Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 11-20

Decentralized AI and the Future of AI Rights Management

Er. Lucky Jha
ABESIT, Crossings Republik, Ghaziabad, Uttar Pradesh 201009
luckyjha200405@gmail.com

Date of Submission: 01-02-2026 Date of Acceptance: 15-02-2026 Date of Publication: 03-03-2026

ABSTRACT

As artificial intelligence (AI) systems scale across sectors, the regimes governing who may access, use, audit, license, and benefit from models, weights, datasets, prompts, and outputs remain fragmented. "AI rights management" (AIRM) refers to the technical, legal, and institutional mechanisms that allocate these rights and duties across creators, data contributors, model publishers, deployers, and end-users. Centralized approaches—terms of service enforced by platforms, siloed registries, and proprietary compliance APIs—struggle to provide transparency, composability, and cross-jurisdictional enforceability, especially when models and content are remixed across organizational and national boundaries. This manuscript argues that decentralized identity, verifiable provenance, content authenticity, and programmable licensing—coordinated by ledgers and decentralized storage—offer a credible path to future-proof AIRM. We synthesize insights from emerging regulations (e.g., the EU AI Act, the EU Data Act), public-law guidance (e.g., U.S. Copyright Office positions on human authorship), standards (W3C Verifiable Credentials, Decentralized Identifiers, PROV), and industry efforts (C2PA, IPFS, Solid pods, open and responsible AI licensing). Building on this base, we propose a layered architecture: (1) decentralized identity and role binding; (2) machine-verifiable rights assertions and provenance; (3) tokenized or programmable licensing and revenue distribution; (4) auditability and dispute resolution through cryptographic attestations and governed data trusts. Methodologically, we employ a design-science synthesis with normative legal analysis and scenario-based evaluation in creative media and dataset contribution contexts. The results show how decentralized primitives can make AI rights legible and enforceable *ex ante* (through embedding rights in artifacts and workflows) rather than *ex post* policing. We conclude with a scope and limitations section that surfaces governance pitfalls (e.g., sybil risk and unequal bargaining power), regulatory alignment challenges, and open research questions on watermark

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 11-20

robustness, cross-chain portability, and human-centric remedies.

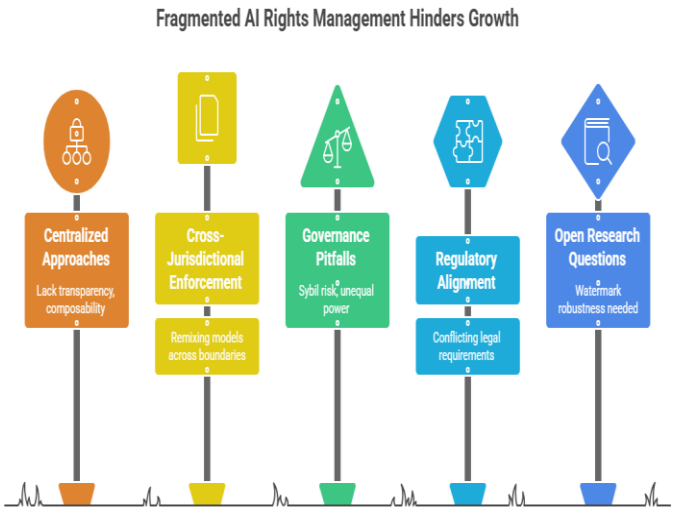

Figure-1.Fragmented AI Rights Management Hinders Growth

KEYWORDS

Decentralized AI, Rights Management, Provenance, Verifiable Credentials, Decentralized Identifiers, C2PA, Data Trusts, Programmable Licensing, EU AI Act, Copyright

INTRODUCTION

AI has complicated long-standing questions of authorship, ownership, and accountability. A single output (e.g., an image or code snippet) may reflect the creative labor of a prompt engineer, the weights learned from numerous copyrighted works, and inference-time adaptations informed by user data. If we cannot trace *who did what, when, and under which rights*, then royalty payments, takedown requests, and safety audits become speculative rather than evidence-based. Modern legislation and guidance already signal a shift toward *verifiable* AI practices. The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) establishes harmonized rules for AI governance, including transparency obligations for certain systems and disclosure around training and evaluation practices. In parallel, the EU Data Act clarifies who can use which data, on what terms, and under which conditions—critical for defining access and portability across AI value chains.

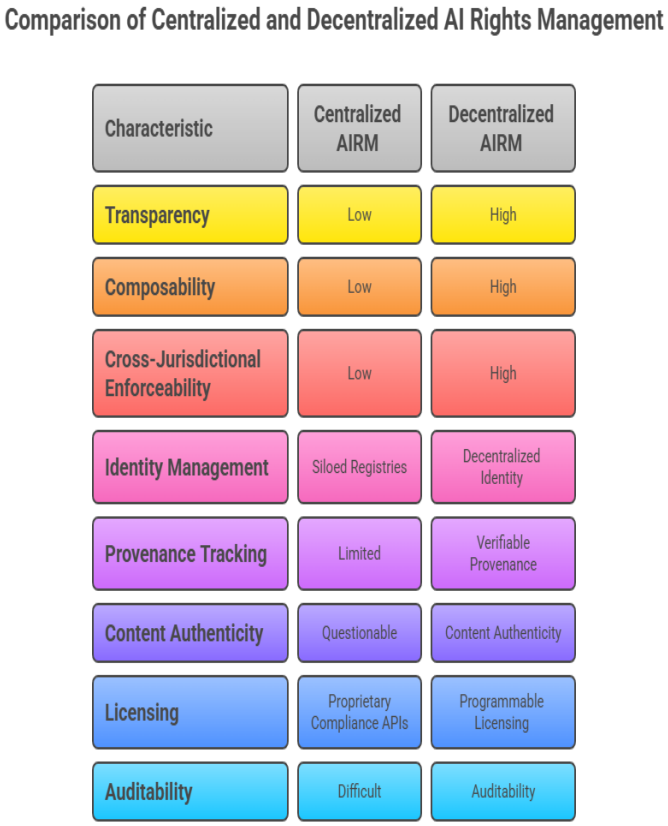

Figure-2.Comparison of Centralized and Decentralized AI Rights Management

On authorship and copyrightability, the U.S. Copyright Office's (USCO) 2023 policy statement confirms that works generated solely by AI lack copyright protection in the United States absent sufficient human authorship—though AI-assisted works can qualify when a human's creative contribution is evident and original; courts have upheld this stance in *Thaler v. Perlmutter*. These legal anchors coexist with international conversations

convened by WIPO to map unresolved IP issues in AI (e.g., training exceptions, inventorship/authorship, and data provenance).

Yet policy alone cannot scale AIRM. Central registries are brittle; proprietary APIs fragment compliance; and "click-through" licenses are neither machine-actionable nor composable across platforms. Decentralized primitives—cryptographic identities, attestations, content authenticity manifests, and distributed ledgers—allow rights and duties to travel *with* the artifact (dataset, model card, or output) and be evaluated at use-time. *Decentralization here is not "blockchain for everything"*, but a careful choreography of standards (e.g., W3C Verifiable Credentials and DIDs), provenance models (W3C PROV), and authenticity signals (C2PA), optionally anchored to content-addressed storage (IPFS) and governed enclaves (data trusts and Solid pods) to bind rights to entities and evidence.

Finally, licensing regimes are evolving: the Open Source Initiative released an "Open Source AI Definition 1.0" delineating freedoms and access conditions; responsible-use licenses (e.g., RAIL) embed behavioral constraints; Creative Commons clarifies how CC-licensed works interact with AI training under various jurisdictions. Together, these signal a rights landscape that must be machine-readable, enforceable, and portable.

LITERATURE REVIEW

From DRM to AIRM

Traditional digital rights management (DRM) limited copying and access through centralized control—a poor fit for AI's recombinant workflows. Recent scholarship argues for decentralized DRM designs that store rights metadata on public ledgers, validate it in permissioned domains, and enforce payouts via smart contracts—demonstrated persuasively in the music industry. These insights generalize: AI ecosystems need transparent rights registries, globally consistent metadata, and automatic settlement to reconcile competing claims among model builders, dataset contributors, rights-holders, and downstream creators.

Legal foundations under flux

The EU AI Act codifies risk-based obligations; while not an IP statute, its documentation and transparency requirements, combined with the EU Data Act's provisions for access/portability and the Data Governance Act's stewardship models, create a compliance spine for rights-aware AI. In the U.S., USCO's 2023 policy and subsequent litigation (*Thaler*) affirm the centrality of human authorship, leaving unresolved questions about training exceptions and style emulation (topics the Office continues to analyze in ongoing reports). WIPO's multi-session "Conversation on IP and AI" outlines domain-agnostic issues (e.g., ownership of outputs, data and model provenance, liability) that motivate standards-based solutions.

Identity, credentials, and provenance

W3C's Decentralized Identifiers (DID) and Verifiable Credentials (VC) specifications enable cryptographically verifiable claims about entities (people, organizations, devices) and artifacts (datasets, models), including role assignments (e.g., "rights-holder," "data trustee," "model maintainer"). Provenance standards (W3C PROV) provide a common data model to express *who used what to produce what*, across pipelines. Content authenticity manifests from the Coalition for Content Provenance and Authenticity (C2PA) allow creators and tools to embed tamper-evident metadata that records capture, editing, and generation steps; this is increasingly proposed to tag AI-generated outputs and tie them back to source claims.

Content addressing and storage

InterPlanetary File System (IPFS) identifies content by its cryptographic fingerprint (CID), allowing rights manifests and artifacts to be bound to immutable identifiers; this is useful for deduplicating royalties and proving that "this exact artifact" was used. Meanwhile, Solid pods (decentralized personal data stores) and data trusts (institutional stewards) present governance patterns for consent, revocation, and equitable sharing—essential when training data contains personal or community-contributed assets.

Licensing and norms

The Open Source Initiative's Open Source AI Definition clarifies freedoms (use, study, modify, share) in the AI context, stressing access to the "preferred form of modification" (often, weights plus training code/recipes). Responsible AI Licenses (RAIL) introduce behavior-based restrictions for high-risk uses, blending access with guardrails. Creative Commons has published primers on how CC licenses intersect with AI training, underscoring jurisdictional variance and limits of license-based "anti-training" provisions.

Documentation for accountability

"Model Cards" and "Datasheets for Datasets" are widely adopted patterns for disclosing intended use, performance, and data lineage; decentralized AIRM can render these disclosures trustworthy by cryptographically binding them (and later updates) to the model/dataset artifact and signer identities.

Collectively, the literature and standards point to a convergent technical stack for AIRM: decentralized identity and roles, verifiable claims and provenance, authenticity manifests for outputs, content addressing for artifacts, and programmable licensing for usage and revenue settlement.

METHODOLOGY

This work follows a design-science and normative legal analysis approach:

1. **Problem framing and requirements elicitation**
2. We synthesize regulatory obligations (EU AI Act, Data Act; USCO guidance), community norms (OSI, CC), and technical affordances (DID/VC, PROV, C2PA, IPFS, Solid, data trusts) to derive requirements for AI rights management: (R1) identity-bound roles; (R2) machine-readable rights and duties; (R3) tamper-evident provenance; (R4) content authenticity and disclosure; (R5) programmable licensing and settlement; (R6) consent, revocation, and data minimization; (R7) cross-jurisdictional interpretability.
3. **Artifact design: a layered, decentralized AIRM architecture**
    - **Layer A (Identity & Roles):** Assign DIDs to human actors, organizations, and automated agents; issue VCs for roles such as "dataset rights-holder," "model author," "licensee," or "trustee."
    - **Layer B (Provenance & Claims):** Use PROV to encode data lineage, training/inference steps, and contributions (with hash-linked manifests).
    - **Layer C (Authenticity & Disclosure):** Attach C2PA content credentials to generated artifacts (images, audio, text) with attestations describing generative model identity, version, and prompts.
    - **Layer D (Content Addressing & Storage):** Address all artifacts (datasets, model snapshots, cards, manifests) via IPFS CIDs;

index them on a ledger or registry for discoverability and audit.

- **Layer E (Licensing & Settlement):** Express licenses as machine-readable policies (e.g., JSON-LD) that smart contracts interpret to authorize uses, meter consumption, and split royalties among contributors; allow escrow or stablecoin settlement to reduce FX friction.
- **Layer F (Governance & Remedies):** Instantiate data trusts for community datasets; use Solid pods for individual data control; specify dispute flows (arbitration, appeals) and emergency revocation procedures.

4. **Evaluation by scenarios**

We apply the architecture to two representative scenarios—(S1) creative media generation with third-party assets, and (S2) collaborative dataset contribution to a foundation model—evaluating whether the design satisfies R1–R7, and where practical or legal gaps remain.

5. **Validation strategy**

We align architectural choices with specific articles/clauses in the EU AI Act (documentation and transparency), the Data Act (access/portability), and USCO human-authorship principles; we also map to standards profiles (DID/VC, PROV, C2PA). This "standard-anchored" validation emphasizes interoperability and regulatory readiness rather than benchmark performance.

RESULT

Scenario S1: Rights-aware creative generation

A studio commissions a mixed-media advertisement that blends human-shot footage, licensed music stems, and AI-generated textures. The production stack implements Layers A–E:

- The studio, music publisher, and post-production vendors use DIDs; each party holds VCs asserting their roles. When an editor imports a music stem, the NLE reads a VC that encodes territorial and media-type restrictions. Attempted uses outside the license scope trigger an *ex ante* warning rather than an *ex post* content ID dispute.
- Every render attaches a C2PA manifest stating the capture device for footage, the editing software chain, and any generative models with version hashes. Downstream platforms ingest the asset and validate the manifest, enabling: (i) audience disclosure, (ii) internal risk routing for ad policy, and (iii) automatic routing of a micro-royalty to the publisher on each play per the machine-readable license.
- If the studio later updates the color grade, the new render inherits the lineage via PROV, ensuring auditors can reconstruct the entire pipeline.

Outcome: The rights become *portable and machine-verifiable*. Royalty splits are enforced by contract code; disclosures satisfy platform and regulatory policies; provenance reduces disputes and accelerates clearances.

Scenario S2: Community data contribution to a foundation model

A consortium builds a multilingual speech model from citizen-science contributions.

- Contributors host audio in personal Solid pods. Consent (purpose, duration, allowed uses) is expressed as a VC; revocation travels with the data pointer, enabling future retraining filters.
- A data trust governs the corpus; revenues from commercial inference users flow via programmable splits to the trust and, pro-rata, to contributor wallets.
- Training jobs materialize PROV graphs (source IDs, preprocessing, augmentations) and checksum snapshots; model releases ship with signed Model Cards and dataset Datasheets hash-bound to the weights.
- When an enterprise customer deploys the model, its inference service checks license terms (e.g., prohibitions on surveillance use) and automatically withholds settlement if the usage category is disallowed.

Outcome: Contributors retain meaningful agency, and the model's lineage remains auditable. The architecture demonstrates compliance readiness for documentation/transparency regimes while preserving opt-out pathways and economic participation.

Observed advantages and trade-offs

- **Legibility & auditability:** Binding rights to artifacts via CIDs and to roles via VCs yields *verifiable* compliance, reducing "he said, she said" disputes.
- **Settlement efficiency:** Smart-contract splits reduce intermediaries and reconcile long tails of micro-royalties (as seen in decentralized DRM research).
- **Compliance by construction:** C2PA + PROV manifests support disclosure obligations and trust signals across platforms.
- **Governance burden:** Data trusts and Solid pods introduce operational complexity; unequal bargaining power may still produce extractive terms without procedural safeguards.

CONCLUSION

Decentralized AIRM reframes enforcement from *platform policing* to *embedded verifiability*. Identity standards (DID/VC) let us encode roles and permissions; provenance (PROV) and authenticity (C2PA) make AI pipelines reconstructable and outputs self-describing; content addressing (IPFS) ties claims to immutable artifacts; programmable licenses and settlement distribute value at line-rate. This stack complements emerging regulatory obligations (e.g., transparency and documentation in the EU AI Act) and aligns with copyright doctrines that prioritize human creativity while clarifying the status of AI-assisted works.

The near-term trajectory suggests *more* machine-readable policy. The Open Source AI Definition 1.0 will pressure vendors to disclose the "preferred form of modification," while responsible-use licenses (RAIL) and platform policies will continue to gate high-risk uses. Meanwhile, public authorities are still working through the thorniest questions—training on copyrighted materials, style emulation, and collective rights—topics the U.S. Copyright Office has continued to examine in recent reports.

Our results show that decentralized primitives can *practically* improve rights legibility, ex-ante compliance, and fair compensation—provided we address governance challenges and standardize profiles that vendors and creators can adopt with minimal friction.

SCOPE AND LIMITATIONS

Scope

This manuscript synthesizes law, standards, and systems literature to propose a general-purpose AIRM architecture. It is technology- and jurisdiction-agnostic by design, referencing EU and U.S. anchors and internationally recognized standards bodies (W3C, Joint Development Foundation/C2PA). It targets workflows spanning creative media, software/code generation, and data-centric model training.

Limitations

First, *binding law varies by jurisdiction* and remains in flux; implementers must map licenses and consents to local contract and consumer-protection law. Second, *provenance is not infallible*: C2PA/PROV attestations rely on trustworthy hardware/soft-ware roots; falsified or stripped manifests remain risks, and watermarking of AI outputs is adversarial. Third, *governance complexity*: data trusts and Solid pods can reintroduce centralization (via trustees or identity providers), and they require sustained funding and community oversight. Fourth, *privacy and ethics*: even with consent VCs, training on sensitive data may be undesirable or unlawful; differential privacy or synthetic data may be needed but can degrade utility. Finally, *interoperability*: cross-chain portability and standard license semantics are nascent; multi-vendor adoption requires profiles, test suites, and liability backstops. Despite these constraints, progressive deployment—starting with content authenticity and model/dataset documentation bound to identities—can deliver immediate value while the broader ecosystem matures.

REFERENCES

- *Coalition for Content Provenance and Authenticity. (2025). C2PA Specifications, Version 2.2.*
- *Creative Commons. (2025). Understanding CC licenses and AI training: A legal primer.*
- *European Parliament and Council. (2024). Regulation (EU) 2024/1689 on artificial intelligence (AI Act). Official Journal of the European Union.*
- *European Parliament and Council. (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union.*
- *European Parliament and Council. (2022). Regulation (EU) 2022/868 on European data governance (Data Governance Act). Official Journal of the European Union.*
- *Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92.*
- *Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In Proceedings of FAT* (pp. 1–10).*
- *Open Data Institute. (2019). Data trusts: Lessons from three pilots.*
- *Open Source Initiative. (2025). Open Source AI Definition 1.0.*
- *Responsible AI Licenses. (2024/2025). RAIL License FAQ.*
- *Solid Project. (n.d.). About Solid. (Accessed August 19, 2025).*
- *U.S. Copyright Office. (2023). Copyright registration guidance: Works containing AI-generated material. Policy Statement.*
- *Thaler v. Perlmutter, 1:22-cv-01564 (D.D.C. Aug. 18, 2023) (Memorandum Opinion).*
- *Thaler v. Perlmutter, No. 23-5233 (D.C. Cir. Mar. 2025).*
- *W3C. (2013). PROV-DM: The PROV Data Model. Recommendation.*
- *W3C. (2022). Decentralized Identifiers (DIDs) v1.0. Recommendation.*
- *W3C. (2025). Verifiable Credentials Data Model v2.0. Recommendation.*
- *WIPO. (2020). Revised issues paper on intellectual property policy and artificial intelligence.*
- *WIPO. (2021). Non-fungible tokens (NFTs) and copyright. WIPO Magazine, 4.*
- *Ciriello, R. F., Torbensen, A. C. G., Hansen, M. R. P., & Müller-Bloch, C. (2023). Blockchain-based digital rights management systems: Design principles for the music industry. Electronic Markets, 33, Article 5.*
- *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*

- *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, 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*
- *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.*
- *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, 14(1), 179–192.*
- *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., & 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*
- *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.*
- *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).*
- *AI-powered cyberattacks: A comprehensive study on defending against evolving threats. (2023). International Journal of Current Science, 13(4), 644–661.*
- *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, 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, 10(3), 42. https://doi.org/10.63345/ijrmeet.org.v10.i3.6*
- *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*
- *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.*
- *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, 13(2), 995–1028.*
- *Jaiswal, I. A., & Goel, O. (2025). Optimizing content management systems with caching and automation. Journal of Quantum Science and Technology, 2(2), 34–44.*
- *Tiwari, S., & Gola, D. K. K. (2024). Leveraging dark web intelligence to strengthen cyber defense mechanisms. Journal of Quantum Science and Technology, 1(1), 104–126.*
- *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, 10(1), 40. https://doi.org/10.63345/ijrmeet.org.v10.i1.6*
- *Yadav, N., Bhardwaj, A., Jeyachandran, P., Goel, O., Goel, P., & Jain, A. (2024). Streamlining export compliance through SAP GTS: A case study in high-tech industries. International Journal of Research in Modern Engineering and Emerging Technology, 12(11), 74.*
- *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., & 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*
- *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. (2024). Cybersecurity in autonomous vehicles: Safeguarding connected transportation systems. Journal of Quantum Science and Technology, 1(2), 153–173.*
- *Yadav, N., Aravind, S., Bikshapathi, M. S., Prasad, P. M., Jain, S., & Goel, P. (2024). Customer satisfaction through SAP order management automation. Journal of Quantum Science and Technology, 1(4), 393–413.*
- *Saha, B., & Goel, P. (2024). Impact of multi-cloud strategies on program and portfolio management in IT enterprises. Journal of Quantum Science and Technology, 1(1), 80–103.*
- *Jaiswal, I. A., & Solanki, S. (2025). Data modeling and database design for high-performance applications. International Journal of Creative Research Thoughts, 13(3), m557–m566. 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, 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, 11(8), 2188.*
- *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*
- *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.*
- *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, 13(2), 3165.*
- *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, 11(8), 2149.*
- *Dommari, S., & Kumar, S. (2021). The future of identity and access management in blockchain-based digital ecosystems. International Journal of General Engineering and Technology, 10(2), 177–206.*
- *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, 13(2), 199–238.*
- *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, 11(4), 2284.*
- *Jaiswal, I. A., & Verma, L. (2025). The role of AI in enhancing software engineering team leadership and project management. International Journal of Research and Analytical Reviews, 12(1), 111–119. http://www.ijrar.org/IJRAR25A3526.pdf*
- *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*
- *Yadav, N., Abdul, R., Bradley, S., Satya, S. S., Singh, N., Goel, O., & Chhapola, A. (2024). Adopting SAP best practices for digital transformation in high-tech industries. International Journal of Research and Analytical Reviews, 11(4), 746–769. http://www.ijrar.org/IJRAR24D3129.pdf*
- *Saha, B., & Chhapola, A. (2020). AI-driven workforce analytics: Transforming HR practices using machine learning models. International Journal of Research and Analytical Reviews, 7(2), 982–997.*
- *Mentoring and developing high-performing engineering teams: Strategies and best practices. (2025). Journal of Emerging Technologies and Innovative Research, 12(2), h900–h908. http://www.jetir.org/papers/JETIR2502796.pdf*
- *Tiwari, S. (2021). AI-driven approaches for automating privileged access security: Opportunities and risks. International Journal of Creative Research Thoughts, 9(11), c898–c915. http://www.ijcrt.org/papers/IJCRT2111329.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, 14(4), 810.*
- *Implementing chatbots in HR management systems for enhanced employee engagement. (2021). Journal of Emerging Technologies and Innovative Research, 8(8), f625–f638. 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, 1(1), 108–130.

- *Dommari, S. (2022). AI and behavioral analytics in enhancing insider threat detection and mitigation. International Journal of Research and Analytical Reviews, 9(1), 399–416.*
- *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.*
- *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.*
- *Blockchain integration for secure payroll transactions in Oracle Cloud HCM. (2020). International Journal of Novel Research and Development, 5(12), 71–81.*
- *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.*
- *Exploring the security implications of quantum computing on current encryption techniques. (2021). Journal of Emerging Technologies and Innovative Research, 8(12), g1–g18.*
- *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.*
- *Robotic process automation (RPA) in onboarding and offboarding: Impact on payroll accuracy. (2023). International Journal of Current Science, 13(2), 237–256.*
- *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.*
- *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*