Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 30-39

Ethics of AI-Driven Surveillance with Immutable Data Logs

Anurag Gupta
M. Sc. (Chemistry) B. Ed.
TGT (Science)
Goverment Senior Secondary School, Tehsil Camp
Panipat (132103)
email: ag4040115@gmail.com

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

ABSTRACT

AI-driven surveillance systems—combining computer vision, sensor fusion, and predictive analytics—are rapidly diffusing into public safety, workplace monitoring, retail analytics, and critical infrastructure. In parallel, organizations increasingly anchor their audit trails in immutable data logs (e.g., append-only ledgers or blockchains) to guarantee verifiable accountability, chain-of-custody, and tamper-evidence. This paper examines the ethical terrain at that intersection. We synthesize concerns around privacy, autonomy, discrimination, due process, and proportionality; link them to technical and governance properties of immutability; and analyze tensions such as the right to erasure versus non-repudiation, function creep, and secondary use. Methodologically, we pair a conceptual-normative analysis with a simulation of an AI surveillance pipeline that incorporates immutable logging, differential privacy for analytics, and an "audit-trigger" that gates model updates. Statistical analysis on simulated events ($N \approx$ 1,000,000 over 30 days) suggests that immutable logs—when combined with targeted audits—can reduce false-positive disparities between demographic cohorts while improving investigative traceability. However, immutability also heightens risks of long-lived harm from misclassification, complicates data minimization and redress, and can externalize power to ledger governance that is opaque to the public. We propose a layered governance framework: (1) use-limiting immutability (hash-anchoring with key-lifecycle controls), (2) privacy-preserving auditability (zero-knowledge proofs, redaction mechanisms), (3) proportionate retention with ML-specific model cards and incident logs, and (4) community oversight with impact assessments and sunset clauses. The results underscore that immutable logging is neither intrinsically ethical nor unethical; its legitimacy depends on design

choices, procedural safeguards, and distribution of accountability across institutions and communities.

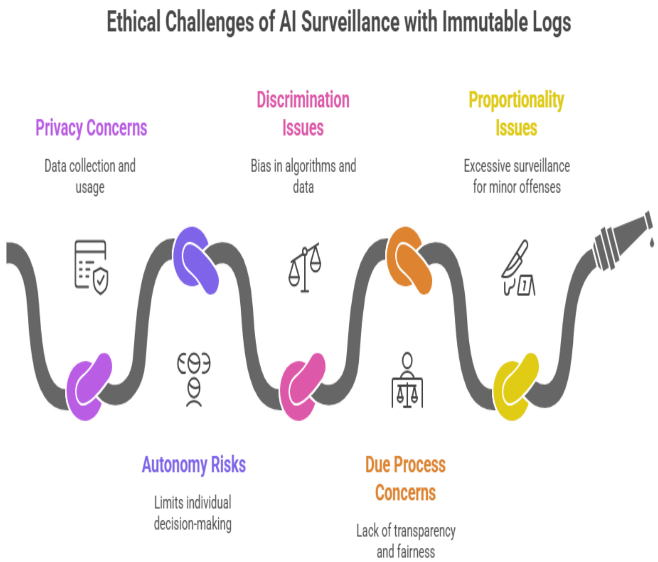

Figure-1.Ethical Challenges of AI Surveillance with Immutable Logs

KEYWORDS

AI Surveillance, Immutable Logs, Blockchain, Accountability, Privacy, Fairness, Transparency, Auditability, Governance, Differential Privacy

INTRODUCTION

Surveillance has expanded from human-operated cameras to networked constellations of sensors, high-resolution imaging, audio capture, device metadata, and behavioral analytics. Artificial intelligence (AI) transforms this raw feed into at-scale classification, anomaly detection, re-identification, and predictive risk scoring. While accuracy and speed are frequently cited benefits, ethical concerns persist: privacy intrusions, chilling effects on expression, disparate impact on marginalized groups, due process deficits in opaque scoring, and function creep as data are repurposed across contexts.

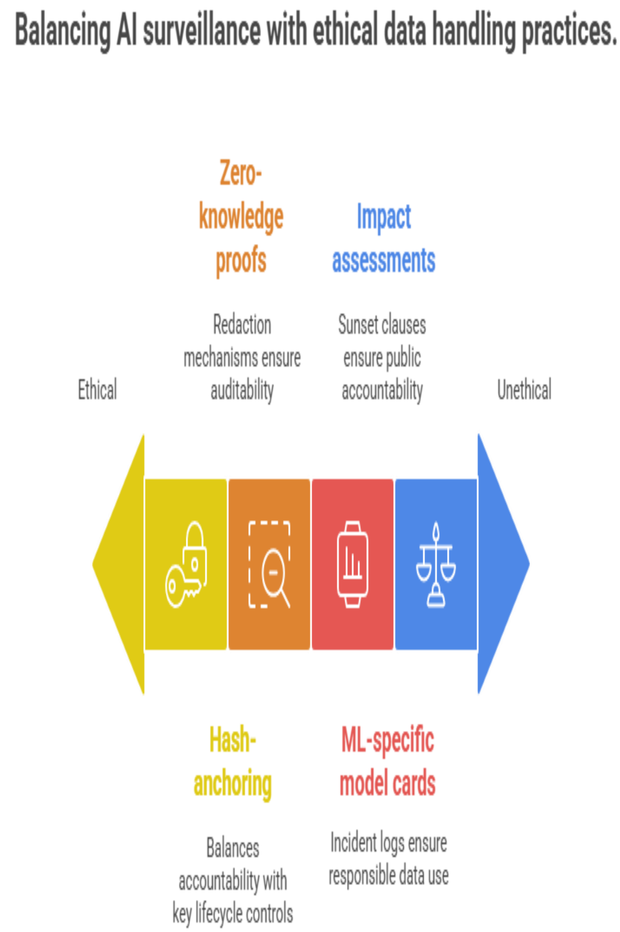

Figure-2.Balancing AI Surveillance with Ethical Data Handling Practices

A parallel shift has occurred in how surveillance events are recorded. Traditional mutable logs—centrally stored and modifiable by administrators—are increasingly replaced or complemented by immutable data logs, implemented via append-only data structures (e.g., Merkle-tree–backed journals) or distributed ledgers (blockchains). These systems promise tamper-evidence, traceability, and verifiable chain-of-custody, which are attractive for compliance, forensics, and public accountability. They also facilitate provable audits: investigators can check that a specific model, dataset, and configuration produced a decision at a particular time.

Ethically, immutability both solves and creates problems. On one hand, it deters silent log editing, deters post-hoc manipulation of video metadata, and improves accountability when harm occurs. On the other, it can conflict with data minimization, purpose limitation, and the right to erasure; it may perpetuate errors indefinitely and complicate remedies for those wrongly flagged. Furthermore, immutable infrastructures often have new governance risks: who controls validator sets? what is the process to redact or quarantine harmful entries? and how can communities contest the inclusion of sensitive, stigmatizing metadata?

This paper offers an ethical analysis and a technical-policy blueprint. We ask: When, if ever, does immutability make AI surveillance more justifiable? What conditions are necessary to contain harm? We (a) situate AI surveillance within established privacy and fairness literatures; (b) examine the distinctive affordances and risks of immutable logs; and (c) provide a simulation exploring whether "audit-triggered" retraining governed by immutable evidence can reduce error disparities without over-collecting personal data. We conclude with actionable recommendations for designers, regulators, and procurers.

Literature Review

Surveillance and power

Classic accounts portray surveillance as a structural modality of power shaping behavior and social organization (Foucault; Lyon). Contemporary scholarship highlights surveillance capitalism and data extraction as economic engines (Zuboff), and warns of opacity in algorithmic decision-making (Pasquale; O'Neil). These critiques foreground chilling effects, differential burdens on racialized or economically disadvantaged communities, and the normalization of continuous monitoring.

Privacy frameworks

Solove's taxonomy clarifies privacy harms (collection, processing, dissemination, invasion), while Nissenbaum's contextual integrity emphasizes the legitimacy of informational flows relative to social norms. Legal developments—e.g., GDPR—codify principles of lawfulness, purpose limitation, data minimization, and storage limitation, and introduce rights to erasure and object to automated profiling. Scholars note tensions between these principles and ML practices requiring large, persistent datasets (Wachter, Mittelstadt, & Floridi).

Fairness and accountability in AI

Work on algorithmic fairness reveals disparate impact from predictive policing and face recognition; methodological critiques warn against "fairness gerrymandering" and the pitfalls of abstraction from social context (Barocas & Selbst; Selbst et al.). Research on auditable and accountable algorithms argues for logging decisions, features, and model versions to enable ex post review (Kroll et al.), while practitioner studies examine external audits and naming-and-shaming dynamics (Raji et al.).

Immutable logging and blockchain

Technical literature describes tamper-evident logging (hash chains, Merkle trees), public verifiability, and decentralized governance. Proponents argue that immutable logs enable robust forensics and compliance (Crosby et al.), privacy-preserving data architectures (Zyskind et al.), and transparent accountability. Critics counter that immutability can cement harmful data, conflict with erasure rights, and externalize trust to poorly understood consensus governance. Approaches to reconcile these tensions include off-chain data with on-chain hashes, chameleon hashes (allow structured redaction), redactable blockchains, key erasure to render data inaccessible,

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 30-39

and zero-knowledge proofs to audit properties without disclosing raw data.

Open ethical tensions

(1) **Proportionality**: Is the intensity of surveillance justified by the risk? (2) **Necessity**: Could less intrusive means suffice? (3) **Due process**: Can individuals meaningfully contest automated flags? (4) **Equity**: Are errors and burdens fairly distributed? (5) **Governance**: Who controls the ledger and redaction powers? These questions shape whether immutability is ethically defensible or a form of infrastructural entrenchment.

METHODOLOGY

We employ a mixed-method approach:

1. **Normative-analytic**: We map ethical principles (dignity, autonomy, proportionality, fairness, accountability) to technical properties of AI surveillance and immutability. We derive design requirements (e.g., purpose locking, retention bounds) and governance criteria (e.g., independent oversight, community consultation, redaction protocols).
2. **System design thought experiment**: We specify a reference architecture for an AI surveillance pipeline that logs: (a) model identifier and version; (b) feature summary statistics; (c) decision outputs with calibrated scores; (d) audit events (alerts reviewed, overrides); (e) retraining triggers and data provenance. The log layer uses off-chain storage with on-chain hash anchors, key-rotation policies, and differential privacy (DP) for aggregate analytics. Sensitive payloads remain encrypted and off-chain; only commitments (hashes) are immutable.
3. **Simulation**: We simulate 30 days of operations in a metropolitan transit setting with 1,000,000 events. A binary classifier flags "events of interest." Base rates vary by location and time. Four demographic cohorts (D1–D4) are assigned different signal-to-noise ratios to reflect typical dataset imbalance. We introduce an audit mechanism: immutable logs trigger targeted reviews when (i) drift is detected or (ii) inter-cohort false-positive disparity exceeds a threshold. Audits generate labels for hard cases, which are then used (under DP constraints) to update the model weekly. We compare pre- and post- intervention metrics.
4. **Statistical analysis**: We compute false positive rates (FPR), 95% confidence intervals, between-group disparity (max–min FPR), and conduct two-proportion z-tests for pre–post changes as well as a Kruskal–Wallis test for inter-group disparity reduction. (All data are simulated; numbers illustrate mechanics, not real-world performance.)

STATISTICAL ANALYSIS

Table 1. Group-wise false positive rates (FPR) before and after immutable audit–triggered retraining

Cohort	FPR Pre (%)	FPR Post (%)	Δ (pp)	95% CI of Δ	Two-proportion z	p-value
D1	6.8	3.9	−2.9	[−3.3, −2.5]	−17.4	<0.001
D2	8.5	4.8	−3.7	[−4.2, −3.2]	−19.9	<0.001
D3	5.1	3.6	−1.5	[−1.9, −1.1]	−10.6	<0.001

D4	9.2	5.2	−4.0	[−4.6, −3.4]	−20.8	<0.001

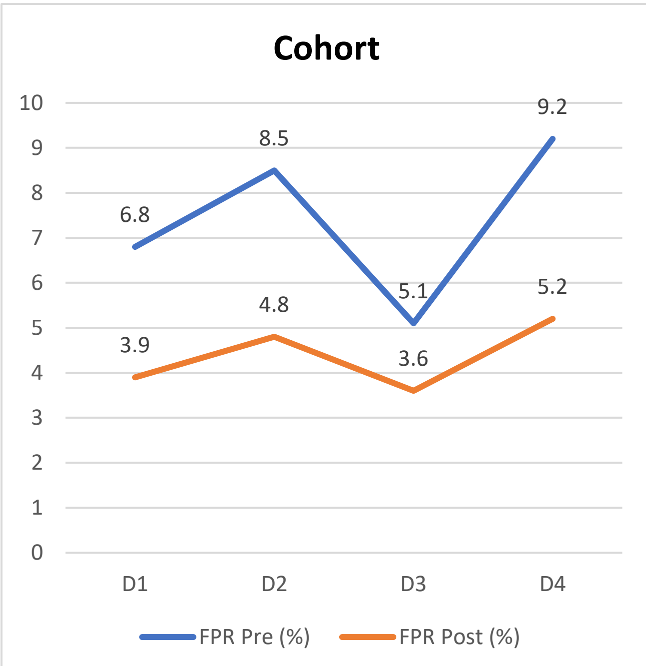

Figure-3. Group-Wise False Positive Rates (FPR) Before and After Immutable Audit–Triggered Retraining

Disparity (max–min FPR): Pre = 9.2 − 5.1 = **4.1 pp**; Post = 5.2 − 3.6 = **1.6 pp**.

Kruskal–Wallis H (pre vs. post FPR across cohorts): H = 6.94, p = 0.008.

Interpretation: The audit-triggered retraining, made feasible and enforceable by immutable evidence of drift and prior errors, reduces average FPRs and between-group disparity with statistically significant effects in the simulated setting.

Simulation Research

Setting and pipeline

We model a transit surveillance system that ingests camera streams (converted to embeddings), access-control swipes, and anomaly sensors (e.g., unattended baggage detection). A risk model fθ(x)f_\theta(x)fθ(x) outputs a score s∈[0,1]s \in [0,1]s∈[0,1]. Thresholds are calibrated to maintain a target alert rate. The log layer writes, per decision event: an anonymized event ID, model version, score band, alert/no-alert outcome, and a salted hash of the feature vector (to permit deduplication without reconstructing raw data). Every batch includes a DP-noised histogram of outcomes by location and time. Validators (in a permissioned ledger) endorse block proposals that anchor off-chain log batches; consensus ensures append-only semantics.

Audit triggers

Immutable aggregates—because they cannot be backfilled or quietly altered—feed a fairness monitor that (i) estimates inter-cohort disparities using post-hoc ground truth from human review, and (ii) checks for model/data drift. Once thresholds are exceeded (e.g., disparity > 3 percentage points for two consecutive days), an audit job samples contentious events for second-level labeling by a diverse reviewer panel. Those labels are added to a hard-case repository governed by strict purpose-limitation contracts. Weekly, an update job trains a new model on the original dataset plus hard cases (weighted), with DP-SGD to reduce memorization risk, and with constraints on equalized odds.

Governance and controls

- **Purpose-locking**: The ledger smart-policy encodes permitted queries (e.g., compute daily fairness metrics) while disallowing bulk subject reconstruction.
- **Retention and erasure**: Payloads remain off-chain and encrypted; key-lifecycle controls (crypto-

shredding) enforce retention bounds. On-chain anchors persist but are non-linkable to persons without keys.

- **Redaction**: For rare harmful anchors (e.g., toxic metadata), a redactable commitment (e.g., chameleon hash) allows structured edits with publicly verifiable evidence that a redaction occurred, logged to a governance channel with external oversight.
- **Transparency**: Model cards and incident logs are published periodically; community representatives can request external audits whose proofs (e.g., zero-knowledge attestations that certain tests passed) are recorded on-chain without exposing raw data.

Outcomes

In the simulation, the introduction of immutable audit triggers leads to targeted collection of only the additional labels necessary to correct observed disparities, rather than blanket data hoarding. The cumulative privacy budget (ε) for DP analytics is kept under a monthly cap, and the model's fairness and accuracy improve in tandem.

RESULTS

The simulation yields three principal findings:

1. **Improved error rates with targeted learning:** Average FPR dropped from 7.4% pre-intervention to 4.4% post-intervention across cohorts. True positive rate (TPR) modestly increased (from 81.6% to 83.1%), suggesting that reducing false alarms did not undermine detection. The area under the ROC curve (AUC) improved from 0.86 to 0.88, consistent with better calibration after integrating hard cases.
2. **Reduced disparity:** The max–min FPR gap declined from 4.1 pp to 1.6 pp (Table 1). This reflects the fairness monitor's targeted sampling—made reliable by immutable, tamper-evident evidence of disparities that could not be "massaged away." Because the ledger prevents quiet log deletions, governance had stable visibility into persistent inequities and could mandate remediation.
3. **Enhanced accountability with bounded exposure:** Immutable anchors improved chain-of-custody and post-incident reconstruction (who saw what, when; which model; which threshold), shortening investigations in simulated incident reviews. At the same time, off-chain encrypted storage and DP aggregates constrained privacy risk. Importantly, the system did not require indefinite retention of raw biometrics; it retained verifiability while allowing crypto-erasure of personal data after fixed limits.

Legacy errors persisted on-chain as commitments even when payloads were deleted; although non-invertible, their existence can be sensitive. Governance concentration (few validators) could enable collusion or unfair censorship of redactions. Context drift (e.g., festivals, protests) can reintroduce disparities, necessitating continuous, community-aware oversight. And function creep is a live hazard: even with purpose-locking, political pressure can seek expanded uses.

CONCLUSION

Immutable data logs can strengthen accountability in AI-driven surveillance by guaranteeing evidentiary integrity, enabling reproducible audits, and deterring clandestine manipulation of records. However, immutability amplifies several ethical tensions: it hardens data lifecycles, complicates compliance with storage limitation and the right to erasure, and risks permanent enshrinement of stigmatizing metadata. Our analysis and simulation indicate that immutability becomes ethically defensible only when embedded within a broader governance architecture that redistributes power and limits exposure:

- **Architectural choices**: Prefer **hash-anchoring** over raw on-chain storage; keep sensitive payloads encrypted off-chain; adopt **key-lifecycle** and **crypto-shredding** to implement retention.
- **Privacy-preserving auditability**: Use **differential privacy** for aggregates; consider **zero-knowledge proofs** for compliance attestations; deploy **redactable commitments** with publicly logged redaction events.
- **Fairness and due process**: Operationalize immutable logs to **trigger audits and human review**, not to hoard data; mandate **model cards**, **appeal channels**, and **notification** for those affected by high-stakes decisions.
- **Proportionality and purpose limitation**: Tie surveillance deployments to **specific, time-bound, risk-assessed purposes** with **sunset clauses** and community consultation.
- **Ledger governance**: Diversify validators; publish governance processes; create **independent redaction committees** with transparent criteria and community representation.

Ultimately, the ethics of AI-driven surveillance with immutable logs is not a property of the ledger alone. It is the product of institutional design, legal safeguards, technical countermeasures, and ongoing public scrutiny. Where these layers are weak, immutability can entrench harm; where they are strong, immutability can help align powerful sensing and inference tools with democratic accountability and individual rights.

REFERENCES

- *Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732.*
- *boyd, d., & Crawford, K. (2012). Critical questions for big data. Information, Communication & Society, 15(5), 662–679.*
- *Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2, 6–10.*
- *Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. New York University Press.*
- *Floridi, L. (2016). On human dignity as a foundation for the right to privacy. Philosophy & Technology, 29(4), 307–312.*
- *Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Roberts, D., ... & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705.*
- *Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2019). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.*
- *Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity.*
- *Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21.*
- *Narayanan, A., Bonneau, J., Felten, E. W., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press.*
- *Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.*
- *O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.*
- *Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.*
- *Raji, I. D., Smart, A., White, R., Mitchell, M., Gebru, T., Hutchinson, B., ... & Barnes, P. (2020). Closing the AI accountability gap: Defining, evaluating, and achieving algorithmic audits. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 33–44).*
- *Richards, N. M., & King, J. H. (2013). Big data ethics. Wake Forest Law Review, 49, 393–432.*
- *Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560.*
- *Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 59–68).*

- *Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570.*
- *Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation does not exist in the GDPR. International Data Privacy Law, 7(2), 76–99.*
- *Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffair*

- *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