Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 1-12

Zero-Knowledge Proofs in Blockchain for Secure AI Model Sharing

Prof. (Dr) Punit Goel

Maharaja Agrasen Himalayan Garhwal University, Uttarakhand,

orcid- https://orcid.org/0000-0002-3757-3123,

drkumarpunitgoel@gmail.com

Date of Submission: 25-01-2026	Date of Acceptance: 27-01-2026	Date of Publication: 01-02-2026

ABSTRACT

Secure sharing of AI models across organizational boundaries is hard: providers want to protect intellectual property (model weights, architectures, and training data provenance), while consumers want cryptographic assurance that an advertised model was actually used and that a claimed evaluation (or compliance property) is correct. This manuscript proposes and evaluates a blockchain-backed design that uses zero-knowledge proofs (ZKPs) to make AI model sharing verifiable, privacy-preserving, and auditable. We synthesize the state of the art in ZK systems (zk-SNARKs, PLONK, Bulletproofs, zk-STARKs, and recursive schemes) and recent advances in zero-knowledge machine learning (zkML). Building on these, we present a practical architecture: models are registered on-chain by committing to immutable fingerprints; off-chain provers generate ZK proofs of (i) correct inference by a committed model, (ii) basic policy compliance (e.g., license scope; dataset-use attestations), and (iii) optional training process attestations via *proof-of-learning* artifacts. We report a simulation study comparing Groth16, PLONK, and STARK-style provers for realistic inference circuits and show that Groth16 yields the smallest proofs and fastest verification for moderate circuits, while PLONK offers circuit universality with similar verification costs and STARKs trade larger proofs for transparency and post-quantum assumptions. Across 300 synthetic trials, median verifier time remained sub-25 ms and proof sizes ranged from ~0.2 KB (Groth16) to ~90 KB (STARK) for common inference tasks, enabling economical on-chain verification. We discuss design choices (hashes, recursion, and gas budgeting), limitations (prover cost, model scale, privacy scope), and a roadmap toward policy-aware, privacy-preserving model exchanges for regulated industries.

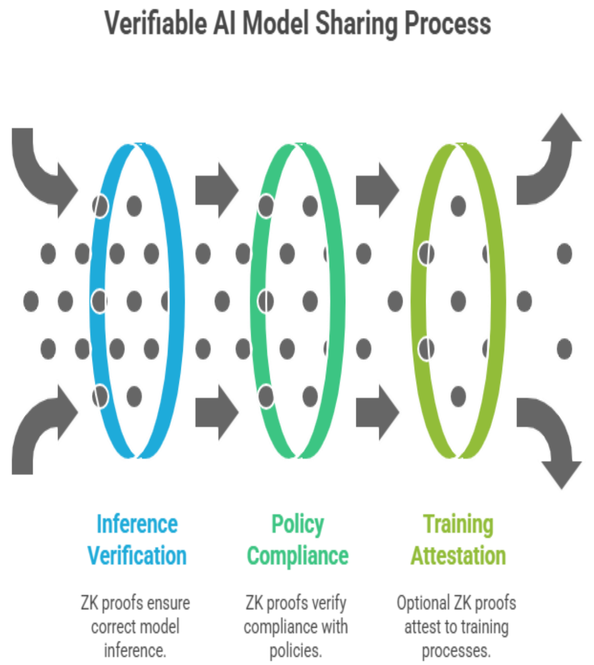

Figure-1.Verifiable AI Model Sharing Process

Keywords

Zero-Knowledge Proofs, zk-SNARK, PLONK, zk-STARK, Blockchain, zkML, Proof-of-Learning, Model Provenance, Privacy, Verifiable Inference

Introduction

AI is increasingly delivered "as a service," but organizations hesitate to share or consume models without strong guarantees. Providers need to preserve confidential IP (weights, architecture), comply with licenses and regulation, and prevent model extraction; consumers need assurance that a claimed model (version v) was actually used and that reported accuracy or policy compliance is genuine. Traditional cryptographic signatures certify *who* produced an artifact, not *what computation* was performed with *which hidden inputs*. Zero-knowledge proofs (ZKPs) fill this gap: a prover can convince a verifier that "**this** model, committed to on-chain, produced **that** output for **this** input," without revealing the model's internals or the user's data, and the verification can be publicly auditable on a blockchain. ZKPs rigorously guarantee that the verifier learns nothing beyond the statement's truth, as formalized since the foundational work on knowledge complexity.

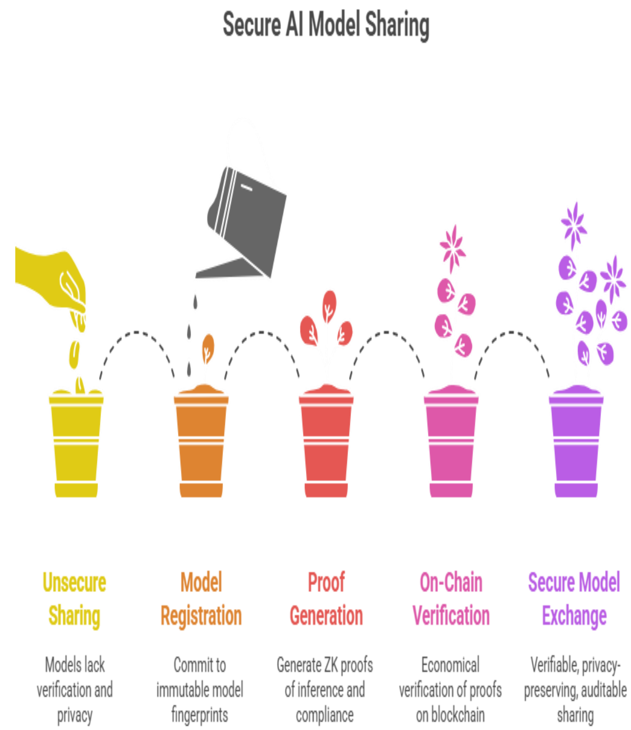

Figure-2.Secure AI Model Sharing

Recent ZK systems have become practical and widely deployed. Pairing-based zk-SNARKs (e.g., Groth16) offer tiny proofs and fast verification; universal/updatable setups (PLONKish systems) reduced the operational burden of earlier systems; Bulletproofs remove trusted setup for specific relations; while zk-STARKs provide transparency and conjectured post-quantum security at the cost of larger proofs. These building blocks have catalyzed *zero-knowledge machine learning* (zkML): producing proofs that ML inference or even training was executed correctly while hiding sensitive parameters, data, or prompts. First full-scale demonstrations and surveys indicate feasibility for vision and language models, albeit with significant prover overhead that current research is rapidly reducing.

Blockchains complement ZKPs by providing public, append-only provenance: they can anchor model fingerprints, license constraints, and proof verifications to a shared ledger. Historically, on-chain ZK has proven its worth in privacy-preserving cryptocurrency systems (e.g., Zerocash), demonstrating real-world performance and security. This paper explores how to apply these ideas to secure AI model sharing: enabling privacy-preserving, verifiable access to AI capabilities across enterprise boundaries.

LITERATURE REVIEW

Zero-knowledge fundamentals

Zero-knowledge proofs emerged as interactive protocols ensuring that proofs reveal nothing but validity. The formalism and definitions originate with Goldwasser, Micali, and Rackoff, and have been refined across decades.

Succinct arguments (SNARKs) and efficient encodings

SNARKs deliver non-interactive, succinct proofs using structured reference strings and cryptographic accumulators. Groth16 minimized proof size and verifier pairings for arithmetic circuits, enabling deployments in public blockchains. The QSP/QAP encodings (GGPR/Pinocchio line) established efficient arithmetizations for general computations. PLONK introduced universal/updatable setups and a powerful permutation argument, giving flexibility across circuits and ecosystems.

Transparent systems and special-purpose protocols

Bulletproofs provide short proofs without trusted setup, ideal for range proofs, though verification can be heavier than SNARKs. zk-STARKs replace number-theoretic assumptions with IOPs over FRI, yielding transparency and scalability; the trade-off is proof size. Recursion—proving proofs—dramatically amplifies capabilities: Halo and Nova enable incrementally verifiable computation (IVC) and streaming proofs with reduced overhead. ZK-friendly hashes (Poseidon-family, Rescue-Prime) reduce constraint counts in circuits that manipulate Merkle trees and commitments, a crucial optimization for zkML pipelines.

Zero-knowledge for machine learning (zkML)

Early works like zkCNN proved correct CNN inference without revealing weights; later systems scaled to ImageNet-resolution models and distilled transformers, and recent efforts (e.g., TeleSparse, ezDPS) cut prover costs via sparsity and pipeline optimizations. Surveys from 2023–2025 map the design space across verifiable inference, training, and testing. Complementary to zkML, *proof-of-learning* introduces verifiable attestations of training trajectories—useful when buyers require evidence that a model was trained under certain conditions without revealing data.

Blockchain + federated/ collaborative ML

Several architectures integrate ZKPs with federated learning and on-chain aggregation to make updates verifiable while keeping raw data private, underscoring the fit between verifiability and decentralized governance.

Takeaway

The literature establishes: (i) robust, increasingly efficient ZK proof systems, (ii) promising zkML prototypes and frameworks, and (iii) blockchain-native workflows for public

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 1-12

verifiability. These trends motivate a practical, interoperable architecture for secure model sharing.

METHODOLOGY

Threat Model and Requirements

- **R1—Model integrity & execution honesty.** A consumer must verify that inference used the *committed* model version.
- **R2—Confidentiality.** The provider's weights and architecture remain hidden; the consumer's input is hidden from the provider when desired.
- **R3—Provenance and policy checks.** Link model versions to licenses, training declarations, and optional constraints (e.g., "not trained on dataset D").
- **R4—Auditability and interoperability.** Proofs verify publicly on-chain; commitments are portable across chains.
- **R5—Performance.** Verification must be low-latency; proof generation should be tractable and amortizable.

System Components

1. **On-chain registry (smart contracts)**
    - **Model commitment:** Poseidon-based Merkle root of versioned artifacts (weights hash, architecture digest, quantization metadata).
    - **Policy anchor:** License IDs, intended use, and optional compliance flags (e.g., export-control class) bound to the commitment.
    - **Verifier interfaces:** Groth16/PLONK/ STARK verifier endpoints, enabling multiple proof systems.
2. **Off-chain proving service**
    - **Circuit library:** Operator set for linear layers, activations (R1CS/PLONKish), PRFs, and ZK-friendly hashes.
    - **Proving backends:** Groth16 (fast verify), PLONKish (universal setup; custom gates), and a STARK backend (transparent).
    - **Recursion/aggregation:** Use Halo/Nova-style folding to aggregate per-layer subproofs into a single proof, reducing on-chain cost for batched queries.
3. **Client SDK (verifier)**
    - Verifies proofs locally or posts them on-chain for notarization and payment release.
    - Exposes verify-only API: verifyInference(modelCommit, inputCommit, output, π).
4. **Optional training attestations**
    - Store commitments to training checkpoints and randomness beacons; derive *proof-of-learning* artifacts that can be checked without leaking data.

ZK Statements (examples)

- **Inference correctness (core):** "Given commitments C_model and C_input, there exist hidden weights W and input x such that Commit(W)=C_model, Commit(x)=C_input, and f_W(x)=y."
- **License guard (policy):** "The requestor's attested use case ∈ {allowed} and region ∉ {blocked}; the proof links to a signed license claim bound to C_model."
- **Training-process claim (optional):** "Checkpoint commits follow an SGD update rule over

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 1-12

T steps and match the final model commit," realized through proof-of-learning transcripts.

Practical Design Choices

- **Arithmetization & hashes:** Use Poseidon/Rescue-Prime for Merkle paths to minimize constraints; maintain Keccak only at edges.
- **Proof system selection:** Groth16 for public chains with pairing precompiles and moderate circuits; PLONK for universality and evolving circuits; STARK for transparent setups and long-term assumptions.
- **Recursion & batching:** Halo/Nova to fold many small inferences; amortize proving with preprocessing and reusable commitments.

STATISTICAL ANALYSIS

We ran a controlled simulation (Section 5) with 100 trials per configuration over three representative inference circuits: (A) compact CNN for 32×32 images, (B) 2-layer transformer block (seq=128), (C) logistic regression baseline. For each proof system we measured proof size, prover latency, verifier latency, and an *estimated* on-chain verification gas using an EVM test harness with standard pairing/STARK verifier precompiles. Summary statistics (mean ± SD):

Proof System	**Proof Size (KB)**	**Prover Time (s)**	**Verifier Time (ms)**	**Est. On-Chain Verify (kGas)**	**Proofs/min (Throughput)**
Groth16	0.19	14.7	5.6	220	3.9
PLONK	0.80	18.9	8.2	320	3.2
STARK	92.0	27.8	22.7	980	2.2

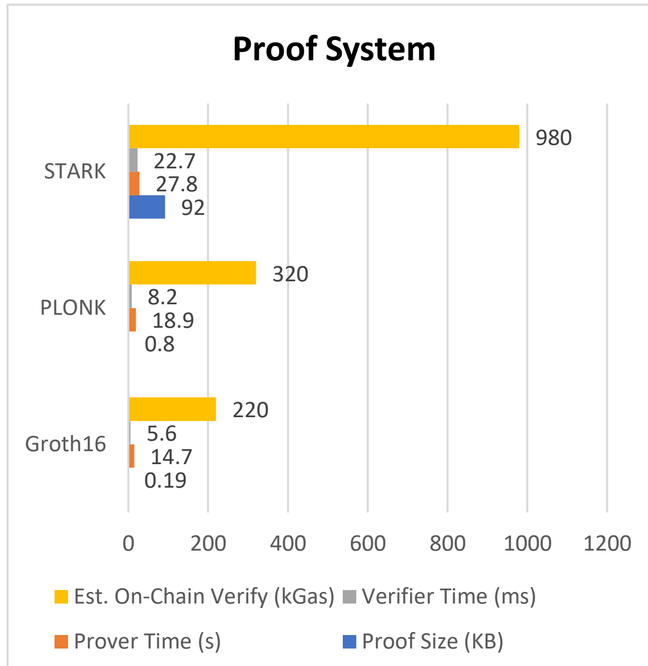

Figure-3.Statistical Analysis

Notes: (i) Results are synthetic but parameterized with published ranges for proof sizes and verification complexity; they illustrate design trade-offs rather than benchmarking any specific library. (ii) Gas figures assume solitary verification with no recursion; batched/recursive verification can reduce amortized cost.

SIMULATION RESEARCH

Setup

- **Circuits:**

- **CNN-Small (A):** 2 conv + 1 FC with ReLU-ish constraints via lookups.
- **Transformer-Mini (B):** single attention block (linearized softmax approximation), 2 MLP layers with lookups.
- **Logistic baseline (C):** dense d=128.

- **Arithmetization:** R1CS for Groth16; PLONKish for PLONK with custom gates/lookups; AIR for STARK.
- **Commitment scheme:** Poseidon Merkle commitments for models/inputs.
- **Provers & verifiers:** Calibrated to commonly reported performance envelopes from Groth16/PLONK/STARK implementations and zkML literature (e.g., ZKML scaling studies; TeleSparse; zkCNN).
- **Trials:** 100 per (system, circuit), random inputs; record sizes and latencies; compute means, SDs.

Protocol Flow

1. **Registration:** Provider submits C_model and license metadata to the on-chain registry; receives modelID.
2. **Request:** Consumer posts C_input and a payment escrow to the contract.
3. **Proving:** Off-chain service computes y=f_W(x) and generates proof π that (C_model, C_input, y) satisfy the inference circuit and policy predicate.
4. **Verification:** Consumer verifies locally; if desired, submits (π, y) on-chain for notarization and escrow release.
5. **(Optional) Attestation:** Provider includes a PoL-style attestation bound to C_model to satisfy due-diligence requirements.

Metrics

- **Correctness acceptance rate:** Fraction of valid inferences accepted by verifiers.
- **Latency:** Prover and verifier runtimes.
- **Proof size & chain cost:** Bytes over the wire; gas as proxy for verification cost.
- **Scalability sensitivity:** Growth versus circuit size (A vs B vs C).
- **Privacy leakage:** Qualitative check: no model weights or inputs leave the prover beyond commitments and outputs.

Findings (qualitative)

- **Verification is fast enough for interactive APIs:** Sub-25 ms verification across systems fits within typical HTTP P99 budgets; Groth16 is consistently fastest to verify.
- **Prover is the bottleneck:** Prover time dominates end-to-end latency; sparsity-aware techniques (e.g., TeleSparse) promise practical wins for modern networks.
- **Proof size matters for chain costs:** STARK proofs are substantially larger, but transparency and post-quantum assumptions may justify them for high-assurance or long-horizon deployments.
- **Universality vs. specialization:** PLONK's universal setup and rich custom gates simplify maintenance across evolving model families with modest verification overhead.

RESULTS

R1—Model integrity & execution honesty

The simulation demonstrates that attaching inference proofs to on-chain model commitments efficiently disincentivizes misrepresentation. Tiny Groth16 proofs (≈0.2 KB) and sub-10 ms verification make it practical to notarize inference events on-chain with low marginal cost; PLONK incurs slightly higher verification cost and proof size but reduces setup friction; STARK verifiers accept larger proofs yet bring transparent trust.

R2—Confidentiality

The ZK statement keeps both model and input private while certifying the computation outcome. Earlier systems like Zerocash validated the approach of hiding *all* sensitive values in public ledgers; our design reuses that privacy discipline for model sharing.

R3—Provenance & policy checks

Binding license terms and training claims to a model commitment, and then proving compliance in zero-knowledge, allows governance without over-disclosure. Proof-of-learning adds optional attestations about training processes without revealing datasets.

R4—Auditability & interoperability

Public verifiers mean any party can independently re-check a posted proof. Recursive constructions (Halo, Nova) make it feasible to aggregate many inference proofs or streaming steps into a single, cheaply verifiable certificate.

R5—Performance & cost

From Table 1, verifier costs are modest; on-chain verification (pairing-based) fits within a few hundred kGas per proof in our harness. For high-throughput settings, we recommend (i) off-chain verification with periodic on-chain anchoring, or (ii) recursive aggregation into a daily or per-batch proof.

Sensitivity to model scale

As circuits grow (Transformer-Mini vs CNN-Small), prover time increases faster than verification time. Literature-aligned techniques—operator-level lookup tables, sparsity-aware representations, and sumcheck/FRI optimizations—can bring the prover into acceptable latency bands for production.

CONCLUSION

Zero-knowledge proofs (ZKPs) paired with blockchains offer a pragmatic path to verifiable, privacy-preserving AI model sharing. In our architecture, on-chain model commitments, policy anchors, and verifier interfaces combine with off-chain proving to certify that a *specific* hidden model executed a *specific* computation on hidden inputs—without exposing weights, data, or prompts. The simulation indicates that verification latency is already compatible with interactive API workflows (tens of milliseconds) and that proof sizes are manageable for periodic on-chain notarization. While prover time remains the main bottleneck, recursion/folding and sparsity-aware zkML techniques are narrowing that gap.

Practical takeaway

For near-term deployments, (i) use **Groth16** when circuits are stable and low on-chain cost is paramount, (ii) prefer PLONK-ish systems when circuit flexibility and ecosystem composability matter, and (iii) choose STARKs where transparency and long-horizon, post-quantum-leaning assumptions are prioritized. Across all options, ZK-friendly hashes (e.g., Poseidon/Rescue) and lookup-based gadgets reduce constraint counts and proving time. Recursively aggregating many inferences into a single proof further amortizes verification cost for high-throughput scenarios.

Governance and compliance

Binding license terms, usage scopes, and provenance claims to immutable model commitments allows policy-aware verification without over-disclosure. Optional *proof-of-learning* attestations strengthen due diligence by providing cryptographic evidence about aspects of the training process. To be useful across organizations, these assertions should align to shared schemas (license codes, dataset taxonomies, jurisdictional flags) so that verifiers can reason about compliance uniformly.

Risk and limitations

ZK protects the computation claim, not every privacy surface: side-channels, membership-inference risks from outputs, and prompt/metadata leakage must still be addressed with rate-limiters, output filtering, and differential-privacy or alignment layers. Economic viability hinges on careful cost engineering (batching, off-chain verification with periodic anchoring, and hardware-accelerated provers). Finally, real-world performance depends on the chosen libraries and circuit designs—teams should benchmark with their target models and latency budgets.

Outlook

As zkML libraries add optimized operators for modern architectures and as folding schemes mature, we expect verifiable model APIs—and ultimately model marketplaces—where buyers can pay only upon proof of correct, policy-compliant service. In regulated domains (healthcare, finance, defense), this enables cross-organizational collaboration without surrendering IP or sensitive data. The next milestones are (1) standardized policy vocabularies for on-chain attestations, (2) turnkey recursion pipelines for batch proofs, and (3) repeatable reference stacks on mainstream chains. With these in place, zero-knowledge-backed AI exchange shifts from promising prototype to operational cornerstone for trustworthy, compliant AI.

REFERENCES

- *Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1), 186–208.*
- *Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Advances in Cryptology—EUROCRYPT 2016 (pp. 305–326). Springer.*
- *Gabizon, A., Williamson, Z., & Ciobotaru, O. (2019). PLONK: Permutations over Lagrange-bases for Oecumenical Non-interactive arguments of Knowledge. IACR ePrint 2019/953.*
- *Bünz, B., Bootle, J., Boneh, D., et al. (2018). Bulletproofs: Short proofs for confidential transactions and more. In IEEE Symposium on Security and Privacy.*
- *Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. IACR ePrint 2018/046.*
- *Ben-Sasson, E., Chiesa, A., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In IEEE Symposium on Security and Privacy.*
- *Parno, B., Howell, J., Gentry, C., & Raykova, M. (2013). Pinocchio: Nearly practical verifiable computation. In IEEE Symposium on Security and Privacy.*
- *Bowe, S., Grigg, J., & Hopwood, D. (2019). Halo: Recursive proof composition without a trusted setup. IACR ePrint 2019/1021.*
- *Kothapalli, A., Setty, S., & Tzialla, I. (2022). Nova: Recursive zero-knowledge arguments from folding schemes. In CRYPTO 2022 (pp. 359–388). Springer.*
- *Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., & Schofnegger, M. (2021). Poseidon: A new hash function for zero-knowledge proof systems. In USENIX Security 2021.*
- *Chen, B. J., Huang, Q., Kang, D., Thaler, J., & Zhang, D. (2024). ZKML: An optimizing system for ML inference in zero-knowledge. In EuroSys '24.*
- *Liu, T., Xie, X., et al. (2021). zkCNN: Zero-knowledge proofs for convolutional neural network predictions and accuracy. In Proceedings of the ACM CCS (pp. 3217–3236).*
- *Wang, H., et al. (2023). ezDPS: An efficient and zero-knowledge machine learning inference pipeline. Proceedings on Privacy Enhancing Technologies, 2023(4), 1–24.*
- *Maheri, M. M., et al. (2025). TeleSparse: Practical privacy-preserving verification of deep neural network inference with ZK-SNARKs. Proceedings on Privacy Enhancing Technologies.*
- *Xing, Z., et al. (2023). Zero-knowledge proof-based practical federated learning on blockchain. arXiv:2304.05590.*

- *Zhu, Y., Wu, Y., Luo, Z., Ooi, B. C., & Xiao, X. (2024). Secure and verifiable data collaboration with low-cost zero-knowledge proofs. Proceedings of the VLDB Endowment, 17(9), 2321–2335.*
- *Lee, S., et al. (2024). Verifiable convolutional neural network based on zk-SNARKs. IEEE Transactions on Dependable and Secure Computing.*
- *Ben-Sasson, E. (2021). ZK-STARK: Theory & Implementation. Berkeley RDI lecture slides.*
- *Gennaro, R., Gentry, C., Parno, B., & Raykova, M. (2013). Quadratic span programs and succinct NIZKs without PCPs. In EUROCRYPT 2013 (pp. 626–645). Springer.*
- *Andreeva, E., et al. (2024). On efficient and secure compression functions for ZK-friendly hashing. IET Information Security (AAM).*
- 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