



Artificial Intelligence, Digital Surveillance and Citizen Rights in Indian Democracy

Dr. Kalpesh Rasiklal Rakholia

Professor - SSCIT

Swarnim Startup & Innovation University-

Gandhinagar, Gujarat

ORCID id - <https://orcid.org/0009-0007-2284-2195>



<http://www.gjirp.org/> || Vol. 2 No. 3 (2026): August Issue

Date of Submission: 21-06-2026

Date of Acceptance: 11-07-2026

Date of Publication: 01-08-2026

Abstract —The convergence of artificial intelligence and digital surveillance technologies with the machinery of the state has created one of the most consequential legal and constitutional challenges facing contemporary Indian democracy. From facial recognition deployment by police forces to allegations of spyware use against journalists and activists, the expanding capacity of the state to monitor, profile, and predict citizen behaviour tests the boundaries of constitutionally guaranteed rights to privacy, free expression, and equality. This paper examines the evolving legal and institutional framework governing artificial intelligence and digital surveillance in India, tracing its foundations through the Supreme Court's privacy jurisprudence in *People's Union for Civil Liberties v. Union of India* and *Justice K.S. Puttaswamy v. Union of India*, the ongoing judicial scrutiny of state surveillance practices in the *Pegasus* litigation, and recent regulatory developments

including the Digital Personal Data Protection Act, 2023, and the India AI Governance Guidelines, 2025. The paper argues that while India possesses a constitutionally grounded doctrine of privacy and proportionality, the governance of artificial-intelligence-enabled surveillance remains largely dependent on voluntary, non-binding instruments, leaving significant gaps in accountability, transparency privacy, and citizen redress.

Keywords — artificial intelligence, digital surveillance, privacy, facial recognition, Pegasus, data protection, AI governance, Indian democracy

Introduction

Artificial intelligence and digital surveillance technologies have moved, within the space of a decade, from the periphery of state administration to its operational core. Facial recognition



systems assist police investigations, algorithmic tools inform welfare distribution and identity verification, predictive analytics increasingly shape policing priorities, and communication interception technologies, both lawful and, as recent litigation suggests, potentially unlawful, form part of the state's security apparatus. These technologies promise significant gains in administrative efficiency, public safety, and service delivery. They simultaneously carry the capacity to enable forms of monitoring, profiling, and control that were technically infeasible in earlier eras, raising urgent questions about the adequacy of existing constitutional and statutory protections for citizen rights.

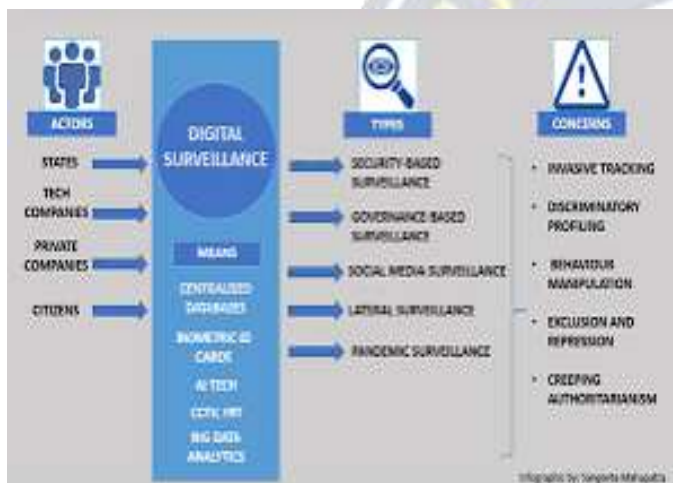


Fig. 1: Digital Surveillance and the Threat to Civil Liberties in India

Source: <https://www.giga-hamburg.de/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india>

India's experience with these questions has been shaped by a series of landmark judicial interventions beginning well before the current era of artificial intelligence, including the Supreme Court's 1997 ruling on telephone tapping and its 2017 recognition of privacy as a fundamental right. These precedents

have since been tested against a new generation of technologies: biometric identification at national scale through Aadhaar, facial recognition technology deployed by state police forces, and allegations of the use of sophisticated commercial spyware against journalists, opposition politicians, and civil society actors. At the same time, India's regulatory response to artificial intelligence specifically has, as of the most recent developments, taken the form of non-binding guidance rather than binding legislation, raising questions about whether existing legal tools are adequate to govern a rapidly advancing and increasingly opaque set of technologies.

This paper undertakes a systematic examination of the legal and constitutional framework governing artificial intelligence and digital surveillance in India, situating it within the broader question of how a constitutional democracy reconciles the administrative and security benefits of these technologies with its foundational commitments to individual liberty, equality, and democratic accountability.

Objectives of the Study

This study seeks to achieve the following objectives:

To trace the constitutional foundation of privacy protection in India as it applies to state surveillance, from *People's Union for Civil Liberties v. Union of India* through *Justice K.S. Puttaswamy v. Union of India*.

To examine the *Pegasus* spyware litigation as a case study in the challenges of judicial oversight of covert state surveillance capacity.

To assess the statutory and regulatory framework governing data processing and artificial intelligence, including the Digital

Personal Data Protection Act, 2023, and the India AI Governance Guidelines, 2025.

To analyse the deployment of specific technologies, particularly facial recognition, within Indian law enforcement, and the rights concerns this raises.

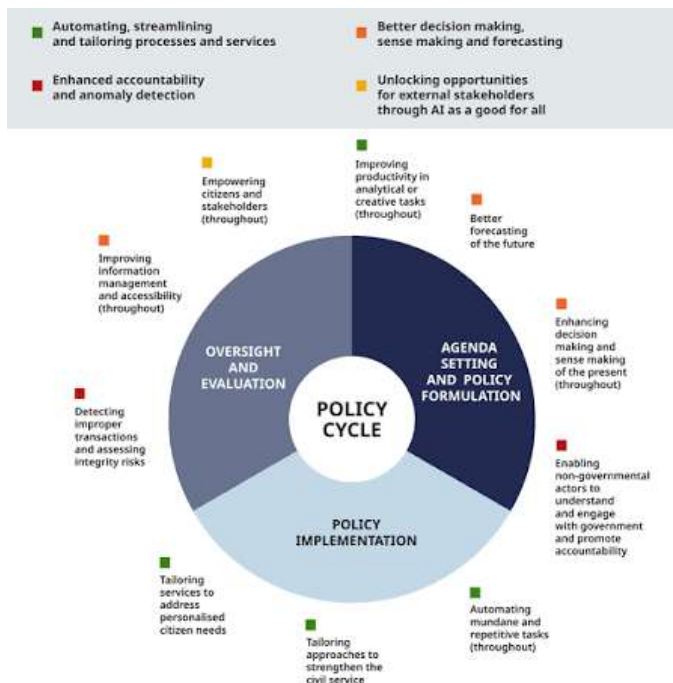


Fig. 2: The Policy Cycle

Source: https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/how-artificial-intelligence-is-accelerating-the-digital-government-journey_d9552dc7.html

To evaluate the adequacy of current oversight mechanisms in ensuring accountability for AI-enabled and digital surveillance practices.

To identify the structural gaps between constitutional doctrine and the practical governance of emerging surveillance technologies, and to propose directions for reform.

Research Methodology

This paper adopts a doctrinal, descriptive-analytical research methodology, drawing on constitutional provisions, statutory texts, reported and ongoing judicial proceedings, government notifications and policy documents, and professionally published legal and policy commentary. Given the pace of regulatory change in this field, particular reliance is placed on contemporaneous reporting and analysis of developments through 2025 and 2026, including the AI Governance Guidelines and the operationalisation of the DPDP Rules. The study does not involve primary empirical data collection; it synthesises existing legal, judicial, and institutional material into an evaluative account of the current governance landscape. Case law has been selected for its doctrinal significance in shaping Indian privacy and surveillance jurisprudence, while policy instruments have been selected for their direct relevance to the regulation of artificial intelligence and surveillance technology.

Literature Review

The literature on artificial intelligence, digital surveillance, and citizen rights in India can be organised around four principal strands: the constitutional foundation of privacy as a check on surveillance, judicial engagement with covert surveillance technology, the statutory data protection regime, and the emerging, largely voluntary framework for AI governance.

The earliest strand traces to *People's Union for Civil Liberties v. Union of India*, reported at (1997) 1 SCC 301, in which the



Supreme Court examined the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885, following revelations, prompted by a Central Bureau of Investigation report, of widespread unauthorised telephone tapping of politicians. Commentary on the case, including analysis by Lawbhoomi, CaseMine, and the National Law University Jodhpur-affiliated review published in the NUJS Law Review, converges on the finding that the Court, while upholding the constitutionality of the provision itself, held that telephone conversations fall within the right to privacy protected under Article 21, and are also protected as an exercise of free speech under Article 19(1)(a), such that any interception must satisfy the "procedure established by law" standard. The Court accordingly issued detailed procedural guidelines mandating that interception orders be issued only by the Home Secretary at the central or state level, subject to defined review committees and time limits, guidelines that were later incorporated into Rule 419A of the Indian Telegraph Rules.

That later jurisprudence culminated in *Justice K.S. Puttaswamy v. Union of India*, reported at (2017) 10 SCC 1, in which a nine-judge bench unanimously held privacy to be an independent fundamental right under Article 21, connected to Articles 14 and 19, and articulated a three-part proportionality test, legality, legitimate aim, and proportionality, for assessing the validity of any state action infringing that right. Analysis published by the India Corporate Law blog of Cyril Amarchand Mangaldas, examining the post-*Puttaswamy* surveillance landscape, observes that the judgment directly reshaped the legal standard against which subsequent surveillance practices, including biometric identification and communications interception, must be assessed, effectively elevating the *PUC*L procedural safeguards into a constitutionally mandated proportionality framework rather than a matter of statutory interpretation alone.

The practical stakes of this doctrinal framework were tested directly in the *Pegasus* spyware litigation. According to reporting and case analysis from the Supreme Court Observer, SCC Online, and Live Law-affiliated outlets such as Verdictum, the matter arose after an international investigative consortium, the Pegasus Project, revealed in July 2021 that a leaked list of approximately 50,000 phone numbers, including around 300 associated with Indian nationals, among them journalists, politicians, and current or former court officials, had been identified as potential surveillance targets using NSO Group's Pegasus spyware. In *Manohar Lal Sharma v. Union of India*, 2021 SCC OnLine SC 985, the Supreme Court, dissatisfied with the Union Government's refusal to file a substantive affidavit on the ground of national security, appointed an independent Technical Committee, overseen by a retired Supreme Court judge, to investigate the allegations, emphasising in its order that the state cannot invoke national security as a blanket shield against judicial scrutiny where fundamental rights are implicated. Subsequent reporting by Verdictum and LawChakra indicates that the Technical Committee examined a limited sample of devices, found malware on a subset of them without being able to conclusively confirm Pegasus specifically, and noted possible non-cooperation from the government during the investigation, while a parallel Supervisory Committee recommended legislative reform to strengthen privacy protection and cybersecurity. Commentary on this litigation, including analysis published in the SCC Online blog, treats the case as illustrative of the structural difficulty courts face in adjudicating covert surveillance claims where the state controls the evidentiary record and can invoke national security to limit disclosure, a difficulty that persists notwithstanding the doctrinal clarity offered by *Puttaswamy*.





A third strand of literature addresses the statutory data protection framework that has emerged in the aftermath of *Puttaswamy*. As documented in earlier analysis of the Digital Personal Data Protection Act, 2023, and its accompanying Rules notified in November 2025, India's data protection regime establishes obligations on data fiduciaries and rights for data principals, enforced through the Data Protection Board of India. Scholarly and industry commentary, however, consistently flags that the Act contains broad exemptions permitting government processing of personal data for purposes including sovereignty, security of the state, and public order, exemptions that have drawn criticism for potentially permitting surveillance-related data processing without the procedural safeguards otherwise required of private data fiduciaries, an area of continuing debate as the Act's phased implementation proceeds toward full effect by May 2027.

The fourth and most recent strand of literature concerns the governance of artificial intelligence itself, as distinct from data processing generally. According to the Ministry of Electronics and Information Technology's own publication, corroborated by law firm analyses from Khaitan & Co and Saikrishna & Associates, MeitY released the India AI Governance Guidelines on 5 November 2025, following a public consultation process that began with a draft released in early 2025 and received more than 2,500 stakeholder submissions. Commentary converges on the finding that the Guidelines adopt a deliberately "lightweight," non-binding, techno-legal approach, built around seven guiding principles and proposing institutional structures such as an AI Governance Group and an AI Safety Institute, while explicitly relying on existing laws, including the IT Act, the DPDPA Act, and the Bharatiya Nyaya Sanhita, to address AI-related harms rather than introducing a dedicated, binding AI statute. Commentary published in the

Good Men Project and NRI Affairs, drawing on human rights advocacy perspectives, argues that this voluntary framework is particularly inadequate for high-risk state applications of AI, including surveillance, predictive policing, and welfare automation, where the absence of binding obligations leaves affected citizens without effective avenues for redress; the same commentary cites documented failures in AI-based facial recognition systems used for welfare verification, noting degraded accuracy in poor lighting conditions, on lower-end devices, and for individuals with darker skin tones, contributing to wrongful exclusion of intended beneficiaries from welfare entitlements.

Finally, literature specifically addressing facial recognition technology in Indian policing, including a policy brief published by the Takshashila Institution, documents the mandatory Standardisation Testing and Quality Certification requirements now imposed by MeitY on CCTV systems used in such deployments, while noting the absence of a dedicated statutory framework governing the specific use of facial recognition by law enforcement, including matters such as permissible use cases, data retention periods, accuracy thresholds, and independent audit requirements, an omission that the literature identifies as a significant gap relative to the sensitivity of biometric surveillance in a policing context.

Taken together, this literature demonstrates a distinctive pattern in the Indian context: an unusually well-developed constitutional doctrine of privacy and proportionality, forged through *PUC*L and *Puttaswamy* and tested through the *Pegasus* litigation, coexisting with a still-emerging and largely non-binding regulatory apparatus for the specific technologies, artificial intelligence and biometric surveillance in particular, that pose the most acute contemporary risks to the rights that doctrine is meant to protect.





Constitutional and Judicial Framework

The constitutional starting point for assessing state surveillance and AI-enabled monitoring in India is Article 21's guarantee of life and personal liberty, now authoritatively interpreted in *Puttaswamy* to encompass an independent right to privacy, alongside Article 19(1)(a)'s guarantee of speech and expression, which extends, as established in *PUC*L, to private communications. The *Puttaswamy* proportionality test, legality, legitimate state aim, and proportionality of means, now functions as the operative constitutional standard against which surveillance measures, whether conducted through telephone interception, biometric identification, or AI-enabled monitoring, must be assessed.

The *Pegasus* litigation illustrates both the strength and the limitations of this doctrinal framework in practice. On one hand, the Supreme Court's willingness to reject the government's blanket invocation of national security, and its appointment of an independent Technical Committee, reflects meaningful judicial insistence on accountability even in sensitive surveillance matters. On the other hand, the Committee's constrained findings, an inability to conclusively confirm the use of Pegasus specifically despite detecting malware on some examined devices, together with reported difficulties obtaining full cooperation from the government, illustrate the practical evidentiary asymmetry that citizens and even courts face when confronting covert state surveillance capacity.

Statutory and Regulatory Framework

Beyond constitutional doctrine, the statutory landscape governing digital surveillance and AI comprises several overlapping instruments. The Indian Telegraph Act, 1885, as

read with the procedural safeguards established in *PUC*L and codified in Rule 419A of the Indian Telegraph Rules, together with Section 69 of the Information Technology Act, 2000, and the associated Information Technology (Procedure for Interception) Rules, 2009, govern lawful interception of communications. The Digital Personal Data Protection Act, 2023, together with the DPDP Rules, 2025, establishes India's first comprehensive data protection regime, though its exemptions for government processing in the interest of state security and public order remain a subject of continuing scrutiny.

For artificial intelligence specifically, India currently lacks a dedicated, binding statute. The India AI Governance Guidelines, 2025, issued by MeitY under the IndiaAI Mission, instead adopt what has been described in industry and policy commentary as a "techno-legal," principle-based approach, relying on graded liability, existing sectoral laws, and voluntary compliance mechanisms, with binding obligations reserved for identified high-risk use cases on a case-by-case basis. The Guidelines propose institutional architecture, including a central AI Governance Group and a proposed AI Safety Institute, intended to develop technical standards and coordinate India's engagement in international AI governance forums, but do not, as currently framed, impose direct statutory obligations on state deployment of AI for surveillance or policing purposes.

Application to Emerging Technologies: Facial Recognition and Predictive Policing

The deployment of facial recognition technology by Indian police forces illustrates the practical stakes of this governance gap. While the Ministry of Electronics and Information Technology has imposed quality certification requirements on





the underlying CCTV hardware used in such systems, policy analysis from the Takshashila Institution notes the continued absence of a dedicated statutory framework specifically addressing the use of facial recognition in policing, including matters of accuracy thresholds, permissible use cases, data retention, and independent oversight. Documented accuracy failures in AI-based identity verification systems used for welfare delivery, particularly the degraded performance of facial recognition under poor lighting conditions, on lower-end devices, and for individuals with darker skin tones, further illustrate how algorithmic bias in AI systems deployed by the state can produce tangible harm to citizen rights and entitlements, harms that existing, largely voluntary governance instruments are not currently structured to remedy through binding accountability mechanisms.

Discussion and Analysis

The Indian experience with artificial intelligence and digital surveillance reveals a persistent structural asymmetry: constitutional doctrine, forged over decades through *PUC*L and *Puttaswamy*, has developed a demanding standard of legality, necessity, and proportionality for state intrusions into privacy, while the specific statutory and regulatory instruments needed to operationalise that standard for contemporary AI-enabled surveillance technologies remain comparatively underdeveloped. The *Pegasus* litigation demonstrates that even the Supreme Court's considerable institutional authority can be constrained by the inherent opacity of covert surveillance capability and the state's control over the relevant evidentiary record. The DPDP Act's broad government exemptions, and the deliberately non-binding character of the AI Governance Guidelines, suggest a regulatory posture that continues to prioritise administrative flexibility and innovation-friendliness over binding, enforceable accountability for state deployment

of these technologies, notwithstanding express constitutional commitments to proportionality established in *Puttaswamy*.

This asymmetry carries particular significance for a democracy, since the capacities enabled by AI and digital surveillance, mass biometric identification, algorithmic profiling, communications interception, and predictive policing, are precisely the tools most capable of chilling dissent, enabling discriminatory targeting, and eroding the conditions for free political participation if deployed without adequate transparency and independent oversight. The literature's consistent identification of a gap between constitutional aspiration and regulatory implementation suggests that India's next phase of legal development in this field will need to focus less on articulating further doctrinal principles, which are already comparatively well developed, and more on building binding, enforceable, and independently supervised mechanisms specific to AI and surveillance technology.

Conclusion

India's constitutional and judicial framework for protecting citizen rights against state surveillance is doctrinally sophisticated, grounded in a continuous line of jurisprudence from *People's Union for Civil Liberties v. Union of India* through *Justice K.S. Puttaswamy v. Union of India*, and tested, if imperfectly, through the ongoing *Pegasus* litigation. Yet this doctrinal sophistication coexists with a regulatory landscape for artificial intelligence and emerging surveillance technologies that remains, as of the most recent developments in late 2025, predominantly voluntary and non-binding, leaving significant categories of state AI deployment, including facial recognition and predictive policing, without dedicated, enforceable safeguards. Bridging this gap will require translating the proportionality standard articulated in *Puttaswamy* into binding





sector-specific legislation governing AI-enabled surveillance, strengthening independent oversight mechanisms with genuine investigative and enforcement authority, and ensuring that the exemptions available to government data processing under the DPDP Act do not become a structural loophole through which the constitutional right to privacy is diluted in practice.

References

- Gupta, S. K. (2022). Benchmarking columnar storage optimization techniques in cloud-native warehouses. *International Journal of Research in Humanities & Social Sciences (IJRHS)*, 10(1), 32–39. <https://doi.org/10.63345/ijrhs.net.v10.i1.1>
- Bharucha, S. (2019, November 23). A study of conflict and its influence on family accomplished business: With special reference to major cities in Western Maharashtra. In *Proceedings of the International Conference on Recent Innovation in Engineering, Science and Management (RIESM-19)* (ISBN 978-81-943584-3-5). Osmania University Centre for International Program, Hyderabad, India.
- Gupta, S. K. (2022). Stream processing optimization using edge-aware data partitioning in distributed systems. *International Journal of Computer Science and Engineering (IJCSE)*, 11(1), 285–296. <https://www.iaset.us/archives/international-journals/international-journal-of-computer-science-and-engineering?page=18>
- Bharucha, S., & Kumar, D. (2020). To study about the family business association and conflict. *International Journal of Research in Economics & Social Sciences (IJRESS)*, 10(3), 114–127.
- Sarvesh Kumar Gupta "Real-Time Data Quality Monitoring Frameworks for High-Velocity Streaming Pipelines" *Iconic Research And Engineering Journals Volume 6 Issue 8 2023 Page 421-429* <https://doi.org/10.64388/IREV6I8-1719275>
- Saini, V. K., Bharucha, S., Kumar, A., & Rana, P. (2025). *Strategic horizons: Leading with vision in a changing world*. Yashita Prakashan Private Limited.
- Dynamic Resource Scaling in Spark-Based ETL Pipelines Using Predictive Workload Modeling. (2023). *Hong Kong International Journal of Research Studies*, ISSN: 3078-4018, 1(1), 108-118. <https://doi.org/10.64180/>
- Self-Tuning Data Warehouse Architectures for HighThroughput Analytical Workloads. (2023). *International Journal of Engineering Fields*, ISSN: 3078-4425, 1(1), 51-59.
- Joshi, J., Bharucha, S., Jadhav, D. R. R., & Rastogi, M. (2025). *Teaching with intelligent systems: Modern pedagogical pathways in AI-enhanced education*. Wissira Research Lab. <https://doi.org/10.63345/book.wrl.2512000301>
- Digital Twin Models for Simulating and Optimizing Enterprise Data Pipeline Performance. (2024). *AI Tech International Journal*, ISSN: 3079-4749, 2(2), 71-82. <https://techaijournal.com/index.php/AIjournal/article/view/39>
- Gupta, S. K. (2023). Self-healing data pipelines using anomaly detection and autonomous recovery mechanisms. *International Journal of Research in All Subjects in Multi Languages (IJRSMML)*, 11(10), 54–61. <https://doi.org/10.63345/ijrsmml.v11.i10.1>
- Sarvesh Kumar Gupta. (2024). Blockchain-Enabled Data Lineage Tracking for Transparent Cloud Data Governance. *Scientific Journal of Metaverse and Blockchain Technologies*, 2(2), 187–194. <https://doi.org/10.36676/sjmbt.v2.i2.49>
- Sarvesh Kumar Gupta. (2024). Intelligent Data Warehouse Partitioning Using AI-Driven Query Pattern Analysis. *Modern Dynamics: Mathematical Progressions*, 1(2), 540–547. <https://doi.org/10.64170/mdmp.v1.i2.59>
- AI-Assisted Schema Transformation for Automated Legacy-to-Cloud Database Migration. (2026). *Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT)*, 3(1), Mar (50-57). <https://doi.org/10.63345/sjaibt.v3.i1.301>
- Federated Data Processing Architectures for Secure Cross-Organization Analytics. (2026). *World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE)* U.S. ISSN: 3070-6203, 2(2), May (60-68). <https://doi.org/10.63345/wjftcse.v2.i2.201>
- Sarvesh Kumar Gupta. (2025). Secure Data Migration Strategies on AWS Cloud. *International Journal of Computational and Experimental Science and Engineering*, 11(3). <https://doi.org/10.22399/ijcesen.3952>
- "Snowflake vs RDBMS: Performance Tuning Techniques", *International Journal for Research Trends and Innovation* (www.ijrti.org), ISSN:2456-3315, Vol.10, Issue 5, page no.c825-c832, May-2025, Available :<http://www.ijrti.org/papers/IJRTI2505296.pdf>





- Sarvesh Kumar Gupta, "Hybrid Cloud Pipelines for Regulated Industries", *IJRAR - International Journal of Research and Analytical Reviews (IJRAR)*, E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.705-712, May 2025, Available at : <http://www.ijrar.org/IJRAR25B4662.pdf>
- Sarvesh kumar Gupta, "Modernizing Legacy Data Systems in Agile Environments", *IJRAR - International Journal of Research and Analytical Reviews (IJRAR)*, E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.713-721, June 2025, Available at : <http://www.ijrar.org/IJRAR25B4663.pdf>
- Sarvesh Kumar Gupta, 2025. "Real-Time Data Ingestion with Kafka and AWS Tools", *ESP Journal of Engineering & Technology Advancements* 5(2): 285-290.
- Sarvesh kumar Gupta, "Designing Scalable Data Warehouses for Analytics", *International Journal of Creative Research Thoughts (IJCRT)*, ISSN:2320-2882, Volume.13, Issue 7, pp.h868-h876, July 2025, Available at :<http://www.ijcert.org/papers/IJCRT2507898.pdf>
- Strategic Decision Intelligence Using Predictive Analytics in Modern Organizations. (2026). *Global Journal of Innovative Research Perspectives (GJIRP)*, 2(2), May (1-8). <https://doi.org/10.63345/gjirp.v2.i2.201>
- Sarvesh kumar Gupta. Best practices for oracle to PostgreSQL migration. *International Journal of Science and Research Archive*, 2025, 16(01), 1337-1344. Article DOI: <https://doi.org/10.30574/ijrsra.2025.16.1.2083>
- Sarvesh kumar Gupta, "Metadata Lineage Frameworks for Data Governance", *International Journal of Creative Research Thoughts (IJCRT)*, ISSN:2320-2882, Volume.13, Issue 9, pp.c895-c903, September 2025, Available at :<http://www.ijcert.org/papers/IJCRT2509332.pdf>
- Gupta, S. K. (2025). Machine Learning Integration in Spark-Based Pipelines. *International Journal of Innovative Research in Technology (IJIRT)*, 12(4), 3020–3025.
- Sarvesh Kumar Gupta, 2025. "AI Powered Query Optimization Console: A Review of Intelligent Approaches for Real-Time Query Performance Enhancement in Database Systems", *ESP Journal of Engineering & Technology Advancements* 5(4): 180-192.
- Bharucha, S. (2026). Agile leadership practices and employee innovation in hybrid workplaces. *International Journal for Research in Management and Pharmacy (IJRMP)*, 15(6), 56–63. <https://doi.org/10.63345/ijrmp.v15.i6.1>
- Sarvesh Kumar Gupta. Cloud ETL optimization with AWS glue and spark. *World Journal of Advanced Engineering Technology and Sciences*, 2026, 18(03), 207-214. Article DOI: <https://doi.org/10.30574/wjaets.2026.18.3.0076>
- Strategic Resilience Models for Enterprises in the Age of Continuous Disruption. (2026). *E-Journal of Science and Emerging Technologies (EJSET)*, 2(2), May (26-33). <https://doi.org/10.63345/ejset.v2.i2.201>
- Bharucha, S. (2023). Digital legacy and innovation balance in family-owned enterprises. *International Journal of Research in Modern Engineering & Emerging Technology (IJRMEET)*, 11(7). <https://doi.org/10.63345/ijrmeet.org.v11.i7.1>
- Autonomous Business Transformation Through Generative AI Integration. (2026). *Global Journal of Innovative Research Perspectives (GJIRP)*, 2(2), Apr (83-91). <https://doi.org/10.63345/gjirp.v2.i2.101>
- Bharucha, S. (2023). Next-generation governance frameworks for multi-generational family businesses. *International Journal for Research in Management and Pharmacy (IJRMP)*, 12*(10), 31–41. <https://doi.org/10.63345/ijrmp.v12.i10.5>
- Strategic Leadership for Hybrid Human–AI Workforce. (2025). *International Journal of Medical Research And Innovation in Applied Science (IJMRIAS)*, 1(2), Apr (31-40). <https://doi.org/10.63345/ijmrias.v1.i2.101>
- Bharucha, S. (2022). Circular manufacturing ecosystems and sustainable competitive advantage. *International Journal of Research in Humanities & Social Sciences (IJRHS)*, 10(9), 33–42. <https://doi.org/10.63345/ijrhs.net.v10.i9.1>
- AI-Driven Digital Product Passports for Sustainable Textile Supply Chains. (2025). *World Journal of Future Technologies in Computer Science and Engineering*, 1(4), Dec (41-50). <https://doi.org/10.63345/wjftcse.v1.i4.301>
- Bharucha, S. (2022). Predictive restructuring frameworks for organizational renewal. *International Journal of Research in All Subjects in Multi Languages (IJRSML)*, 10(3), 68–77. <https://doi.org/10.63345/ijrsml.v10.i3.1>
- Bharucha, S. (2024). Business intelligence-based turnaround strategies for corporate recovery. *International Journal for Research in Education (IJRE)*, 13 (8), 10–19. <https://doi.org/10.63345/ijre.v13.i8.1>
- Generative AI and the Reinvention of Management Education. (2026). *Scientific Journal of Artificial Intelligence and Blockchain*



