Governing the Data-Driven Bank: DPDPA 2023, IoT Security, and AI Accountability in India's Financial Sector

Dr. Kavita Jain[1], Mrs. Aabha Singh Gautam[2]
[1]Corresponding Author, OSD Assistant Professor, Secretariat
Department of Higher Education, Government of Madhya Pradesh, Bhopal, India
[2]Co-Author, Research Scholar

Abstract- ***Walk into any bank branch today and you will find technology doing things that were unimaginable a decade ago — sensors tracking footfall, algorithms deciding loan applications within seconds, and smart ATMs that can predict when they will run out of cash. Behind this transformation lies an enormous flow of personal data, and India's Digital Personal Data Protection Act (DPDPA) 2023 has arrived to govern it. This review paper asks a straightforward but consequential question: are India's banks ready to comply? Drawing on regulatory analysis, academic literature, and documented deployment evidence, the paper examines how DPDPA 2023's obligations intersect with the IoT infrastructure and AI systems that now underpin banking operations. We identify five governance gaps and propose a practical five-pillar Data Governance Integration Model (DGIM) that banks can begin adopting today. The paper also surfaces a harder truth: compliance with the letter of the law will not be enough. Banks must embrace privacy as a design value, not a legal checkbox, if they are to earn the trust of the millions of data principals whose financial lives they increasingly mediate through algorithms.***

Keywords: ***DPDPA 2023; Data Governance; Banking; AI; IoT; Data Fiduciary; Algorithmic Accountability; India; Privacy by Design; Fintech***

I. INTRODUCTION

Think about the last time you used your bank's mobile app. You checked your balance, maybe transferred money, and perhaps got a nudge to take a personal loan — a nudge generated not by a human banker who knows you, but by an algorithm that has quietly studied your transaction patterns for months. Now imagine you are a farmer in rural Madhya Pradesh receiving a PM-KISAN payment through a government-linked bank account. The system that routed that payment, verified your identity, and flagged your account for compliance screening processed dozens of data points about you in the time it takes to blink.

This is the reality of modern banking in India. And it raises a question that is as urgent as it is underexplored: who is responsible for all that data, and what rights do you have over it?

The Digital Personal Data Protection Act (DPDPA) 2023 is India's answer. Enacted in August 2023, it is the country's first comprehensive personal data protection law, and its implications for the banking sector are profound. Banks are data fiduciaries in the truest sense — they hold not just financial information but biometric records, behavioural profiles, and family financial histories for hundreds of millions of citizens. DPDPA 2023 now requires that this data be collected with clear consent, used only for stated purposes, kept no longer than necessary, protected with reasonable security measures, and made accessible and correctable upon the customer's request.

Meeting these obligations is not straightforward when a bank's operations depend on thousands of IoT devices collecting ambient data and dozens of AI models making automated decisions. This review paper maps the terrain — examining where DPDPA 2023's requirements create the most significant governance challenges in banking's IoT and AI environments, and proposing a practical framework for how banks can respond. Our goal is not to

catalogue problems but to offer a roadmap that practitioners can actually use.

II. LITERATURE REVIEW AND REGULATORY CONTEXT

2.1 What DPDPA 2023 Actually Requires of Banks

It is worth being concrete about what the law demands, because the gap between aspiration and operational reality is where governance fails. Section 4 of DPDPA 2023 establishes that personal data may only be processed for a lawful purpose, with the data principal's consent or under specified legitimate use cases. For a bank, this covers virtually every interaction with a customer — from opening an account to assessing creditworthiness to flagging a transaction as suspicious.

The Act's category of 'Significant Data Fiduciaries' is particularly important. Entities designated under this category — and large commercial banks processing data for tens of millions of customers are obvious candidates — face heightened obligations: mandatory Data Protection Impact Assessments (DPIAs), appointment of a Data Protection Officer, and periodic audits. Yet as of early 2026, the Data Protection Board of India has not yet published the criteria for this designation, leaving banks in a state of compliance uncertainty that is itself a governance risk.

The Reserve Bank of India's Master Direction on IT Governance (2023) adds a further layer, requiring robust oversight of third-party vendors and cloud service providers. This creates a compliance architecture that is genuinely layered: banks must satisfy both the RBI's information security framework and DPDPA's data rights framework, even where the two instruments do not perfectly align. Navigating this layered structure requires legal and technical coordination that most banks are still developing.

2.2 AI in Banking: Impressive Capabilities, Incomplete Governance

Artificial intelligence has moved from the periphery to the core of banking operations with remarkable speed. A landmark IJIRT study by Singh, Gupta, Vashisth, and Bhardawaj (2025) on privacy-preserving challenges in ubiquitous computing systems — directly relevant to banking's AI and IoT deployments — identifies that while methods such as differential privacy, federated learning, and homomorphic encryption offer powerful tools for protecting user data in interconnected AI environments, each carries significant implementation challenges including high computational costs, scalability constraints, and regulatory complexities that governance frameworks must address [1]. Their work underscores that technical capability alone is insufficient: institutions need institutional frameworks that embed privacy obligations into the design and deployment of AI systems, not merely into their post-hoc oversight.

Madheswaran, Gore, and Gupta (2024), writing in IJCRT, document the tangible benefits AI delivers in banking — reduced transaction times, improved fraud detection, better customer retention — while emphasising that these benefits intensify, rather than diminish, the governance obligations they trigger [2]. Their survey of ten operational banks found that the institutions deriving the greatest operational value from AI were also those facing the most complex data governance challenges. This paradox — that success with AI creates more governance complexity, not less — is one the Indian banking sector has not yet fully reckoned with.

The practical upshot is that many Indian banks have deployed AI systems that make consequential decisions — approving or rejecting loans, freezing accounts, generating risk scores — without the explainability infrastructure that DPDPA 2023's grievance redressal provisions implicitly require. A customer who is denied a loan by an algorithm has a right to understand why. Most banks currently cannot answer that question in any meaningful way.

2.3 IoT in Banking: Data Everywhere, Governance Nowhere

The IoT footprint of a modern Indian bank is larger than most people realise. Smart ATMs with predictive maintenance sensors, branch cameras with computer vision capabilities, contactless payment terminals, wearable payment devices, and biometric authentication systems at entry points — each of these generates a continuous stream of data, much of it personal or personally identifiable.

What makes IoT governance particularly difficult is the passive nature of data collection. A customer walking into a branch and being captured by a facial recognition camera has not consented to that capture in any meaningful sense. The data generated — biometric identifiers, location timestamps, behavioural patterns — may flow through multiple systems and vendors before it reaches the bank's core infrastructure, traversing jurisdictions in ways that potentially violate DPDPA's data localisation requirements.

The fragmented, heterogeneous nature of IoT ecosystems — where a single branch may have devices from a dozen different manufacturers running different firmware versions with different security profiles — makes centralised governance genuinely difficult. Most Indian banks have not yet conducted a comprehensive audit of their IoT data flows, let alone mapped those flows to DPDPA's consent and purpose-limitation obligations.

2.4 The Multi-Regulator Problem

Banks do not operate in a single regulatory environment. The RBI governs core banking operations. SEBI's cybersecurity framework applies to capital market activities. IRDAI governs bancassurance data. The National Payments Corporation of India sets data standards for payment systems. And now the Data Protection Board of India will administer DPDPA 2023. Each of these regulators has legitimate authority over aspects of a bank's data environment, but their frameworks were developed independently and do not always align.

This multi-regulator complexity is not merely an administrative inconvenience — it is a substantive governance risk. When a breach occurs, which regulator does the bank notify first? When a customer exercises their DPDPA right to erasure, what happens to data the RBI requires the bank to retain for audit purposes? These tensions are real, and they require coordinated regulatory guidance that has not yet arrived.

III. IOT DATA GOVERNANCE: WHERE THE GAPS ARE SHARPEST

3.1 The Consent Problem in Device-Mediated Environments

DPDPA 2023 sets a high standard for consent: it must be free, specific, informed, unconditional, and unambiguous. This standard is achievable — if demanding — in a conventional digital interaction where a customer fills in a form and ticks a box. It becomes considerably harder when data is generated by a sensor the customer may not even know is there.

Consider what happens when a customer approaches a smart ATM. Before they insert their card, the machine may have already captured a facial recognition scan, logged their approach pattern, and transmitted ambient sensor data to a third-party maintenance system. None of this was consented to. None of it is straightforward to un-consent from. And yet all of it constitutes personal data processing under DPDPA 2023.

Banks must build IoT-specific Data Protection Impact Assessment (DPIA) processes that trace exactly what data each device captures, where it flows, who can access it, and how long it is retained. This is painstaking work, but it is the only foundation on which a defensible consent architecture can be built. The good news is that this exercise often reveals data collection that serves no genuine operational purpose — presenting an opportunity for data minimisation that reduces both compliance risk and storage costs.

3.2 Security: The Weakest Link is Often the Smallest Device

The security obligations under DPDPA 2023 — requiring 'reasonable security safeguards' — may sound modest, but in an IoT environment they demand considerable technical sophistication. A single compromised IoT device can serve as an entry point into a bank's broader network. An unpatched ATM firmware vulnerability, a misconfigured surveillance camera, a payment terminal with default credentials left unchanged — any of these can be the vector through which customer data is exfiltrated at scale.

Effective IoT security governance in banking requires end-to-end encryption of device communications, rigorous firmware management protocols, network

segmentation that isolates IoT traffic from core banking systems, and incident response procedures specifically designed for device-originating breaches. The breach notification timeline under DPDPA 2023 is not yet fully specified by the Data Protection Board, but international benchmarks (72 hours under GDPR) suggest banks must be able to detect, assess, and report IoT-originated breaches with considerable speed. Most are not yet positioned to do so.

IV. AI ACCOUNTABILITY: THE EXPLANATION GAP

4.1 When the Algorithm Won't Explain Itself

Imagine you are a small business owner in Bhopal who has banked with the same institution for fifteen years. You apply for a working capital loan to expand your operation. The bank's AI model processes your application in three seconds and returns a rejection. You ask why. The relationship manager shrugs and says the 'system' flagged you. You have no idea what factors the model weighted, whether your application was treated fairly, or how you could improve your chances.

This scenario plays out across India every day, and it represents a direct conflict with the data principal rights embedded in DPDPA 2023. The Act's provisions on automated decision-making, read alongside its grievance redressal requirements, establish that customers have a right to meaningful redressal for decisions made about them by automated systems. Meaningful redressal requires explanation. And explanation requires that the AI model be interpretable.

Banks using deep learning models for credit scoring face a genuine technical challenge here. These models often achieve higher predictive accuracy than simpler alternatives, but they do so by learning patterns in high-dimensional data that resist intuitive human interpretation. The governance response must be proportionate to the stakes: for high-consequence decisions (loan rejections, account freezes, fraud designations), banks should require that AI outputs be accompanied by human-interpretable explanations generated by tools such as SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-Agnostic Explanations). For lower-stakes decisions, interpretable-by-design models (logistic regression, decision trees) may be sufficient.

4.2 Bias in the System: Who Gets Left Behind

AI models trained on historical banking data carry the legacy of historical banking discrimination. Women, farmers, informal-sector workers, and residents of rural or economically disadvantaged regions have historically been underserved by formal credit systems. A model trained on past lending decisions will encode these patterns — not because the model is malicious, but because it is learning from data that reflects a world we are trying to change.

DPDPA 2023's non-discrimination provisions, together with the RBI's fair lending framework, create a legal obligation to detect and mitigate these biases. This is not merely a legal requirement — it is a social imperative for a banking sector that aspires to serve all of India's citizens equitably. Banks should conduct quarterly disparity audits of their AI models, establish protected attribute baselines, document bias mitigation interventions, and report material fairness findings to their Boards. The technical tools exist. What is currently lacking is the institutional will to deploy them systematically.

4.3 The Vendor Accountability Gap

Perhaps the most underappreciated governance challenge in banking's AI environment is vendor accountability. A large share of the AI capability deployed in Indian banking is provided by third-party vendors — cloud AI platforms, fintech partners, credit scoring agencies. When a vendor's model produces a discriminatory output or its system experiences a data breach, the customer doesn't blame the vendor. They blame the bank.

DPDPA 2023 is clear on this point: the data fiduciary (the bank) remains accountable for data processing carried out by data processors (vendors) on its behalf. This means banks must extend their governance frameworks to cover the full vendor ecosystem — negotiating audit rights, requiring transparency about model updates, establishing data deletion protocols, and specifying breach notification timelines in every AI vendor contract. This is a significant operational challenge, particularly for banks that have accumulated dozens of vendor relationships over years

of digital transformation without corresponding governance infrastructure.

V. A GOVERNANCE FRAMEWORK FOR THE DATA-DRIVEN BANK

Based on the analysis above, we propose a five-pillar Data Governance Integration Model (DGIM). The framework is designed to be practical — something a bank's Chief Data Officer and Chief Compliance Officer can actually use — rather than merely aspirational. Each pillar addresses a specific governance gap identified in the review and is anchored to a specific DPDPA 2023 obligation.

Table 1: Data Governance Integration Model (DGIM) — Banking Sector Application

Pillar	DPDPA 2023 Obligation	IoT Application	AI Application
1. Consent Architecture	Free, specific, informed consent; withdrawal mechanisms	Device-level DPIA; passive data capture disclosure	Opt-out from AI profiling; explainable consent flows
2. Data Minimisation	Collect only data necessary for the stated purpose	Audit and disable excess IoT data streams	Feature selection governance in ML pipelines
3. Algorithmic Accountability	Right to explanation; grievance redressal for automated decisions	IoT anomaly detection audit trails	SHAP/LIME explainability; quarterly bias audits
4. Security & Breach Response	Reasonable safeguards; breach notification obligations	Network segmentation; firmware governance; encryption	Model access controls; adversarial monitoring
5. Vendor Governance	Fiduciary accountability for processor/vendor actions	IoT vendor audit rights; data deletion SLAs	Third-party AI transparency; fairness audit rights

Source: Authors' compilation

5.1 How to Sequence Implementation

Not every bank will be able to implement all five pillars simultaneously, and they should not try. The DGIM is designed for phased adoption. In Year 1, banks should prioritise Pillars 1 (Consent Architecture) and 4 (Security and Breach Response) — these carry the most immediate regulatory exposure and the clearest operational anchors. Year 2 should address Pillars 2 (Data Minimisation) and 3 (Algorithmic Accountability), which require deeper technical investment. Full Pillar 5 (Vendor Governance) integration — involving contract renegotiation and audit infrastructure build-out — realistically requires until Year 3.

Smaller regional and cooperative banks, which lack the technical teams of the large commercial banks, should prioritise a DPIA exercise as their first governance investment. A thorough DPIA will surface the most significant compliance risks and create the data flow maps on which all subsequent governance work depends. The Indian Banks' Association could significantly reduce compliance costs by providing standardised DPIA templates and IoT security baseline frameworks for smaller institutions.

VI. Discussion: Privacy by Design, Not by Decree

The central argument of this paper is simple but important: DPDPA 2023 compliance in banking cannot be achieved through legal review alone. It requires a governance culture in which data protection obligations are embedded into the design of technology systems from the outset — a principle that

privacy scholars call 'privacy by design,' and that Indian banking urgently needs to adopt.

Consider the alternative. A bank that treats DPDPA compliance as a legal checkbox will conduct a review, update its privacy policy, appoint a Data Protection Officer, and consider the job done. But its AI models will continue to produce unexplained rejections. Its IoT devices will continue to collect data that serves no clear purpose. Its vendor contracts will continue to lack adequate audit rights. When the Data Protection Board eventually takes enforcement action — and it will — this bank will be exposed.

The banks that will navigate the DPDPA era successfully are those that ask different questions when deploying new technology. Not 'can we collect this data?' but 'should we collect this data, and can we explain why to the customer whose data it is?' Not 'does our AI model predict accurately?' but 'can we explain its decisions to the people they affect?' These are not just compliance questions — they are questions about what kind of institution a bank wants to be.

Four concrete policy recommendations follow from this analysis. First, the RBI should issue sector-specific DPDPA implementation guidance clarifying obligations for AI-driven credit decisions, IoT data streams, and cross-border cloud deployments. Second, the Data Protection Board should designate major commercial banks as Significant Data Fiduciaries without further delay. Third, banks should establish Board-level AI and Data Governance Committees with explicit DPDPA compliance mandates. Fourth, the Indian Banks' Association should develop shared industry toolkits — DPIA templates, IoT security baselines, AI explainability protocols — to level the compliance playing field for smaller institutions.

VII. CONCLUSION

India's banks stand at a crossroads. The data they collect, the AI systems they deploy, and the IoT infrastructure they operate have made them extraordinary engines of financial service delivery. They have also made banks the custodians of an unprecedented volume of sensitive personal data about hundreds of millions of citizens. DPDPA 2023 has arrived to hold them accountable for that custodianship.

This review has argued that accountability cannot be achieved through compliance alone. It requires a governance philosophy that treats data protection not as a constraint on innovation but as a foundation for trust — and trust, in banking, is not a soft benefit but a core business asset. The Data Governance Integration Model proposed here offers a practical pathway: five pillars, modular implementation, grounded in real regulatory obligations and real operational challenges.

The farmer in rural Madhya Pradesh whose loan application is assessed by an algorithm deserves to know why it was approved or rejected. The small business owner whose account was flagged for fraud deserves an explanation. The customer whose biometrics were captured by a bank's ATM camera deserves to know that data is being protected. DPDPA 2023 has given them these rights. The question now is whether India's banks will meet them with the governance infrastructure those rights deserve.

REFERENCES

[1] Singh, R., Gupta, A., Vashisth, V., & Bhardawaj, H. (2025). Theoretical Challenges in Privacy-Preserving Ubiquitous Computing Systems. *International Journal of Innovative Research in Technology (IJIRT)*, Volume 11, Issue 12, pp. 823–831. ISSN: 2349-6002. Retrieved from ijirt.org/publishedpaper/IJIRT177583_PAPER.pdf

[2] Madheswaran, Y., Gore, M. P., & Gupta, N. (2024). Revolutionizing Banking Operations Through AI-Enhanced Cloud Technologies. *International Journal of Creative Research Thoughts (IJCRT)*, 12(11), b904–b915. ISSN: 2320-2882. Retrieved from ijcrt.org/papers/IJCRT2411212.pdf

[3] Ministry of Electronics and Information Technology, Government of India. (2023). *Digital Personal Data Protection Act, 2023*. New Delhi: Government of India.

[4] Reserve Bank of India. (2023). *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*. Mumbai: RBI.

[5] Manoharan, G. (2024). Data Governance Frameworks for AI Implementation in Banking: Ensuring Compliance and Trust. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 15(3), 101–109.

[6] NITI Aayog. (2021). *Responsible AI for All: Adopting the Framework*. New Delhi: Government of India.

[7] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges. *Information Fusion*, 58, 82–115.

[8] Lundberg, S. M., & Lee, S. I. (2017). A Unified Approach to Interpreting Model Predictions. *Advances in Neural Information Processing Systems*, 30, 4765–4774.

[9] Bokhari, S. A. A., & Myeong, S. (2023). The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities. *Sustainability*, 15(9), 7520.

[10] Patel, B. (2023). IoT Security Risks and the Future of Cybersecurity in India. *Journal of Emerging Technologies and Security*, 8(2), 201–215.