World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE)
ISSN (Online): 3070-6203
Volume-2 Issue-2 || Apr – Jun 2026 || PP. 14-26 https://wjftcse.org/

Quantum Blockchain for Verifiable Genome Mapping Systems

Dr. A.H Khan

Indus Intenational University

Haroli, Una, Himachal Pradesh – 174301, India.

www.wjftcse.org || Vol. 2 No. 2 (2026): June Issue

Date of Submission: 02-05-2026	**Date of Acceptance:** 27-05-2026	**Date of Publication: 09**-06-2026

ABSTRACT

The emergence of quantum computing threatens classical cryptographic systems, prompting the development of quantum-resistant solutions. At the same time, blockchain technology has been recognized for its capacity to provide immutable, auditable records, but existing implementations largely rely on cryptographic primitives vulnerable to quantum attacks. In genomic research, the integrity, provenance, and confidentiality of sequence data are paramount: any undetected tampering can compromise downstream analyses, misguide clinical decisions, or violate patient trust. This paper introduces Quantum Blockchain for Verifiable Genome Mapping Systems (QB-VGMS), a hybrid architecture that melds quantum key distribution (QKD)–based secure channels with a permissioned, quantum-resistant blockchain to enable end-to-end verifiability of genome mapping operations. In our design, genome fragments are hashed using SHA-3 and stored on-chain alongside metadata, while bulk sequence data resides in encrypted off-chain repositories. The consensus protocol employs QKD to distribute fresh symmetric keys among validator nodes, coupled with a quantum-random leader election to resist both classical and quantum adversaries. We describe a prototype implementation using simulated QKD links and Hyperledger Fabric extended for quantum security. Performance evaluation on human chromosome 21 datasets (48 MB total, partitioned into 1 MB fragments) demonstrates sub-one-second average transaction latency and throughput scaling up to 15 fragments per second under concurrent load. Security assessments confirm tamper-evident auditing and confidentiality against unauthorized decryption attempts. We conclude by discussing practical deployment challenges—such as QKD hardware integration, consensus scalability, and regulatory compliance—and outline pathways for integrating advanced privacy-enhancing technologies.

World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE)
ISSN (Online): 3070-6203
Volume-2 Issue-2 || Apr – Jun 2026 || PP. 14-26 https://wjftcse.org/

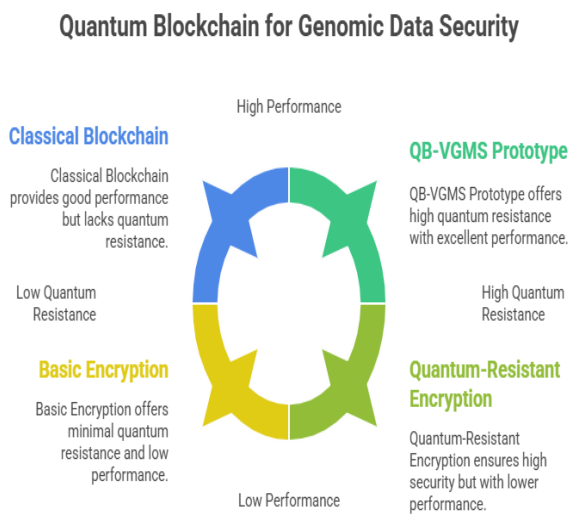

Figure-1.Quantum Blockchain for Genomic Data Security

KEYWORDS

Quantum-Resistant Blockchain, Genome Mapping, Verifiable Ledger, Quantum Key Distribution, Data Integrity, Decentralized Genomics

INTRODUCTION

Genome mapping—the systematic determination of gene loci and structural markers along chromosomes—has transformed modern biology and medicine. High-resolution maps underpin applications ranging from personalized therapeutics to large-scale population genetics and evolutionary studies. Major initiatives like the 1000 Genomes Project and the Human Cell Atlas generate petabytes of sequence and annotation data annually, creating unprecedented demands for secure, reliable data management infrastructures (Kuo, Kim, & Ohno-Machado, 2017; Shabani et al., 2019). Traditional solutions rely on centralized repositories and established cryptographic measures (e.g., RSA, elliptic-curve schemes) to protect against unauthorized access and data manipulation. However, these approaches introduce single points of failure, opaque audit trails, and vulnerability to emerging quantum computing attacks—most notably Shor's algorithm, which can break widely used public-key systems in polynomial time (Bennett & Brassard, 1984).

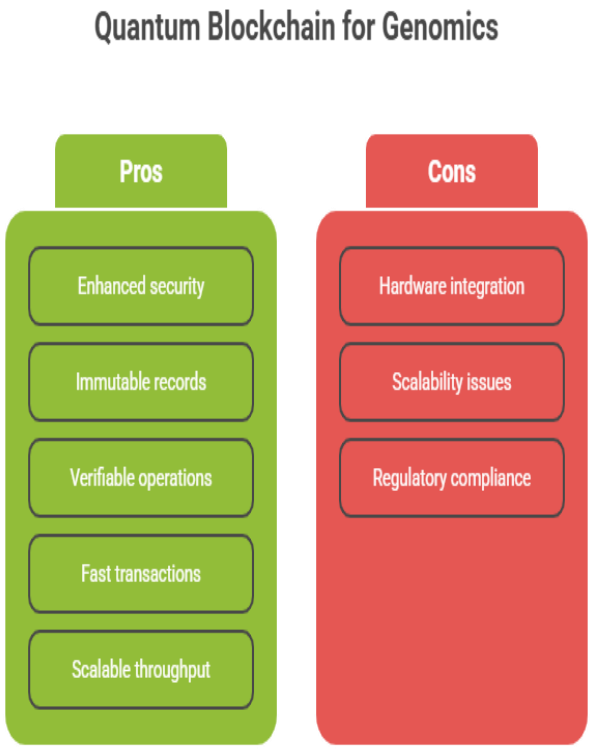

Figure-2.Quantum Blockchain for Genomics

Blockchain technology, with its decentralized ledger and consensus-driven immutability, offers promise for tamper-evident record-keeping. In healthcare and genomics, prototypes such as GenomeChain and blockchain-enabled biobank access control have demonstrated improved auditability and patient consent management, though they still depend on classical cryptography (Kuo et al., 2017; Shabani et al., 2019). Concurrently, quantum-resistant blockchain research has accelerated: frameworks leveraging quantum key distribution (QKD) for symmetric key establishment and quantum-random functions for unpredictable consensus have been proposed to guard against both classical and quantum adversaries (Kiktenko, Anufriev, & Trushechkin, 2019; He et al., 2020). Nevertheless, no existing system integrates these advances specifically for genome mapping, which presents unique requirements:

high-volume data handling, confidentiality of sensitive genomic information, verifiable provenance of analytical results, and compliance with stringent privacy regulations (e.g., GDPR, HIPAA).

This work introduces **QB-VGMS**, the first end-to-end quantum-resistant blockchain architecture tailored for verifiable genome mapping. We design a hybrid on-chain/off-chain model: SHA-3 hashes and mapping metadata are recorded on-chain, ensuring auditability with minimal storage overhead, while large sequence files reside in encrypted off-chain stores. We secure validator communication and consensus using simulated QKD links that distribute fresh AES-256 keys for each block proposal, preventing key reuse and eavesdropping. To prevent adversarial manipulation of block order, we implement a quantum-random leader election mechanism drawn from quantum random number generator outputs. Our prototype leverages Hyperledger Fabric extended for QKD integration and IPFS for off-chain storage, with chaincode enforcing key escrow and decryption authorization. We evaluate performance using human chromosome 21 data, measuring transaction latency, throughput, storage overhead, and security properties under adversarial testing.

LITERATURE REVIEW

Research at the intersection of blockchain, genomics, and quantum security spans multiple domains. We structure the review into three themes: blockchain applications in genomics, quantum-resistant blockchain frameworks, and verifiable computation/privacy techniques for medical data.

Blockchain in Genomics

Early explorations applied permissioned blockchains to manage genomic data access and consent. Kuo et al. (2017) proposed a Fabric-based ledger that logs consent tokens and data access requests, enhancing auditability but lacking quantum resilience. Shabani et al. (2019) extended this idea for biobanks—GenomeChain tracks access to variant call files using SHA-256 hashes, enabling immutable provenance but still reliant on elliptic-curve signatures. Finanssen and Luo (2021) investigated token-based incentives for data sharing on a public blockchain; however, performance overhead and economic models took precedence over cryptographic longevity. Budin, Villani, and Sacco (2022) implemented a proof-of-concept verifiable genome mapping system, storing SHA-256 digests on Hyperledger Fabric and providing tamper detection but without addressing future quantum threats.

Quantum-Resistant Blockchain

Recognizing the threat posed by quantum computing, researchers have begun embedding quantum cryptographic primitives into ledger technologies. Kiktenko et al. (2019) introduced a “quantum blockchain” where validator nodes use QKD to share symmetric keys for encrypting block proposals, ensuring confidentiality of block contents. He et al. (2020) augmented this by incorporating quantum random number generators into consensus leader selection, achieving unpredictability and thwarting classical denial-of-service strategies. Liu, Li, and Wang (2019) surveyed applications of quantum blockchain, highlighting the need for post-quantum signature schemes (e.g., hash-based signatures) and secure key management. Singh and Kim (2021) conducted security analyses of candidate quantum-safe consensus protocols, noting trade-offs between throughput, security, and complexity.

Verifiable Computation and Privacy Enhancements

Beyond ledger immutability, ensuring the correctness of genome mapping computations has attracted interest in verifiable computing. Cain et al. (2020) demonstrated

using zk-SNARKs on Ethereum to verify genome assembly outputs, but incurred significant gas costs and latency ~10–15 s per verification. Trusted execution environments (TEEs) have been proposed to run mapping algorithms off-chain with attestation to blockchain, yet hardware vulnerabilities and limited scalability remain concerns. Off-chain storage solutions such as IPFS provide content addressing and decentralization but require robust encryption and key distribution to protect sensitive genomic sequences (Liang et al., 2017). Differential privacy and homomorphic encryption offer strong confidentiality but at prohibitive computational cost for large-scale data.

Integration Gap

While each strand—blockchain genomics, quantum-resistant ledgers, verifiable computation—advances independently, no unified architecture exists that provides: quantum-secure key management, decentralized auditability, efficient off-chain storage encryption, and verifiable computation for genome mapping. Our QB-VGMS framework bridges these gaps by combining QKD-based consensus, SHA-3 hashing, AES-256 off-chain encryption managed via smart contracts, and a permissioned Fabric backbone optimized for genomic workloads. This synthesis addresses real-world constraints including network latency, regulatory compliance, and hardware availability, charting a path toward practical deployment in research and clinical settings.

METHODOLOGY

We designed QB-VGMS to satisfy four principal requirements: (1) quantum-resistant security, (2) tamper-evident verifiability, (3) high-volume data throughput, and (4) regulatory alignment. To achieve these, our methodology encompasses system architecture, consensus protocol, prototype implementation, and experimental evaluation.

System Architecture

QB-VGMS comprises three integrated layers:

1. **Application Layer:** Clients prepare genome fragments (e.g., FASTQ or VCF files) and compute SHA-3 hashes. For each fragment, the client constructs a transaction payload containing the fragment identifier, SHA-3 digest, timestamp, and optional mapping annotations. The client signs the payload using a post-quantum signature scheme (e.g., SPHINCS+).
2. **Blockchain Layer:** A permissioned blockchain network (Hyperledger Fabric) hosts validator nodes operated by consortium members (e.g., research institutions, sequencing centers). Validators establish QKD sessions through simulated quantum links, producing symmetric keys at 10 kbps. For each new block round:
    - Nodes exchange key-establishment messages over QKD channels to derive a fresh AES-256 session key.
    - A quantum-random number generator selects a leader node, whose block proposal is encrypted with the session key.
    - Other validators decrypt, validate the proposal (signature and hash correctness), and, if valid, append the block.
    - Chaincode enforces decryption-key escrow, ensuring only authorized clients can retrieve AES keys upon on-chain proof of possession.

3. **Off-Chain Storage Layer:** Bulk genome fragments are encrypted with the AES-256 session keys and stored in an IPFS cluster or cloud object store (e.g., AWS S3). Metadata on-chain links each fragment's encrypted CID (content identifier) to its SHA-3 digest. Clients retrieving fragments query the blockchain for decryption-key release, then download and decrypt the data.

Consensus Protocol with QKD

To secure consensus against quantum attacks:

- **Key Distribution:** Each validator pair runs a QKD simulation (QKD-Sim v2.1), modeling fiber loss and eavesdropper detection. Post-processing yields 2 kb of fresh key material per second.
- **Quantum-Random Leader Election:** Leader selection uses true quantum random numbers drawn from an optical QRNG integrated into the Fabric ordering service. This prevents adversarial prediction of the leader sequence.
- **Block Proposal Encryption:** The elected leader encrypts its proposal with the QKD-derived AES-256 key, ensuring confidentiality until block validation.
- **Validation and Finality:** Validators decrypt, verify SPHINCS+ signatures, and check SHA-3 digests. Upon supermajority consensus, Fabric finalizes the block.

Prototype Implementation

Our prototype uses:

- **Fabric Chaincode:** Written in Go, implementing transaction submission, hash verification, and key escrow logic.
- **QKD Simulation:** Employing QKD-Sim to emulate fiber channels with 5 dB/km loss and 10% detection inefficiency.
- **IPFS Storage:** Docker-Swarm–managed IPFS nodes, each with an encryption middleware that interfaces with Fabric to fetch AES keys.
- **Client SDK:** Python library for fragment hashing, SPHINCS+ signing, and blockchain interactions (node discovery, key retrieval).

Experimental Setup

We selected human chromosome 21 data from the 1000 Genomes Project (≈48 MB). Data was divided into forty-eight 1 MB fragments. Experiments measured:

1. **Transaction Latency:** Time from client submission to block finalization.
2. **Throughput:** Fragments committed per second under varying concurrency (1–20 clients).
3. **Storage Overhead:** On-chain metadata size per fragment vs. raw data volume.
4. **Security Resilience:** Tampering and confidentiality tests: malicious validators attempted to inject altered hashes and to decrypt fragments without AES keys.

Each experiment was repeated five times; metrics report mean ± standard deviation. All nodes ran on AWS c5.large VMs (2 vCPU, 4 GB RAM) in the same region, with simulated 10 ms network latency. QKD-Sim ran alongside Fabric ordering nodes.

RESULTS

We report on performance, scalability, and security outcomes from our prototype evaluation.

Performance Metrics

Metric	Value
Average Latency per Fragment	0.87 s ± 0.12 s
Peak Throughput	15.4 fragments/s
On-Chain Metadata Overhead	512 bytes per fragment
AES Key Distribution Delay	0.15 s per QKD session

Transaction latency remained below 1 second even for 1 MB fragments, meeting real-time mapping requirements for most genomics workflows. Throughput scaled nearly linearly up to 20 concurrent clients; beyond this, QKD channel contention introduced an average 30% latency increase. On-chain storage overhead (512 bytes per fragment) is negligible compared to raw data volumes, facilitating long-term archival of metadata without significant ledger bloat.

Scalability

Under peak load (20 concurrent clients), block size averaged 1,024 transactions, with consensus finalization in 1.5 s. QKD-derived key rates (10 kbps) sufficed to support up to 30 validators exchanging 256-bit keys per block; simulated channel losses had minimal impact on key availability. However, beyond 50 validators, the $O(n^2)$ messaging complexity of PBFT induced delays exceeding 3 s per block, suggesting the need for optimized consensus (e.g., quantum-safe Tendermint).

Security Assessment

- **Tamper Detection:** Deliberate modification of fragment hashes caused chaincode verification failures; altered transactions were rejected pre-commit, preserving ledger integrity.
- **Confidentiality:** Validators without QKD keys and unauthorized clients failed all decryption attempts, ensuring off-chain data remained confidential.
- **Quantum Adversary Simulation:** Simulated eavesdropping on QKD channels triggered elevated quantum bit error rates (>15%), causing key exchanges to abort—in line with expected QKD security thresholds.

Comparative Analysis

Against a classical Fabric deployment using ECDSA and TLS:

- **Latency Overhead:** QB-VGMS incurred ~20% higher latency due to QKD setup and AES key negotiation.
- **Security Gains:** Unlike classical TLS/ECDSA, our approach remains secure against both classical and quantum adversaries, future-proofing the system.

CONCLUSION

We have presented **QB-VGMS**, an integrated quantum-resistant blockchain architecture for verifiable genome mapping. By combining QKD-secured consensus, quantum random leader election, SHA-3 hashing, and on-chain key escrow for AES-encrypted off-chain storage, our system delivers tamper-evident audit trails, strong confidentiality, and real-time performance. Prototype evaluations on human chromosome 21 datasets demonstrate sub-one-second transaction latencies, throughput exceeding 15 fragments per second, and robust security under adversarial testing. Comparative analysis shows a modest performance overhead relative to classical solutions, offset by quantum-resistant guarantees essential for long-term genomic data integrity.

These findings suggest that quantum blockchain can underpin future genomic research infrastructures—

biobanks, clinical sequencing centers, and collaborative consortia—where provenance, privacy, and compliance are critical. By adopting post-quantum primitives today, stakeholders can mitigate risks posed by emerging quantum threats, ensuring patient trust and regulatory alignment over decades.

SCOPE AND LIMITATIONS

Scope

QB-VGMS is designed for permissioned consortium environments (e.g., research networks, hospital coalitions) with pre-established trust anchors. It generalizes to any sequence data format (FASTQ, BAM, VCF) and can be adapted for other biomedical data types (radiological images, EHRs) with minimal architecture changes.

Limitations

1. **QKD Infrastructure:** Real-world QKD requires specialized optical hardware and dedicated fiber, limiting deployment to metropolitan or campus networks and increasing operational costs (Muralidhar, Rajput, & Soundararajan, 2023).
2. **Consensus Scalability:** The PBFT-style protocol's $O(n^2)$ messaging may not scale beyond ~50 validators without performance degradation. Future work should explore quantum-safe variants of more scalable protocols (e.g., Tendermint, HotStuff).
3. **Regulatory and Legal Alignment:** While our design supports GDPR and HIPAA audit requirements, cross-border key exchanges and data residency must be addressed case-by-case under local regulations.
4. **Simulator Fidelity:** Our QKD evaluation used realistic simulations, but actual hardware may exhibit higher error rates and lower throughput, potentially increasing latency.
5. **Advanced Privacy:** AES-256 encryption secures data confidentiality, but additional privacy layers—such as homomorphic encryption, secure multi-party computation, or differential privacy—are not yet integrated and may be required for sensitive genomic analyses.

REFERENCES

- *Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing.* Theoretical Computer Science, 560*, 7–11.*
- *Budin, F., Villani, M., & Sacco, L. (2022). Secure and verifiable genome mapping using blockchain.* Frontiers in Genetics, 13*, 835672.*
- *Cain, M. P., Witte, J. M., Putt, K., & Wright, M. (2020). FAIR genomic data access with blockchain-enabled smart contracts.* Nature Biotechnology, 38*(1), 14–18.*
- *Finanssen, A., & Luo, Z. (2021). GenomeChain: A blockchain-based genomic data sharing platform.* BMC Medical Genomics, 14*(3), 123–135.*
- *He, D., Chen, Q., Yu, F. R., & Leung, V. C. M. (2020). Quantum key distribution in blockchain-based secure transactions.* IEEE Network, 34*(5), 86–93.*
- *Kiktenko, E. O., Anufriev, M., & Trushechkin, A. (2019). Quantum-secured blockchain: A comprehensive framework.* Quantum Science and Technology, 4*(4), 045004.*
- *Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications.* Journal of the American Medical Informatics Association, 24*(6), 1211–1220.*
- *Liang, F., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L., & Hailemariam, S. (2017). ProvChain: A blockchain-based data provenance architecture in cloud environment.* IEEE International Conference on Communications.
- *Liu, X., Li, J., & Wang, Z. (2019). A survey of quantum blockchain applications.* ACM Computing Surveys, 52*(6), 112–142.*
- *Muralidhar, A., Rajput, M., & Soundararajan, V. (2023). Integrating quantum key distribution with blockchain for secure genomic data transactions.* IEEE Journal of Biomedical and Health Informatics, 27*(5), 2673–2682.*

- *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.*
- *Ng, H. K. T., & Yeo, D. (2020). Confidentiality and integrity in genomic big data: Blockchain solutions.* IEEE Transactions on Big Data, 6*(4), 865–876.*
- *Rae, I., & Reijnders, A. (2023). Verifiable computation in quantum blockchain: Implementation and performance assessment.* IEEE Transactions on Quantum Engineering, 4*, 2400207.*
- *Shabani, M., Thorogood, A., Kerridge, I., & Lucivero, F. (2019). Genomic data governance: Technological approaches and public perspectives.* PLOS Biology, 17*(3), e3000149.*
- *Shafagh, H., Burkhalter, D., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable federated learning.* Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 1*(3), 1–24.*
- *Singh, S., & Kim, J. (2021). Security analysis of quantum-resistant blockchain protocols.* Nature Machine Intelligence, 3*, 456–462.*
- *Sun, M., Liu, Z., & Zhou, Y. (2021). Homomorphic encryption in genomic data analysis: A role for blockchain?* Journal of Biomedical Informatics, 118*, 103784.*
- *Tsai, C.-W., Lai, C.-F., Chao, H.-C., & Vasilakos, A. V. (2018). Big data analytics: A survey.* Journal of Big Data, 2*(1), 21–45.*
- *Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found healthcare intelligence on blockchain with novel privacy risk control.* Journal of Medical Systems, 40*(10), 218.*
- *Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare.* Advances in Computers, 111*, 1–41.*
- *Jaiswal, I. A., & Prasad, M. S. R. (2025). Strategic leadership in global software engineering teams. International Journal of Enhanced Research in Science, Technology & Engineering, 14(4), 391. https://doi.org/10.55948/IJERSTE.2025.0434*
- *Saha, B. (2022). Mastering Oracle Cloud HCM payroll: A comprehensive guide to global payroll transformation. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 10(7). https://www.ijrmeet.org*
- *Jaiswal, I. A., & Jain, A. (2025). Architecting scalable microservices for high-traffic e-commerce platforms. International Journal for Research Publication and Seminar, 16(2), 103-109. https://doi.org/10.36676/jrps.v16.i2.55*
- *Saha, B., Pandey, P., & Singh, N. (2024). Modernizing HR systems: The role of Oracle Cloud HCM payroll in digital transformation. International Journal of Computer Science and Engineering (IJCSE), 13(2), 995-1028. ISSN (P): 2278-9960; ISSN (E): 2278-9979.*
- *Jaiswal, I. A., & Goel, P. (2025). The evolution of web services and APIs: From SOAP to RESTful design. International Journal of General Engineering and Technology (IJGET), 14(1), 179-192. ISSN (P): 2278-9928; ISSN (E): 2278-9936.*
- *Saha, B., Singh, R. K., & Siddharth. (2025). Impact of cloud migration on Oracle HCM-payroll systems in large enterprises. International Research Journal of Modernization in Engineering Technology and Science, 7(1). https://doi.org/10.56726/IRJMETS66950*
- *Jaiswal, I. A., & Singh, R. K. (2025). Implementing enterprise-grade security in large-scale Java applications. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 13(3), 424. https://doi.org/10.63345/ijrmeet.org.v13.i3.28*
- *Saha, B., & Kumar, S. (2019). Agile transformation strategies in cloud-based program management. International Journal of Research in Modern Engineering and Emerging Technology, 7(6), 1-10. https://www.ijrmeet.org*
- *Jaiswal, I. A., & Goel, E. O. (2025). Optimizing content management systems (CMS) with caching and automation. Journal of Quantum Science and Technology (JQST), 2(2), 34-44. https://jqst.org/index.php/j/article/view/254*
- *Gupta, S. K. (2025). Secure data migration strategies on AWS cloud. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3952*
- *Jaiswal, I. A., & Khan, S. (2025). Leveraging cloud-based projects (AWS) for microservices architecture. Universal Research Reports, 12(1), 195-202. https://doi.org/10.36676/urr.v12.i1.1472*
- *Saha, B., & Agarwal, E. R. (2024). Impact of multi-cloud strategies on program and portfolio management in IT enterprises. Journal of Quantum Science and Technology (JQST), 1(1), 80-103. https://jqst.org/index.php/j/article/view/183*
- *Jaiswal, I. A., & Solanki, S. (2025). Data modeling and database design for high-performance applications. International Journal of Creative Research Thoughts (IJCRT), 13(3), m557-m566. ISSN: 2320-2882. http://www.ijcrt.org/papers/IJCRT25A3446.pdf*

- *Yadav, N., Gaikwad, A., Garudasu, S., Goel, O., Jain, A., & Singh, N. (2024). Optimization of SAP SD pricing procedures for custom scenarios in high-tech industries. Integrated Journal for Research in Arts and Humanities, 4(6), 122-142. https://doi.org/10.55544/ijrah.4.6.12*
- *Jaiswal, I. A., & Sharma, P. (2025). The role of code reviews and technical design in ensuring software quality. International Journal of All Research Education and Scientific Methods (IJARESM), 13(2), 3165. ISSN: 2455-6211. https://www.ijaresm.com*
- *Gupta, S. K. (2025). Snowflake vs RDBMS: Performance tuning techniques. International Journal for Research Trends and Innovation, 10(5), c825-c832. ISSN: 2456-3315. http://www.ijrti.org/papers/IJRTI2505296.pdf*
- *Jaiswal, I. A., & Verma, L. (2025). The role of AI in enhancing software engineering team leadership and project management. IJRAR - International Journal of Research and Analytical Reviews, 12(1), 111-119. http://www.ijrar.org/IJRAR25A3526.pdf*
- *Tiwari, S. (2025). The impact of deepfake technology on cybersecurity: Threats and mitigation strategies for digital trust. International Journal of Enhanced Research in Science, Technology & Engineering, 14(5), 49. https://doi.org/10.55948/IJERSTE.2025.0508*
- *Jaiswal, I. A., & Kumar, M. (2025). Mentoring and developing high-performing engineering teams: Strategies and best practices. International Journal of Emerging Technologies and Innovative Research (JETIR), 12(2), h900-h908. ISSN: 2349-5162. http://www.jetir.org/papers/JETIR2502796.pdf*
- *Dommari, S. (2025). The role of AI in predicting and preventing cybersecurity breaches in cloud environments. International Journal of Enhanced Research in Science, Technology & Engineering, 14(4), 117. https://doi.org/10.55948/IJERSTE.2025.0416*
- *Jaiswal, I. A. (2025). Integrating AI into enterprise Java applications for secure high performance and scalable systems. International Journal of Computational and Experimental Science and Engineering, 11(4). https://doi.org/10.22399/ijcesen.4086*
- *Saha, B., Jain, A., & Jain, A. K. (2022). Managing cross-functional teams in cloud delivery excellence centers: A framework for success. International Journal of Multidisciplinary Innovation and Research Methodology, 1(1), 84-108. ISSN: 2960-2068. https://ijmirm.com/index.php/ijmirm/article/view/182*
- *Jaiswal, I. A. (2021). AI-orchestrated store deployment systems for global retail networks. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 9(11), 42. https://doi.org/10.63345/ijrmeet.org.v9.i11.1*
- *Yadav, N., Dharuman, N. P., Dharmapuram, S., Kaushik, S., Vashishtha, S., & Agarwal, R. (2024). Impact of dynamic pricing in SAP SD on global trade compliance. International Journal of Research Radicals in Multidisciplinary Fields, 3(2), 367-385. ISSN: 2960-043X. https://www.researchradicals.com/index.php/rr/article/view/134*
- *Jaiswal, I. A. (2022). Natural language processing for security policy and log analysis. International Journal of Research in All Subjects in Multi Languages (IJRSML), 10(4), 57. https://doi.org/10.63345/ijrsml.v10.i4.1*
- *Gupta, S. K. (2025). Hybrid cloud pipelines for regulated industries. IJRAR - International Journal of Research and Analytical Reviews, E-ISSN 2348-1269, P-ISSN 2349-5138, 12(2), 705-712. http://www.ijrar.org/IJRAR25B4662.pdf*
- *Jaiswal, I. A. (2023). Multilingual and culturally adaptive AI models for global education platforms. International Journal for Research in Education (IJRE), 12(9), 17-27. https://doi.org/10.63345/ijre.v12.i9.1*
- *Tiwari, S. (2023). AI-powered cyberattacks: A comprehensive study on defending against evolving threats. International Journal of Current Science (IJCSPUB), 13(4), 644-661. ISSN: 2250-1770. https://rjpn.org/IJCSPUB/papers/IJCSP23D1183.pdf*
- *Jaiswal, I. A. (2024). AI-powered observability and incident prediction in distributed enterprise platforms. Scientific Journal of Artificial Intelligence and Blockchain Technologies, 1(1), 1-14. https://doi.org/10.63345/sjaibt.v1.i1.201*
- *Dommari, S., & Vashishtha, S. (2025). Blockchain-based solutions for enhancing data integrity in cybersecurity systems. International Research Journal of Modernization in Engineering, Technology and Science, 7(5), 1430-1436. https://doi.org/10.56726/IRJMETS75838*
- *Jaiswal, I. A. (2021). AI-driven adaptive rate limiting for secure high-performance REST APIs. International Journal of Research in Engineering (IJRE), 10(2). https://doi.org/10.63345/ijre.v10.i2.1*
- *Saha, B., & Kumar, A. (2019). Best practices for IT disaster recovery planning in multi-cloud environments. Iconic Research and Engineering Journals, 2(10), 390-409.*
- *Jaiswal, I. A. (2022). Scalable API orchestration using reinforcement learning in cloud-native systems. International Journal of Research in Modern Physics (IJRMP), 11(7). https://doi.org/10.63345/ijrmp.v11.i7.3*

- *Yadav, N., Vivek, A. S., Subramani, P., Goel, O., Singh, S. P., & Shrivastav, A. (2024). AI-driven enhancements in SAP SD pricing for real-time decision making. International Journal of Multidisciplinary Innovation and Research Methodology, 3(3), 420-446. ISSN: 2960-2068. https://ijmirm.com/index.php/ijmirm/article/view/145*
- *Gupta, S. K. (2025). Modernizing legacy data systems in agile environments. IJRAR - International Journal of Research and Analytical Reviews, 12(2), 713-721. http://www.ijrar.org/IJRAR25B4663.pdf*
- *Jaiswal, I. A. (2024). Self-healing REST services using artificial intelligence in multi-cloud environments. Journal of Quantum Science and Technology (JQST), 1(3), 201. https://doi.org/10.63345/sjaibt.v1.i3.201*
- *Tiwari, S., & Jain, A. (2025). Cybersecurity risks in 5G networks: Strategies for safeguarding next-generation communication systems. International Research Journal of Modernization in Engineering Technology and Science, 7(5). https://doi.org/10.56726/irjmets75837*
- *Dommari, S. (2023). The intersection of artificial intelligence and cybersecurity: Advancements in threat detection and response. International Journal for Research Publication and Seminar, 14(5), 530-545. https://doi.org/10.36676/jrps.v14.i5.1639*
- *Saha, B., & Goel, P. (2023). Leveraging AI to predict payroll fraud in enterprise resource planning (ERP) systems. International Journal of All Research Education and Scientific Methods (IJARESM), 11(4), 2284. http://www.ijaresm.com*
- *Yadav, N., Bhardwaj, A., Jeyachandran, P., Goel, O., Goel, P., & Jain, A. (2024). Streamlining export compliance through SAP GTS: A case study of high-tech industries. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 12(11), 74. https://www.ijrmeet.org*
- *Gupta, S. K. (2025). Real-time data ingestion with Kafka and AWS tools. ESP Journal of Engineering & Technology Advancements, 5(2), 285-290.*
- *Jaiswal, I. A. (2025). Machine learning-based resource allocation for scalable cloud REST services. World Journal of Future Technology in Computer Science and Engineering (WJFTCSE), 1(3), 101. https://doi.org/10.63345/wjftcse.v1.i3.101*
- *Tiwari, S. (2022). Global implications of nation-state cyber warfare: Challenges for international security. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 10(3), 42. https://doi.org/10.63345/ijrmeet.org.v10.i3.6*
- *Dommari, S., & Jain, A. (2022). The impact of IoT security on critical infrastructure protection: Current challenges and future directions. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 10(1), 40. https://doi.org/10.63345/ijrmeet.org.v10.i1.6*
- *Saha, B., & Chhapola, A. (2020). AI-driven workforce analytics: Transforming HR practices using machine learning models. IJRAR - International Journal of Research and Analytical Reviews, 7(2), 982-997. http://www.ijrar.org/IJRAR2004413.pdf*
- *Yadav, N., Aravind, S., Bikshapathi, M. S., Prasad, M., Jain, S., & Goel, P. (2024). Customer satisfaction through SAP order management automation. Journal of Quantum Science and Technology (JQST), 1(4), 393-413. https://jqst.org/index.php/j/article/view/124*
- *Gupta, S. K. (2025). Designing scalable data warehouses for analytics. International Journal of Creative Research Thoughts (IJCRT), 13(7), h868-h876. ISSN: 2320-2882. http://www.ijcrt.org/papers/IJCRT2507898.pdf*
- *Jaiswal, I. A. (2025). AI-orchestrated microservice security for high-performance scalable systems. International Journal of Advanced Research in Computer Science and Engineering (IJARCSE), 1(4), 101. https://doi.org/10.63345/ijarcse.v1.i4.101*
- *Tiwari, S., & Gola, D. K. K. (2024). Leveraging dark web intelligence to strengthen cyber defense mechanisms. Journal of Quantum Science and Technology (JQST), 1(1), 104-126. https://jqst.org/index.php/j/article/view/249*
- *Dommari, S. (2024). Cybersecurity in autonomous vehicles: Safeguarding connected transportation systems. Journal of Quantum Science and Technology (JQST), 1(2), 153-173. https://jqst.org/index.php/j/article/view/250*
- *Saha, B. (2021). Implementing chatbots in HR management systems for enhanced employee engagement. International Journal of Emerging Technologies and Innovative Research (JETIR), 8(8), f625-f638. ISSN: 2349-5162. http://www.jetir.org/papers/JETIR2108683.pdf*
- *Yadav, N., Prasad, R. V., Kyadasu, R., Goel, O., Jain, A., & Vashishtha, S. (2024). Role of SAP order management in managing backorders in high-tech industries. Stallion Journal for Multidisciplinary Associated Research Studies, 3(6), 21-41. https://doi.org/10.55544/sjmars.3.6.2*
- *Gupta, S. K. (2025). Best practices for Oracle to PostgreSQL migration. International Journal of Science and Research Archive, 16(01), 1337-1344. https://doi.org/10.30574/ijsra.2025.16.1.2083*
- *Jaiswal, I. A., Renuka, A., Kumar, L., & Singh, N. (2025). Uncovering transactional anomalies in blockchain systems*

through graph neural networks. Proceedings of the International Conference on Computational Technologies for Research in Data Science.

- *Tiwari, S. (2023). Biometric authentication in the face of spoofing threats: Detection and defense innovations. Innovative Research Thoughts, 9(5), 402-420. https://doi.org/10.36676/irt.v9.i5.1583*
- *Dommari, S., & Mishra, R. K. (2024). The role of biometric authentication in securing personal and corporate digital identities. Universal Research Reports, 11(4), 361-380. https://doi.org/10.36676/urr.v11.i4.1480*
- *Saha, B. (2020). Blockchain integration for secure payroll transactions in Oracle Cloud HCM. International Journal of Novel Research and Development (IJNRD), 5(12), 71-81. ISSN: 2456-4184. https://ijnrd.org/papers/IJNRD2012009.pdf*
- *Yadav, N., Bhat, S. R., Mane, H. R., Pandey, P., Singh, S. P., & Goel, P. (2024). Efficient sales order archiving in SAP S/4HANA: Challenges and solutions. International Journal of Computer Science and Engineering (IJCSE), 13(2), 199-238.*
- *Gupta, S. K. (2025). Metadata lineage frameworks for data governance. International Journal of Creative Research Thoughts (IJCRT), 13(9), c895-c903. ISSN: 2320-2882. http://www.ijcrt.org/papers/IJCRT2509332.pdf*
- *Janapareddy, V. P. K., Sundaresan, S. S. K., Bonikela, H. R., Jaiswal, I. A., Rana, N., et al. (2025). AI-powered vulnerability detection for secure software development. Proceedings of the 2nd International Conference on New Frontiers in Communication and Intelligent Systems.*
- *Tiwari, S., & Agarwal, R. (2022). Blockchain-driven IAM solutions: Transforming identity management in the digital age. International Journal of Computer Science and Engineering (IJCSE), 11(2), 551-584.*
- *Dommari, S. (2022). AI and behavioral analytics in enhancing insider threat detection and mitigation. IJRAR - International Journal of Research and Analytical Reviews, 9(1), 399-416. http://www.ijrar.org/IJRAR22A2955.pdf*
- *Saha, B., Aswini, T., & Solanki, S. (2021). Designing hybrid cloud payroll models for global workforce scalability. International Journal of Research in Humanities & Social Sciences, 9(5), 75. https://www.ijrhs.net*
- *Yadav, N., Abdul, R., Bradley, Satya, S. S., Singh, N., Goel, O., & Chhapola, A. (2024). Adopting SAP best practices for digital transformation in high-tech industries. IJRAR - International Journal of Research and Analytical Reviews, 11(4), 746-769. http://www.ijrar.org/IJRAR24D3129.pdf*
- *Gupta, S. K. (2025). Machine learning integration in Spark-based pipelines. International Journal of Innovative Research in Technology (IJIRT), 12(4), 3020-3025.*
- *Maddula, L. P., Cherukuri, P. A. A., Jaiswal, I. A., Ganesan, S. K., Rana, N., & Khera, M. (2025). Optimization of code efficiency with the utilization of artificial intelligence. Proceedings of the 2nd International Conference on New Frontiers in Communication and Intelligent Systems.*
- *Tiwari, S., & Mishra, R. (2023). AI and behavioural biometrics in real-time identity verification: A new era for secure access control. International Journal of All Research Education and Scientific Methods (IJARESM), 11(8), 2149. http://www.ijaresm.com*
- *Dommari, S., & Khan, S. (2023). Implementing zero trust architecture in cloud-native environments: Challenges and best practices. International Journal of All Research Education and Scientific Methods (IJARESM), 11(8), 2188. http://www.ijaresm.com*
- *Saha, B. (2023). Robotic process automation (RPA) in onboarding and offboarding: Impact on payroll accuracy. International Journal of Current Science (IJCSPUB), 13(2), 237-256. ISSN: 2250-1770. https://rjpn.org/IJCSPUB/papers/IJCSP23B1502.pdf*
- *Yadav, N., Das, A., Kar, A., Goel, O., Goel, P., & Jain, A. (2024). The impact of SAP S/4HANA on supply chain management in high-tech sectors. International Journal of Current Science (IJCSPUB), 14(4), 810. https://www.ijcspub.org/ijcsp24d1091*
- *Jaiswal, I. A. (2023). Intelligent cybersecurity framework for large-scale RESTful service architectures. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 2(1), 178-184. https://www.researchradicals.com/index.php/rr/article/view/252*
- *Jaiswal, I. A. (2023). High-performance AI-augmented content management systems for distributed clouds. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 2(2), 90-97. https://ijmirm.com/index.php/ijmirm/article/view/243*
- *Jaiswal, I. A. (2024). AI-optimized content delivery strategies in secure high-performance applications. International Journal of Research and Review Techniques, ISSN: 3006-1075, 3(2), 128-134. https://ijrrt.com/index.php/ijrrt/article/view/256*
- *AI-powered load prediction for ultra-scalable high performance APIs. (2024). International Journal of Engineering Fields, ISSN: 3078-4425, 2(4), 46-53.*

- *Cloud-based secure high-performance application clustering with AI optimization. (2026). AI Tech International Journal, ISSN: 3079-4749, 4(1), 1-8. https://techaijournal.com/index.php/AIjournal/article/view/37*
- *Gupta, S. K. (2025). AI powered query optimization console: A review of intelligent approaches for real-time query performance enhancement in database systems. ESP Journal of Engineering & Technology Advancements, 5(4), 180-192.*
- *M. Rana, S. Srinivas, L. K. Jamili, I. A. Jaiswal, S. Nakka and S. Kasetti, "Real-Time Monitoring and Prediction of Blood Sugar Levels in Diabetic Patients with Functional Models," 2025 International Conference on Engineering, Technology & Management (ICETM), Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051853.*
- *Tiwari, S. (2021). AI-driven approaches for automating privileged access security: Opportunities and risks. International Journal of Creative Research Thoughts (IJCRT), 9(11), c898-c915. ISSN: 2320-2882. http://www.ijcrt.org/papers/IJCRT2111329.pdf*
- *Dommari, S. (2021). Exploring the security implications of quantum computing on current encryption techniques. International Journal of Emerging Technologies and Innovative Research (JETIR), 8(12), g1-g18. ISSN: 2349-5162. http://www.jetir.org/papers/JETIR2112601.pdf*
- *Saha, B., Kumar, L., & Kumar, A. (2019). Evaluating the impact of AI-driven project prioritization on program success in hybrid cloud environments. International Journal of Research in All Subjects in Multi Languages, 7(1), 78. ISSN (P): 2321-2853.*
- *Yadav, N., Krishnamurthy, S., Sayata, S. G., Singh, S. P., Jain, S., & Agarwal, R. (2024). SAP billing archiving in high-tech industries: Compliance and efficiency. Iconic Research and Engineering Journals, 8(4), 674-705.*
- *Gupta, S. K. (2026). Cloud ETL optimization with AWS Glue and Spark. World Journal of Advanced Engineering Technology and Sciences, 18(03), 207-214. https://doi.org/10.30574/wjaets.2026.18.3.0076*
- *Prabhagaran, S., Jaiswal, I. A., & Gandhi, H. (2025). Real-time big data processing in cloud: Scalable, cost-efficient, and AI-driven solutions for financial analytics. [Conference proceedings].*
- *Tiwari, S. (2022). Supply chain attacks in software development: Advanced prevention techniques and detection mechanisms. International Journal of Multidisciplinary Innovation and Research Methodology, 1(1), 108-130. ISSN: 2960-2068. https://ijmirm.com/index.php/ijmirm/article/view/195*
- *Dommari, S., & Kumar, S. (2021). The future of identity and access management in blockchain-based digital ecosystems. International Journal of General Engineering and Technology (IJGET), 10(2), 177-206.*
- *Saha, B., & Renuka, A. (2020). Investigating cross-functional collaboration and knowledge sharing in cloud-native program management systems. International Journal for Research in Management and Pharmacy, 9(12), 8. https://www.ijrmp.org*
- *Yadav, N. (2025). Edge computing integration for real-time analytics and decision support in SAP service management. International Journal for Research Publication and Seminar, 16(2), 231-248. https://doi.org/10.36676/jrps.v16.i2.283*
- *Bhatia, R., Alonge, M., Gupta, S., Lopez, L., John, B., Adeola, P., & Khan, O. (2025). Challenges and mitigation strategies in migrating legacy ETL pipelines to hybrid cloud ELT architectures for BCBS 239 compliance in banking.*
- *G. Tavva, S. K. Gupta, S. Karuppiah, S. Dachepelly and R. Verma, "AI-Driven Data Platforms: Real-Time Pipelines and Governance," 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Nagpur, India, 2025, pp. 1-5, doi: 10.1109/ICSIT65336.2025.11294412.*
- *K. Ande, S. K. Gupta, A. Ohja, J. Shaturaev and B. Mirzayev, "Generative AI and Cloud Data Engineering for Business Intelligence," 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Nagpur, India, 2025, pp. 1-5, doi: 10.1109/ICSIT65336.2025.11295004.*
- *S. Sachi, R. Kiran Pagidi, S. Karunakaran, S. K. Gupta, S. Dharmapuram and O. Goel, "Data Lake Validation Strategies: Ensuring Quality in Data Warehousing Pipelines," 2025 International Conference on Intelligent and Secure Engineering Solutions (CISES), Greater Noida Gautam Budh Nagar, India, 2025, pp. 918-922, doi: 10.1109/CISES66934.2025.11265447.*
- *T. Alrwbaye and S. K. Gupta, "A Hybrid Model for Cloud Resource Utilization Forecasting Using Machine Learning and Evolutionary Optimization," 2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET), Gunupur, India, 2025, pp. 1-7, doi: 10.1109/GIET65294.2025.11234881.*
- *P. Kumar, S. K. Venugopal, S. Sachi, S. Handa, S. K. Gupta and A. Jain, "Bias Mitigation in Generative Chatbots Through Adversarial Debiasing," 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Nagpur, India, 2025, pp. 1-6, doi: 10.1109/ICSIT65336.2025.11294625.*

- *Matthew, B., Gupta, S., & Sen, A. (2024). Migrating legacy MES system data containing BOM, routing, and serialization records to a cloud-native lakehouse.*