



QuantumMedLedger: A Post-Quantum Secure Blockchain Framework for Healthcare

Pasupunooti Anusha¹, Nallabelly Nithin², Mamidala Nandha Kishori², Miriyala Sriram Reddy², Nittu Mounika²

¹Assistant Professor, ²UG Student, ^{1,2}Department of Computer Science and Engineering (Data Science)

^{1,2}Vaagdevi College of Engineering (UGC-Autonomous), Bollikunta, Warangal, 506005, Telangana

Abstract

The rapid adoption of digital healthcare systems has significantly increased the use of Electronic Health Records (EHR), online appointment platforms, and digital prescription management. While these technologies enhance accessibility and operational efficiency, they also introduce critical challenges related to data confidentiality, secure authentication, record integrity, and protection against unauthorized access. Healthcare data contains highly sensitive personal and medical information, making security a primary concern. Ensuring secure communication and verified access between patients and doctors remains a major challenge in maintaining trust and privacy within digital healthcare environments. Many existing healthcare management systems rely on centralized storage models and basic authentication mechanisms, exposing them to risks such as data breaches, impersonation attacks, and unauthorized record modification. Although basic encryption mechanisms may be applied to protect stored data, key management and authentication processes often rely on standard approaches without decentralized verification or advanced cryptographic reinforcement. As a result, centralized architecture creates a single point of failure, increasing vulnerability to unauthorized access, data tampering, and weak identity verification. Limited transparency and auditability further restrict effective monitoring of data usage and system activities. To address these issues, the proposed system introduces Quantum Crypt (QC), a hybrid security approach that integrates blockchain technology with Post-Quantum Cryptography (PQC) concepts and advanced encryption mechanisms. Medical reports and prescriptions are secured using the Advanced Encryption Standard in Cipher Block Chaining mode (AES-CBC), with encryption keys generated through a quantum-inspired mechanism. Authentication is enhanced through a lattice-inspired model implemented via Qiskit-based quantum circuit simulation to ensure secure key validation between patients and doctors. Blockchain integration using Web3 and smart contracts ensures immutable storage of healthcare records, improving transparency, strengthening data integrity, and enabling controlled access within the digital healthcare ecosystem.

Keywords: Digital Healthcare Security, Post-Quantum Cryptography, Advanced Encryption Standard, Decentralized Healthcare Systems.

1. Introduction

The exponential growth of digital healthcare systems and the widespread adoption of electronic health records (EHRs) have revolutionized the way medical data is collected, stored, and utilized. However, these advancements have also introduced significant challenges related to data security, privacy,

and interoperability. Healthcare organizations, being custodians of sensitive patient information, are increasingly vulnerable to data breaches, unauthorized access, and other cyber threats. According to recent reports, healthcare data breaches have surged in frequency, compromising millions of patient records globally and underscoring the urgent



need for robust data management and sharing frameworks. To address these challenges, blockchain technology has emerged as a transformative solution that offers unparalleled security, transparency, and decentralization for managing healthcare data. Blockchain technology, initially introduced as the foundation of cryptocurrencies like Bitcoin, has evolved to find applications in various domains, including supply chain management, finance, and healthcare. The fundamental attributes of blockchain decentralization, immutability, transparency, and cryptographic security make it particularly suitable for addressing the complex requirements of healthcare data sharing. In a blockchain-based system, data is stored in a decentralized ledger that is distributed across a network of participants. Each transaction on the blockchain is verified through consensus mechanisms and secured using advanced cryptographic techniques, ensuring data integrity and resistance to tampering.

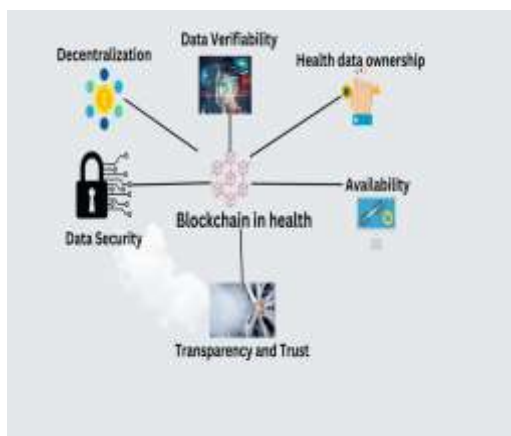


Fig. 1: The role of blockchain to secure medical records.

Despite its potential, the adoption of blockchain in healthcare is not without challenges. Healthcare systems are inherently complex and involve a diverse set of stakeholders, including patients, healthcare providers, insurers, researchers, and regulatory bodies. These stakeholders often have conflicting interests and varying levels of trust, which complicates data sharing and access control. Moreover, healthcare data is highly

sensitive and subject to stringent privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Any blockchain-based solution must comply with these regulations while providing a secure and efficient mechanism for data sharing.

2. Literature Survey

Ryu, et al. [1] proposed a new authentication protocol to prevent and address such issues within hospital systems. The proposed protocol encrypts medical records on a private blockchain, allowing them to be securely shared among institutions, hospitals, and insurance companies, ensuring data recovery even if a ransomware attack paralyzes the server. Additionally, the protocol facilitates the systematic sharing of patient medical records between hospitals or between hospitals and insurance companies by distributing session keys. They demonstrated that the proposed protocol provides 11 security properties, including forward and backward secrecy, user untraceability, and resistance to replay attacks. They also evaluate the communication and computational costs, proving that the protocol is feasible for practical use.

Zhao, et al. [2] implemented a decentralized management system with enhanced security and operational efficiency. Considering the scenario of Electronic Magnetic Records (EMRs) requiring confirmation of multiple doctors to improve safety, the proposed solution leverages Shamir's Secret Sharing to enable multi-party authorization, thereby enhancing privacy protection. Meanwhile, the scheme utilizes Bloom filter and vector operation to achieve efficient data search.

Wenhua, et al. [3] mentioned advantages and disadvantages motivated them to provide an advancement and comprehensive study regarding the applicability of blockchain technology. They focused on the healthcare



security issues in blockchain and sorted out the security risks in six layers of blockchain technology by comparing and analyzing existing security measures.

Alsadhan, et al. [4] introduced significant privacy concerns, particularly regarding data privacy. Internet of Medical Things (IoMT) devices often collect and store large amounts of data about patients' health. These data could be used to track patients' movements, monitor their health habits, and even predict their future health risks. This extensive data collection and surveillance could be a major invasion of patient privacy. Thus, privacy-preserving research in an IoMT context is an important area of research that aims to mitigate these privacy issues. They comprehensively applied the PRISMA methodology to analyze, review, classify, and compare current approaches of preserving patient data privacy within IoMT blockchain-based healthcare environments.

Sharma, et al [5]. employed to protect these transactions against such attacks. However, the security of blockchain relies on the computational complexity of certain mathematical functions, and because of the evolution of quantum computers, its security may be breached in real-time in the near future. Therefore, researchers are focused on combining quantum key distribution (QKD) with blockchain to enhance blockchain network security. This new technology is known as quantum-secured blockchain.

Ghosh, et al. [6] evaluated 144 articles that discussed the importance and limits of using blockchain technologies to improve healthcare operations. The objective is to demonstrate the technology's potential uses and highlight the difficulties and possible sectors for future blockchain research in the healthcare domain. They started with an extensive background study of blockchain and its features. Then, they focused on providing an extensive literature review of the selected articles to

highlight the current research themes in blockchain-based healthcare systems.

Liu, et al. [7] developed a quantum-secure blockchain (QSB) scheme by introducing a consensus mechanism quantum proof of authority (QPoA) and an identity-based quantum signature (IQS)—wherein QPoA is used for new block generation and IQS is used for transaction signing and verification. Second, QPoA is developed by adopting a quantum voting protocol to achieve secure and efficient decentralization for the blockchain system, and a quantum random number generator (QRNG) is deployed for randomized leader node election to protect the blockchain system from centralized attacks like distributed denial of service (DDoS).

Ajakwe, et al. [8] investigated the mainstream security challenges associated with the transmissibility of medical records, the evolutionary security strategies for maintaining confidentiality, and the existential enablers of trustworthy and transparent authorization and authentication before data transmission can be carried out. The review adopted the PRISMA-SPIDER methodology for a systematic review of 122 articles, comprising 9 surveys (7.37%) for qualitative analysis, 109 technical papers (89.34%), and 4 online reports (3.27%) for quantitative studies.

Venugopal, et al. [9] combined the privacy and security advantages of encryption and decentralized networks offered by Blockchain technology with the scalability of distributed systems to provide an effective secure platform for big data applications. The framework is based on the principles of confidentiality and immutability to ensure the security and privacy of health care data. The framework is designed to support a wide range of information sources and use cases including patient records, clinical research, medical imaging, genomic data, and pharmaceutical trials. It is also designed to be compatible with existing distributed computing and data querying technologies such as Hadoop and



Spark, which will help organizations to improve the accessibility of health care data.

Alabdulatif, et al. [10] proposed methodology addresses computational efficiency and scalability issues via the implementation of lightweight cryptographic techniques, achieving an average authentication delay of 0.059 milliseconds, which represents a 4000-fold improvement compared to current approaches. The model exhibited a significant decrease in memory use, requiring just 0.0198 MB in contrast to the 96.98 MB required by benchmark models, and attains an average signature verification duration of 0.00092 milliseconds. The findings demonstrate the model's capability for safe, efficient, and scalable applications in e-health, which guarantees privacy and adherence to regulatory norms.

3. Proposed Methodology

This research introduces a post-quantum secure healthcare framework that integrates blockchain technology, simulated quantum key generation, and AES-based encryption to ensure secure management of electronic health records (EHR). The Django-based application provides role-based access for doctors and patients, enabling secure appointment booking, medical report upload, and prescription management. It implements QC where PQC key generation mechanisms are used to derive encryption keys, while AES-CBC encryption ensures confidentiality of medical files during storage and transmission. A blockchain smart contract stores metadata securely, providing immutability and traceability of healthcare transactions. Quantum-based authentication logic validates user interactions between participants. The system combines decentralized blockchain security with encrypted file storage to enhance privacy, integrity, and controlled data sharing.



Fig. 2: Proposed system architecture.

User Registration and Authentication:

Users register as doctors or patients through the Django interface, and their details are stored via blockchain smart contract functions. Login validation checks user credentials and role type to control access to system features. This ensures only authorized participants can interact with healthcare data.

Appointment Booking and Medical Report Upload:

Patients select doctors and upload medical reports through the application. Uploaded files are processed before storage, preparing them for encryption. Metadata related to appointments is recorded on the blockchain for traceability.

PQC Key Generation: The system generates encryption keys using a simulated quantum key generation process. Random bases and measurement operations produce a shared symmetric key. This key acts as the foundation for secure data encryption.

AES Encryption of Medical Files: Medical reports and prescription files are encrypted using AES in CBC mode. The generated quantum-inspired key is applied to ensure confidentiality. Encrypted files are stored locally while preventing unauthorized access.

Blockchain Smart Contract Integration:

Using Web3, healthcare metadata such as patient details, report references, and prescription information is stored in blockchain smart contracts. This ensures immutability and transparent transaction



logging. The blockchain layer prevents tampering with healthcare records.

Quantum-Based Authentication Exchange:

A simulated quantum authentication mechanism validates communication between users. Key exchange logic verifies matching authentication keys before allowing sensitive operations. This step strengthens access control between doctor and patient interactions.

Prescription Generation and Secure Retrieval: Doctors generate prescriptions which are encrypted and linked to blockchain records. Patients can securely download decrypted reports through authorized access. The workflow maintains confidentiality while enabling efficient healthcare collaboration.

Post-Quantum Cryptography: Kyber

Kyber is a Key Encapsulation Mechanism (KEM) from the lattice-based family. It is designed to be secure against quantum attacks and is a finalist / recommended algorithm for post-quantum key exchange. Kyber provides a compact, efficient way for two parties to agree on a symmetric key: one side generates an encapsulation and ciphertext; the other decapsulates to retrieve the shared secret. It is well-suited for encrypting large files by deriving a symmetric key (e.g., AES) to perform the actual bulk encryption.

Below are the core internal operations presented as a sequence of logical steps (suitable for your methods chapter or implementation notes).

- **Parameter setup (system init)**

- System defines security parameters (module dimension, modulus q , noise distribution) and chooses public parameters A (matrix) and hash function/specific KDF. These are fixed for the scheme instance (e.g., Kyber512/768/1024).

- **Key generation (Recipient / Server)**

- Generate a secret vector s sampled from the error/noise distribution.
- Sample an error vector e .
- Compute public key $pk = A \cdot s + e$ (matrix-vector multiplication modulo q).
- Optionally compute and store a small public seed that can deterministically derive A .
- Output (pk, sk) where $sk =$ secret s plus auxiliary values (sometimes hashed).

- **Encapsulation (Sender / Client)**

- Sender obtains recipient pk .
- Sender samples random seed r (or derives from randomness+context) and derives ephemeral secret m or ephemeral s' .
- Compute ephemeral ciphertext $c = A \cdot s' + e' + \text{encode}(m, pk)$ (noise added) — ciphertext includes compressed polynomials.
- Derive shared secret $K = \text{KDF}(m, c, pk)$ (hashing ephemeral secret + ciphertext to produce symmetric key).
- Send ciphertext c to the recipient. The encapsulated output is (c, K) .

- **Decapsulation (Recipient)**

- Recipient uses sk and received c to compute $m' = \text{decode}(c - pk \cdot s)$ (effectively removing the public-component and recovering small message plus noise correction).



- Compute $K' = \text{KDF}(m', c, pk)$. If decoding fails or an invalid ciphertext is detected, use a fallback (e.g., hashed secret) to avoid revealing information (CCA-secure variant).
- K' should equal K if no transmission error / manipulation occurred.

● Key usage

- Both parties now share symmetric key K . Use K with a symmetric cipher (e.g., AES-GCM or an authenticated stream cipher) to encrypt/decrypt large files (the EHR files).
- Optionally rotate or rekey for session management.

● Security notes

- Kyber's security relies on the hardness of Module problems.
- Proper parameter selection and constant-time implementation are critical to resist side-channel attacks.
- Use authenticated encryption when encrypting files and include metadata/timestamps to avoid replay attacks.

4. Results description

Fig. 3 depicts the patient registration process where new users securely create accounts within the system. Upon successful signup, blockchain transaction details confirm that user information has been recorded through smart contract execution. This process ensures immutability and transparency by storing registration data in the decentralized ledger. The system validates user information through backend processing before blockchain submission. The registration workflow

establishes secure identity management while enabling role-based access for future healthcare interactions. The figure demonstrates the integration between user registration, decentralized storage, and secure onboarding mechanisms.

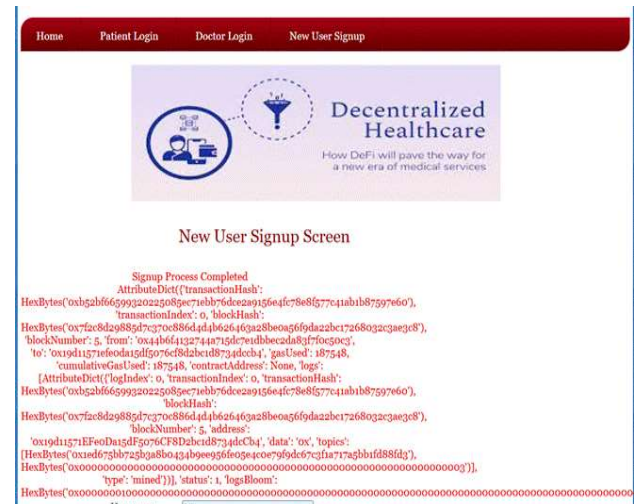


Fig. 3: Patient signup screen

Fig. 4 illustrates the doctor registration workflow, enabling healthcare professionals to securely join the decentralized platform. The system verifies submitted details and records them through blockchain transactions using smart contract functions. Successful registration ensures role-based privileges for accessing appointment and prescription features. The process demonstrates interaction between Django backend services and blockchain infrastructure via Web3 communication. Secure registration ensures trusted identity verification within the healthcare ecosystem. The figure highlights the decentralized authentication mechanism used for onboarding healthcare providers into the system.



Fig. 4: Doctor signup screen

Fig. 5 depicts the patient dashboard where available doctors are listed to facilitate appointment booking. Patients can review healthcare providers and initiate interactions required for consultation workflows. The system prepares backend processes for secure data handling once appointment selection occurs. This stage connects user interaction with encryption modules and blockchain storage mechanisms used during appointment confirmation. Role-based access ensures that only authenticated patients can perform scheduling operations. The figure represents the transition from user interaction to secure healthcare workflow execution within the decentralized framework.



Fig. 5: View doctors list in patient's page for the book appointment.

Fig. 6 illustrates the successful appointment confirmation process between a patient and doctor within the blockchain-enabled system.

The displayed transaction information verifies that appointment metadata has been securely stored using smart contract execution. Uploaded medical reports undergo encryption using AES-CBC combined with Kyber-inspired key generation before storage. Blockchain integration ensures tamper-resistant record keeping and transparent verification of appointment details. This stage demonstrates coordination between encryption modules, Django processing logic, and decentralized ledger infrastructure. The figure highlights secure workflow completion for appointment creation in the healthcare platform.



Fig. 6: Patient confirmed appointment with doctor.

Fig. 7 depicts the doctor's dashboard after successfully uploading a prescription for a patient appointment. The system encrypts prescription data before storing associated metadata on the blockchain through smart contract updates. Role-based authorization ensures only verified doctors can modify patient records. Backend processing manages secure communication between encryption modules and decentralized storage services. The successful update confirms integrity and traceability of prescription records within the system. This figure demonstrates how secure medical decision-making integrates with



blockchain technology and encryption workflows.



Fig. 7: Doctor dashboard with prescription upload successfully.

Fig. 8 illustrates the patient dashboard where generated prescriptions are available for viewing and download after doctor approval. The system retrieves encrypted files and performs secure decryption to ensure confidentiality during access. Blockchain storage guarantees that prescription records remain immutable and verifiable. Patients can access finalized healthcare outcomes through controlled authorization mechanisms. This stage completes the secure lifecycle from appointment scheduling to prescription delivery. The figure demonstrates successful collaboration between encryption processes, blockchain storage, and decentralized healthcare workflows.



Fig. 8: Doctors prescription shows in patient dashboard.

5. Conclusion

The Quantum Med Ledger project presents a secure and decentralized healthcare management framework designed to enhance the protection, integrity, and accessibility of electronic health records using blockchain technology and advanced encryption mechanisms. The system successfully integrates Django-based web architecture with Ethereum smart contracts to enable tamper-resistant storage and transparent healthcare transactions. By incorporating Kyber-inspired key generation with AES-CBC encryption, the project ensures strong confidentiality for sensitive medical data during storage and transmission. Role-based authentication allows secure interaction between patients and doctors while maintaining controlled access to healthcare information. The implementation improves system performance by reducing risks associated with centralized data storage, minimizing unauthorized modifications, and ensuring reliable verification through blockchain transaction receipts. Performance improvements are achieved through efficient encryption workflows, automated smart contract execution, and secure file handling mechanisms that streamline appointment scheduling, prescription management, and report retrieval processes.

References

- [1] Ryu J, Kim T. Enhancing Hospital Data Security: A Blockchain-Based Protocol for Secure Information Sharing and Recovery. *Electronics*. 2025; 14(3):580. <https://doi.org/10.3390/electronics14030580>
- [2] Zhao A, Tian H. Secure Sharing of Electronic Medical Records Based on Blockchain and Searchable Encryption. *Electronics*. 2025; 14(13):2679. <https://doi.org/10.3390/electronics14132679>



- [3] Wenhua Z, Qamar F, Abdali T-AN, Hassan R, Jafri STA, Nguyen QN. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics*. 2023; 12(3):546. <https://doi.org/10.3390/electronics12030546>
- [4] Alsadhan A, Alhogail A, Alsalamah H. Blockchain-Based Privacy Preservation for the Internet of Medical Things: A Literature Review. *Electronics*. 2024; 13(19):3832. <https://doi.org/10.3390/electronics13193832>
- [5] Sharma P, Choi K, Krejcar O, Blazek P, Bhatia V, Prakash S. Securing Optical Networks Using Quantum-Secured Blockchain: An Overview. *Sensors*. 2023; 23(3):1228. <https://doi.org/10.3390/s23031228>
- [6] Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain Application in Healthcare Systems: A Review. *Systems*. 2023; 11(1):38. <https://doi.org/10.3390/systems11010038>
- [7] Liu A, Chen X-B, Xu S, Wang Z, Li Z, Xu L, Zhang Y, Chen Y. A Secure Scheme Based on a Hybrid of Classical-Quantum Communications Protocols for Managing Classical Blockchains. *Entropy*. 2023; 25(5):811. <https://doi.org/10.3390/e25050811>
- [8] Ajakwe SO, Saviour II, Ihekoronye VU, Nwankwo OU, Dini MA, Uchechi IU, Kim D-S, Lee JM. Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum. *Big Data and Cognitive Computing*. 2024; 8(9):121. <https://doi.org/10.3390/bdcc8090121>
- [9] Venugopal LK, Rajaganapathi R, Birjepatil A, Raja SE, Subramaniam G. A Novel Information Security Framework for Securing Big Data in Healthcare Environment Using Blockchain. *Engineering Proceedings*. 2023; 59(1):107. <https://doi.org/10.3390/engproc2023059107>
- [10] Alabdulatif A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. *Information*. 2025; 16(3):219. <https://doi.org/10.3390/info16030219>
- [11] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. *Journal of Science & Technology*, 10(6), 28–36. <https://doi.org/10.46243/jst.2025.v10.i06.pp28-36>
- [12] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. *Journal of Science & Technology*, 10(6), 28–36. <https://doi.org/10.46243/jst.2025.v10.i06.pp28-36>
- [13] Todupunuri, A. (2025). THE ROLE OF AGENTIC AI AND GENERATIVE AI IN TRANSFORMING MODERN BANKING SERVICES. *American Journal of AI Cyber Computing Management*, 5(3), 85–93. <https://doi.org/10.64751/ajaccm.2025.v5.n3.pp85-93>
- [14] Todupunuri, A. . (2024). Artificial Intelligence Ethics: Investigating Ethical Frameworks, Bias Mitigation, and Transparency in AI Systems to Ensure



- Responsible Deployment and Use of AI Technologies. International Journal of Innovative Research in Science, Engineering and Technology, 13(09), 1–14. <https://doi.org/10.15680/ijirset.2024.1309002>
- [15] Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. American Journal of AI Cyber Computing Management, 5(4), 463–474. <https://doi.org/10.64751/ajacm.2025.v5.n4.pp463-474>
- [16] Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI Cyber Computing Management, 5(4), 451–462. <https://doi.org/10.64751/ajacm.2025.v5.n4.pp451-462>
- [17] Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.
- [18] Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). <https://doi.org/10.56975/jaaf.v1i4.501636>
- [19] Srinivasa Kalyan Immadi. (2025). Harnessing Artificial Intelligence In Oracle Hcm: Revolutionising Workforce Management With Automation And Predictive Analytics. International Journal of Data Science and IoT Management System, 4(4), 7–13. <https://doi.org/10.64751/ijdim.2025.v4.n4.pp7-13>
- [20] S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology, 16(1). <https://doi.org/10.71097/ijst.v16.i1.1403>
- [21] Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.
- [22] Cyril, H. P. (2025). Event-Driven Provisioning Architectures For Modern Telecom Networks: Overcoming Legacy Limitations And Enabling Autonomous 6g Operations. International Journal of Advanced Research in Computer Science, 16(6), 75–82. <https://doi.org/10.26483/ijarcs.v16i6.7389>
- [23] Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s),



1270–1285.

<https://doi.org/10.12732/ijam.v38i4s.685>

- [24] Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. *Journal of Emerging Technologies and Innovative Research*.

- [25] Reddy, S. K. R. (2021). Strengthening the Security of Loyalty Reward Systems: An In-Depth Analysis of Emerging Cyber Threats and Protection Mechanisms. *Journal of Computational Analysis and Applications*, 29(6).

- [26] Poojari, R. (2026). Privacy-Preserving Generative AI in Healthcare Systems Using Federated Learning Approaches. *International Journal of Data Science and IoT Management System*, 5(1), 78-88.

- [27] Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. *American Journal of AI Cyber Computing Management*, 5(2), 42–50. <https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50>

- [28] Saikumar, B. (2024). Optimizing Crew Scheduling and Absence Management using Microservices: Enhancing Reliability and Efficiency in Crew

Management Systems. *International Journal of Enhanced Research in Management & Computer Applications*, 13(11), 50–55.

<https://doi.org/10.55948/ijermca.2024.0116>

- [29] Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. *International Journal of Enhanced Research in Science, Technology & Engineering*, 12(11), 111–117.

<https://doi.org/10.55948/ijerste.2023.111>