Int. Comp. Tech. & Sci. J.
ISSN : 3139-146X | Vol 1, Issue 1, Oct – Dec, 2025

PUBLISHED BY
ERUDEXA PUBLISHING

Review & Perspective Article

Received: 22 Oct 2025 | Accepted: 25 Nov 2025 | Published: 18 Dec 2025

Beyond GDPR: The Architectural Challenge of Data Sovereignty and Confidential Computing in the Post-2024 Era

Mr. Tayabur Rahman Laskar

Freelancer, BCA Graduate, Gauhati University, Assam

ORCID: https://orcid.org/0009-0009-0241-5123

DOI: https://doi.org/10.5281/zenodo.19918374

Abstract

As organizations migrate legacy datasets to cloud-native architectures, the tension between Big Data analytics and data privacy regulations has reached a critical inflection point. With the full operationalization of India's Digital Personal Data Protection (DPDP) Act in 2025 and the tightening of GDPR enforcement, the concept of "Data Sovereignty" has evolved from a legal footnote to a primary architectural constraint. This paper reviews the limitations of traditional "encryption-at-rest" standards in the face of these new laws. We analyze emerging solutions, specifically **Confidential Computing** (using hardware-based Trusted Execution Environments) and **Federated Learning**, which promise to decouple data processing from data visibility. Market analysis suggests the Confidential Computing sector alone will expand to over USD 14 billion by late 2025. We argue that the future of software engineering lies not in centralized data lakes, but in decentralized, privacy-preserving compute fabrics.

Keywords: Data Sovereignty, DPDP Act 2023, Confidential Computing, Federated Learning, GDPR, Cloud Security, Big Data Governance.

1. Introduction

The promise of Big Data has traditionally been predicated on centralization: aggregating vast amounts of information into "Data Lakes" to extract insights. However, the geopolitical and legal landscape of 2024–2025 has fundamentally fractured this model.

The introduction of India's *Digital Personal Data Protection (DPDP) Act, 2023*—and its subsequent rule notifications in 2025—has created a stringent framework where the "sovereignty" of data is paramount. Similarly, the European Union's GDPR continues to impose heavy fines for cross-border data leakage. For the computer science community, this presents a unique challenge: How do we design distributed systems that are efficient enough for real-time analytics but rigid enough to respect national borders?

This paper reviews the technical shifts required to survive in this new regulatory environment, moving beyond simple encryption to "Privacy-Preserving Computation."

2. The Failure of Traditional Encryption

Historically, data privacy was handled via two mechanisms:

1. **Encryption at Rest:** Protecting data when stored on a disk (e.g., AES-256).
2. **Encryption in Transit:** Protecting data moving over the network (e.g., TLS 1.3).

2.1 The "Data in Use" Gap

The vulnerability lies in the third state: **"Data in Use."** To analyze data—whether for training a Machine Learning model or running an SQL query—it must typically be decrypted in the server's Random Access Memory (RAM). This brief window of decryption creates a vector for attack and a potential violation of strict privacy laws if the server is located in a non-compliant jurisdiction or accessible by the cloud provider's administrators.

3. The Rise of Confidential Computing

To address the "Data in Use" problem, the industry is shifting toward **Confidential Computing**. This paradigm utilizes hardware-based Trusted Execution Environments (TEEs), such as Intel SGX (Software Guard Extensions) or AMD SEV (Secure Encrypted Virtualization).

3.1 Mechanism of Action

TEEs create a secure "enclave" within the CPU. Data is decrypted only inside this hardware-isolated enclave, processed, and then immediately re-encrypted before leaving the CPU. This ensures that the cloud provider (e.g., AWS, Azure, or Google Cloud) never has technical access to the raw customer data, solving the "trust" issue in public clouds.

3.2 Market Adoption

Recent industry reports from 2025 indicate that the global Confidential Computing market is undergoing explosive growth. Valued at approximately USD 9.04 billion in 2024, it is projected to reach USD 14.84 billion by the end of 2025, driven largely by the BFSI (Banking, Financial Services, and Insurance) and Healthcare sectors. This suggests that "enclave-based processing" is becoming a standard deployment target for high-value software.

4. Federated Learning: Moving the Model, Not the Data

For Artificial Intelligence applications, moving massive datasets to a central server is becoming legally risky under the DPDP Act. **Federated Learning (FL)** offers a decentralized alternative.

1. **Local Training:** Instead of uploading user photos or financial logs to a server, a lightweight AI model is sent to the user's device (or a local edge server).
2. **Update Aggregation:** The model learns from local data and sends only the *mathematical updates* (weights/gradients) back to the central server, not the raw data itself.
3. **Privacy Implications:** This technique is crucial for compliance, as it ensures that personal identifiers never leave the user's control. However, as noted in recent reviews (2025), FL is

not a silver bullet; it requires protection against "gradient leakage" attacks where attackers try to reverse-engineer data from the model updates.

5. Conclusion

The era of "capture everything, sort it later" is over. The *International Comprehensive Technology and Science Journal* recognizes that the future of Big Data is inextricably linked to privacy engineering. For freelance developers and system architects, this means that knowledge of legal frameworks (like the DPDP Act) is now as essential as knowledge of database schemas. The adoption of Confidential Computing and Federated Learning is not merely a trend but a necessary evolution. We are moving toward a "Zero Trust" data lifecycle where the software engineer's goal is to prove that they *cannot* see the user's data, rather than promising they won't look at it.

Article Publication Details
This article is published in the **International Comprehensive Technology and Science Journal**, ISSN 3139-146X (Online). In Volume 1 (2025), Issue 1 (October-December)
The journal is published and managed by **Erudexa Publishing**.

Acknowledgements
We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

Data availability
No datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable. This study did not involve human or animal subjects.

Funding
The authors declare that no funding was received for this work.

Competing interests
The authors declare that they have no competing interests.

References

1. Government of India, "The Digital Personal Data Protection Act, 2023," *The Gazette of India*, Aug. 2023. (Notified Rules 2025).
2. Precedence Research, "Confidential Computing Market Size to Hit USD 1281.26 Bn by 2034," *Global Market Insights*, Jan. 2025.

3. S. Saha et al., "A multifaceted survey on privacy preservation of federated learning: Progress, challenges, and opportunities," *Artificial Intelligence Review*, vol. 57, no. 1, 2024.
4. H. Schwarz, "Comprehensive Review on Privacy-Preserving Machine Learning Techniques," *Edu Journal of International Affairs and Research*, vol. 3, no. 2, 2024.
5. Endor Labs, "The Most Common Security Vulnerabilities in AI-Generated Code," *Endor Labs Research Blog*, Aug. 2025.

Publisher's Note