STEPS PROPOSED

QKD is an innovator technology which allows for secure and uncrackable exchange of encryption keys between two parties using the principles of quantum mechanics. In this section, we will discuss the steps involved in designing a QKD system for optical fiber communication as shown in Figure 1, with a focus on care, respect, truth, utility, security, and positivity.

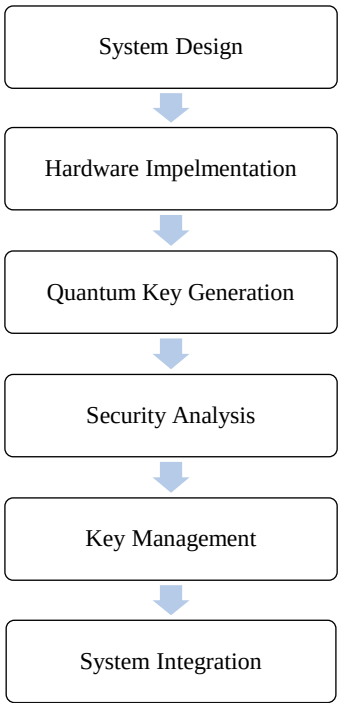

Figure 1. Design steps.

System Design

The first step in designing a QKD system is to define the system architecture and specify the required hardware components. This includes selecting the type of quantum communication protocol to be used (e.g. BB84, E91), the optical fiber type (e.g. single-mode, multi-mode), and the wavelength of the quantum signals. The design should also consider the transmission distance, the number of users, and the required key generation rate [33].

Hardware Implementation

After the system design is complete, the next step is to implement the hardware components, which typically include a quantum signal source, a modulator, an optical fiber, a photon detector, and a classical communication channel. The quantum signal source generates the quantum states to be transmitted over the optical fiber, while the modulator encodes the key information onto the quantum states. The photon detector detects the quantum states at the receiver end, and the classical communication channel is used for the exchange of classical information between the two parties [34].

Quantum Key Generation

The next step is to generate the quantum keys using the implemented hardware components. This involves the transmission and reception of quantum states, followed by error correction and privacy amplification to generate secure keys. The error correction process helps to eliminate bit errors introduced during transmission, while privacy amplification ensures that the keys are secure against eavesdropping attacks.

Security Analysis

After the keys have been generated, a security analysis should be carried out to ensure that the keys are indeed secure. This involves estimating the amount of information leaked to an eavesdropper during the key generation process and verifying that the keys meet the desired security requirements.

Key Management

Once the keys have been generated and their security has been verified, the keys must be securely distributed to the intended recipients. This involves key distribution strategies such as one-time pad or advanced encryption standard (AES) encryption and ensuring that the keys are stored and managed securely.

System Integration

The final step is to integrate the QKD system with the existing communication infrastructure. This involves connecting the QKD system to the classical communication channel and ensuring interoperability with existing communication protocols.

In conclusion, designing a QKD system for optical fiber communication requires careful consideration of the system architecture, hardware implementation, quantum key generation, security analysis, key management, and system integration. By following these steps, it is possible to design a secure and reliable QKD system that enables the secure exchange of encryption keys by principles of quantum mechanics. This technology holds great promise for secure communication in a variety of applications, including government, military, and financial institutions.

It is important to approach this design process with care, respect, and truth, by ensuring that the system is designed with the utmost regard for security, utility, and fairness. By following these principles, we can build a positive and secure future for quantum communication.

DISCUSSION

In an age increasingly dependent on digital communication, the need for robust and unhackable security measures is paramount. Customary encryption methods that are effective today, are vulnerable to future advances in computational power, particularly the development of quantum computers. Enter

QKD, a revolutionary technology leveraging the principles of quantum mechanics to guarantee secure key exchange. This study delves into the recent strides made in QKD, specifically focusing on its implementation and performance within optical fiber communication networks.

QKD offers a fundamentally different approach to encryption. Instead of relying on mathematical complexity, it exploits the laws of physics to ensure secure key distribution. The core principle lies in encoding cryptographic keys onto single photons, the fundamental particles of light. Any attempt to eavesdrop on these photons inevitably alters their quantum state, alerting the legitimate parties to the intrusion. This "eavesdropping detection" mechanism is what sets QKD apart and provides its inherent security. While the theory behind QKD is well-established, its practical implementation, especially over optical fiber networks, presents significant challenges. Optical fibers, the backbone of modern communication infrastructure, introduce various impairments that can degrade the fragile quantum signals. These impairments include:

- *Attenuation:* Signal loss over distance, reducing photon arrival rates.
- *Dispersion:* Pulse broadening, leading to errors in photon detection.
- *Noise:* Background photons, obscuring the legitimate signal.

Despite these challenges, significant progress has been made in deploying QKD systems over optical fiber. Researchers have successfully demonstrated the transmission of secure keys over extended distances, achieved higher key generation rates, and developed robust protocols that mitigate the effects of fiber impairments.

Current research is heavily focused on optimizing QKD systems for real-world deployment in optical fiber networks. Some key findings and advancements include:

- *Increased Transmission Distances:* Using advanced single-photon detectors and sophisticated error correction techniques, researchers have extended the reach of QKD systems. Some experiments have demonstrated secure key exchange over hundreds of kilometers of standard optical fiber.
- *Higher Key Generation Rates:* Improving the efficiency of single-photon sources and detectors allows for faster key generation. These advancements are crucial for practical applications where high data throughput is required.
- *Tolerance to Fiber Impairments:* Novel QKD protocols have been developed to mitigate the effects of attenuation, dispersion, and noise in optical fiber. These protocols often involve complex quantum state preparation and measurement techniques.
- *Integration with Classical Networks:* Integrating QKD systems with existing classical communication infrastructure is essential for widespread adoption. Efforts are underway to develop hybrid networks where QKD is used to secure the encryption keys for traditional data transmission methods.
- *Twin-Field QKD (TF-QKD):* This protocol bypasses the fundamental distance limitations associated with standard QKD protocols, allowing secure key exchange over substantially longer distances. Recent implementations have shown promising results in metropolitan-area fiber networks.

The results achieved so far are encouraging, demonstrating the feasibility of QKD in optical fiber communication. However, several challenges remain before QKD can be widely deployed. These include:

- *Cost:* The cost of QKD systems, particularly single-photon detectors, is still relatively high. Reducing the cost of these components is crucial for making QKD more accessible.
- *Standardization:* Establishing standardized QKD protocols and interfaces will facilitate interoperability between different vendors' equipment and accelerate adoption.
- *Security Certification:* Developing rigorous security certification processes for QKD systems is essential for building trust and ensuring that they meet the required security standards.

Looking ahead, QKD holds immense potential for securing critical infrastructure, protecting sensitive data, and enabling new applications that require ultra-secure communication. As research and development efforts continue, we can expect to see:

- More compact and affordable QKD systems.
- Wider deployment of QKD in metropolitan-area networks and long-haul communication links.
- Integration of QKD with quantum computing for enhanced security solutions.

QKD represents a paradigm shift in cybersecurity, offering a fundamentally secure approach to key distribution. While challenges remain, the impressive progress made in QKD implementation over optical fiber communication networks underscores its potential to safeguard our digital future. As the threat landscape evolves, QKD is poised to become an increasingly important tool for protecting critical information and ensuring secure communication in an increasingly interconnected world. The journey from theoretical concept to practical deployment is well underway, paving the way for a quantum-secured future.

CONCLUSION

The development and deployment of QKD systems in optical fiber communication are essential steps towards securing our digital future against the threats posed by quantum computers. While challenges remain in terms of distance limitations, cost, and integration, ongoing research and expansion efforts are steadily addressing these hurdles. QKD offers a fundamentally different approach to security, based on the unyielding laws of physics, guaranteeing confidentiality in an era where classical cryptographic systems may become obsolete. As quantum computing continues to advance, QKD represents a vital investment in the long-term security and privacy of our sensitive data transmitted over optical fiber networks. The future of secure communication in a quantum world hinges on the continued development and wider adoption of QKD technology.

REFERENCES

1. Liyakat KK. Analysis for Field Distribution in Optical Waveguide Using Linear FEM Method. Journal of Optical Communication Electronics (JOOCE). 2023; 9(1): 23–8.
2. Liyakat KS, Liyakat KK. Dispersion Compensation in Optical Fiber: A Review. Journal of Telecommunication Study (JTS). 2023; 8(3): 14–9.
3. Kazi Sultanabanu Sayyad Liyakat. Electronics with Artificial Intelligence Creating a Smarter Future: A Review. Journal of Communication Engineering and Its Innovations (JOCEI). 2023; 9(3): 38–42.
4. Liyakat KS, Liyakat KK. IoT Based Arduino-Powered Weather Monitoring System. Journal of Telecommunication Study (JTS). 2023; 8(3): 25–31.
5. Khadake S, Kawade S, Moholkar S, Pawar M. A Review of 6G Technologies and Its Advantages Over 5G Technology. In Techno-Societal 2016, International Conference on Advanced Technologies for Societal Applications. Cham: Springer International Publishing; 2022 Dec 9; 1043–1051. https://doi.org/10.1007/978-3-031-34644-6_107.
6. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, Sawant VA. Review of AI in Power Electronics and Drive Systems. In 2024 IEEE 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC). 2024 Feb 23; 94–99. doi: 10.1109/PARC59193.2024.10486488
7. Dudgikar AB, Ingalgi AA, Jamadar AG, Swami OR, Khadake SB, Moholkar SV. Intelligent battery swapping system for electric vehicles with charging stations locator on IoT and cloud platform. Int J Adv Res Sci Commun Technol. 2023 Jan; 3(1): 204–8. DOI: 10.48175/IJARSCT-7867
8. Khadake SB, Patil VJ. Prototype Design & Development of Solar Based Electric Vehicle. In 2023 IEEE 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON). 2023 Dec 29; 1–7. doi: 10.1109/SMARTGENCON60755.2023.10442455.
9. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, Sawant VA. A Comprehensive Analysis of Artificial Intelligence Integration in Electrical Engineering. In 2024 IEEE 5th

International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). 2024 Jan 18; 484–491. doi: 10.1109/ICMCSI61536.2024.00076
10. Khadake SB, Dolli SP, Rathod KS, Waghmare MO, Deshpande MA. An overview of intelligent traffic control system using PLC and use of current data of vehicle travels. JournalNX-A Multidisciplinary Peer Reviewed Journal. 2021, 1–4.
11. Magar SS, Sugandhi AS, Pawar SH, Khadake SB, Mallad HM. Harnessing Wind Vibration, a Novel Approach towards Electric Energy Generation-Review. Int J Adv Res Sci Commun Technol. 2024 Oct; 4(2): 73–82. DOI: 10.48175/IJARSCT-19811.
12. Khadake SB, Padavale PV, Dhere PM, Lingade BM. Automatic Hand Dispenser and Temperature Scanner for Covid-19 Prevention. Int J Adv Res Sci Commun Technol. 2023 Jun; 3(2): 362. https://ijarsct.co.in/A11364.pdf
13. Landage SS, Chavan SR, Kokate PA, Lohar SP, Pawar MK, Khadake SB. Solar Outdoor Air Purifier With Air Quality Monitoring System. In Synergies of Innovation: Proceedings of Ncstem 2023. 2024 Sep; 260–266. At: https://www.researchgate.net/publication/383631190_Solar_Outdoor_Air_Purifier_with_Air_Quality_Monitoring_System
14. Khadake SB. Detecting salient objects of natural scene in a video's using spatio-temporal saliency & colour map. JournalNX-A Multidisciplinary Peer Reviewed Journal. 2016; 2(8): 30–5. Retrieved From Https://Repo.Journalnx.Com/Index.Php/Nx/Article/View/1070 .
15. Khadake Suhas B. Detecting Salient Objects In A Video's By Using spatio-Temporal Saliency & Colour Map. Int J Innov Eng Res Technol. 2021; 3(8): 1–9. Https://Repo.Ijiert.Org/Index.Php/Ijiert/Article/View/910.
16. Bhosale PS, Kokare PD, Potdar DS, Waghmode SD, Sawant VA, Khadake SB. DTMF Based Irrigation Water Pump Control System. Synergies of Innovation: Proceedings of Ncstem. 2023; 267–73. Available At: https://www.researchgate.net/publication/383629320_DTMF_Based_Irrigation_Water_Pump_Control_System
17. Pramod Korake, Harshwardhan Murade, Rushikesh Doke, Vikas Narale, Khadake Suhas B, Chavan Aniket S. Automatic Load Sharing of Distribution Transformer using PLC. Synergies of Innovation: Proceedings of NCSTEM 2023. 2024 Sep; 253–259. Available At: https://www.researchgate.net/publication/383628063_Automatic_Load_Sharing_of_Distribution_Transformer_using_PLC
18. Khadake SB, Kashid PJ, Kawade AM, Khedekar SV, Mallad HM. Electric vehicle technology battery management–review. Int J Adv Res Sci Commun Technol. 2023 Sep; 3(2): 319–25. Available at: https://www.researchgate.net/publication/374263508_Electric_Vehicle_Technology_Battery_Management_-_Review
19. Chounde A, Gopnarayan BB, Patil KB, Kamble SS. Human Health Care System: A New Approach towards Life. Grenze International Journal of Engineering & Technology (GIJET). 2024 Jun 15; 10(2): 5487–5494.
20. Patil VJ, Mallad HM, Gopnarayan BB, Pati KB. Maximize Farming Productivity through Agriculture 4.0 based Intelligence, with use of Agri Tech Sense Advanced Crop Monitoring System. Grenze International Journal of Engineering & Technology (GIJET). 2024 Jun 15; 10(2): 5127–5134.
21. Khadake SB, Khedekar SV, Kawade AM, Vyavahare SS, Kashid PJ, Chounde Amol B, Mallad HM. Solar Based Electric Vehicle Charging System: Review. Int Adv Res Sci Commun Technol. 2024 Dec; 4(2): 42–57. DOI: 10.48175/IJARSCT-22705
22. Randive Akshay B, Sneha Kiran Gaikwad, Khadake Suhas B, Mallad HM. Biodiesel: A Renewable Source of Fuel. Int Adv Res Sci Commun Technol. 2024 Dec; 4(3): 225–240. DOI: 10.48175/IJARSCT-22836 Available at https://www.researchgate.net/publication/387352609_Biodiesel_A_Renewable_Source_of_Fuel
23. Veena C, Sridevi M, Liyakat KK, Saha B, Reddy SR, Shirisha N. HEECCNB: An Efficient IoT-Cloud Architecture for Secure Patient Data Transmission and Accurate Disease Prediction in Healthcare Systems. In 2023 IEEE Seventh International Conference on Image Information Processing (ICIIP). 2023 Nov 22; 407–410. doi: 10.1109/ICIIP61524.2023.10537627. Available at: https://ieeexplore.ieee.org/document/10537627

24. Kazi KS. Computer-Aided Diagnosis in Ophthalmology: A Technical Review of Deep Learning Applications. In: Transformative Approaches to Patient Literacy and Healthcare Innovation. IGI Global Scientific Publishing; 2024; 112–35. https://doi.org/10.4018/979-8-3693-3661-8.ch006 Available at: https://www.igi-global.com/chapter/computer-aided-diagnosis-in-ophthalmology/342823
25. Kazi KS. AI-Driven-IoT (AIIoT)-Based Decision Making in Kidney Diseases Patient Healthcare Monitoring: KSK Approach for Kidney Monitoring. In: AI-Driven Innovation in Healthcare Data Analytics. IGI Global Scientific Publishing; 2025; 277–306. https://doi.org/10.4018/979-8-3693-7277-7.ch009
26. Pradeepa M, Jamberi K, Sajith S, Bai MR, Prakash A. Student health detection using a machine learning approach and IoT. In 2022 IEEE 2nd Mysore sub section International Conference (MysuruCon). 2022 Oct 16; 1–5. Available at: https://ieeexplore.ieee.org/document/9972445
27. Kazi KS, Mahant MA. Machine Learning-Driven Internet of Things (MLIoT)-Based Healthcare Monitoring System. In: Digitalization and the Transformation of the Healthcare Sector. IGI Global Scientific Publishing; 2025; 205–236. https://doi.org/10.4018/979-8-3693-9641-4.ch007
28. Mulani AO, Liyakat KK, Warade NS, Patil A, Kolte MT, Kinage K, Rana M, Salunkhe SS, Jadhav VS, Nagrale M. ML-powered Internet of Medical Things Structure for Heart Disease Prediction. J Pharmacol Pharmacother. 2025; 0976500X241306184. doi:10.1177/0976500X241306184
29. Odnala S, Shanthy R, Bharathi B, Pandey C, Rachapalli A, Liyakat KKS. Artificial Intelligence and Cloud-Enabled E-Vehicle Design with Wireless Sensor Integration. SSRN Electron J. 2025. https://doi.org/10.2139/ssrn.5107242
30. Neeraja P, Kumar RG, Kumar MS, Liyakat KKS, Vani MS. DL-Based Somnolence Detection for Improved Driver Safety and Alertness Monitoring. 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India. 2024; 589–594. doi: 10.1109/IC2PCT60090.2024.10486714. Available at: https://ieeexplore.ieee.org/document/10486714
31. Priya Mangesh Nerkar, Bhagyarekha Ujjwalganesh Dhaware. Predictive Data Analytics Framework Based on Heart Healthcare System (HHS) Using Machine Learning. J Adv Zool. 2023; 44(Spl Issue 2): 3673–3686. Available at: https://jazindia.com/index.php/jaz/article/view/1695
32. Priya Nerkar, Sultanabanu. IoT-Based Skin Health Monitoring System. Int J Biol Pharm Allied Sci. 2024; 13(11): 5937–5950. https://doi.org/10.31032/IJBPAS/2024/13.11.8488
33. Khadake SB, Chounde AB, Suryagan AA, MHM, Khadatare MR. AI-Driven-IoT(AIIoT) Based Decision Making System for High-Blood Pressure Patient Healthcare Monitoring, 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India. 2024; 96–102. doi: 10.1109/ICSCNA63714.2024.10863954.
34. Sayyad Liyakat, Khadake SB, Chounde AB, Suryagan AA, MHM, Khadatare MR. AI-Driven-IoT(AIIoT) Based Decision Making System for High-Blood Pressure Patient Healthcare Monitoring. 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India. 2024; 96–102. doi: 10.1109/ICSCNA63714.2024.10863954.

