**Journal for Civil and Criminal Law for Legislative Studies**
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

# Cybercrime and Emerging Legal Challenges

**Shweta Shorey**
Assistant professor
MMH College ,Ghaziabad
ORCID id - https://orcid.org/0009-0007-3736-0535

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

| **Date of Submission:** 23-06-2026 | **Date of Acceptance:** 08-07-2026 | **Date of Publication:** 03-08-2026 |
|---|---|---|

**Abstract— The rapid expansion of digital connectivity has transformed the nature and scale of criminal activity, giving rise to a category of offences that transcend physical borders, traditional jurisdiction, and conventional modes of investigation. This paper examines the legal response to cybercrime, with particular focus on the Indian statutory and judicial framework, situating it within a broader discussion of emerging challenges such as data breaches, artificial-intelligence-enabled fraud, cross-border jurisdictional conflict, and the tension between digital surveillance and the constitutional right to privacy. The paper traces the evolution of India's cyber law regime from the Information Technology Act, 2000, through its 2008 amendment, the Supreme Court's landmark free-speech ruling in *Shreya Singhal v. Union of India*, the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*, and the recent operationalisation of the Digital Personal Data Protection Act, 2023. It further considers institutional responses, including the Indian Cybercrime Coordination Centre, and evaluates the persistent gap created by India's continued non-accession to the Budapest Convention on Cybercrime. The paper concludes that while India's legal framework has matured considerably, emerging technologies continue to outpace legislative and enforcement capacity, necessitating continuous legal reform, institutional strengthening, and greater international cooperation.**

**Keywords— cybercrime, Information Technology Act, data protection, digital privacy, cyber law, Budapest Convention, artificial intelligence, jurisdiction**

## Introduction

The transition of human activity into digital space has been accompanied by a corresponding migration of criminal conduct. Cybercrime today spans an extraordinarily wide

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

spectrum: financial fraud, identity theft, ransomware extortion, online harassment, child sexual abuse material, corporate data breaches, critical infrastructure attacks, and, increasingly, offences facilitated or amplified by artificial intelligence, including deepfake-enabled fraud and impersonation. Unlike traditional crime, cybercrime is frequently borderless in character; a perpetrator located in one jurisdiction may target victims across multiple countries using infrastructure hosted in yet another, creating profound challenges for investigation, evidence-gathering, and prosecution.

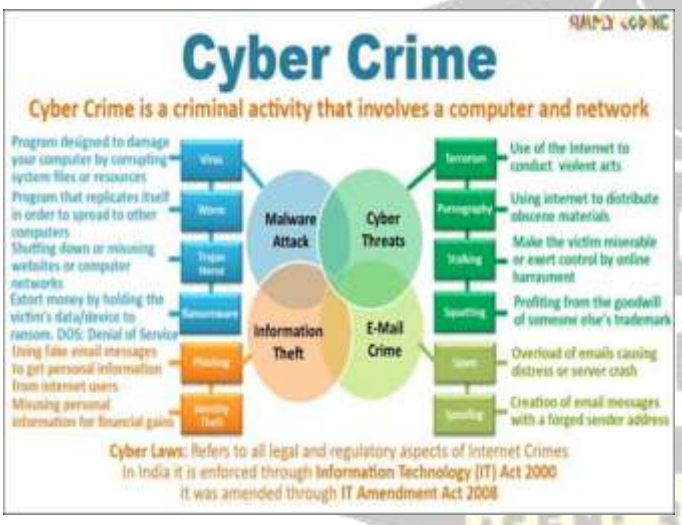


***Fig. 1: Investigative Challenges in New age Cyber Crimes***

***Source:*** ***https://www.linkedin.com/pulse/investigative-challenges-new-age-cyber-crimes-patil***

Legal systems worldwide have struggled to keep pace with the speed of technological change. Laws drafted to address the internet of the early 2000s often prove inadequate for a landscape now shaped by cloud computing, encrypted communication, cryptocurrency, and generative artificial intelligence. India presents a particularly instructive case study in this regard. As one of the world's largest and fastest-growing digital economies, India has experienced a corresponding surge in cybercrime, prompting successive waves of legislative and judicial intervention beginning with the Information Technology Act, 2000, and continuing through the recent Digital Personal Data Protection Act, 2023. This paper examines that evolving legal architecture and identifies the emerging challenges that continue to test its adequacy.

The importance of this inquiry lies in the widening divergence between the pace of technological innovation and the pace of legal adaptation. Cybercrime law is not a static field; it is one in which yesterday's adequate regulatory framework can rapidly become obsolete in the face of new attack vectors and new categories of harm. Understanding the structure, strengths, and gaps of the existing legal response is therefore essential to anticipating the reforms that will be needed as digital threats continue to evolve.

**Objectives of the Study**

This study seeks to achieve the following objectives:

To trace the legislative evolution of cyber law in India, from the Information Technology Act, 2000, through the Information Technology (Amendment) Act, 2008, to the Digital Personal Data Protection Act, 2023, and its accompanying Rules.

To examine landmark judicial pronouncements that have shaped the constitutional and statutory contours of India's cyber law regime, particularly *Shreya Singhal v. Union of India* and *Justice K.S. Puttaswamy v. Union of India*.

To assess the institutional mechanisms established for cybercrime prevention, reporting, and coordination, including the Indian Cybercrime Coordination Centre.

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

To analyse India's position with respect to international cybercrime cooperation frameworks, particularly the Budapest Convention on Cybercrime.

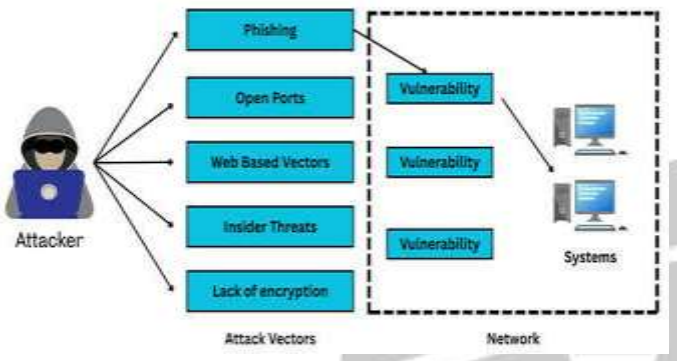


***Fig. 2: Attack workflow through different attack vectors: schematic flow diagram that maps common entry vectors to the attacker lifecycle stages.***

***Source:*** ***https://www.mdpi.com/2813-2203/4/3/25***

To identify emerging legal challenges posed by new technologies, including artificial intelligence, cryptocurrency, and cross-border data flows.

To propose directions for legal and institutional reform to address the persistent gap between technological change and regulatory capacity.

**Research Methodology**

This paper follows a doctrinal, descriptive-analytical research methodology, relying on secondary sources including statutory texts, reported judicial decisions, government notifications, reports of international bodies such as the Council of Europe, and peer-reviewed and professionally published legal commentary. The study does not involve primary empirical data collection; instead, it synthesises existing legal and institutional material to construct an evaluative account of the current state of cybercrime law and its emerging challenges. Case law and statutory provisions have been selected on the basis of their recognised doctrinal significance and contemporaneity, with particular attention paid to developments that have occurred through 2023 to 2026, reflecting the rapidly evolving character of this field.

**Literature Review**

The literature on cybercrime and its legal regulation in India converges around several major themes: the statutory foundation laid by the Information Technology Act, judicial elaboration of constitutional limits on cyber-regulation, the emergence of a dedicated data protection regime, and the persistent gap in international cooperation.

The Information Technology Act, 2000, is treated across the literature as India's foundational cyber law statute, providing legal recognition to electronic records and digital signatures while criminalising offences such as unauthorised access, data theft, and the introduction of computer viruses. Commentary on the Information Technology (Amendment) Act, 2008, most notably the well-documented controversy surrounding Section 66A, situates this amendment as both an attempt to modernise the framework and, ultimately, a cautionary illustration of the risks of vague and overbroad drafting in the digital context. Section 66A criminalised sending, through a computer resource, information that was "grossly offensive" or had a "menacing character," offences carrying penalties of up to three years' imprisonment. Analysis published by the Supreme Court Observer and by Internet Freedom Foundation documents that the provision was challenged after several high-profile arrests over social media posts, including the arrest of two women in

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

Palghar over a Facebook post concerning the shutdown of Mumbai following a political leader's death.

In *Shreya Singhal v. Union of India*, reported at (2015) 5 SCC 1, a two-judge bench of the Supreme Court struck down Section 66A in its entirety, holding it unconstitutionally vague and overbroad, and therefore violative of the freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution, without being saved by the reasonable restrictions permitted under Article 19(2). Commentary on the judgment, including analysis from Civilsdaily and the Wikipedia-hosted case summary corroborated by primary judgment excerpts, emphasises the Court's articulation of the "chilling effect" doctrine, recognising that vague criminal provisions targeting online speech can deter legitimate expression even where prosecution does not ultimately follow. Notably, subsequent research by the Internet Freedom Foundation, using data compiled through its "Zombie Tracker" project, found that prosecutions under Section 66A continued, and in fact increased, even after the provision was struck down, prompting the Supreme Court to issue supplementary directions in October 2022 instructing state governments to ensure police did not continue to register cases under the invalidated section. This body of literature is significant because it illustrates a recurring theme in cyber law scholarship: that judicial invalidation of a problematic provision does not automatically translate into administrative or police-level compliance, exposing an implementation gap that parallels concerns raised in other areas of Indian criminal law enforcement.

A second significant strand of literature addresses the constitutional foundation for digital privacy protection. In *Justice K.S. Puttaswamy v. Union of India*, reported at (2017) 10 SCC 1, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Article 21, and connected to the freedoms guaranteed under Articles 14 and 19, thereby overruling earlier decisions in *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh*, which had held that the Constitution did not expressly protect privacy. Commentary from Record of Law and the Human Dignity Trust identifies the Court's formulation of a three-part test for any state action infringing privacy, requiring legality, a legitimate state aim, and proportionality, as the judgment's most consequential doctrinal contribution, subsequently informing statutory data protection design in India.

Building on the constitutional foundation laid by *Puttaswamy*, the Digital Personal Data Protection Act, 2023, represents, in the literature's assessment, India's first comprehensive statutory data protection regime. Analysis from the Press Information Bureau, the Wikipedia-documented legislative history, and law-firm commentary published by Lexology and Baker Botts converge on the timeline of the Act's operationalisation: passed by Parliament in early August 2023 and assented to by the President on 11 August 2023, the Act remained largely dormant pending subordinate rule-making until the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules, 2025, along with the formal establishment of the Data Protection Board of India, in mid-November 2025. Commentary from CookieYes and Scrut.io notes that implementation is proceeding in a phased manner, with certain provisions taking effect immediately and the remaining provisions scheduled to come into force by May 2027, reflecting a deliberate calibration between regulatory ambition and industry readiness.

A further significant theme in the literature concerns institutional response mechanisms. According to the Council of Europe's Octopus Cybercrime Community country profile on

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

India and corroborating commentary from Legal Blur, the Indian Cybercrime Coordination Centre (I4C), together with the National Cyber Crime Reporting Portal, was inaugurated by the Ministry of Home Affairs in January 2020 as a centralised institutional response to the rising volume of cybercrime complaints, with particular emphasis on offences against women and children. This literature situates I4C as an important operational advance, though it does not resolve the deeper jurisdictional and cross-border evidentiary challenges that characterise much of contemporary cybercrime.

Finally, a substantial body of literature addresses India's continued non-participation in the Budapest Convention on Cybercrime, the first binding international treaty on cybercrime, in force since 2004 and, as of the most recent reporting reflected on the Council of Europe's own tracking page, ratified by 81 states. Analysis from the Centre for Internet and Society, the Observer Research Foundation, and academic commentary published through the Institute of Legal Education converges on the explanation that India has declined accession primarily on grounds of sovereignty, citing its non-participation in the treaty's original drafting process and concerns regarding cross-border data-sharing obligations with foreign law enforcement agencies under the Convention's mutual assistance provisions. This literature notes that India has instead pursued cooperation through bilateral Mutual Legal Assistance Treaties and membership in the G7's 24/7 network of cybercrime contact points, while simultaneously supporting a parallel, Russian-led effort at the United Nations to develop an alternative international cybercrime instrument, a position that commentators such as the Observer Research Foundation suggest may merit reconsideration given the escalating scale and cross-border character of cybercrime affecting India.

Taken together, the literature demonstrates that India's cyber law framework has evolved considerably over the past two decades, moving from a narrowly drafted, technology-recognition-oriented statute to a constitutionally anchored data protection regime informed by explicit judicial articulation of privacy as a fundamental right. At the same time, the literature consistently identifies unresolved structural gaps: continuing non-compliance with judicial rulings at the enforcement level, the absence of a fully binding international cooperation framework, and the still-emerging character of institutional responses to increasingly sophisticated forms of cyber-enabled harm.

**Statutory and Regulatory Framework**

India's principal cybercrime statute remains the Information Technology Act, 2000, which criminalises offences including unauthorised access to computer systems, data theft, the spread of viruses, cyber terrorism, and identity theft, while also establishing a framework for the legal recognition of electronic records and digital signatures. The Information Technology (Amendment) Act, 2008, expanded this framework substantially, introducing provisions on cyber terrorism, data protection obligations for corporate bodies handling sensitive personal data, and intermediary liability under Section 79, while also introducing the now-invalidated Section 66A.

Beyond the IT Act, the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, incorporates provisions directly applicable to cyber-enabled offences, including provisions on cheating, forgery, and identity-related fraud that are increasingly invoked in cases involving online financial fraud. The Digital Personal Data Protection Act, 2023, together with the DPDP Rules, 2025, constitutes India's first dedicated data protection statute, establishing obligations on "data

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

fiduciaries" regarding consent, purpose limitation, data minimisation, breach notification, and the rights of "data principals," enforced through the newly constituted Data Protection Board of India. The Act applies extraterritorially to entities processing the personal data of individuals in India, even where such processing occurs outside Indian territory, reflecting an approach broadly consistent with the extraterritorial reach seen in comparable international data protection regimes.

**Judicial Pronouncements**

Judicial intervention has played a decisive role in shaping the constitutional boundaries of India's cyber law regime. In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act as unconstitutionally vague, while upholding the constitutionality of Section 69A, which permits government-directed blocking of online content subject to procedural safeguards, and reading down Section 79 to clarify that intermediaries are obligated to remove content only upon receiving a court order or a notification from an appropriate government authority. The judgment remains the primary doctrinal reference point for the limits of state power to regulate online speech in India, and continuing litigation, including matters before the Court concerning the implementation of its 2015 ruling, indicates that its enforcement remains an active and unresolved concern.

In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court's recognition of privacy as an independent fundamental right under Article 21 supplied the constitutional foundation without which a comprehensive data protection statute would arguably have lacked doctrinal grounding. The Court's three-part proportionality test, requiring legality, legitimate aim, and proportionality for any state action infringing privacy, has since informed subsequent debate over surveillance legislation, data localisation requirements, and the scope of permissible government access to personal data, including in the design of exemptions under the DPDP Act relating to national security and law enforcement.

**Institutional Mechanisms and International Cooperation**

Institutionally, cybercrime prevention and investigation in India is coordinated principally through the Indian Cybercrime Coordination Centre, established by the Ministry of Home Affairs in January 2020 alongside the National Cyber Crime Reporting Portal, which provides citizens a centralised mechanism to report cyber offences, with particular institutional focus on crimes against women and children. The Indian Computer Emergency Response Team (CERT-In) additionally performs a technical coordination role concerning cybersecurity incidents and vulnerability reporting.

At the international level, India's cybercrime cooperation architecture remains comparatively underdeveloped relative to its domestic statutory framework. India has not acceded to the Budapest Convention on Cybercrime, notwithstanding its status as the principal binding multilateral instrument in this field, citing concerns regarding sovereignty and its exclusion from the Convention's original drafting process. India instead relies on a network of bilateral Mutual Legal Assistance Treaties and participation in the G7's 24/7 network of cybercrime contact points, while also engaging with parallel efforts at the United Nations to negotiate an alternative international cybercrime treaty. This divergence from the dominant international framework has practical consequences for cross-border evidence-gathering and extradition in cybercrime matters, an issue repeatedly flagged in the literature as a significant

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

constraint on effective prosecution of transnational cyber offences.

**Emerging Legal Challenges**

Several emerging challenges test the adequacy of the existing legal framework. First, the proliferation of generative artificial intelligence has given rise to new categories of harm, including deepfake-enabled fraud, voice-cloning scams, and AI-generated disinformation, for which existing statutory provisions, drafted with earlier technological paradigms in mind, provide at best an indirect and interpretively strained basis for prosecution. Second, the growth of cryptocurrency and decentralised financial systems has complicated the tracing and recovery of proceeds of cybercrime, an area in which regulatory clarity in India remains incomplete. Third, cloud computing and the cross-border storage of data raise persistent jurisdictional questions regarding which state's law governs access to evidence, a challenge that international frameworks such as the Budapest Convention were specifically designed to address, but from which India remains outside. Fourth, the tension between national security and law enforcement access to encrypted communications, on one hand, and the constitutional privacy protections articulated in *Puttaswamy*, on the other, continues to generate unresolved policy debate, particularly as the DPDP Act's exemptions for government processing are tested against constitutional proportionality standards. Finally, the phased implementation timeline of the DPDP Act, extending to May 2027, means that a substantial period of regulatory transition lies ahead, during which enforcement capacity, institutional design, and compliance practices across industry remain in active development.

**Discussion and Analysis**

The trajectory of India's cyber law framework demonstrates a pattern in which legislative and judicial responses have generally lagged behind the emergence of new technological harms, followed by a period of doctrinal consolidation once judicial or public pressure reaches a critical point, as seen in the progression from the IT Act's original text through the 2008 amendment, the *Shreya Singhal* correction, the *Puttaswamy* constitutional foundation, and finally the DPDP Act. This pattern suggests that cyber law reform in India has tended to be reactive rather than anticipatory, addressing harms after they have become sufficiently visible or contested rather than preemptively regulating emerging technology.

The persistence of prosecutions under the invalidated Section 66A years after the Supreme Court's ruling illustrates a recurring implementation gap between judicial pronouncement and administrative compliance, a concern that parallels similar enforcement deficits observed in other areas of Indian criminal procedure. Similarly, India's continued non-accession to the Budapest Convention, notwithstanding growing acknowledgment within policy circles of the practical costs of remaining outside the dominant international cooperation framework, reflects an unresolved tension between sovereignty concerns and the operational necessities of prosecuting inherently transnational cybercrime.

The DPDP Act and its associated Rules represent a significant maturation of India's legal response, translating the constitutional principle established in *Puttaswamy* into an operative statutory and institutional regime. However, its phased implementation timeline, extending several years beyond initial notification, means that its practical effectiveness cannot yet be comprehensively assessed, and questions regarding the scope of government exemptions and the

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

independence of the Data Protection Board remain subjects of ongoing scrutiny.

## Conclusion

India's legal response to cybercrime has evolved substantially since the enactment of the Information Technology Act, 2000, moving through significant judicial correction in *Shreya Singhal v. Union of India*, constitutional foundation-building in *Justice K.S. Puttaswamy v. Union of India*, and, most recently, the operationalisation of a comprehensive statutory data protection regime under the Digital Personal Data Protection Act, 2023. This evolution reflects a legal system actively grappling with the challenges posed by an increasingly digital society. Nevertheless, significant gaps persist: continuing enforcement of judicially invalidated provisions, the absence of accession to the principal international cybercrime cooperation instrument, and the still-unresolved legal treatment of emerging technologies such as generative artificial intelligence and cryptocurrency. Addressing these gaps will require not merely further legislative drafting, but sustained institutional capacity-building, closer international cooperation, and a continuing judicial commitment to ensuring that constitutional protections keep pace with the technologies that increasingly mediate everyday life.

## 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 (IJRSML), 11(10), 54–61. https://doi.org/10.63345/ijrsml.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.ijcrt.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/ijsra.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.ijcrt.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*

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): 3143-1070
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 11 – 20
https://jcclls.org/

*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 Technologies (SJAIBT), 1(2), Jun (1-9). https://doi.org/10.63345/sjaibt.v1.i2.301*