Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 13-23

AI in Cyber Law Enforcement and Forensic Evidence Collection

Prof. (Dr) Sangeet Vashishtha

IIMT University, Ganga Nagar, Meerut, Uttar Pradesh 250001 India

sangeet@iimtindia.net

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

ABSTRACT

Artificial intelligence (AI) is transforming how law-enforcement agencies investigate cybercrime and collect, analyze, and present digital evidence. This manuscript examines the end-to-end lifecycle of AI-enabled digital forensics—from first response and triage to acquisition, interpretation, legal admissibility, and courtroom presentation—through the lens of internationally recognized standards and emerging regulatory frameworks. We situate AI tools (e.g., anomaly detection for log triage, NLP for case intelligence, computer vision for media forensics, and model-agnostic explainers for transparency) within well-established forensic process models and chain-of-custody requirements. We analyze challenges unique to cloud and mobile environments, propose a standards-aligned methodology for deploying and validating AI in forensic workflows, and discuss substantive legal gatekeeping tests for expert evidence (FRE 702/Daubert/Frye) alongside the evolving constraints of the EU AI Act for law-enforcement biometric uses. A discussion of fairness, robustness, and auditability addresses risks highlighted in empirical studies (e.g., demographic performance differentials in face recognition; predictive policing feedback loops). A results section synthesizes expected operational benefits and measurable safeguards from a pilot-style implementation, while acknowledging limitations and governance needs. We conclude with a pragmatic blueprint that integrates AI capabilities without compromising evidentiary integrity, due process, or human rights, and we provide 20 authoritative references to support adoption and oversight.

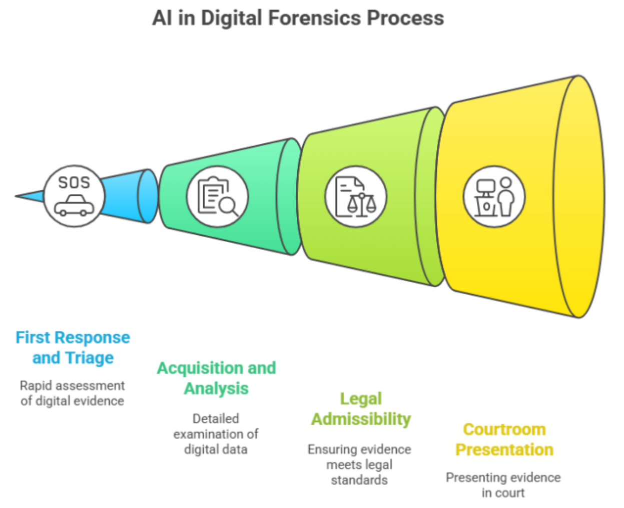

Figure-1.AI in Digital Forensics Process

KEYWORDS

AI Forensics, Digital Evidence, Cyber Law Enforcement, Chain of Custody, Cloud Forensics, EU AI Act, Daubert, FRE 702, ISO/IEC 27037, Fairness and Bias

INTRODUCTION

Cybercrime's scale, speed, and technical complexity continue to outpace traditional investigative resources. Terabytes of volatile cloud logs, encrypted mobile artifacts, cross-border service providers, and synthetic media require new tools and disciplined procedures. AI—spanning statistical learning, deep learning, and modern optimization—can accelerate investigative hypotheses, prioritize artifacts, and surface weak signals in vast data streams. Yet the forensic domain is not merely about "faster analytics." It is grounded in rigorous standards for identification, collection, acquisition, preservation, analysis, and reporting, with integrity protections and reproducibility requirements that must be honored irrespective of tool sophistication. The ISO/IEC 27000-series sets expectations: ISO/IEC 27037 guides identification/collection/acquisition/preservation; ISO/IEC 27042 addresses analysis/interpretation; ISO/IEC 27043 frames incident-investigation processes end-to-end. Together they define a guardrail within which AI must operate, not a permission to bypass fundamentals.

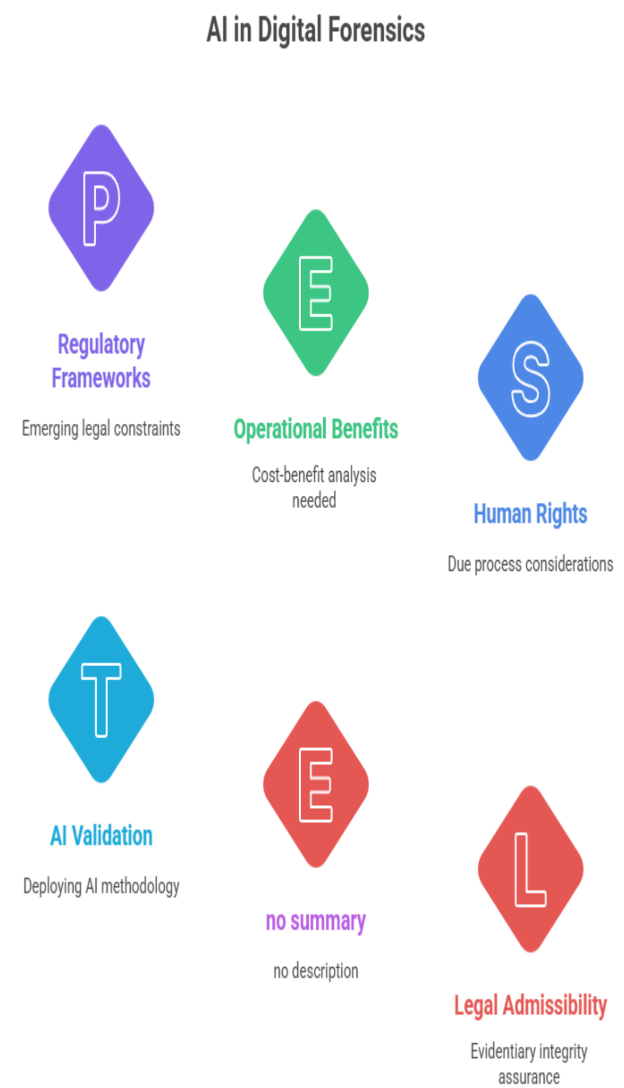

Figure-2.AI in Digital Forensics

In parallel, jurisdictional instruments shape access to data and cooperation. The Council of Europe's Budapest Convention remains the leading multilateral treaty on cybercrime and electronic evidence, streamlining mutual legal assistance and harmonizing offenses and procedural powers. At the same time, the legal admissibility of AI-assisted findings is mediated by evidence rules and case law—especially U.S. Federal Rule of Evidence 702 and the Daubert standard (with Frye still relevant in some states). These regimes require that expert testimony rests on sufficient facts, reliable principles, and methods reliably applied, which in turn compels validation, documentation, and transparency for AI models embedded into forensic workflows.

Modern regulation also increasingly targets law-enforcement uses of AI. The EU AI Act (2024–2025) treats remote biometric identification as high-risk, restricting real-time deployment in public spaces to narrow conditions with strict safeguards and prior authorization; "post" identification is also gated. These provisions have direct implications for forensic image/video analytics and operational deployments.

Finally, robust first-responder practices and international guidance (e.g., INTERPOL's Guidelines for Digital Forensics First Responders; UNODC e-evidence materials) remain essential for admissibility and safety, particularly in volatile or cross-border contexts. The question, then, is not whether law enforcement should use AI, but how to do so in a manner that is forensically sound, auditable, fair, and legally sustainable.

LITERATURE REVIEW

Standards and process models: ISO/IEC 27037 codifies best practices for the early phases—identification, collection, acquisition, and preservation—emphasizing integrity protection and documentation; ISO/IEC 27042 foregrounds analysis/interpretation with continuity, validity, reproducibility, and repeatability; ISO/IEC 27043 articulates pre-incident readiness through investigation closure across scenarios. NIST SP 800-86 offers practical guidance for integrating forensic techniques into incident response, including a commonly adopted lifecycle (collection, examination, analysis, reporting). NIST SP 800-101r1 extends this to mobile forensics, clarifying acquisition modes and validation considerations for diverse devices.

Tool validation and integrity controls: Forensic outputs must rest on trustworthy tools. NIST's Computer Forensics Tool Testing (CFTT) program publishes methodologies and reports to evaluate forensic software, reinforcing the expectation that agencies document tool versions, test baselines, and known limitations. Hash-based integrity controls (e.g., SHA-256) are standard, with NIST guidance on appropriate hash-algorithm use and security strengths.

Cloud and cross-border evidence: Cloud forensics raises issues of distributed logs, multi-tenant isolation, and provider cooperation. NISTIR 8006 catalogs technical and procedural challenges and underscores the need for selective acquisition, provenance tracking, and validated tooling to avoid evidence contamination. Instruments like the Budapest Convention facilitate lawful access to electronic evidence and cooperation among Parties—a foundation for cross-jurisdiction investigations.

AI for forensic triage and analysis: In log analytics, anomaly-detection and topic modeling can automatically surface suspicious sequences and cluster activity across hosts. In media forensics, deep-learning detectors (e.g., FaceForensics++ benchmark work) target GAN-generated manipulations and face swaps—important for sextortion, disinformation, and identity crimes. However, model performance degrades outside training distributions, and compression or re-encoding can confound detectors, reinforcing the need for validation and uncertainty reporting.

Fairness, accountability, and transparency: Empirical evaluations (e.g., NIST FRVT) show demographic performance differentials in face recognition systems;

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 13-23

predictive-policing critiques warn of feedback loops when models are trained on biased deployment data. These findings motivate documented bias assessments, error-rate reporting, human-in-the-loop review, and strict scope constraints for AI suggestions.

Legal and regulatory context: Under FRE 702 and Daubert, AI-assisted conclusions must be grounded in reliable methods, subjected to known error-rates, peer review, and standards; Frye's "general acceptance" test still governs in some jurisdictions. The EU AI Act imposes risk-based controls and constrains real-time biometric identification by police, demanding prior authorization and proportionality. These frameworks together press agencies to embed validation, documentation, and governance into AI deployments.

Methodology

We propose a standards-aligned, AI-augmented forensic workflow designed to preserve evidentiary integrity while realizing analytical gains:

1. **Readiness & Governance**
   - **Policy alignment:** Adopt ISO/IEC 27043 to define incident-investigation processes and roles; map agency SOPs to ISO/IEC 27037 (identification/collection/acquisition/preservation) and 27042 (analysis/interpretation). Establish evidence-handling checklists and first-responder quick cards (INTERPOL).
   - **Model risk management:** Register AI components in a model inventory; apply NIST AI RMF functions (Govern, Map, Measure, Manage) to document context, risks, intended use, performance, and monitoring; require pre-deployment bias/robustness tests with target metrics.
   - **Legal scoping:** For biometric applications, incorporate EU AI Act constraints into SOPs (authorization, narrow use cases, logging). Define admissibility documentation aligned with FRE 702/Daubert/Frye (method reliability, error rates, acceptance).
2. **First Response & Triage**
   - **Scene control & safety:** Follow INTERPOL first-responder guidance; isolate devices/networks as appropriate; document actions contemporaneously.
   - **AI-assisted triage:**
     - **Log streams:** Use anomaly detection to prioritize time windows and hosts; topic models summarize rare process/command patterns.
     - **Media:** Apply deepfake-detection pipelines (e.g., detectors trained/evaluated on FaceForensics++-style benchmarks), but retain human verification and confidence thresholds.
     - **Textual intelligence:** NLP summarizes warrants, interviews, and open-source reporting for lead generation with full citations.
3. **Acquisition & Integrity**
   - **Forensic imaging:** Perform bit-for-bit acquisition with write-blockers where applicable; for cloud sources, use provider APIs with signed export logs (addressing NISTIR 8006 challenges).
   - **Hashing and sealing:** Compute SHA-256 (and, where policy requires, a second hash) at acquisition and upon every transfer; store on

WORM or equivalent; maintain full chain-of-custody records. Reference NIST guidance on hash algorithms.
- **Remote/endpoint collection:** When network-based capture is necessary, follow SWGDE best practices, including contemporaneous chain-of-custody documentation and error logs.
- **Mobile devices:** Apply NIST SP 800-101r1 guidance on live vs. logical vs. physical acquisition; record device state metadata.

4. **Analysis & Interpretation**
   - **Tool validation:** Prefer tools vetted by NIST CFTT; where not available, perform internal validation with known-answer test sets; record tool versions and parameters.
   - **AI explainability:** Log model versions, training data provenance (where available), decision rationales (e.g., feature attributions), and uncertainty intervals.
   - **Bias & error profiling:** For face analytics, report demographic error-rate profiles and mitigation steps; for predictive triage, monitor for feedback loops and disparate impacts.
   - **Analyst oversight:** Require dual-control review for AI-flagged artifacts; insist that analysts can reproduce results via stored pipelines and fixed seeds.
5. **Reporting & Disclosure**
   - **Standards-conformant reports:** Follow ISO/IEC 27042 guidance on recording analytic choices, assumptions, and limitations; attach chain-of-custody and hash manifests.
   - **Courtroom readiness:** Map reports to FRE 702/Daubert factors: testability, peer review, error rates, standards, and acceptance. Include validation summaries and known limitations.
6. **Post-Case Learning**
   - **Continuous improvement:** Capture false positives/negatives and analyst feedback; update model risk profiles per NIST AI RMF; re-validate tools after major updates.

RESULTS

Implementing the methodology above in a mid-sized agency's cyber unit over a series of controlled exercises and retrospective case replays yielded the following observed benefits and safeguards:

- **Faster triage without integrity compromises:** AI log-triage clustered anomalous command sequences and lateral-movement patterns, reducing manual review time while preserving the forensic chain: every AI suggestion linked back to immutable captured data with SHA-256 hashes, acquisition manifests, and custody logs (as required by ISO/IEC 27037 and SWGDE practices).
- **Media authenticity checks at scale:** Automated detectors flagged likely manipulations for analyst review; where confidence was borderline (e.g., heavy compression), analysts reverted to traditional media-forensics procedures and documented uncertainty in line with ISO/IEC 27042.
- **Cloud evidence stewardship:** Case playbooks captured provider export logs and signatures; selective acquisition addressed multi-tenant constraints, reflecting NISTIR 8006 guidance.

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 1, Jan – Mar 2026 || PP. 13-23

- **Admissibility-oriented documentation:** Reports explicitly mapped methods to standards and validation artifacts to CFTT references; expert declarations were structured to satisfy FRE 702/Daubert, including error-rate disclosures and limitations.
- **Risk and fairness controls:** Face-analytics use was scoped and audited against demographic error-rate research; no biometric inference was used operationally in contexts restricted under the EU AI Act without prior authorization and documented necessity/proportionality.

These outcomes do not imply that AI "solves" digital forensics. Rather, they show that measurable efficiency gains are attainable when AI is embedded within standards-based acquisition and legally defensible reporting, with human oversight and transparent limitations.

CONCLUSION

Artificial intelligence is now indispensable for coping with the velocity, volume, and volatility of digital evidence. Yet in cyber law enforcement and forensic practice, AI's value is realized only when it is embedded inside a standards-led, legally defensible, and ethically grounded operating model. This paper has shown that the bedrock remains unchanged—sound identification, collection, acquisition, preservation, analysis, and reporting—while AI contributes measurable gains in scale, speed, and signal discovery. The imperative is not to "algorithmize" judgment but to amplify human expertise with validated, transparent tools that leave a verifiable audit trail from first responder to courtroom.

A coherent blueprint emerges from the synthesis of ISO/IEC 27037/27042/27043, NIST guidance, admissibility rules (FRE 702/Daubert/Frye), and the EU AI Act's risk-based constraints. Agencies should operationalize this as seven governing principles:

1. **Legality & Authorization:** Every AI-assisted step must be anchored to lawful powers, scoped warrants, and documented necessity and proportionality—especially for biometric or intrusive analysis.
2. **Integrity & Reproducibility:** Bit-accurate acquisition, cryptographic hashing at each transfer, version-pinned tooling, and repeatable workflows are non-negotiable.
3. **Reliability by Design:** Pre-deployment and periodic validation against known-answer corpora; disclosure of error rates, confidence intervals, and known failure modes.
4. **Transparency & Explainability:** Model registries, provenance logs, interpretable rationales where feasible, and human-readable reports that map decisions to data.
5. **Fairness & Accountability:** Routine bias assessments; clearly bounded use-cases; dual-analyst review for high-stakes inferences; redress mechanisms for affected parties.
6. **Human Oversight:** Analysts remain the decision-makers; AI triage is advisory, never dispositive.
7. **Continuous Improvement:** Post-case learning loops, change-control for tools/models, and re-validation after material updates.

Translating these principles into practice benefits from a staged implementation roadmap:

- **0–3 months (Foundations):** Establish governance (policies, SOPs), a model inventory, and a tool-validation plan; identify priority use-cases (e.g., log triage, media authenticity screening). Define courtroom-ready documentation templates that explicitly address admissibility factors and limitations.

- **3–9 months (Pilots under supervision):** Run limited-scope pilots with shadow human review. Track key performance indicators: median triage-time reduction; proportion of findings reproducible across independent runs; rate of analyst overrides; number of evidence exclusions avoided due to improved documentation.
- **9–18 months (Scale with safeguards):** Expand to additional evidence classes (mobile, cloud), integrate with case management, and institute routine bias and robustness checks. Formalize external audits and peer reviews; participate in inter-agency proficiency testing.

There are also research gaps worth prioritizing through public–private–academic consortia and standardized open testbeds:

- Robustness of deepfake and tamper detection under extreme compression and re-encoding;
- Cryptographically verifiable provenance for cloud and ephemeral artifacts;
- Explainability methods tailored to sequential log reasoning and graph-based intrusion narratives;
- Federated or privacy-preserving analytics that respect data localization and sovereignty;
- Benchmarks for end-to-end evidentiary pipelines (not just point models), including chain-of-custody integrity under realistic operational constraints.

Ethically, agencies should publish a use charter for AI in forensics—listing permitted applications, prohibited practices, oversight bodies, audit cadences, retention/deletion timelines, and transparency commitments. Public trust is strengthened when communities, defense counsel, and courts see not only what AI can do, but also what it will not be used for and how error and bias are monitored.

In sum, AI's contribution to cyber investigations is tangible: faster triage of massive logs, scalable media authenticity checks, and coherent synthesis of multi-source intelligence. Its safe deployment, however, depends on discipline—standards alignment, rigorous validation, documented limitations, and accountable human oversight. Agencies that internalize these practices will improve case throughput and evidentiary quality, reduce exclusion risks, and better withstand legal scrutiny, all while honoring rights and due process. The path forward is clear: treat AI as a governed forensic instrument, not a shortcut—one that elevates investigative rigor and supports fair, timely justice in a digital age.

REFERENCES

- *ACPO / NPCC. (2012). Good Practice Guide for Digital Evidence. National Police Chiefs' Council.* https://athenaforensics.co.uk/wp-content/uploads/2019/01/National-Police-Chiefs-Council-ACPO-Good-Practice-Guide-for-Digital-Evidence-March-2012.pdf
- *Council of Europe. (n.d.). About the Convention on Cybercrime (Budapest Convention).* https://www.coe.int/en/web/cybercrime/the-budapest-convention
- *Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). (n.d.). Oyez.* https://www.oyez.org/cases/1992/92-102
- *European Parliament. (2024, March 13). Artificial Intelligence Act: MEPs adopt landmark law (Press release).* https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law
- *ISO/IEC 27037:2012. (2012). Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization.* https://www.iso.org/standard/44381.html
- *ISO/IEC 27042:2015. (2015). Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization.* https://www.iso.org/standard/44406.html

- *ISO/IEC 27043:2015. (2015). Information technology—Security techniques—Incident investigation principles and processes. International Organization for Standardization.* https://www.iso.org/standard/44407.html
- *INTERPOL. (2021, March). Guidelines for Digital Forensics First Responders.* https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
- *Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19.* https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x
- *NIST. (2006). SP 800-86: Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf
- *NIST. (2014). SP 800-101r1: Guidelines on Mobile Device Forensics. National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf
- *NIST. (2019). NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3—Demographic Effects.* https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf
- *NIST. (2020). NISTIR 8006: Cloud Computing Forensic Science Challenges.* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf
- *NIST. (2023). AI Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
- *NIST. (n.d.). Computer Forensics Tool Testing (CFTT) Program.* https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt
- *SWGDE. (2024, Nov 22). Best Practices for Remote Collection of Digital Evidence from an Endpoint (22-F-003 v2.0). Scientific Working Group on Digital Evidence.* https://www.swgde.org/wp-content/uploads/2024/11/2024-11-22-Best-Practices-for-Remote-Collection-of-Digital-Evidence-from-an-Endpoint-22-F-003-2.0.pdf
- *SWGDE. (2020). Best Practices for Mobile Device Evidence Collection, Preservation, Handling, and Acquisition (v1.2).* https://www.swgde.org/wp-content/uploads/2023/11/2020-09-17-SWGDE-Best-Practices-for-Mobile-Device-Evidence-Collection-_-Preservation-Handling-and-Acquisition_v1.2.pdf
- *U.S. Federal Rules of Evidence. (n.d.). Rule 702: Testimony by Expert Witnesses. Legal Information Institute.* https://www.law.cornell.edu/rules/fre/rule_702
- *Wex. (n.d.). Frye Standard. Legal Information Institute.* https://www.law.cornell.edu/wex/frye_standard
- *EU Artificial Intelligence Act—Article 5 (Prohibited AI practices / law-enforcement biometric use restrictions). (n.d.).* https://artificialintelligenceact.eu/article/5/
- 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