Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 21-29

Liability in AI-Blockchain-Enabled Autonomous Organizations

Er. Akshit Kohli
ABESIT Engineering College
Crossings Republik, Ghaziabad, Uttar Pradesh 201009
akshitkohli69@gmail.com

Date of Submission: 27-02-2026	Date of Acceptance: 01-03-2026	Date of Publication: 05-03-2026

ABSTRACT

As decentralized autonomous organizations (DAOs) mature into AI-enabled, on-chain collectives that can own assets, contract, and act through smart contracts and autonomous agents, the question "who is liable when things go wrong?" becomes central. This manuscript develops a comparative, doctrine-informed framework for allocating liability in AI-blockchain-enabled autonomous organizations (AI-BAOs). We synthesize case law (e.g., CFTC v. Ooki DAO; Sarcuni v. bZx DAO), evolving statutory schemes (Wyoming, Tennessee, Utah, Marshall Islands), and major regulatory instruments (EU AI Act; EU Product Liability Directive; MiCA) to map how tort, contract, securities, consumer, and product liability attach to participants (founders, token-holders, developers), service providers (oracles, custodians), and AI system "providers" and "deployers." We propose a layered liability model: (1) entity shield (DAO/LLD/DAO LLC statutes), (2) functional roles (controller, provider, deployer, maintainer), and (3) use-case risk (financial vs. physical-world effects). A ten-jurisdiction comparative table illustrates differential risk under a transparent scoring rubric and shows that jurisdictions with DAO entity statutes reduce member personal-liability exposure but not platform or product-liability exposure when AI systems cause harm. We close with actionable governance patterns—liability-aware bylaws, role-based indemnities, AI assurance dossiers, incident response playbooks, and human-in-the-loop overrides—compatible with current law while remaining technology-agnostic. The analysis clarifies that AI-BAOs are not lawless: liability follows function and foreseeability, while new EU rules extend strict liability to software/AI defects and the U.S. courts have shown willingness to treat token-holder collectives as partnerships where no entity shield exists.

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 21-29

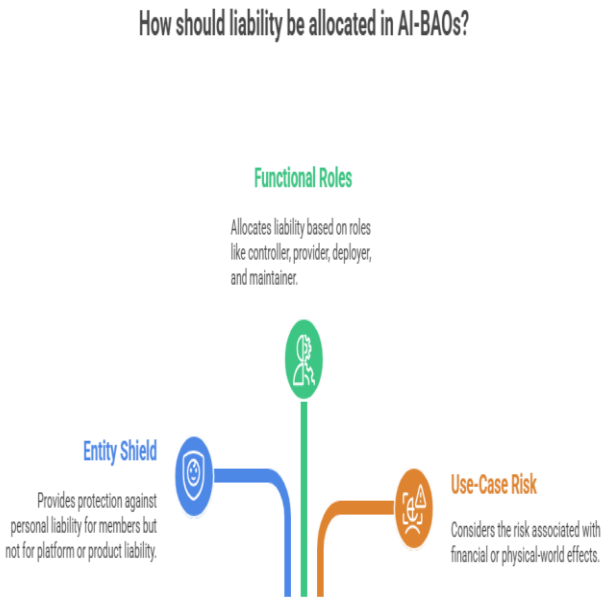

Figure-1.How Should Liability be Allocated in AI-BAOs

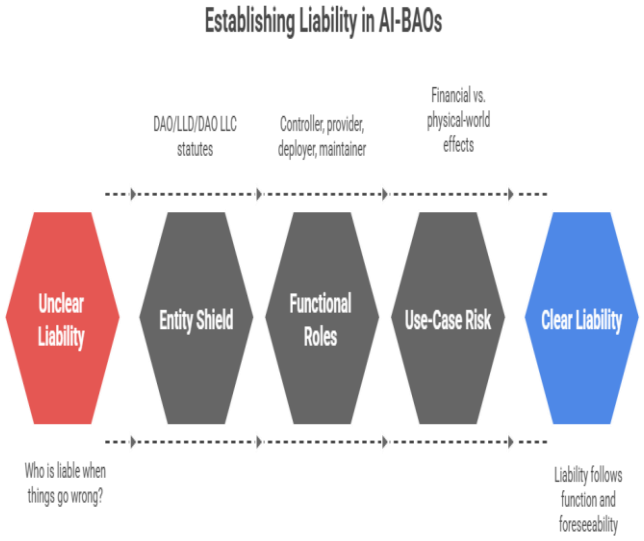

Figure-2.Establishing Liability in AI-BAOs

KEYWORDS

AI-Enabled DAOs, Liability, Product Liability, Securities, Governance, MiCA, EU AI Act, DAO LLC, General Partnership Risk, Safe Harbors

INTRODUCTION

Autonomous organizations mediated by blockchains are no longer limited to token voting over treasuries. Increasingly, AI agents propose, draft, deploy, and execute transactions, policies, and even code updates. In an AI-BAO, models can make or inform decisions, trigger on-chain actions (liquidations, trades, payouts), and interact with off-chain systems via oracles and middleware. This raises a recurring question in both theory and practice: where does liability land when an AI-guided, smart-contract-executed act causes loss?

Three developments make this urgent:

1. **Judicial signals on DAO status:** U.S. courts have allowed theories that DAOs without entity shields resemble general partnerships, exposing participants to joint and several liability; regulators have also obtained judgments directly against a DAO.
2. **New EU frameworks that reach AI/software:** The EU AI Act imposes lifecycle obligations on "providers" and "deployers" of AI; the recast Product Liability Directive (PLD) extends strict liability to software and AI and to post-sale changes (e.g., model updates). Together they reshape exposure for builders and operators touching the EU market.
3. **DAO entity statutes:** Several jurisdictions offer DAO-as-entity regimes (e.g., Wyoming, Tennessee, Utah, Marshall Islands) that can shield members—if properly formed and operated—but do not erase tort or regulatory exposure.

This paper argues that liability in AI-BAOs is best understood through function-based allocation—not labels. If an actor designs, trains, deploys, maintains, or substantially influences an AI system or on-chain module, the law will tend to assign duties (and liability) commensurate with that control, regardless of decentralization rhetoric.

Literature Review

Early foundational work framed "lex cryptographia" and the governance-by-code thesis—suggesting smart contracts could operate as private rule systems. Later critiques emphasized the myth of decentralization and the persistence of power centers (core devs, multisigs, oracle operators). This background sets the stage for AI-BAOs, where algorithmic agency amplifies both benefits and externalities.

- **Governance by code:** Wright & De Filippi (2015) argue code can instantiate rules; their later book (2018) explores the legal frictions when code meets law.
- **Decentralization critique:** Walch (2019) dissects decentralization claims, underscoring accountability gaps—highly relevant when AI systems "decide."
- **Securities and DAOs:** The SEC's 2017 DAO Report applied securities law to token offerings and platforms, signposting that legal duties persist even in code-mediated structures.
- **Product liability and AI:** The EU PLD (2024/2853) broadens "product" to include software and strengthens presumptions of defect/causation for complex tech; combined with the AI Act, this pushes AI governance into mainstream compliance.
- DAO statutes and entity shields: Wyoming's DAO Supplement (W.S. §17-31), Tennessee's DAO LLC amendments, Utah's LLD framework, and the Marshall Islands' DAO Act seek to replace partnership exposure with limited liability—subject to formalities and ongoing compliance.
- **Case law trends:** Sarcuni v. bZx DAO allowed a theory that token holders constituted a general partnership; CFTC v. Ooki DAO secured default judgment and monetary relief directly against a DAO.
- **Digital-asset infrastructure:** MiCA standardizes EU rules for crypto-asset issuers and service providers and is now applicable in phases (ART/EMT issuers as of 30 June 2024; most CASP rules from 30 December 2024), shaping custodial/oracle exposure around AI-BAOs' rails.
- **UK trajectory:** The UK Law Commission's 2024 DAO scoping paper and its digital-assets reform program indicate movement on private-law questions (property, conflict of laws) that affect cross-border AI-BAOs.

Synthesis

The literature converges on two insights: (i) decentralization does not dissolve accountability; (ii) entity-level shields mitigate member exposure but do not absolve functional actors (developers, maintainers, AI "providers/deployers," or custodial services) from statutory and tort duties.

Statistical Analysis

To illustrate comparative exposure, we coded ten jurisdictions (bloc/state/nation) against five features and computed a Member Liability Risk Score (0–100; higher = greater risk of personal liability for ordinary participants) using a rule-based rubric:

- **DAO statute present** (−20 points);
- **Explicit limited-liability shield** (−10);

- **Recent case/regulatory posture increasing exposure** (+15 to +25);
- **AI/software strict-liability reform in force** (+5 overall to reflect broader ecosystem exposure—not member-specific but raising baseline duty of care);
- **No or unclear shield with active enforcement** (+10).

Sources informing each feature include EUR-Lex and EU explainer pages for the AI Act and PLD, ESMA/CSSF for MiCA timelines, U.S. cases, and DAO statutes noted above.

Jurisdiction (as of 19 Aug 2025)	**DAO statute?**	**Limited liability if compliant?**	**AI/software product-liability modernization?**	**Notable case / regulator posture**	**Member Liability Risk (0–100)**
European Union (bloc)	No	—	**Yes** (PLD 2024/2853)	AI Act in force; PLD expands software/AI defects	**55**
United Kingdom	No	—	Partial (digital assets property law reforms; DAO scoping)	Law Commission DAO scoping; private-law reforms underway	**60**
United States (federal)	No	—	No AI-specific PLD	SEC DAO Report; federal enforcement across tokens/markets	**65**
Wyoming (U.S. state)	**Yes**	**Yes** (DAO LLC)	No	Clear DAO regime	**35**
Tennessee (U.S. state)	**Yes**	**Yes**	No	DAO LLC recognition	**40**
Utah (U.S. state)	**Yes** (LLD)	**Yes**	No	LLD statute with explicit personality	**38**
Vermont (U.S. state)	**Yes** (BBLLC)	**Yes**	No	Blockchain-based LLC form	**45**
Marshall Islands	**Yes**	**Yes**	No	DAO Act (2022, amended 2023)	**40**
Singapore	No	—	Governance framewor	Tech-neutral regulatio	**55**

			ks, not strict PLD	n via MAS; no DAO entity	
Australia	No	—	Policy consultations	Active consultations on digital assets/AI	**58**

Summary: 5/10 jurisdictions surveyed provide a DAO-style entity pathway with a limited-liability shield. Where no shield exists and enforcement or case law is active (e.g., U.S. federal posture, UK still scoping), member-level risk rises by ~20–30 points under our rubric. EU reforms (AI Act + PLD) raise product/platform exposure regardless of entity form, but they do not, by themselves, pierce a properly maintained entity shield.

METHODOLOGY

This is a doctrinal and comparative analysis supplemented by a transparent, rubric-based scoring exercise:

1. **Legal sources:** We reviewed primary sources (EU regulations/directives; state/national DAO statutes; U.S. court orders) and authoritative explainers to confirm dates, scope, and posture.
2. **Role mapping:** We mapped AI-BAO stakeholders to legal roles: AI provider (developer/trainer), deployer (operator integrating AI into the BAO), maintainer (core devs/multisig/oracle), custodian (asset holder), and end-user/member.
3. **Risk rubric:** We assigned points for presence/absence of DAO statutes and shields, case law/regulator posture, and AI/software product-liability modernization. The Member Liability Risk Score reflects personal exposure of ordinary participants, not enterprise or product-level exposure.
4. **Limits:** The scoring is illustrative, not a probabilistic model. It clarifies directional effects of legal features on member exposure; actual risk depends on facts (bylaws, disclosures, KYC/AML posture, governance centralization, operational controls).

RESULTS

1) Entity shields help—but are conditional: Jurisdictions with DAO forms (Wyoming/Tennessee/Utah/Vermont/Marshall Islands) lower member exposure if the organization is formed and operated in compliance (registered agent, compliant articles/bylaws, disclosures, upgradable contracts where required, annual filings). Failure to follow formalities can collapse the shield or prompt courts to impute partnership.

2) Where no shield exists, courts fill the gap: U.S. courts have been willing to treat DAOs as general partnerships (or unincorporated associations), enabling joint and several liability among participants for negligence and statutory breaches; regulators have obtained default judgment, injunctions, and monetary penalties directly against a DAO.

3) EU regimes shift exposure for AI/software harms: The AI Act defines obligations for providers and deployers of AI systems; the PLD (2024/2853) modernizes strict product liability to cover software and AI and contemplates post-sale changes like model updates—critical where an AI agent in a BAO is iteratively improved. These rules raise platform and vendor exposure even when member shields exist.

4) MiCA binds the rails: For AI-BAOs that issue tokens or rely on EU-facing CASPs, MiCA's phased application standardizes issuer and service-provider duties, indirectly

shaping governance (e.g., custody, market abuse constraints) for on-chain actions triggered by AI agents.

5) AI-specific governance must be embedded: Because liability follows foreseeability and control, operational controls (model documentation, dataset provenance, pre-deployment testing, human-in-the-loop approvals for high-risk actions, fallback/kill switches, audit logging, prompt/library whitelisting, and incident response runbooks) are decisive in showing due care under negligence and regulatory standards.

DISCUSSION

Functional allocation beats labels

An AI-BAO may call itself "decentralized," yet if a multisig, core team, or foundation configures or meaningfully controls the AI agent (e.g., model weights, policies, or guardrails), those actors look like **providers** or **deployers** for AI Act purposes and like **controllers/maintainers** for tort and consumer law. Entity shields protect members, **not** careless or deceptive practices by controllers or service providers.

Pathways to reduce liability without stifling autonomy:

- **Adopt an entity wrapper** (DAO LLC/LLD/BBLLC or equivalent) and keep formalities **current** (registered agent, annual reports, disclosures).
- **Role clarity by design:** In bylaws and interface docs, identify **AI provider/deployer/maintainer** roles, allocate duties (testing, monitoring, rollback authority), and document **approval chains** for high-impact actions.
- **AI assurance dossiers:** Maintain a living evidence pack: data lineage, model cards, evaluation reports, red-team findings, oracle dependencies, and change logs (to address PLD burdens of proof and AI Act conformity).
- **User-facing transparency:** Risk disclosures to token-holders and end-users; clear terms for recourse, indemnity, and dispute resolution (with jurisdiction/venue clauses mindful of **private international law** uncertainty).
- **Fallbacks and human overrides:** For actions with physical or large financial externalities, require M-of-N human sign-offs or circuit-breakers; log decisions immutably.
- **Insurance and reserves:** Consider D&O-style covers adapted to DAO managers, incident contingency funds, and bug bounty programs.

CONCLUSION

AI-blockchain-enabled autonomous organizations represent a compelling organizational frontier where code, incentives, and machine intelligence converge. The law is catching up—not by creating a vacuum, but by extending familiar doctrines and enacting targeted regimes. The EU AI Act and new PLD set a comprehensive compliance baseline for AI and software; MiCA harmonizes crypto rails. U.S. courts, meanwhile, have shown they will pierce decentralization rhetoric and treat unwrapped DAOs as general partnerships—and regulators can obtain judgments against the DAO itself. Entity statutes (Wyoming, Tennessee, Utah, Vermont, Marshall Islands) meaningfully lower member exposure when used correctly, but they do not immunize providers, deployers, or maintainers of AI-driven systems from liability for defects, misrepresentations, unfair practices, or negligence.

For AI-BAOs, liability follows function and foreseeability: those who design, train, deploy, or materially control AI oracles and smart contracts must own commensurate duties of care. The

practical path forward is neither to abandon autonomy nor to pretend law doesn't apply, but to engineer liability-aware governance—formal wrappers, role-based obligations, auditable AI assurance, and human-in-the-loop controls—so that innovation and accountability can co-exist.

REFERENCES

- ***Regulation (EU) 2024/1689.*** *Artificial Intelligence Act. Official Journal of the European Union (12 July 2024).*
- *European Commission. (2024, August 1). AI Act enters into force.*
- ***Directive (EU) 2024/2853.*** *On liability for defective products (recast Product Liability Directive). Official Journal of the European Union (23 October 2024).*
- *European Commission. (2024). Liability for defective products (PLD overview).*
- *European Securities and Markets Authority (ESMA). (2023–2025). Markets in Crypto-Assets (MiCA) implementation materials.*
- *Commission de Surveillance du Secteur Financier (CSSF). (2024). MiCAR: Entry into application timelines.*
- *U.S. Securities and Exchange Commission. (2017). Report of Investigation: The DAO, Exchange Act Release No. 81207.*
- *U.S. Commodity Futures Trading Commission. (2023). Order and Default Judgment: CFTC v. Ooki DAO (N.D. Cal., June 8, 2023).*
- *Hunton Andrews Kurth. (2023, June 20). CFTC wins default judgment against Ooki DAO (case summary).*
- *Sarcuni v. bZx DAO, No. 3:22-cv-00618, 2023 WL 2657633 (S.D. Cal. Mar. 27, 2023) (order on motions to dismiss).*
- *Dechert LLP. (2023, April 11). Federal court holds DAO members can be treated as general partners (client update).*
- *Wyoming Secretary of State. (2024). Decentralized Autonomous Organization Supplement (W.S. §17-31).*
- *K&L Gates. (2022, Aug. 4). Tennessee's limited-liability statute for DAOs.*
- *Utah Code Ann. tit. 48, ch. 5 (2023/2024). Decentralized Autonomous Organizations Act (LLD).*
- *Republic of the Marshall Islands. (2023). Decentralized Autonomous Organization (Amendment) Act 2023.*
- *Law Commission (England & Wales). (2024, July 11). Decentralised Autonomous Organisations: Scoping Paper.*
- *Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. SSRN.*
- *De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.*
- *Walch, A. (2019). Deconstructing "decentralization": Exploring the core claim of crypto systems. In Regulating Blockchain: Techno-Social and Legal Challenges.*
- *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*