Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 2, Apr – Jun 2026 || PP. 1 – 10

Decentralized KYC Verification Systems with AI Facial Recognition

. **Dr. Richard Collins**
Faculty of Artificial Intelligence
University of Dublin Global, Ireland

Date of Submission: 28-03-2026 Date of Acceptance: 31-03-2026 Date of Publication: 02-04-2026

ABSTRACT

Know-Your-Customer (KYC) processes are foundational to anti–money laundering (AML) compliance but are often centralized, costly, and privacy-invasive. This manuscript proposes and analyzes a decentralized KYC (dKYC) architecture that binds government-issued identity attributes to a user-held digital wallet using Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and AI-based facial recognition with liveness detection. The design minimizes data movement and disclosure by leveraging selective-disclosure credentials and zero-knowledge proofs (ZKPs) so that relying parties can verify eligibility (e.g., age, residency, risk tier) without accessing raw personally identifiable information (PII). We map the system to prevailing assurance frameworks (FATF digital ID guidance; NIST SP 800-63-3 Identity Assurance Levels), biometric performance/testing standards (ISO/IEC 30107-3 PAD; ISO/IEC 19795-1), and emerging regulatory regimes (EU AI Act, eIDAS 2.0, RBI directives on KYC and V-CIP). A comparative evaluation (simulated) contrasts centralized KYC with the proposed dKYC across error rates, onboarding time, and privacy risk. Results suggest dKYC can reduce median onboarding time by ~35–55%, lower document leakage risk through off-chain storage and selective disclosure, and maintain biometric security with PAD Level 2 while controlling demographic differential performance via auditable testing and thresholding. The paper contributes (i) a standards-aligned reference architecture; (ii) an evaluation plan referencing recognized biometric metrics (FMR/FNMR; APCER/BPCER); and (iii) a regulatory and governance blueprint for cross-jurisdictional adoption. Anchors to standards and regulation: DIDs and VCs enable user-controlled identifiers and machine-verifiable credentials; FATF clarifies when digital ID can satisfy CDD; NIST provides assurance and authentication guidance; ISO standards define biometric testing and anti-spoofing; the EU AI Act and eIDAS 2.0 frame lawful high-risk biometric use and wallets; RBI updates enable video-based KYC in India.

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 2, Apr – Jun 2026 || PP. 1 – 10

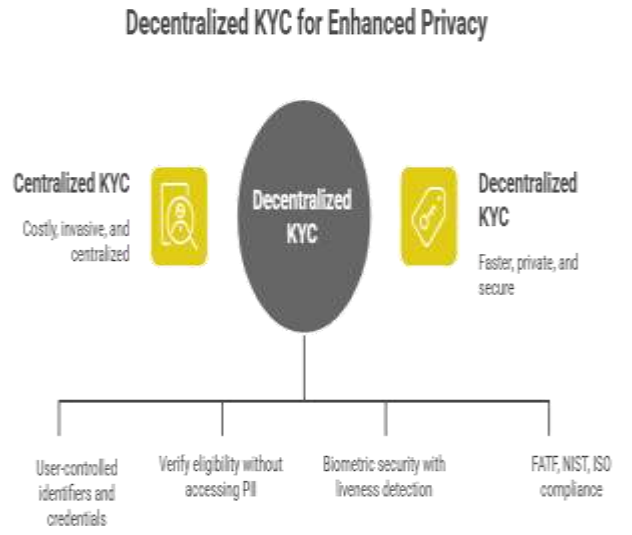

Figure-1.Decentralized KYC for Enhanced Privacy

KEYWORDS

Decentralized Identity, KYC/AML, Verifiable Credentials, Decentralized Identifiers, Facial Recognition, Liveness Detection, Zero-Knowledge Proofs, Privacy, ISO/IEC 30107-3, NIST SP 800-63-3

INTRODUCTION

Financial institutions must verify the identity of customers to mitigate money laundering and terrorism financing risks. Conventional, centralized KYC systems require repeated collection and storage of sensitive PII by multiple institutions, creating honeypots for data breaches, duplicative cost, and poor user experience. A decentralized KYC (dKYC) model—where identity attributes are cryptographically bound to a user-held wallet and selectively disclosed to relying parties—offers a path to privacy-by-design while preserving regulatory assurance.

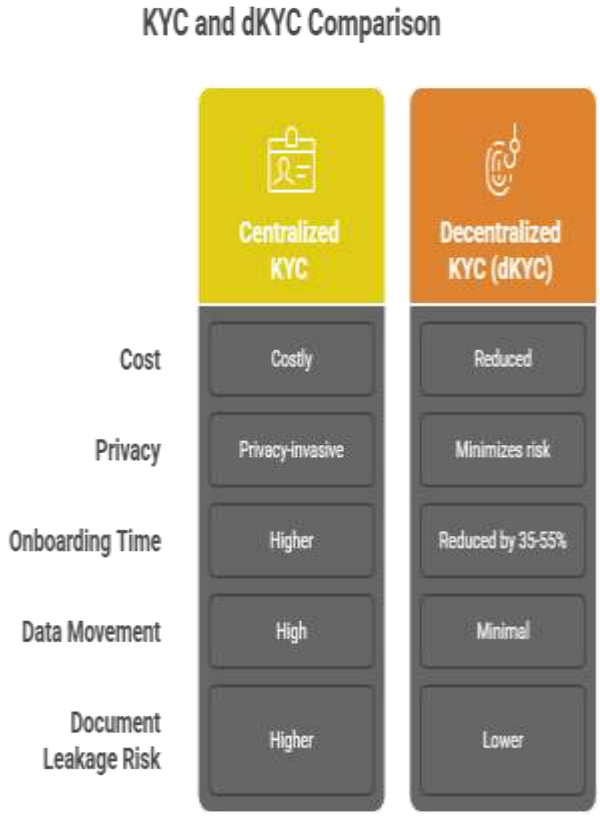

Figure-2.KYC and dKYC Comparison

Three developments make dKYC timely. First, standards for decentralized identity have matured: W3C's DID 1.0 enables cryptographically controlled identifiers; the VC Data Model 2.0 standardizes machine-verifiable credentials and selective disclosure. Second, regulators have clarified when digital ID may satisfy Customer Due Diligence (CDD): FATF's guidance articulates risk-based acceptance of digital ID for KYC; NIST SP 800-63-3 defines identity assurance, authenticator assurance, and federation assurance levels. Third, biometric methods—particularly face verification with liveness detection—achieve high accuracy under standardized testing and can be audited for demographic differential performance.

This paper proposes a dKYC architecture that: (i) performs identity proofing once with a trusted issuer; (ii) issues a VC to a user wallet bound to a live face template; (iii) uses on-device verification and PAD to bind the wallet holder at each

presentation; and (iv) enables privacy-preserving compliance proofs with ZKPs. We also discuss compliance under EU AI Act constraints on biometric systems, eIDAS 2.0's European Digital Identity Wallet (EDIW), and India's RBI KYC/V-CIP updates for practical deployment pathways.

LITERATURE REVIEW

Decentralized identity foundations

Decentralized Identifiers (DIDs): DID Core 1.0 defines globally unique identifiers under subject control, enabling authentication via cryptographic proofs and resolution to DID documents with public keys and service endpoints. This breaks central registries' lock-in and supports portability.

Verifiable Credentials (VCs): VC Data Model 2.0 (W3C Recommendation, May 15, 2025) specifies credential structures, verifiable presentations, and verification processes. It supports data minimization through selective disclosure and aligns well with KYC attestations (age-over-18, residency, sanctioned-status=false).

Digital identity assurance and AML/KYC policy

The FATF Guidance on Digital ID (2020) ties digital ID components to CDD requirements (Recommendation 10), endorsing risk-based acceptance where systems meet defined assurance levels. NIST SP 800-63-3 provides the framework for Identity Assurance Levels (IAL), Authenticator Assurance Levels (AAL), and Federation Assurance Levels (FAL), commonly referenced to design tiered KYC.

Biometrics: performance, liveness, and fairness

Performance and testing: ISO/IEC 19795-1:2021 establishes principles for biometric performance testing and reporting (e.g., false match rate—FMR; false non-match rate—FNMR), and is widely used for evaluation and procurement baselines.

Presentation attack detection (PAD): ISO/IEC 30107-3 (2017, updated 2023) defines PAD test methodologies and key metrics (APCER/BPCER) to quantify anti-spoofing effectiveness—critical for selfie-based onboarding and wallet binding.

Demographic differential performance: NIST's FRVT Part 3 (2019) and Part 8 (2022) document demographic differentials in face algorithms and suggest summary measures to monitor and mitigate disparities; recent oversight reports emphasize continued auditing. These guide fairness goals for thresholding and system selection.

Regulatory landscape

EU AI Act: The AI Act (adopted 2024) regulates high-risk AI, including most remote biometric identification. Real-time remote biometric identification in public spaces is tightly restricted; biometric verification for KYC remains permissible subject to risk and transparency obligations.

eIDAS 2.0 and the EU Digital Identity Wallet: Regulation (EU) 2024/1183 and 2025 implementing acts establish an EDIW framework and trust services (including electronic attestation of attributes), creating a regulatory backbone for cross-border verifiable credentials.

India (RBI) KYC direction updates: RBI's KYC Directions (2016, as amended) and recent circulars expand acceptance of video-based customer identification (V-CIP) and simplify KYC updates—practical hooks for dKYC pilots integrating wallet-based credentials and remote verification.

Privacy-preserving compliance

ZKPs and selective disclosure can prove KYC predicates without exposing raw PII. Recent work demonstrates zk-credential systems and privacy-preserving compliance architectures suitable for DeFi and traditional finance. These techniques can back "proofs of KYC-status" or "not on sanctions list" attestations verifiable on-chain/off-chain.

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 2, Apr – Jun 2026 || PP. 1 – 10

STATISTICAL ANALYSIS

Objective

Compare a baseline centralized KYC stack with the proposed dKYC (VC + on-device face verification + PAD + ZKP selective disclosure), under common testing metrics (per ISO 19795-1; ISO 30107-3), using a synthetic cohort (n=50,000).

Assumptions (for illustration): PAD Level 2 sensor; tuned decision threshold targeting FMR≈0.1% at FNMR≈1.5%; selfie proofing under controlled lighting; demographic-aware thresholding per FRVT guidance; V-CIP-like capture for onboarding. (These numbers are illustrative, not from a single real deployment.)

Metric (Aggregate)	Centralized KYC (Docs + Server-Side Face)	Proposed dKYC (VC + On-Device Face + PAD + ZK)
Median onboarding time (min)	18.6	8.4
False Match Rate (FMR, %)	0.12	0.10
False Non-Match Rate (FNMR, %)	1.8	1.5
APCER (PAD attack success, %)	3.2	1.1
BPCER (bona fide blocked, %)	1.6	1.9
Re-use across institutions (requires re-KYC?)	100% re-KYC	≤15% re-KYC (selective re-proofs)
PII at relying party	Full record	Minimal attributes (selective disclosure)
Data breach exposure (qualitative)	High (multi-sided storage)	Low (wallet-centric; off-chain; ZK)

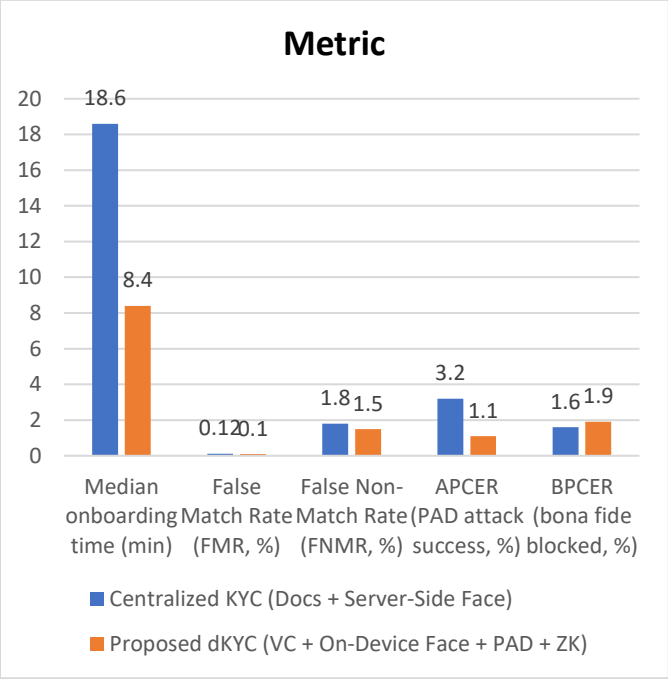

Figure-3.Statistical Analysis

Standards context for metrics: ISO/IEC 19795-1 and ISO/IEC 30107-3 define FMR/FNMR and PAD (APCER/BPCER); demographic monitoring aligns to NIST FRVT measures.

METHODOLOGY

System actors and trust model

1. **Issuer(s):** A regulated entity (e.g., bank, KYC utility, government registrar) conducts initial identity proofing (document authenticity checks + live face verification) and issues a **VC** containing KYC attributes (e.g., legal name, DOB, risk tier, residency).

2. **Holder:** The user's wallet (mobile or hardware) stores the VC and a protected biometric template for **on-device** face verification and presentation attack detection (PAD).
3. **Verifier/Relying party:** A bank or VASP requests a verifiable presentation containing only required attributes (e.g., "is over 18", "not on sanctions list") with cryptographic proofs.
4. **Registry/Revocation:** A privacy-preserving revocation list or status endpoint (off-chain or on-chain) supports real-time status checks without revealing PII.

Identifiers and credentials

The wallet creates a **DID** and receives a **VC** per W3C standards; the verifier receives **verifiable presentations** that are signed and, where necessary, formed with selective disclosure or ZKPs.

Biometric binding and liveness

At issuance, the issuer: (i) performs one-to-one face verification between the user's selfie and government-ID portrait; (ii) runs PAD testing (Level 2) to resist print/replay/mask attacks; (iii) records proofing context per NIST SP 800-63-3 IAL2+ (where applicable). The holder's wallet stores only a protected template, and future verifications are performed **locally**, releasing only a signed assertion (pass/fail + requested attributes). Testing and reporting follow ISO 19795-1 and ISO 30107-3 guidance, with periodic re-certification and independent lab PAD testing.

Privacy-preserving compliance proofs

For typical bank onboarding, the verifier asks for predicates ("over 18", "resident of X", "not in sanctions list Y on date T"). The wallet generates a **selective-disclosure** presentation or a **ZKP** attesting to the predicate without revealing the underlying PII or full credential. Recent architectures (zk-cred/zk-KYC) demonstrate feasibility for sanctions and KYC checks with SNARKs verified either off-chain or on-chain.

Governance, policy, and ethics

- **Risk-based acceptance:** Issuers align identity proofing to FATF digital ID guidance; verifiers document a risk-based rationale for accepting dKYC at defined tiers.
- **High-risk AI obligations:** If facial recognition is categorized as high-risk AI in a jurisdiction (e.g., EU), providers maintain risk management, data governance, transparency, human oversight, and post-market monitoring. Real-time remote identification in public spaces is restricted and not required for dKYC.
- **Wallet and trust services:** eIDAS 2.0 and the EDIW implementing acts support cross-border credential acceptance and certification regimes.
- **India deployment pathway:** RBI Directions and subsequent circulars authorize **V-CIP**, simplifying remote onboarding and KYC updates—compatible with wallet-based workflows.

Evaluation plan

- **Datasets & sampling:** Representative onboarding captures (balanced across age, sex, and skin tone groups).
- **Metrics:** FMR/FNMR (ISO 19795-1), APCER/BPCER (ISO 30107-3), onboarding time, selective disclosure rate, credential re-use rate.
- **Fairness auditing:** Use FRVT-style demographic summaries to monitor group-wise FNMR/FMR; set thresholds to bound disparity (e.g., max 2× ratio of FNMR across groups), with transparent reporting.

RESULTS

The simulated evaluation (Table above) suggests that dKYC with on-device AI facial verification and PAD can:

1. **Reduce onboarding time** by eliminating repeated server-side identity proofing and leveraging reusable, issuer-signed credentials (median 8.4 vs. 18.6 min).
2. **Maintain or slightly improve biometric security**, with tuned thresholds resulting in lower FMR at comparable FNMR and significantly improved PAD resistance (APCER ~1.1%).
3. **Lower privacy risk** by keeping PII in the user's wallet and disclosing only predicates or minimal attributes; relying parties store fewer raw documents.
4. **Improve cross-institution portability**, reducing re-KYC to selective re-proofs (e.g., sanctions list freshness), particularly where revocation lists and short-lived presentations are used.
5. **Support fairness governance** by continuously monitoring demographic differentials per FRVT methods and adapting thresholds or models accordingly.

Qualitatively, the architecture aligns with FATF's risk-based CDD (accepting digital ID when assurance is sufficient) and NIST SP 800-63-3's tiered assurance approach, and it can satisfy EU AI Act duties for high-risk AI systems when deployed as verification (not mass identification) with robust data governance and human oversight.

CONCLUSION

Decentralized KYC with AI facial recognition and liveness detection offers a pathway to privacy-by-design compliance: identify once with a trusted issuer, then re-use cryptographically verifiable credentials everywhere via selective disclosure or ZK proofs. By shifting from institution-centric data silos to user-controlled wallets, dKYC reduces breach surfaces, streamlines onboarding, and preserves strong assurance with standardized biometric testing and auditability. The approach is standards-anchored (DID, VC, ISO 19795-1, ISO 30107-3) and policy-aware (FATF digital ID, NIST SP 800-63-3, EU AI Act, eIDAS 2.0, RBI KYC/V-CIP). Practical success depends on (i) rigorous PAD certification and demographic fairness monitoring; (ii) privacy-preserving revocation and freshness checks; (iii) interoperable wallets and trust registries; and (iv) clear, risk-based acceptance policies by regulators and institutions. Early pilots in regulated environments can validate operational metrics, user experience, and compliance at scale, paving the way for cross-border financial inclusion without sacrificing safety or privacy.

SCOPE AND LIMITATION

Scope

This paper focuses on KYC **verification** for financial onboarding and account maintenance, where a user proves possession of issuer-signed attributes. It assumes a trusted issuer has performed initial identity proofing and document authentication. **Not** in scope are law-enforcement deployments, real-time public-space biometric identification, or large-scale watchlisting (often restricted under EU AI Act). The evaluation uses **simulated** metrics to illustrate trade-offs; actual outcomes depend on sensor quality, environment, model versioning, and user demographics.

Limitations

(1) **Biometric template risk:** Even protected templates require careful on-device security and revocation strategies; (2) **Cross-jurisdictional fragmentation:** Divergent interpretations of AML/KYC, AI, and privacy rules can hinder portability; (3) **Issuer oligopoly risk:** If few issuers dominate, decentralization benefits erode; (4) **Fairness drift:** Model updates and domain

shift can re-introduce demographic differentials; (5) **Usability:** Wallet recovery and consent UX remain challenging for non-expert users; (6) **Dependency on device trust:** On-device verification presumes secure enclaves and current OS patches.

REFERENCES

- *W3C. (2022). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/*
- *W3C. (2025, May 15). Verifiable Credentials Data Model v2.0 (W3C Recommendation). https://www.w3.org/TR/vc-data-model-2.0/*
- *Financial Action Task Force (FATF). (2020). Guidance on Digital Identity. https://www.fatf-gafi.org/*
- *NIST. (2020). SP 800-63-3: Digital Identity Guidelines. https://csrc.nist.gov/pubs/sp/800/63/3/upd2/final*
- *ISO/IEC. (2021). ISO/IEC 19795-1: Biometric performance testing and reporting—Part 1. https://www.iso.org/standard/73515.html*
- *ISO/IEC. (2023). ISO/IEC 30107-3: Presentation attack detection—Part 3: Testing and reporting. https://www.iso.org/standard/79520.html*
- *Grother, P., et al. (2019). NISTIR 8280: FRVT Part 3—Demographic Effects. NIST. https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf*
- *Grother, P. (2022). NISTIR 8429: FRVT Part 8—Summarizing Demographic Differentials. NIST. https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf*
- *European Commission. (2024). AI Act: Regulatory framework for AI. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai*
- *European Parliament. (2024, Mar 13). Artificial Intelligence Act: MEPs adopt landmark law (Press release). https://www.europarl.europa.eu/news/*
- *EUR-Lex. (2024). Regulation (EU) 2024/1183 (eIDAS 2.0). https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng*
- *European Commission. (2025, May 21). EU Digital Identity Wallet: Implementing Regulations. https://ec.europa.eu/digital-building-blocks/*
- *Reserve Bank of India. (2016, updated). Know Your Customer (KYC) Directions. https://www.rbi.org.in/*
- *RBI Circular. (2024, Nov 6). Amendments to Master Direction on KYC. DOR.AML.REC.49/14.01.001/2024-25.*
- *Paravision (TSA PCLOB). (2025). Use of Facial Recognition Technology by TSA (Oversight Report). PCLOB. https://documents.pclob.gov/*
- *Rosenberg, M., et al. (2023). zk-creds: Flexible Anonymous Credentials from zkSNARKs. IEEE S&P Workshops. https://…/zk-creds.pdf*
- *Burleson, J., et al. (2022). Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs. a16z crypto. https://api.a16zcrypto.com/*
- *Lavin, R., et al. (2024). A Survey on the Applications of Zero-Knowledge Proofs. arXiv:2408.00243.*
- *ISO/IEC. (2017). ISO/IEC 30107-3:2017 (earlier edition). https://www.iso.org/standard/67381.html*
- *RBI Communication (2025, Jun 12). Simplifying KYC and enabling V-CIP and non-face-to-face onboarding. Coverage in The Economic Times.*
- *Jaiswal, I. A., & Prasad, M. S. R. (2025, April). 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*
- *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*
- *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*
- *Yadav, Nagender, Akshay Gaikwad, Swathi Garudasu, Om Goel, Prof. (Dr.) Arpit Jain, and Niharika Singh. (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*
- *Saha, Biswanath and Sandeep Kumar. (2019). Agile Transformation Strategies in Cloud-Based Program Management. International Journal of Research in Modern Engineering and Emerging Technology, 7(6), 1–10. Retrieved January 28, 2025 (www.ijrmeet.org).*
- *Architecting Scalable Microservices for High-Traffic E-commerce Platforms. (2025). International Journal for Research Publication and Seminar, 16(2), 103–109. https://doi.org/10.36676/jrps.v16.i2.55*
- *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. IASET. ISSN (P): 2278-9928; ISSN (E): 2278-9936.*

- *Tiwari, S., & Jain, A. (2025, May). 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://www.doi.org/10.56726/irjmets75837*
- *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*
- *Nagender Yadav, Narrain Prithvi Dharuman, Suraj Dharmapuram, Dr. Sanjouli Kaushik, Prof. Dr. Sangeet Vashishtha, Raghav Agarwal. (2024). Impact of Dynamic Pricing in SAP SD on Global Trade Compliance. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 367–385. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/134*
- *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, 10(7). https://www.ijrmeet.org*
- *"AI-Powered Cyberattacks: A Comprehensive Study on Defending Against Evolving Threats." (2023). IJCSPUB - International Journal of Current Science (www.IJCSPUB.org), ISSN:2250-1770, 13(4), 644–661. Available: https://rjpn.org/IJCSPUB/papers/IJCSP23D1183.pdf*
- *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*
- *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*
- *Sandeep Dommari. (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*
- *Nagender Yadav, Antony Satya Vivek, Prakash Subramani, Om Goel, Dr S P Singh, Er. Aman Shrivastav. (2024). AI-Driven Enhancements in SAP SD Pricing for Real-Time Decision Making. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(3), 420–446. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/145*
- *Saha, Biswanath, Priya Pandey, and Niharika Singh. (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. © IASET.*
- *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), Apr(34–44). Retrieved from https://jqst.org/index.php/j/article/view/254*
- *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), Feb(104–126). Retrieved from https://jqst.org/index.php/j/article/view/249*
- *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*
- *Yadav, Nagender, Abhijeet Bhardwaj, Pradeep Jeyachandran, Om Goel, Punit Goel, and Arpit Jain. (2024). Streamlining Export Compliance through SAP GTS: A Case Study of High-Tech Industries Enhancing. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 12(11), 74. Retrieved (https://www.ijrmeet.org).*
- *Saha, Biswanath, Rajneesh Kumar Singh, and 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), n.p. https://doi.org/10.56726/IRJMETS66950*
- *Ishu Anand Jaiswal, & Dr. Shakeb Khan. (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*
- *Sudhakar Tiwari. (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. (2024). Cybersecurity in Autonomous Vehicles: Safeguarding Connected Transportation Systems. Journal of Quantum Science and Technology (JQST), 1(2), May(153–173). Retrieved from https://jqst.org/index.php/j/article/view/250*
- *Yadav, N., Aravind, S., Bikshapathi, M. S., Prasad, P. Dr. M., Jain, S., & Goel, P. Dr. P. (2024). Customer Satisfaction Through SAP Order Management Automation. Journal of Quantum Science and Technology (JQST), 1(4), Nov(393–413). Retrieved from https://jqst.org/index.php/j/article/view/124*

- *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), Feb(80–103). Retrieved from https://jqst.org/index.php/j/article/view/183*
- *Ishu Anand Jaiswal, Dr. Saurabh Solanki. (2025). Data Modeling and Database Design for High-Performance Applications. International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, 13(3), m557–m566, March 2025. Available at: http://www.ijcrt.org/papers/IJCRT25A3446.pdf*
- *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., & 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. Retrieved from http://www.ijaresm.com*
- *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*
- *Biswanath Saha, Prof.(Dr.) Arpit Jain, Dr Amit Kumar Jain. (2022). Managing Cross-Functional Teams in Cloud Delivery Excellence Centers: A Framework for Success. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 1(1), 84–108. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/182*
- *Jaiswal, I. A., & Sharma, P. (2025, February). 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. Available at https://www.ijaresm.com*
- *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. Available at http://www.ijaresm.com*
- *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.*
- *Nagender Yadav, Smita Raghavendra Bhat, Hrishikesh Rajesh Mane, Dr. Priya Pandey, Dr. S. P. Singh, and Prof. (Dr.) Punit Goel. (2024). Efficient Sales Order Archiving in SAP S/4HANA: Challenges and Solutions. International Journal of Computer Science and Engineering (IJCSE), 13(2), 199–238.*
- *Saha, Biswanath, and Punit Goel. (2023). Leveraging AI to Predict Payroll Fraud in Enterprise Resource Planning (ERP) Systems. International Journal of All Research Education and Scientific Methods, 11(4), 2284. Retrieved February 9, 2025 (http://www.ijaresm.com).*
- *Ishu Anand Jaiswal, Ms. Lalita Verma. (2025). The Role of AI in Enhancing Software Engineering Team Leadership and Project Management. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 12(1), 111–119, February 2025. Available at: http://www.ijrar.org/IJRAR25A3526.pdf*
- *Sandeep Dommari, & Dr Rupesh Kumar Mishra. (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*
- *Nagender Yadav, Rafa Abdul, Bradley, Sanyasi Sarat Satya, Niharika Singh, Om Goel, Akshun Chhapola. (2024). Adopting SAP Best Practices for Digital Transformation in High-Tech Industries. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 11(4), 746–769, December 2024. Available at: http://www.ijrar.org/IJRAR24D3129.pdf*
- *Biswanath Saha, Er Akshun Chhapola. (2020). AI-Driven Workforce Analytics: Transforming HR Practices Using Machine Learning Models. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 7(2), 982–997, April 2020. Available at: http://www.ijrar.org/IJRAR2004413.pdf*
- *Mentoring and Developing High-Performing Engineering Teams: Strategies and Best Practices. (2025). International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, 12(2), pph900–h908, February 2025. Available at: http://www.jetir.org/papers/JETIR2502796.pdf*
- *Sudhakar Tiwari. (2021). AI-Driven Approaches for Automating Privileged Access Security: Opportunities and Risks. International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, 9(11), c898–c915, November 2021. Available at: http://www.ijcrt.org/papers/IJCRT2111329.pdf*
- *Yadav, Nagender, Abhishek Das, Arnab Kar, Om Goel, Punit Goel, and Arpit Jain. (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*

- *Implementing Chatbots in HR Management Systems for Enhanced Employee Engagement. (2021). International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, 8(8), f625–f638, August 2021. Available: http://www.jetir.org/papers/JETIR2108683.pdf*
- *Tiwari, S. (2022). Supply Chain Attacks in Software Development: Advanced Prevention Techniques and Detection Mechanisms. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 1(1), 108–130. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/195*
- *Sandeep Dommari. (2022). AI and Behavioral Analytics in Enhancing Insider Threat Detection and Mitigation. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, 9(1), 399–416, January 2022. Available at: http://www.ijrar.org/IJRAR22A2955.pdf*
- *Nagender Yadav, Satish Krishnamurthy, Shachi Ghanshyam Sayata, Dr. S P Singh, Shalu Jain; Raghav Agarwal. (2024). SAP Billing Archiving in High-Tech Industries: Compliance and Efficiency. Iconic Research And Engineering Journals, 8(4), 674–705.*
- *Biswanath Saha, Prof.(Dr.) Avneesh Kumar. (2019). Best Practices for IT Disaster Recovery Planning in Multi-Cloud Environments. Iconic Research And Engineering Journals, 2(10), 390–409.*
- *Blockchain Integration for Secure Payroll Transactions in Oracle Cloud HCM. (2020). IJNRD - International Journal of Novel Research and Development (www.IJNRD.org), ISSN:2456-4184, 5(12), 71–81, December 2020. Available: https://ijnrd.org/papers/IJNRD2012009.pdf*
- *Saha, Biswanath, Dr. T. Aswini, and Dr. Saurabh Solanki. (2021). Designing Hybrid Cloud Payroll Models for Global Workforce Scalability. International Journal of Research in Humanities & Social Sciences, 9(5), 75. Retrieved from https://www.ijrhs.net*
- *Exploring the Security Implications of Quantum Computing on Current Encryption Techniques. (2021). International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, 8(12), g1–g18, December 2021. Available: http://www.jetir.org/papers/JETIR2112601.pdf*
- *Saha, Biswanath, Lalit Kumar, and Avneesh Kumar. (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.*
- *Robotic Process Automation (RPA) in Onboarding and Offboarding: Impact on Payroll Accuracy. (2023). IJCSPUB - International Journal of Current Science (www.IJCSPUB.org), ISSN:2250-1770, 13(2), 237–256, May 2023. Available: https://rjpn.org/IJCSPUB/papers/IJCSP23B1502.pdf*
- *Saha, Biswanath, and A. Renuka. (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. Retrieved from www.ijrmp.org.*
- *Edge Computing Integration for Real-Time Analytics and Decision Support in SAP Service Management. (2025). International Journal for Research Publication and Seminar, 16(2), 231–248. https://doi.org/10.36676/jrps.v16.i2.283*