# Optimized Blockchain-based KYC Verification: Enhancing Security, Efficiency, and Transparency with Ethereum

B. Vaidianathan, G. Regina Manicka Rajam, R.L. Shyja and
M.R. Anitha

***Abstract---*** *Know your customer (KYC) is the process of confirming user identities and assessing business risks from illicit activity. The manual KYC procedure is insecure, time-consuming, and expensive. With Blockchain technology's immutability, security, and decentralisation, such difficulties can be solved. KYC legal provide blockchain-based KYC verification by validating papers by a trustworthy network participant. This paper proposes an Ethereum-based Optimised KYC Blockchain system with symmetric AES encryption and LZ compression. The distributed ledger, cryptography, compression algorithm, and blockchain technologies make this system transparent, secure, efficient, and optimised. The suggested method uses Distributed Ledger Technology (Blockchain technology) to reduce KYC verification costs for institutions and speed up the process for clients. Our system is superior to conventional techniques since each customer only needs to be verified once, regardless of the number of institutions they want to link to. Since we use the DLT, we can securely communicate verification results with customers, boosting transparency. We created a Proof of Concept (POC) using the Ethereum API, websites as endpoints, and an android app as front office to prove its viability and efficacy. Overall, this strategy enhances customer experience, decreases costs, and boosts customer on boarding transparency.*

***Keywords---*** *AES Encryption, Blockchain System, Distributed Ledger Technology, Homomorphic Encryption, Compression Algorithm, Conventional Methods.*

## I. INTRODUCTION

BLOCKCHAIN technology eliminates the need for trusted third parties, creating an environment where equal trust is established between legitimate users. However, the transparency aspect of blockchain poses a threat to practical applications since every piece of information stored on the blockchain is publicly available. Consequently, applications that involve sensitive or private data requiring confidentiality and security management are not well-suited for traditional blockchain implementations [1]. Fully Homomorphic Encryption (FHE) methods have not been widely considered as end-to-end solutions for data security and privacy challenges. By utilizing the Ethereum Blockchain as a model, this study explores the feasibility and cost-effectiveness of integrating optimized FHE techniques based on lattice cryptography. The objective is to develop a novel and reliable system architecture that enhances security and privacy protection [2-5]. Due to the current limitations of blockchain, FHE computations are executed off-chain, while on-chain users employ non-FHE-based factors to perform instant ciphertext area calculations once smart contracts are published on the blockchain. To illustrate and compare platform evaluation results, a Vickrey auction system is being developed based on FHE and blockchain technology, ensuring that online auction prices remain confidential. Smart contracts autonomously handle both winner selection and fund distribution in real time [6-13].

Know Your Customer (KYC) is the process of identifying and authenticating a consumer's identity while assessing their intent in a business relationship [34-37]. Traditional manual KYC procedures are fraught with inefficiencies, including security vulnerabilities, cumbersome verification processes, and high costs. Blockchain technology, with its immutability, security, and decentralization, presents a viable solution to these challenges. Existing market solutions like kycchain.com and KYC.legal offer tools for verifying documents through a trusted network, but they rely on external trusted entities rather than leveraging the full potential of decentralized ledger technology (DLT). This study proposes an improved KYC blockchain framework based on Ethereum, incorporating proportional LZ compression and AES encryption [38-41].

The proposed system integrates a distributed ledger for transparency, cryptographic security for data protection, compression algorithms for efficiency, and blockchain functionalities for global optimization. By leveraging DLT, the system reduces the costs associated with conventional KYC authentication for organizations while significantly expediting the verification process for customers [42-45]. Unlike traditional approaches that require repeated verifications across different institutions, the proposed system ensures that once a

*B. Vaidianathan, Department of Electronics & Communication Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.*
*E-mail: vaidianathan@dhaanishcollege.in*
*G. Regina Manicka Rajam, Department of Electronics & Communication Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.*
*R.L. Shyja, Department of Electronics & Communication Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.*
*M.R. Anitha, Department of Electronics & Communication Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.*

**DOI: 10.9756/BIJAIP/V15I1/BIJ25002**
**Received: January 13, 2025; Revised: February 11, 2025; Accepted: March 14, 2025; Published: April 10, 2025**

customer undergoes KYC verification, the results can be reused across multiple institutions without redundant procedures. This feature enhances efficiency and minimizes friction in customer onboarding. The use of blockchain ensures that verification results are securely and reliably shared with customers, enhancing transparency. This approach employs Ethereum's API to develop a proof of concept (POC), where web applications serve as endpoints linked to a mobile application for user interactions [46-51]. The feasibility and effectiveness of this approach demonstrate its potential to transform the KYC verification landscape. By reducing verification costs, streamlining the onboarding process, and enhancing transparency, this system significantly improves customer experience while maintaining high security standards [52-59].

Blockchain technology fundamentally transforms the way KYC verification is conducted by addressing key pain points associated with traditional methods. The current system of manual KYC verification requires financial institutions to repeatedly verify a customer's identity each time they establish a new business relationship. This redundancy leads to increased costs, delays, and inefficiencies [60-65]. Furthermore, centralized databases used in traditional KYC processes are prone to security breaches, putting sensitive customer information at risk. The proposed blockchain-based solution resolves these challenges by providing a tamper-proof, decentralized, and immutable record of KYC verifications. The integration of cryptographic techniques such as AES encryption and LZ compression further enhances the system's efficiency and security. AES encryption ensures that sensitive customer data remains protected from unauthorized access, while LZ compression reduces data storage and transmission costs. These optimizations enable a seamless and cost-effective KYC verification process, making it more scalable and accessible for financial institutions [66-71].

Additionally, the use of smart contracts automates key aspects of the KYC process, reducing human intervention and associated risks. Smart contracts allow for the automatic execution of verification procedures once predefined conditions are met. For instance, when a customer submits their documents for verification, the smart contract triggers the authentication process, ensuring that only verified and authorized entities can access the information [72-81]. This automation eliminates manual errors and enhances the accuracy of the verification process. Another advantage of the proposed system is its ability to facilitate cross-institutional KYC verifications. In traditional settings, customers must undergo separate KYC checks for each financial institution they engage with. This repetitive process not only creates inefficiencies but also results in higher costs for both customers and institutions [82-87]. By implementing a blockchain-based solution, a customer's KYC credentials can be stored on the blockchain and accessed by multiple institutions with the customer's consent. This reduces redundancy, accelerates onboarding, and enhances customer convenience [88-91].

The proposed solution also introduces an additional layer of security by employing FHE techniques. Unlike traditional encryption methods that require data decryption for processing, FHE allows computations to be performed directly on encrypted data [92-99]. This ensures that sensitive customer information remains protected throughout the verification process. FHE-based encryption enhances data privacy and eliminates the risk of unauthorized access or data leaks. However, due to the computational complexity of FHE, its execution is performed off-chain to optimize performance and efficiency [100-107]. On-chain computations rely on non-FHE-based methods to conduct real-time ciphertext calculations, ensuring seamless integration with existing blockchain functionalities. Furthermore, the proposed system is designed to comply with regulatory requirements and industry standards [108-112]. Regulatory bodies worldwide impose strict KYC and Anti-Money Laundering (AML) guidelines to prevent financial crimes such as fraud and money laundering. By leveraging blockchain technology, the system ensures compliance with these regulations while maintaining transparency and auditability. Financial institutions can access an immutable record of KYC verifications, facilitating regulatory audits and enhancing accountability [113-117].

To validate the effectiveness of the proposed system, a proof of concept (POC) has been developed using Ethereum's API. The POC includes a web-based interface for institutions and a mobile application for customers. The web-based interface enables institutions to initiate KYC verifications, while the mobile application allows customers to submit their credentials securely [118-124]. Once verified, customers receive a cryptographic token that serves as proof of their KYC status. This token can be presented to other institutions for seamless onboarding without requiring redundant verifications. The evaluation of the POC demonstrates significant improvements in verification speed, cost reduction, and security. Traditional KYC processes often take several days to complete due to manual document checks and approvals. In contrast, the blockchain-based system streamlines the process, reducing verification times to minutes [125-126]. The elimination of intermediaries further lowers costs, making KYC verification more affordable for both institutions and customers. Overall, this study presents a robust and efficient blockchain-based KYC verification system that addresses the limitations of traditional methods. By integrating blockchain, cryptographic security, and FHE-based encryption, the proposed solution enhances data privacy, reduces verification costs, and improves customer experience. The system's ability to facilitate cross-institutional verifications further streamlines the onboarding process, making it a viable alternative to conventional KYC procedures. As blockchain technology continues to evolve, its application in KYC verification has the potential to revolutionize the financial industry, setting new standards for security, transparency, and efficiency.

## II. Literature Survey

Blockchain technology has emerged as a crucial tool for establishing trust among members without relying on Trusted Third Party Companies (TTPs). However, the transparency aspect of blockchain poses challenges, as all transaction data is openly accessible [14]. This openness becomes problematic for applications requiring confidentiality and security, such as those dealing with sensitive or private information. Traditional encryption methods, including Metamorphic Encryption

(MHE), fail to fully address these concerns, making Fully Homomorphic Encryption (FHE) a promising solution [15]. This paper explores the feasibility and cost implications of integrating an FHE-based lattice system into the Ethereum blockchain to create a secure and anonymous framework. Due to blockchain's current limitations, FHE operations are conducted off-chain, while on-chain users can request FHE-based computations for encrypted data after publishing smart contracts. To validate this approach, a Vickrey-based auction system utilizing FHE and blockchain is developed, ensuring confidentiality of bid prices while allowing smart contracts to determine winners and transfer funds autonomously [16].

By leveraging cryptographic techniques, this system ensures privacy without compromising the integrity and reliability of computations. However, implementing a certified homomorphic encryption system poses challenges due to its complexity. In this study, a novel security concept is introduced, integrating data confidentiality with legitimacy in homomorphic encryption [21]. The proposed system incorporates both fully homomorphic and verifiable morphic encryption, creating a certified scheme that meets stringent security requirements. The model ensures protection against plaintext attacks and maintains identity anonymity. Moreover, it is compatible with diverse datasets, reducing computational overhead [22]. A multisite verification system is developed to enhance security and mitigate vulnerabilities associated with traditional homomorphic encryption schemes [23]. Homomorphic encryption allows computations on encrypted data without decryption, making it ideal for applications such as secure cloud computing. Recent advancements in this field have led to various homomorphic encryption schemes, including Certificateless Fully Homomorphic Encryption (CLFHE). This research builds on previous CLFHE models, ensuring semantic security based on Learning with Errors (LWE) problems [24]. Two CLFHE schemes are proposed: one securing data under an undefined oracle model and another offering enhanced privacy in a standard cryptographic framework. These schemes address anonymity concerns while maintaining computational efficiency [25].

Brakerski-Fan-Vercauteren (BFV) homomorphic encryption is widely used for its efficiency in polynomial operations. To optimize its performance, this study develops FPGA-based acceleration techniques. A hardware-accelerated framework is implemented using the Xilinx Virtex-07 FPGA, reducing latency by 7-12 times compared to pure software execution [17]. The accelerator significantly enhances the Simplified Statistics Library, supporting encryption and decryption operations efficiently. By offloading polynomial computations to dedicated hardware, the system achieves substantial speed improvements, making homomorphic encryption more practical for real-world applications [18]. Another significant advancement in homomorphic encryption involves Residue Number System (RNS) optimizations. Two major RNS schemes, Bajard-Eynard-Hasan-Zucca (BEHZ) and Halevi-Polyakov-Shoup (HPS), are analyzed for their performance on CPUs and GPUs. Experimental results indicate that the HPS variant outperforms BEHZ in multi-application environments, demonstrating superior computational efficiency [19]. The GPU-optimized implementation achieves a 51ms processing time for homomorphic operations, making it twice as fast as previous results. This advancement is particularly beneficial for applications requiring deep computation layers, such as neural networks and machine learning models [20].

Sedenion-based homomorphic encryption offers another layer of security by mapping 16-dimensional vectors to encrypted spaces. This approach enables multi-level encryption, enhancing data confidentiality. The security of this system is derived from solving multivariable quadratic equations over bounded rings, making it resistant to post-quantum attacks [28]. The proposed scheme utilizes Frobenius auto-scaling to optimize encryption efficiency while maintaining robustness. Unlike conventional encryption systems, sedenion-based methods provide greater security, making them suitable for applications requiring high levels of confidentiality. Furthermore, the study investigates the integration of Karatsuba's algorithm into homomorphic encryption systems. Traditionally, Fast Fourier Transform (FFT) is employed to accelerate polynomial multiplications [29]. However, Karatsuba's algorithm provides an alternative that reduces computational complexity without compromising security. The hardware-accelerated implementation achieves a 23% reduction in processing time compared to FFT-based methods, demonstrating its viability for homomorphic encryption schemes. The FPGA-based accelerator enhances Fan-Verkouteren homomorphic encryption, achieving a 5.05x speedup for polynomial multiplications and 167.3x for iterative operations [30].

Homomorphic encryption is crucial for privacy-preserving state estimation in cyber-physical systems. This study proposes an encrypted state estimator (ESE) leveraging homomorphic encryption techniques. The approach ensures that sensitive system parameters remain confidential while maintaining accurate state estimations [31]. Hackers gaining unauthorized access to communication channels cannot extract meaningful information, as the encryption scheme effectively conceals critical data. The proposed ESE model is validated through real-world hardware implementations, demonstrating its effectiveness in protecting system integrity. To address practical implementation challenges, a hybrid encryption scheme combining Fully Homomorphic Encryption (FHE) with additively homomorphic techniques is introduced [32]. This hybrid model balances security and computational efficiency, allowing encrypted operations while preserving data privacy. The system is optimized using block-level and region-level flow techniques, improving clock frequency and enhancing polynomial computations. The FPGA implementation of this hybrid encryption scheme achieves significant speed improvements, demonstrating its applicability in secure cloud computing environments [33].

Homomorphic encryption offers a transformative approach to data security, enabling computations on encrypted data without decryption [27]. This study presents novel methodologies for optimizing homomorphic encryption through FPGA acceleration, RNS-based optimizations, and hybrid encryption models. By integrating advanced cryptographic techniques, these innovations enhance security, efficiency, and scalability. Future research will explore further

optimizations, including post-quantum cryptographic solutions and enhanced FPGA architectures for real-time secure computations [26].

## III. Methodology

Requirements elicitation is the process of gathering information regarding the requirements of a system. This method is often referred to as "requirement collecting" in the literature. Attempting to elicit specifications is challenging because there is no absolute certainty that all user demands have been captured simply by asking what the system should or should not do. The system must fulfill the functional criterion of performing what it was designed to accomplish. A functional requirement specifies what a system should achieve, while non-functional requirements define the constraints and conditions under which the system will operate to achieve those goals. These requirements together shape the foundation of a well-defined system that meets user expectations while maintaining efficiency and security. Incorporating a prototype of a decentralized, time-stamped ledger into business and insurance organizations' KYC processes can significantly streamline operations by enabling quicker and more accurate real-time data exchanges among multiple stakeholders. This facilitates faster and more precise verification, reducing errors and improving efficiency. Compared to conventional solutions, a blockchain-based approach is preferable due to its immutable ledger, ease of integration, and significantly lower operational and infrastructure costs. By implementing blockchain, businesses can ensure enhanced security, transparency, and automation in their KYC processes, thus reducing the complexities associated with traditional identity verification methods.

A system's functional requirements define the specific operations and actions it must be capable of performing. These requirements are typically documented in written descriptions to ensure clarity and consistency. A blockchain-based KYC system introduces several crucial functionalities that enhance efficiency and security. One major functional requirement is its ability to minimize duplication in the rectification process while enabling automated lodging of KYC details. This automation has the potential to significantly reduce expenses for all parties involved, from financial institutions to end users. Additionally, the trusted workflow of KYC, powered by technological innovation, provides distinct advantages to companies, regulatory authorities, and consumers worldwide by offering a secure and streamlined verification process. Another vital aspect of the system is its use of one-way hash data formation, which ensures that while a hash value can be generated from plaintext content, it is computationally infeasible to reverse the process and derive the original content from the hash. This feature guarantees data integrity and security by preventing unauthorized modifications or breaches. The blockchain's tamper-resistant nature further strengthens this security framework. The decentralized ledger structure ensures that once data is recorded, it cannot be altered or erased without network consensus, making the system highly resistant to fraud or manipulation. This immutability ensures that all transactions and identity verifications remain secure and traceable, fostering trust among stakeholders.

The overall design of the system is structured to clearly define the various entities involved and their interdependencies. The high-level architecture establishes a framework that integrates these entities into a cohesive and efficient ecosystem. By utilizing blockchain's decentralized nature, the system ensures seamless interaction among users, verification authorities, and service providers. The architecture is designed to support real-time updates while maintaining data privacy and security. Transactions recorded on the blockchain are cryptographically secured, ensuring that only authorized entities can access relevant details. This decentralized approach eliminates the reliance on a central authority, reducing bottlenecks and enhancing operational efficiency (Figure 1).

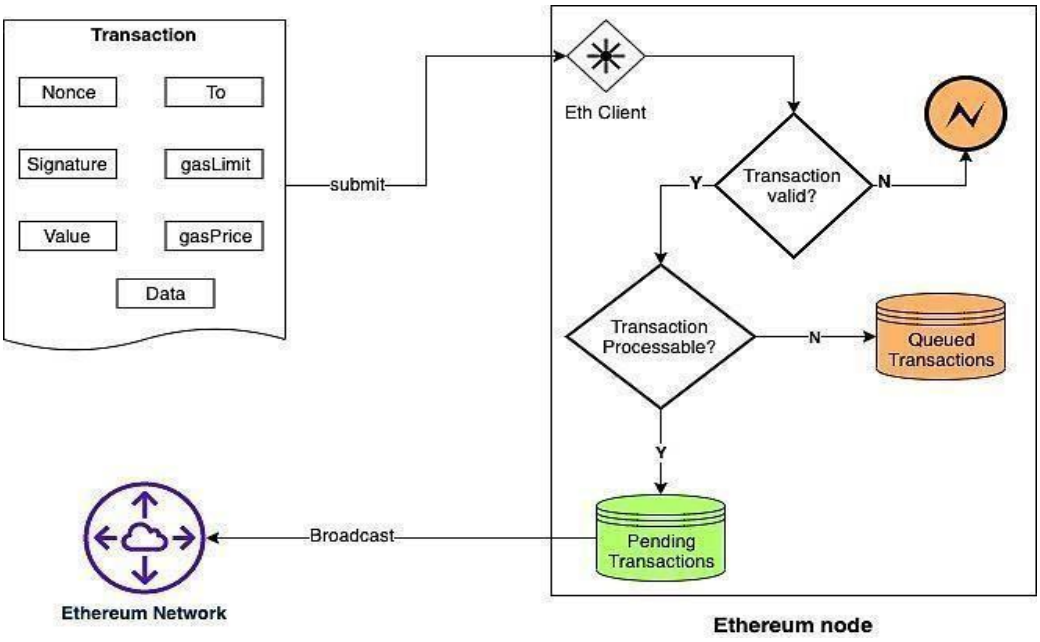


Figure 1: Flowchart

The system's design also prioritizes scalability, ensuring that as more users and organizations adopt the platform, its performance remains optimal. The distributed nature of blockchain enables multiple entities to interact without risking data breaches or inefficiencies commonly associated with traditional centralized systems. This enhances the reliability and robustness of the KYC process, making it more efficient for businesses and regulatory bodies. By leveraging smart contracts, the system can automate various verification processes, reducing the need for manual intervention and expediting KYC approvals. This automation, combined with blockchain's inherent security features, ensures that the system is both reliable and user-friendly. Overall, the integration of blockchain into KYC processes presents a revolutionary approach to identity verification and data management. The system not only enhances security and efficiency but also reduces operational costs and improves user experience. By ensuring transparency, immutability, and decentralized control, the proposed blockchain-based KYC system offers a future-proof solution to the challenges associated with traditional KYC methods.

## IV. Result and Discussion

Blockchain is a distributed network that offers flexibility while ensuring privacy, security, and transparency. Unlike traditional financial or business systems, blockchain does not rely on a centralized intermediary to guarantee transactions. Instead, it ensures that each transaction is individually secured and verified through cryptographic mechanisms. The compliance protocol, an essential part of any blockchain network, has been recently integrated to strengthen security and operational consistency. The consensus algorithm is the fundamental process through which each node in the blockchain network reaches an agreement on the current state of the shared ledger. This synchronization method guarantees that every newly added block represents an accurate version that all participating nodes accept as valid.

One of the core objectives of the blockchain consensus mechanism is to establish trust among unknown peers within a distributed computing environment. Every node must participate in this consensus approach to ensure that transactions remain secure, verifiable, and immutable. The consensus mechanism enables access to agreements, partnerships, and equal rights for all network participants. By ensuring a fair and transparent approach to transaction validation, the algorithm plays a crucial role in the overall functionality of blockchain networks. Strengthening these networks and fostering trust is achieved through well-coordinated strategies, making blockchain a reliable alternative to conventional centralized systems. Various consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), have been developed to enhance security, efficiency, and scalability within blockchain frameworks. Understanding these mechanisms is crucial to comprehending the trust model underlying blockchain technology.

In addition to its role in digital transactions, blockchain technology has applications in manufacturing and quality assurance. A batch packaging log, for instance, plays a vital role in ensuring compliance with Good Manufacturing Practice (GMP) guidelines. This report is crucial as it documents the packaging procedure of a batch and contains all the necessary details required for GMP documentation. It serves as a comprehensive record that tracks the journey of a lot from the distribution phase to the dispatching phase, providing a step-by-step guide that must be followed during the packaging process. The batch packaging log includes real-time data from the packaging process and serves as crucial evidence that all batches have been correctly manufactured, inspected, and validated by production and quality assurance teams.

Moreover, the batch packaging log provides detailed activity records, indicating who performed each task and at what time. This level of transparency ensures accountability and traceability, both of which are fundamental in industries where precision and compliance are essential. For chemical and process manufacturers, a batch manufacturing record (BMR) is an indispensable document. It helps maintain quality control, ensures regulatory compliance, and provides insights into production efficiency. The integration of blockchain technology into batch manufacturing records can further enhance transparency, security, and reliability by providing an immutable and tamper-proof digital ledger for tracking manufacturing processes. As blockchain continues to evolve, its applications in manufacturing, healthcare, finance, and supply chain management will further redefine data security and operational efficiency across industries (Figure 2).

The primary system to be implemented focuses on integrating human movements and actions into its framework. This implementation is crucial as it enables the system to understand user inputs and generate corresponding outputs. The system responsible for capturing human interactions and movements must be accurately configured to ensure that the collected data leads to precise interpretations and subsequent responses. The effectiveness of the system depends largely on its ability to process inputs through various layers and generate appropriate outputs based on the state of the system and the components involved in the processing. The analysis of input data occurs in a depth-wise manner, where pooling layers are utilized to extract relevant features. In this process, sound separation is performed using specialized sound filters at different layers. The accuracy of the input processing is influenced by the layer-wise thickness, which determines the level of detail captured. Various layers of modulation contribute to analyzing and separating the input data, leading to the generation of an appropriate simulation of the required output. This ensures that the system produces results that align with expectations and meet the desired functional criteria.

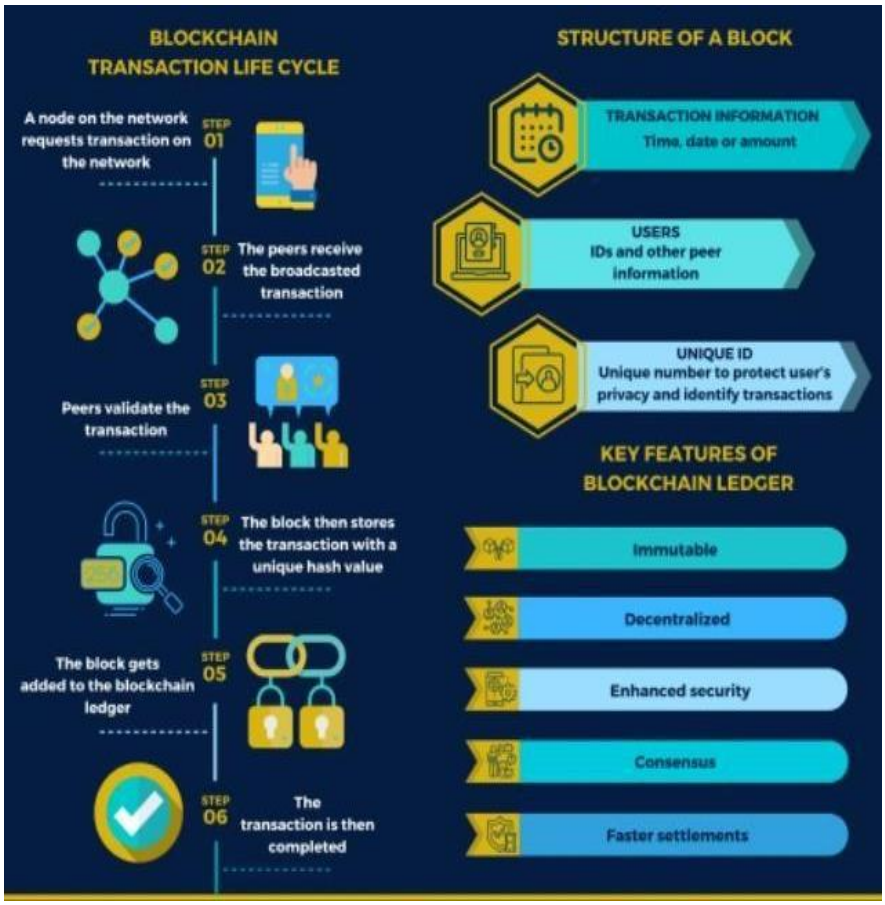


Figure 2: Blockchain Record Creation Works

For individuals who are disabled or unable to perform physical movements, such a system becomes particularly valuable. By understanding the system's responses to different inputs, users can interact with technology in a meaningful way. The system processes and integrates the input, allowing users to comprehend how their interactions influence the output. This is essential for ensuring accessibility and usability. The compatibility algorithm used in the system plays a significant role in selecting the next-generation miner, as seen in blockchain technology. Bitcoin employs a Proof of Work (PoW) compatibility algorithm, which is designed to solve complex mathematical problems efficiently. The high computational requirements for solving these problems make it necessary to identify a nearby block mine to optimize processing. Proof of Work remains a widely used consensus mechanism, though alternative models have been explored for increased efficiency and sustainability. Ethereum, for instance, has transitioned from PoW to Proof of Stake (PoS) as part of its integration process. In PoS, rather than solving computationally intensive puzzles, the guarantor secures the system by staking a certain number of coins. Once a block is proposed, all verifiers approve its legitimacy. The staked amount influences the selection process, ensuring that those with a higher stake have a greater probability of being chosen to validate new blocks. This approach incentivizes participants to act honestly, as their economic investment is at risk. PoS reduces the need for expensive hardware and high energy consumption, making it an attractive alternative to traditional mining methods.

Proof of Burn (PoB) introduces a unique approach where miners demonstrate their commitment by "burning" coins—sending them to an inaccessible address. This process grants them mining rights based on the number of coins they have sacrificed. Although PoB offers an alternative to PoW, it has been criticized for its inefficiency in resource utilization, as it effectively destroys assets without direct utility. Despite this drawback, PoB allows individuals to gain mining privileges without competing in computational power. Variations of this concept exist in blockchain implementations, each designed to balance decentralization, security, and efficiency. Another consensus mechanism, Proof of Capacity (PoC), enables miners to utilize available disk space instead of computational power or financial stakes. Participants with more storage capacity have a higher chance of being selected to mine the next block and receive a reward. In permissioned blockchain networks, this mechanism can be particularly useful, as it distributes mining rights based on resource allocation rather than computational strength. The probability of block creation is adjusted dynamically to ensure fairness among participants. To prevent nodes from winning too frequently or producing blocks in rapid succession, additional algorithms are integrated to regulate the selection process. Various other compliance algorithms exist, including Work Proof, Weight Proof, Validation Proof, and Leased Stake Proof, each catering to different blockchain applications and network structures.

For blockchain platforms such as Ethereum, transaction execution comes with a cost measured in gas. A Fully Homomorphic Encryption (FHE) calculation requires a substantial number of computational operations, resulting in high costs. While blockchain offers robust security and privacy features, the challenge lies in maintaining efficiency and affordability. Addressing this issue requires innovative approaches, particularly in protecting against quantum attacks. Modern anti-quantum auction strategies leverage FHE to secure online bidding processes within blockchain environments. However, the current cost of implementing FHE-based auctions remains a significant barrier, necessitating further optimization. A critical concern in blockchain-based auction systems is ensuring the confidentiality of secret keys. If a seller fails to protect the secrecy of the bidding process, disputes may arise, compromising the integrity of the auction. To mitigate this risk, limitations can be placed on the number of online tenders processed simultaneously. Additionally, implementing bidder reputation scores, reward structures, and penalty mechanisms can enhance trust within the system.

Our proposed paper introduces a scheme that integrates FHE with Ethereum's blockchain to achieve both confidentiality and fairness. This framework ensures that sensitive data remains protected while maintaining the integrity of the bidding process. From a broader perspective, the adoption of lattice-based FHE schemes provides robust post-quantum security. These schemes rely on the hardness of the Shortest Vector Problem (SVP), which remains challenging even for quantum computers. This level of security ensures that blockchain-based auction mechanisms remain resistant to evolving threats posed by quantum computing advancements. The integration of FHE and blockchain technology paves the way for secure, transparent, and decentralized digital interactions. While challenges such as computational overhead and cost persist, continuous advancements in cryptographic techniques and blockchain consensus mechanisms are driving improvements. As these technologies evolve, they will further enhance privacy, security, and efficiency in various applications, including financial transactions, supply chain management, and secure communications. By leveraging blockchain's decentralized nature and FHE's encryption capabilities, organizations can establish trustless ecosystems that prioritize data security without compromising accessibility or usability.

## V. Conclusion

The blockchain-based resolution offers numerous advantages, enabling seamless and secure information exchange among trusted organizations while significantly reducing operational costs. By implementing this approach, the expense of developing a new resolution is minimized to just 19% during KYC handling, leading to substantial savings. Integrating the KYC procedure establishes a standardized user entry framework, making the process more efficient and cost-effective. This standardization eliminates redundant verifications, streamlining identity management across multiple organizations. Furthermore, the implementation of blockchain in KYC enhances security by leveraging its immutable ledger, preventing unauthorized data modifications. This decentralized approach ensures transparency, reducing the risks of fraud and identity theft. Additionally, blockchain technology allows real-time data sharing among relevant entities, accelerating the verification process and enhancing user experience. The concept of an artifact-strong code is introduced as a valuable tool for testing and development. This adaptable framework enables developers and organizations to experiment with new ideas in a test environment before deploying them in real-world applications. By refining and evolving the code, businesses can improve efficiency, practicality, and overall effectiveness. The open-access nature of this solution fosters innovation, as interested parties can modify and optimize the system based on their specific requirements. Overall, blockchain integration in KYC presents a transformative solution, offering cost savings, enhanced security, and increased operational efficiency. The adoption of this approach not only simplifies identity verification processes but also establishes a more reliable and scalable framework for organizations handling sensitive user data.

## References


[1] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "Rated) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory (TOCT)*, vol. 6, no. 3, p. 136, 2014.

[2] R. Vadisetty and A. Polamarasetti, "Gen AI for Real- Time Traffic Prediction and Autoscaling in Cloud Computing Education 4.0," *In 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2024, pp. 735–741.

[3] R. Vadisetty and A. Polamarasetti, "Quantum Computing for Cryptographic Security with Artificial Intelligence," *In 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA)*, 2024, pp. 252–260.

[4] Ahmad, P. Potluri, A. R. Yeruva, P. Satyasriram, S. Harizan, R. Kumar, and D. M. Alsekait, "Energy Efficient Intrusion Detection in a heterogeneous environment of Wireless sensor networks," *International Journal of Intellectual Property Management*, vol. 20, no. 13, pp. 13–1493, 2022.

[5] R. Yeruva and V. Basavegowda Ramu, "AIOps Observability and Performance Impact of AI and ML Applications for Central Nervous System Drug Discoveries," *In EAI/Springer Innovations in Communication and Computing*, Springer, Cham, Switzerland, pp. 239–252, 2023.

[6] D. Kodi and S. Chundru, "Unlocking new possibilities: How advanced API integration enhances green innovation and equity," *In Advances in Environmental Engineering and Green Technologies, IGI Global*, 2025, pp. 437–460.

[7] D. Kodi and B. C. C. Marella, "Fraud Resilience: Innovating Enterprise Models for Risk Mitigation," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 12S, pp. 683–695, Jan. 2025.

[8] C. C. Marella and D. Kodi, "Generative AI for fraud prevention: A new frontier in productivity and green innovation," *In Advances in Environmental Engineering and Green Technologies, IGI Global*, 2025, pp. 185–200.

[9] S. A. Milu, S. Akter, A. Fathima, T. Talukder, I. Islam, and M. I. S. Emon, "Design and Implementation of hand gesture detection system using HM model for sign language recognition development," *J. Data Anal. Inf. Process.*, vol. 12, no. 2, pp. 139–150, 2024.

[10] Vashisth, B. Singh, and R. S. Batth, "QMRNB: Design of an Efficient Q-Learning Model to Improve Routing Efficiency of UAV Networks via Bioinspired Optimizations," *Int. J. Comput. Netw. Appl.*, vol. 10, no. 2, pp. 256–256, 2023.

[11] Vashisth, B. Singh, and R. S. Batth, "UAV Path Planning: Challenges, Strategies, and Future Directions," *In New Innovations in AI, Aviation, and Air Traffic Technology, S. Khalid and N. Siddiqui, Eds. IGI Global Scientific Publishing*, USA, 2024, pp. 150–174.

[12] Vashisth, B. Singh, R. Garg, and S. Kumpsuprom, "BPACAR: Design of a Hybrid Bioinspired Model for Dynamic Collision-Aware Routing with Continuous Pattern Analysis in UAV Networks," *Microsyst. Technol.*, vol. 30, no. 4, pp. 411–421, Nov. 2023.

[13] Ahmed, Z. H., Hameed, A. S., Mutar, M. L., & Haron, H. (2023). An Enhanced Ant Colony System Algorithm Based on Subpaths for Solving the Capacitated Vehicle Routing Problem. *Symmetry*, 15(11), 2020.

[14] Mutar, M. L., Burhanuddin, A., Hameed, S., Yusof, N., Alrifaie, M. F., & Mohammed, A. A. (2020). Multi-objectives ant colony system for solving multi-objectives capacitated vehicle routing problem. *Journal of Theoretical and Applied Information Technology*, 98(24).

[15] Alrifaie, M. F., Ahmed, Z. H., Hameed, A. S., & Mutar, M. L. (2021). Using machine learning technologies to classify and predict heart disease. *International Journal of Advanced Computer Science and Applications*, 12(3).

[16] Hameed, A. S., Aboobaider, B. M., Choon, N. H., Mutar, M. L., & Bilal, W. H. (2018). Review on the methods to solve combinatorial optimization problems particularly: quadratic assignment model. *International Journal of Engineering & Technology*, 7(3.20), 15-20.

[17] M. Faisal et al., "Determining rural development priorities using a hybrid clustering approach: A case study of South Sulawesi, Indonesia," *Int. J. Adv. Technol. Eng. Explor.*, vol. 10, no. 103, 2023.

[18] M. Faisal, T. K. A. Rahman, I. Mulyadi, K. Aryasa, Irmawati, et al., "A novelty decision-making based on hybrid indexing, clustering, and classification methodologies: An application to map the relevant experts against the rural problem," *Decis. Mak. Appl. Manag. Eng.*, vol. 7, no. 2, pp. 132–171, 2024.

[19] S. Panyaram, "Digital Twins & IoT: A New Era for Predictive Maintenance in Manufacturing," *International Journal of Innovations in Electronic & Electrical Engineering*, vol. 10, no. 1, pp. 1-9, 2024.

[20] S. Panyaram, "Automation and Robotics: Key Trends in Smart Warehouse Ecosystems," *International Numeric Journal of Machine Learning and Robots*, vol. 8, no. 8, pp. 1-13, 2024.

[21] S. Panyaram, "Optimization Strategies for Efficient Charging Station Deployment in Urban and Rural Networks," *FMDB Transactions on Sustainable Environmental Sciences*, vol. 1, no. 2, pp. 69–80, 2024.

[22] L. N. R. Mudunuri and V. Attaluri, "Urban development challenges and the role of cloud AI-powered blue-green solutions," *In Advances in Public Policy and Administration, IGI Global*, USA, pp. 507–522, 2024.

[23] Attaluri, "Secure and Scalable Machine-to-Machine Secrets Management Solutions," *Int. J. Mach. Learn. Artif. Intell.*, vol. 5, no. 5, pp. 1–13, Jul. 2024.

[24] V. Attaluri, "Dynamic User Permission Locking Based on Database Role Changes," *Int. J. Adv. Eng. Res.*, vol. 27, no. 1, pp. 1–9, 2024.

[25] V. Attaluri, "Real-Time Monitoring and Auditing of Role Changes in Databases," *Int. Numer. J. Mach. Learn. Robots*, vol. 7, no. 7, pp. 1–13, Nov. 2023.

[26] V. Attaluri, "Securing SSH Access to EC2 Instances with Privileged Access Management (PAM)," *Multidiscip. Int. J.*, vol. 8, no. 1, pp. 252–260, Dec. 2022.

[27] S. Panyaram, "Integrating Artificial Intelligence with Big Data for Real-Time Insights and Decision-Making in Complex Systems," *FMDB Transactions on Sustainable Intelligent Networks.*, vol.1, no.2, pp. 85–95, 2024.

[28] S. Panyaram, "Utilizing Quantum Computing to Enhance Artificial Intelligence in Healthcare for Predictive Analytics and Personalized Medicine," *FMDB Transactions on Sustainable Computing Systems.*, vol. 2, no. 1, pp. 22–31, 2024.

[29] S. Panyaram, "Digital Transformation of EV Battery Cell Manufacturing Leveraging AI for Supply Chain and Logistics Optimization," *International Journal of Innovations in Scientific Engineering*, vol. 18, no. 1, pp. 78-87, 2023.

[30] S. Panyaram, "Connected Cars, Connected Customers: The Role of AI and ML in Automotive Engagement," *International Transactions in Artificial Intelligence*, vol. 7, no. 7, pp. 1-15, 2023.

[31] M. Faisal, Irmawati, T. K. A. Rahman, Jufri, Sahabuddin, Herlinah, and I. Mulyadi, "A hybrid MOO, MCGDM, and sentiment analysis methodologies for enhancing regional expansion planning: A case study Luwu - Indonesia," *Int. J. Math. Eng. Manag. Sci.*, vol. 10, no. 1, pp. 163–188, 2025.

[32] M. Faisal and T. K. A. Rahman, "Optimally enhancement rural development support using hybrid multy object optimization (MOO) and clustering methodologies: A case South Sulawesi - Indonesia," *Int. J. Sustain. Dev. Plan.*, vol. 18, no. 6, pp. 1659–1669, 2023.

[33] Mulyadi, M. Thamrin, M. Faisal, S. Yunarti, Saharuddin, A. Djalil, and S. Mallu, "A hybrid model for palm sugar type classification: Advancing image-based analysis for industry applications," *Ingén. Syst. Inf.*, vol. 29, no. 5, pp. 1937–1948, 2024.

[34] Mutar, M. L., Aboobaider, B. M., & Hameed, A. S. (2017). Rev Vehicle Routing Problem and Future Research Trend. *International Journal of Applied Engineering Research* ISSN, 0973-4562.

[35] Sari, F. A. O., Alrammahi, A. A. H., Hameed, A. S., Alrikabi, H. M. B., Abdul–Razaq, A. A., Nasser, H. K., & AL-Rifaie, M. F. (2022). Networks cyber security model by using machine learning techniques. *Int. J. Intell. Syst. Appl. Eng.*, 10(1), 257-263.

[36] Alrifaie, M. F., Ismael, O. A., Hameed, A. S., & Mahmood, M. B. (2021, December). Pedestrian and objects detection by using learning complexity-aware cascades. *In 2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA)* (pp. 12-17). IEEE.

[37] Hameed, A. S., Aboobaider, B. M., Ngo, H. C., & Mutar, M. L. (2018). Improved discrete differential evolution algorithm in solving quadratic assignment problem for best solutions. *International Journal of Advanced Computer Science and Applications*, 9(12).

[38] Khudhair, A. A., Khudhair, M. A., Jaber, M. M., Awreed, Y. J., Ali, M. H., AL-Hameed, M. R.,... & Hameed10, A. S. (2023). Impact on Higher Education and College Students in Dijlah University after COVID through E-learning. *Computer-Aided Design and Applications*, 104-115.

[39] Hameed, A. S., Mutar, M. L., Alrikabi, H. M. B., Ahmed, Z. H., Abdul–Razaq, A. A., & Nasser, H. K. (2021). A hybrid method integrating a discrete differential evolution algorithm with tabu search algorithm for the quadratic assignment problem: A new approach for locating hospital departments. *Mathematical Problems in Engineering*, 2021(1), 6653056.

[40] Jalil, A. T., Karim, N., Ruhaima, A. A. K., Sulaiman, J. M. A., Hameed, A. S., Abed, A. S.,... & Rayani, Y. (2024). Analytical model for thermoelastic damping in in-plane vibrations of circular cross-sectional micro/nanorings with dual-phase-lag heat conduction. *Journal of Vibration Engineering & Technologies*, 12(1), 797-810.

[41] Hameed, A. S., Aboobaider, B. M., Choon, N. H., Mutar, M. L., & Bilal, W. H. (2018). A comparative study between the branch and cut algorithm and ant colony algorithm to solve the electric meter reader problem in rural areas. *Opcion*, 34(86), 1525-1539.

[42] G. Kaur, B. Singh, R. S. Batth, and R. Garg, "BATFE: Design of a Hybrid Bioinspired Model for Adaptive Traffic Flow Control in Edge Devices," *Microsyst. Technol.*, Dec. 2024.

[43] G. Kaur, B. Singh, and R. S. Batth, "Design of an Efficient QoS-Aware Adaptive Data Dissemination Engine with DTFC for Mobile Edge Computing Deployments," *Int. J. Comput. Netw. Appl.*, vol. 10, no. 5, p. 728, Oct. 2023.

[44] S. S. Mahtab, R. A. Anonto, T. Talukder, A. Raihan, and I. Islam, "Etching Technologies in Semiconductor Manufacturing: A Short Review," *In Proc. Int. Conf. Emerg. Appl. Mater. Sci. Technol.*, Cham: Springer Nature Switzerland, 2024, pp. 319–324.

[45] T. Talukder, "Scanning Magnetometry with a Low Cost NV Diamond Quantum Sensor Probe," *M.S. thesis, Morgan State Univ.*, 2024.

[46] C. C. Marella and A. Palakurti, "Harnessing Python for AI and machine learning: Techniques, tools, and green solutions," *In Advances in Environmental Engineering and Green Technologies*, IGI Global, 2025, pp. 237–250.

[47] B. C. C. Marella and D. Kodi, "Generative AI for fraud prevention: A new frontier in productivity and green innovation," *In Advances in Environmental Engineering and Green Technologies*, IGI Global, 2025, pp. 185–200.

[48] B. C. C. Marella, "Driving Business Success: Harnessing Data Normalization and Aggregation for Strategic Decision-Making," *Int. J. Intell. Syst. Appl. Eng.*, vol. 10, no. 2s, pp. 308–317, Nov. 2022.

[49] B. C. C. Marella, "Data Synergy: Architecting Solutions for Growth and Innovation," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 11, no. 9, pp. 10551–10560, Sep. 2023.

[50] B. C. C. Marella, "From Silos to Synergy: Delivering Unified Data Insights across Disparate Business Units," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 12, no. 11, pp. 11993–12003, Nov. 2024.

[51] B. C. C. Marella, "Scalable Generative AI Solutions for Boosting Organizational Productivity and Fraud Management," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 10s, pp. 1013–1023, Aug. 2023.

[52] Kodi and M. B. C. Chowdari, "Fraud resilience: Innovating enterprise models for risk mitigation," *Journal of Information Systems Engineering and Management*, vol. 10, no. 12s, pp. 683–695, 2024.

[53] V. R. Anumolu and B. C. C. Marella, "Maximizing ROI: The intersection of productivity, generative AI, and social equity," *In Advances in*

*Environmental Engineering and Green Technologies*, IGI Global, 2025, pp. 373–386.

[54] Palakurti and D. Kodi, "Building intelligent systems with Python: An AI and ML journey for social good," *In Advances in Environmental Engineering and Green Technologies, IGI Global*, 2025, pp. 77–92.

[55] Kodi, "Data Transformation and Integration: Leveraging Talend for Enterprise Solutions," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 13, no. 9, p. 13, Sep. 2024.

[56] D. Kodi, "Performance and Cost Efficiency of Snowflake on AWS Cloud for Big Data Workloads," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 12, no. 6, p. 14, Jun. 2024.

[57] S. M. Abdulrahman, R. R. Asaad, H. B. Ahmad, A. A. Hani, S. R. Zeebaree, and A. B. Sallow, "Machine learning in nonlinear material physics," *J. Soft Comput. Data Min.*, vol. 5, no. 1, pp. 122–131, 2024.

[58] S. M. Abdulrahman, A. A. Hani, S. R. Zeebaree, R. R. Asaad, D. A. Majeed, A. B. Sallow, and H. B. Ahmad, "Intelligent home IoT devices: An exploration of machine learning-based networked traffic investigation," *J. Ilm. Ilmu Terapan Univ. Jambi*, vol. 8, no. 1, pp. 1–10, 2024.

[59] H. B. Ahmad, R. R. Asaad, S. M. Almufti, A. A. Hani, A. B. Sallow, and S. R. Zeebaree, "Smart home energy saving with big data and machine learning," *J. Ilm. Ilmu Terapan Univ. Jambi*, vol. 8, no. 1, pp. 11–20, 2024.

[60] S. M. Almufti, H. B. Ahmad, R. B. Marqas, and R. R. Asaad, "Grey wolf optimizer: Overview, modifications and applications," *Int. Res. J. Sci. Technol. Educ. Manag.*, vol. 1, no. 1, p. 1, 2021.

[61] S. Almufti, R. Asaad, and B. Salim, "Review on elephant herding optimization algorithm performance in solving optimization problems," *Int. J. Eng. Technol.*, vol. 7, no. 1, pp. 6109–6114, 2018.

[62] S. Almufti, R. Marqas, and R. Asaad, "Comparative study between elephant herding optimization (EHO) and U-turning ant colony optimization (U-TACO) in solving symmetric traveling salesman problem (STSP)," *J. Adv. Comput. Sci. Technol.*, vol. 8, no. 2, p. 32, 2019.

[63] B. Sallow, R. R. Asaad, H. B. Ahmad, S. M. Abdulrahman, A. A. Hani, and S. R. M. Zeebaree, "Machine learning skills to K–12," *J. Soft Comput. Data Min.*, vol. 5, no. 1, pp. 132–141, 2024.

[64] R. R. Asaad, S. M. Abdulrahman, and A. A. Hani, "Advanced encryption standard enhancement with output feedback block mode operation," *Acad. J. Nawroz Univ.*, vol. 6, no. 3, pp. 1–10, 2017.

[65] R. R. Asaad, S. M. Abdurahman, and A. A. Hani, "Partial image encryption using RC4 stream cipher approach and embedded in an image," *Acad. J. Nawroz Univ.*, vol. 6, no. 3, pp. 40–45, 2017.

[66] Hani, A. B. Sallow, H. B. Ahmad, S. M. Abdulrahman, R. R. Asaad, S. R. M. Zeebaree, and D. A. Majeed, "Comparative analysis of state-of-the-art classifiers for Parkinson's disease diagnosis," *J. Ilm. Ilmu Terapan Univ. Jambi*, vol. 8, no. 2, pp. 409–423, 2024.

[67] R. R. Ihsan, S. M. Almufti, B. M. Ormani, R. R. Asaad, and R. B. Marqas, "A survey on cat swarm optimization algorithm," *Asian J. Res. Comput. Sci.*, vol. 10, no. 2, pp. 22–32, 2021.

[68] R. Vadisetty and A. Polamarasetti, "AI-Augmented Skill Development Roadmaps: Tailoring 12-Month Learning Paths for Future-Ready Careers in Education 4.0 and Industry 4.0," *In 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2024, pp. 655–661.

[69] U. K. Lilhore, V. Dutt, T. A. Kumar, M. Margala, and K. Raahemifar, Math Optimization for Artificial Intelligence: Heuristic and Metaheuristic Methods for Robotics and Machine Learning. De Gruyter, 2025.

[70] M. S. Dilipkumar A. Ode, J. D. K. Krishnendu Roy, M. M. C. Birajlakshmi Ghosh, and R. S. Amar Baliram Abhrange, AI & Chatgpt Tools for Teaching Learning Process. *Redshine Publication*, 2024.

[71] R. Vadishetty, "Efficient Deep Fake Detection Technique on Video and Audio Dataset Using Deep Learning BT - Proceedings of 5th International Ethical Hacking Conference," 2025, pp. 137–155.

[72] C. Koneti, G. C. Saha, and E. Howard, "End-to-End Visibility in Global Supply Chains: Blockchain and AI Integration," *European Economic Letters*, vol. 14, no. 4, pp. 545–555, 2024.

[73] C. Koneti, G. S. Sajja, A. Adarsh, S. S. Yerasuri, G. Mann, and A. Mandal, "Human-Machine Collaboration in Supply Chain Management: The Impact of AI on Workforce Dynamics," *Journal of Informatics Education and Research*, vol. 4, no. 3, pp. 934–943, 2024.

[74] C. Koneti, A. Seetharaman, and K. Maddulety, "Understanding the supply chain efficiency in e-commerce using the blockchain technology," *Library of Progress - Library Science, Information Technology & Computer*, vol. 44, no. 3, pp. 3147–3152, 2024.

[75] M. T. Espinosa-Jaramillo, M. E. C. Zuta, C. Koneti, S. Jayasundar, S. d. R. O. Zegarra, and V. F. M. Carvajal-Ordoñez, "Digital Twins in Supply Chain Operations Bridging the Physical and Digital Worlds using AI," *Journal of Electrical Systems*, vol. 20, no. 10s, pp. 1764–1774, 2024.

[76] H. A. Al-Asadi, M. H. Al-Mansoori, M. Ajiya, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Effects of pump recycling technique on stimulated Brillouin scattering threshold: A theoretical model," *Optics Express*, vol. 18, no. 21, pp. 22339- 22347, 2010.

[77] H. A. Al-Asadi, M. H. Al-Mansoori, M. I. Saripan, and M. A. Mahdi, "Brillouin Linewidth Characterization in Single Mode Large Effective Area Fiber through the Co-Pumped Technique," *International Journal of Electronics, Computer and Communications Technologies (IJECCT)*, vol. 1, no. 1, pp. 16-20, 2010.

[78] H. A. Al-Asadi, M. H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers," *Optics Express*, vol. 19, no. 3, pp. 1842-1853, 2011.

[79] H. A. Al-Asadi, M. H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Analytical study of nonlinear phase shift through stimulated Brillouin scattering in single mode fibre with pump power recycling technique," *Journal of Optics*, vol. 13 no. 10, 2011.

[80] H. A. Al-Asadi, M. H. Abu Bakar, M. H. Al-Mansoori, F. R. Mahamd Adikan, and M. A. Mahdi, "Analytical analysis of second-order Stokes wave in Brillouin ring fiber laser," *Optics. Express*, vol. 19, no. 25, pp. 25741- 25748, 2011.

[81] M. Al-Asadi, Y. A. Al-Asadi, and H. A. Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 3, no. 6, 2012.

[82] M. A. Abed and H. A. Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach," *European Academic Research*, vol 1, pp. 535- 552, 2013.

[83] M. A. Abed and H. A. Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 2, pp. 145-152, 2015.

[84] H. A. Al-Asadi and M. A. Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," *American Journal of Engineering, Technology and Society*, vol 2, no. 5, pp. 105-110, 2015.

[85] H. A. Al-Asadi, "Energy Efficient Hierarchical Clustering Mechanism for Wireless Sensor Network Fields," *International Journal of Computer Applications*, vol. 153, no. 10, pp. 42-46, 2016.

[86] H. A. Al-Asadi, "Hybrid Clustering Methodology using Optical Communication in Wireless Sensor Networks," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 7, no. 1, 2017.

[87] H. A. Al-Asadi, "Mobile Clustering Algorithm for Effective Clustering in Dense Wireless Sensor Networks," *European Journal of Advances in Engineering & Technology (EJAET)*, vol. 4, no. 1, pp. 1-6, 2017.

[88] H. A. Al-Asadi, "Integrated Energy Efficient Clustering Strategy for Wireless Sensor Networks," *The Journal of Middle East and North Africa Sciences*, vol. 3, pp. 8-13, 2017.

[89] H. A. Al-Asadi, M. A. Al-Asadi, and N. A. Noori, "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 874-879, 2018.

[90] H. A. Al-Asadi, and N. A. M. B. A. Hambali, "Experimental evaluation and theoretical investigations of fiber Raman amplifiers and its gain optimization based on single forward pump," *Journal of Laser Applications*, vol. 26, no. 4, 2014.

[91] H. A. Al-Asadi, "Nonlinear Phase Shift due to Stimulated Brillouin Scattering in Strong Saturation Regime for Different Types of Fibers," *Journal of Optical Communications (JOC)*, vol. 36, no. 3, pp. 211–216, 2014.

[92] H. A. Al-Asadi, "A Novel and Enhanced Distributed Clustering Methodology for Large Scale Wireless Sensor Network Fields," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 2, pp. 633-638, February. 2019.

[93] N. F. H. Husshini, N. A. M. A. Hambali, M. H. A. Wahid, M. M. Shahimin, N. Ali, M. N. M. Yasin, and H. A. AL-Asadi, "Stability Multi-Wavelength Fiber Laser Employing Semiconductor Optical Amplifier in Nonlinear Optical Loop Mirror with Different Gain Medium," *SPIE*, vol. 63, no. 5, pp. 1241, 2019.

[94] N. F. H. Husshini, N. A. M. A. Hambali, M. H. A. Wahid, M. M. Shahimin, M. N. M. Yasin, N. Ali, and H. A. AL-Asadi,

"Multiwavelength Fiber Laser Employing Semiconductor Optical Amplifier in Nonlinear Optical Loop Mirror with Polarization Controller and Polarization Maintaining Fiber," *In CAPE2019*, 8 January 2020.

[95] N. F. H. Husshini, N. A. M. A. Hambali, M. H. A. Wahid, M. M. Shahimin, M. N. M. Yasin, N. Ali, and H. A. AL-Asadi, "Characteristics of Multiwavelength Fiber Laser Employing Semiconductor Optical Amplifier in Nonlinear Optical Loop Mirror with Different Length Polarization Maintaining Fiber*," In CAPE2019.* 8 January 2020.

[96] H. A. Al-Asadi, A. Alhassani, N. A. A. Hambali, M. A. AlSibahee, S. A. Alwazzan, and A. M. Jasim, "Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network," *Advances in Science, Technology and Engineering Systems Journal*, vol. 4, no. 5, pp. 306-313, 2019.

[97] H. A. Al-Asadi, M. T. Aziz, M. Dhiya, and A. Abdulmajed, "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS," *Journal of Network Computing and Applications*, vol. 5, no. 1, pp. 10-23, 2020.

[98] H. A. Al-Asadi, L. Mohamad, and M. Nassr, "Self-Phase Modulation Mitigation in Coherent Optical Communication Systems," *International Journal of Microwave and Optical Technology*, vol. 16, no. 6, pp. 618-625, 2021.

[99] H. A. Al-Asadi, "An Optimal Algorithm for Better Efficiency in Multimedia Application on WSN, IET Wireless Sensor Systems," vol. 11, no. 6, pp. 248-258, December 2021.

[100] H. A. Al-Asadi, "1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach," Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments).

[101] H. A. Al-Asadi, R. Hasan, M. Nassr, and M. Anbar, "Power Consumption in Wireless Sensor Network: A Machine Learning Approach, Computing," *Performance and Communication Systems, Clausius Scientific Press*, vol. 6, no. 1, pp. 24-37, 2022.

[102] M. Anbar, M. Nassr, M. Abdallah, E. Vostorgina, M. Kolistratov, and H. A. Al-Asadi, "Sidelobe Canceller Performance Evaluation using Sample Matrix Inversion algorithm, (The 4th 2022 International Youth Conference on Radio Electronics," *In Electrical and Power Engineering (REEPE)*, pp. 1-6, March. 2022.

[103] H. A. Al-Asadi, H. A. Ahmed, A. Al-Hassani, and N. A. M. A. Hambali, "A Novel and Enhanced Routing Protocol for Large Scale Disruption Tolerant Mobile Ad hoc Networks," *International Journal of Computing*, vol. 21, no. 3, pp. 325-332, 2022.

[104] H. A. Al-Asadi, "An Overview of Routing Protocols Performance in Wireless Multimedia Sensor Networks," *3rd Information Technology To Enhance e-learning and Other Application (IT-ELA), Baghdad, Iraq*, pp. 133-139, 2022.

[105] H. A. Al-Asadi, and H. A. Ahmed, "A Tri-Classes Method for Studying the Impact of Nodes and Sinks Number on Received Packets Ratio of MANETs Routing Protocols," *2023 15th International Conference on Developments in eSystems Engineering (DeSE), Baghdad & Anbar, Iraq*, pp. 521-526, 2023.

[106] R. Younes, F. Ghosna, M. Nassr, M. Anbar, and H. A. Al-Asadi, "Predicting BER value in OFDM-FSO systems using Machine Learning techniques," *Optica Pura y Aplicada*, vol. 55, no. 4, pp. 1, 2022.

[107] L. Hasan, M. Nassr, M. Anbar, and H. A. Al-Asadi, "Inverted U-shaped Frequency Reconfigurable Microstrip patch antenna for 5G communication systems, *Optica Pura y Aplicada*," vol. 56, no. 3, pp. 1-5.

[108] H. O. M. Al-Jabry, and H. A. Al-Asadi, "Enhancing Wireless Multimedia Sensor Networks with Optimization Algorithms: A Review," *IEEE Al-Sadiq International Conference on Communication and Information Technology*, pp. 153-158, 2023.

[109] H. Al-Jabry, and H. A. Al-Asadi, "Enhancing Packet Reliability in Wireless Multimedia Sensor Networks using a Proposed Distributed Dynamic Cooperative Protocol (DDCP) Routing Algorithm," *Iraqi Journal for Electrical and Electronic Engineering*, vol.19, no. 2, pp. 158-168.

[110] H. H. K. Al-Maliki and H. A. A. Al-Asadi, "Enhancing Performance in Vehicular Ad Hoc Networks: The Optimization Algorithm Perspective," *Proceedings - International Conference on Developments in eSystems Engineering (DeSE)*, pp. 456–461, 2023.

[111] H. A. Ahmed, and H. A. A. Al-Asadi, "An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks," *Journal of Sensor and Actuator Networks*, vol. 13, no. 2.

[112] C. Koneti, G. C. Saha, H. Saha, S. Acharya, and M. Singla, "The impact of artificial intelligence and machine learning in digital marketing strategies," *European Economic Letters (EEL)*, vol. 13, no. 3, pp. 982–992, 2023.

[113] Garg, A. Mandal, C. Koneti, J. V. Mehta, E. Howard, and S. S. Karmode, "AI-Based Demand Sensing: Improving Forecast Accuracy in Supply Chains," *Journal of Informatics Education and Research*, vol. 4, no. 2, pp. 2903–2913, 2024.

[114] M. Manikandan, V. Jain, C. Koneti, V. Musale, R. V. S. Praveen, and S. Bansal, "Blockchain Technology as a Decentralized Solution for Data Security and Privacy: Applications Beyond Cryptocurrencies in Supply Chain Management and Healthcare," *Library Progress International*, vol. 44, no. 3, pp. 5634–5643, 2024.

[115] Garg, A. Mandal, C. Koneti, J. V. Mehta, E. Howard, and S. S. Karmode, "AI-based demand sensing: Improving forecast accuracy in supply chains," *J. Informatics Educ. Res.*, vol. 4, no. 2, pp. 2903–2913, 2024.

[116] M. Murugan, V. R. Turlapati, C. Koneti, R. V. S. Praveen, A. Srivastava, and S. K. C, "Blockchain-based solutions for trust and transparency in supply chain management," *Library Progress International*, vol. 44, no. 3, pp. 24662–24674, 2024.

[117] S. Sharma, K. Chaitanya, A. B. Jawad, I. Premkumar, J. V. Mehta, and D. Hajoary, "Ethical considerations in AI-based marketing: Balancing profit and consumer trust," *Tuijin Jishu/Journal of Propulsion Technology*, vol. 44, no. 3, pp. 1301–1309, 2023.

[118] T. D. Humnekar, N. Chinthamu, K. Chaitanya, S. Venkatesh, A. K. Mishra, and S. Soni, "Modernized digital marketing strategies to improve customer experience and engagement," *European Economic Letters*, vol. 14, no. 2, pp. 909–916, 2024.

[119] M. Madanan, P. Patel, P. Agrawal, P. Mudholkar, M. Mudholkar and V. Jaganraja, "Security Challenges in Multi-Cloud Environments: Solutions and Best Practices," *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, 2024, pp. 1608-1614.

[120] P. Agrawal, N. Marathe, H. Byeon, and S. K. Singh, Machine Learning: Application and Challenges, p. 222, Xoffencer international book publication house, Chhetak Puri, Gwalior, 2024.

[121] P. Agrawal, R. Arora, W. C. Dietrich, R. L. Haecker, R. Hazeu, and S. Singh, "Method, system, and computer program product for implementing automated worklists," U.S. Patent 8,326,864, Dec. 4, 2012.

[122] R. Ingle, S. Donthu, M. H. K. Kochha, P. Agrawal, A. M. Kulkarni, and B. Viyyapu, "Fake news detection in social media management using deep learning and AI," *Indian Patent Application* 202441050770, 2024.

[123] V. Samatha N. Praba, P. Agrawal, P. Tripathi, N. Jain, and B. Kanwer, "Data security and privacy concerns in cloud-based HRM systems," *J. Informatics Educ. Res.*, vol. 4, no. 3, pp. 1374-1380, 2024.

[124] P. K. Aggarwal, D. H. Rakesh, R. Arya, P. Agrawal, P. Kumar, and H. Y. S., "Chatbots and virtual assistants: Revolutionizing customer service and engagement in marketing," *J. Informatics Educ. Res.*, vol. 4, no. 3, pp. 2044-2049, 2024.

[125] Md S. Miah and Md S. Islam, "Big Data Analytics Architectural Data Cut-Off Tactics for Cyber Security and Its Implication in Digital Forensic," 2022 *International Conference on Futuristic Technologies*, Belgaum, India, 2022, pp. 1-6.

[126] M. Abu Obaida, Md S. Miah, and Md A. Horaira, "Random Early Discard (RED-AQM) Performance Analysis in Terms of TCP Variants and Network Parameters: Instability in High-Bandwidth-Delay Network," *International Journal of Computer Applications*, vol. 27, no. 8, pp. 40-44, 2011.