IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Privacy-Driven Data Architecture in Fintech Platforms: A Comparative Study under GDPR, DPDP, and U.S. State Laws

[1]Sunil Biriya, [2]Umadevi Ramamoorthy
[1]MCA Student, [2] Associate Professor
[1]School of Science and Computer Studies,
[1]CMR University, Bengaluru, India

Abstract: Data privacy is of great concern as fintech grows because financial information is sensitive, and the number of digital transactions is increasing. This paper puts in comparison the three prime data protection models which are the General Data Protection Regulation (GDPR) in the EU, the Digital Personal Data protection (DPDP) Act in India and the United States sector-specific legislation including HIPAA and CCPA. It studies the implications of such models of laws on the design of IT systems in fintech platforms and data architecture. GDPR is rights, rights based, and extraterritorial in nature, as well as global in scope, implying especially rigid adherence to its requirements even on the part of U.S. companies. India DPDP is based on some principles of the GDPR but incorporates such specific requirements as presumed consent and child data protection. Conversely, the U.S. does not have a single law, and therefore there are scattered compliance strategies. In this paper, it has been indicated that despite the laws gaining more transparency, privacy policies are more extensive and difficult to comprehend. To designers of IT systems, this will entail a complex regulatory environment that will require solid principles, such as Privacy by Design, routine Data Protection Impact Assessments (DPIAs) and applications of technologies, including blockchain, to achieve better accountability. The study says that adaptive and privacy-oriented design of systems is necessary in order to address the compliance requirements of different people across the globe and various enforcement issues that are dynamic.

Index Terms: **Data Privacy, Fintech, GDPR, DPDP, U.S. Privacy Laws.**

I Introduction

At their basis, Fintech platforms make use of technology to provide financial solutions, which include but are not limited to mobile banking, online lending, digital payments, blockchain finance and AI tool-driven investments (Reis, et al., 2024). Such systems presuppose gathering, processing, and storage of large volumes of confidential and personal financial information, such as their transaction history, their identification, and the patterns of their behavior. As a result, data privacy is not only just something that companies must do to satisfy legal requirements but the primary prerogative to building user trust and maintaining the integrity of the entire financial system (Reis, et al., 2024). The loss of privacy of such industry may result in serious financial exploits, appropriation of identity, and loss of badges, therefore, underscoring the essence of strong privacy protection mechanisms.

The internationalization of fintech business implies that such services have to move through a complicated and even contradictory system of compliance norms in various jurisdictions. Certain obligations and

principles of the General Data Protection Regulation (GDPR) in the European Union (Zhang, et al., 2024), the Digital Personal Data Protection (DPDP) Bill, and the state-level and sector-specific privacy laws of the United States (Bakare, et al., 2024; Oyewole, et al., 2024) differ and include consent measures and the right of data subjects, cross-border transfers of data and breach notification procedures (Bakare, et al., 2024; Oyewole, et al., 2024; Lim, Oh, 2025). Such fragmentation poses severe risks to fintech companies attempting to adhere to a high level and coordinated compliance as the GDPR is extraterritorial in nature (Ryngaert and Taylor, 2020) and thus can potentially extend its jurisdiction to countries outside of the EU (Davis and Marotta-Wurgler, 2024).

Although there is an increasingly large amount of work on individual privacy laws and the technological side of fintech, a significant research breach still exists in terms of directly linking these legal systems with their implications in the IT system design and data structure. The papers focus either on the effects of laws on privacy policy (Custers, et al., 2017) or the use of a particular technology to enforce them (Singh, 2024; Barati and Rana, 2022), but not many investigate how various legal theories can be applied to specify the implementation detail of data handling, storage and processing in an architectural detail. The latter lack usually leaves the IT system designers without specific advice on how to merge the legal requirements with the scalable and secure technical implementation.

Such paper shall fill this existential knowledge gap by offering a comparative study between the GDPR, the Indian DPDP Bill, as well as the laws of the U.S., with particular reference on what each implies directly on data architecture and IT system design of fintech platforms. Our main goals concern:

- To find the main differences and fundamental principles regarding these three significant privacy frameworks.
- Structuring the way that these differences dictate different or convergent protocols of data gathering, processing, storing and transport inside the IT systems.
- Outlining technical issues and chances of developing privacy-compliant fintech solutions.
- Provides useful lessons to IT systems designers on the ways to make their data architecture more secure and legally sound.

Our findings are a consolidated view as to why the multi-jurisdictional aspect of privacy compliance is a problem that fintech must contend with, a thorough account of the translation practice in the legal-technical translation direction, and a system to analyze the design choices based on the given regulatory requirements. The rest of this paper will be organized in the following manner: in section 2, some background concerning the GDPR, Indian DPDP Bill, and U.S. privacy is given. The section 3 states the methodological approach employed in comparative analysis. The results of the implications on the data architecture and system design are stated in Section 4. Lastly, Section 5 puts a conclusion to the paper and proposes future research tasks.

II Literature Review

The spread of digital technology and the growing importance of personal information have brought about the emergence of complicated laws that are geared towards safeguarding personal privacy. In this section, the literature regarding key data privacy regulations, privacy engineering practices, data architecture and multi-jurisdictional compliance activities is reviewed and the gaps that will be filled by this study are outlined.

Overview of Major Data Privacy Regulations

General Data Protection Regulation (GDPR) The GDPR (Zhang, et al., 2024), adopted by the European Union and adopted on May 25, 2018, has been called one of the strictest and most comprehensive data protection regulations in the world (Ryngaert and Taylor, 2020). It focuses on rights-based approach, in which individuals exert a lot of control over their data. They are lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability (Zhang, et al., 2024). Other more particular provisions of the GDPR included the requirement of Data Protection Impact Assessment (DIPA) in cases of high-risk processing operations (Naqvi and Batool, 2023), nomination of Data Protection Officer (DPOs) (Chintoh, et al., 2025), and stringent high standards on collected consent (Zhang, et al., 2024). Its extraterritorial nature i.e. it applies to any

organization that processes data belonging to our EU citizens regardless of location has greatly contributed to data protection laws being adopted across countries (Ryngaert and Taylor, 2020; Davis and Marotta-Wurgler, 2024). Research has demonstrated that it has had significant effect on business practices such as data storage and computation work procedures (Demirer, et al., 2024) and that it has influenced global debates on the privacy policies (Amoo, et al., 2024).

Digital Personal Data Protection (DPDP) Bill, by India, is arguably a major tread to an uber-regime of data protection in a digital market that is the largest in the world (Bakare, et.al, 2024; Oyewole, et al., 2024). Although inspired by GDPR, special notions aimed at serving the Indian setting are presented in the DPDP Bill. Among them are the introduction of the concept of a "Data Fiduciary" (equivalent to the controller in GDPR) and "Data Principal" (equivalent to data subject in GDPR), as well as something unknown in GDPR, namely the concept of called a "deemed consent" to certain legitimate uses thereof (Bakare, et al., 2024; Oyewole, et al., 2024). The Bill also classifies "Significant Data Fiduciaries" that will have added-on responsibilities and, the Bill envisages a special set regarding the data of children with the age of consent stipulated at 18 (Magalhães, 2021). The similarities and differences are pointed out in acts of comparison especially on data localization, cross-border transfer data procedure and enforcement fines (Bakare, et al., 2024; Oyewole, et al., 2024).

U.S. State Laws (e.g., CCPA/CPRA) Unlike the all-inclusive approach practiced by the EU, the U.S traditionally uses a sectoral and state by- state approach to privacy (Bakare, et al., 2024; Oyewole, et al., 2024; Lim and Oh, 2025). Major federal regulations are the Health Insurance Portability and Accountability Act (HIPAA) with regard to health information and the Children Online Privacy Protection Act (COPPA). Nevertheless, efforts at the state or municipal government levels, especially that of the California Consumer Privacy Act (CCPA) of 2018, have gone a long way towards protecting consumer privacy in the U.S. (WONG, et al., 2023). The CCPA provides the Californians with similar rights to GDPR data subjects such as the right to know, delete and opt-out the sale of the personal information (WONG, et al., 2023). Several other rights were increased, and the CCPA was amended and supplemented by the California Privacy Rights Act (CPRA) and an apparatus to enforce it (the California Privacy Protection Agency (CPPA)) passed in 2020. Several other states such as Virginia (Virginia Consumer Data Protection Act - VCDPA) and Colorado (Colorado Privacy Act - CPA) have since done the same, which is a patch of rules that makes it in some areas difficult to conduct business across the country (Bakare, et al., 2024). The transfer of influence created by GDPR has been studied, with the transfer frequently resulting in companies implementing more harmonious policies in the U.S. (Davis and Marotta-Wurgler, 2024; Amoo, et al., 2024).

Prior Work on Privacy by Design Principles

Privacy by Design (PbD), originally proposed by Ann Cavoukian, advocates privacy protection through system and architectural design and business processes early in the design phase, not as an addition on (TSOHOU, et al., 2020). This front-running process is a premise tenet of the GDPR (Article 25) (Rohendi and Kharisma, 2024) and is beginning to become a recognized tenet in other privacy systems as well. The seven principles underlying PbD present in literatures are proactive not reactive; privacy as the default; privacy embedded into design; full functionality; end to end security; visibility and transparency; and respect of user privacy (TSOHOU, et al., 2020). Some research into methodologies and tools to apply PbD has been done on formal modeling techniques (Torre, et al.), the design of frameworks around privacy engineering (PIRAS, et al., 2019), and into incorporating privacy requirements in software development lives (TSOHOU, et al., 2020). Nevertheless, how to implement such lofty principles into practical reality in form of concretely actionable activities on the part of IT architects and developers working in more or less different kinds of systems is a matter of concern(Torre, et al.; Dorfleitner, et al., 2023).

Data Architecture in IT Systems (especially Fintech) Data architecture identifies the methods an organization gathers, stores, evaluates, unites and employs its data. This is especially crucial in the fintech industry, where the financial data is large, fast, and diverse, voluminous, and subject to strict security and compliance requirements (Reis, et al., 2024; Aldboush and Ferdous, 2023). The previous research is related

to scalable databases, secure protocols of data transmission, fraud detection systems and the application of cloud computing in the area of financial services (Shah, 2023; Dorfleitner, et al., 2023). The effects of regulatory compliance on data architecture have been a recurring trend, especially with regards to the data localization demands and cross-border data flows (Politou, et al., 2018). Blockchain technology would also be tested to provide a solution towards having the higher levels of immutability of data, transparency, and decentralization of identity management, which can help achieve GDPR compliance (Singh, 2014; Barati and Rana, 2022). Even with this movement, data architecture has been frequently talked about in terms of performance or security, rather than in terms of how specific details of the privacy regulation (e.g., different consent granularities, rights of data subjects in different jurisdictions) translate into architectural decisions beyond mere alignment with security codes.

Multi-Jurisdiction Compliance Studies There are a number of publications that lend insight into multi-jurisdictional data privacy compliance complexities. It is also typical to compare GDPR to other regional legal frameworks (e.g., Asian, Latin American, African legislations) and to discuss the "GDPR effect," or the fact that it serves as a global standard setter (Kumar, 2023; Ryngaert and Taylor, 2020; Lim and Oh, 2025). There is also a research on difficulties that are associated with multinational corporations aligning opposite legal demands, especially regarding data transfer machineries and dissimilar definitions of personal data (Politou, et al., 2018). Various studies refer lightly to the phenomenon of the so-called spillover of GDPR in which firms or non-European companies change their habits to comply with GDPR in order to avert legal implications or create an image of a company competent on GDPR (Davis and Marotta-Wurgler, 2024; Amoo, et al., 2024). Yet, there still exists a major research gap on profoundly uniting the analysis of law with the practical implications on IT system designing. Although the problem of compliance has been well-documented (Zaguir, et al., 2024; Voss and Houser, 2019), little is written regarding how IT system designers should go about architecting systems in a way which would be naturally compliant with differing legal interpretations of data subject rights, consent models, and definitions of personal data across multiple jurisdictions and regulatory regimes.

Gaps Justifying This Research

The review recognizes the existing research gaps that provide a rationale for this study:

- Lack of direct translation of legal requirements into technical specifications: PbD has established principles, and guidance is needed on translating granular legal requirements from multiple regulation sources (GDPR, DPDP, U.S. laws) into architectural patterns and design decisions in fintech IT.
- Lack of substantive detail of the architectural implications of regulatory divergence: studies on data privacy in multi-jurisdictional contexts have focused on legal differences. The studies rarely distinguish mindfully or define how the identified legal differences translate into architectural distinctions regarding data models, access controls, data lifecycle management, or processing logic.
- Lack of architectural guidance specifically on fintech: fintech has been well identified as being data sensitive. The architectural guidance available that speaks specifically to data privacy principles addressing the finer nuances of different privacy laws in a financial realm is lacking.
- Operationalizing consent and data subject rights: research on practical architectural solutions for managing dynamic consent preferences, and fulfilling data subject rights (e.g., right to erasure, data portability) across multiple, contrasting regulatory regimes that are also jurisdictional, is scanty.

Therefore this study proposes to fill the gaps identified by the review by providing thematized comparative analysis that offers concrete input to inform IT system design in fintech with particular reference to the architectural implications of the GDPR, Indian DPDP Bill, and U.S. privacy laws on system design.

III Proposed Methodology

In the current research, a qualitative, comparative approach is applied to evaluate the impact of data privacy policies and regulations, that is, the General Data Protection Regulation (GDPR) in the EU, the Digital Personal Data Protection (DPDP) Act in India, and various state-level regulations of data protection, such as the California Consumer Privacy Act (CCPA), in the U.S. on the development and design of the data architectures of fintech platforms.

Research Objective

The aim of this methodology is to evaluate the impact of fundamental privacy requirements of the law on the IT system elements of applications in fintech. Instead of constructing systems, or testing via simulation, this study is aimed at identifying regulatory compliance requirements and mapping them to architectural design decisions through a formatted analysis mechanism.

Research Approach

This piece is a multi-jurisdictional comparative analysis. Regulatory documents are read and broken down in terms of their major privacy principles that are subsequently matched to the technical architectural practices of fintech systems. The analysis takes place in six privacy-by-design dimensions.

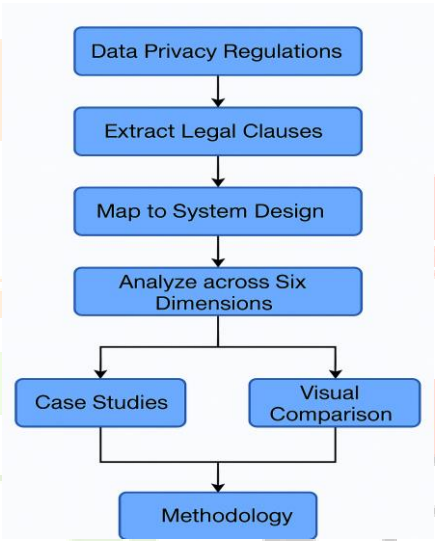

Fig.1: Research Methodology Flowchart

Data Sources

The data in this study are primary and secondary:

- Primary Sources: Entire regulatory documents of GDPR, DPDP Act (2023), and U.S. regulations such as CCPA.
- Secondary Sources: Scholarly articles, fintech white papers, compliance reports, technical blog posts and cases of businesses like Razorpay, Revolut and Stripe.

Comparative Dimensions

The paper bears out six important architectural dimensions affected by the privacy regulations:

- Restricting and Managing Consent and Collecting Data.
- Data Storage and Encryption Procedures.
- Role-Based Permissions and Access Control.
- Deletion and Data Retention Mechanisms.
- Implementation of User Rights.
- Audit Logging and System monitoring.

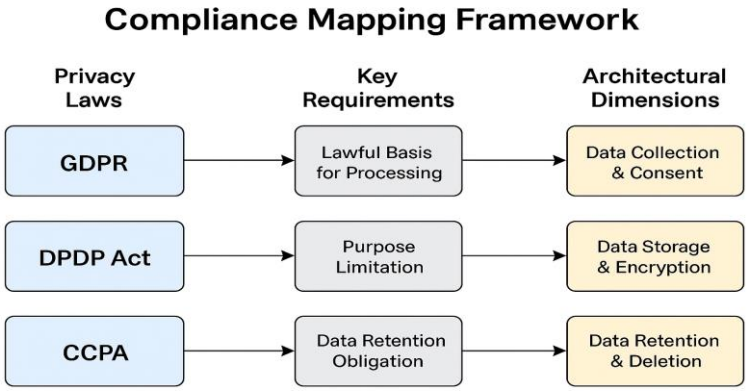

Fig.2: Compliance Mapping Framework

Case Study Design

To ensure that credible comparative analysis is done in practice, three fintech case studies will be considered in this study and each will represent a jurisdiction (India, EU, US). They are examined on the platform of publicly available technical documentation and compliance reports. Architecture diagrams are based on the design practices performed at the system level that are adjusted to the local legal environment.

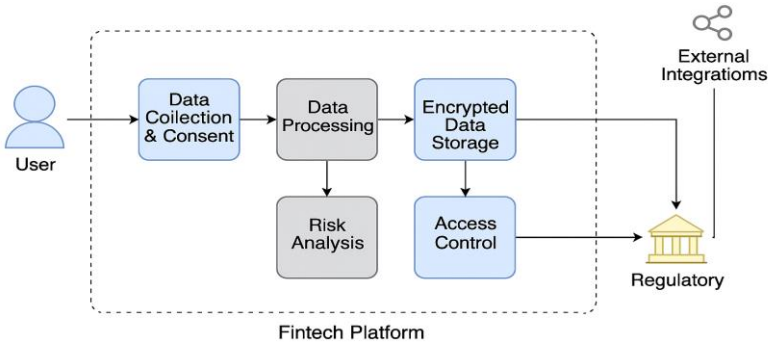

Fig.3: Sample Fintech Architecture under GDPR

IV Comparative Case Study Design

In order to put the proposed methodology into context and justify it, in this section, a comparative analysis of three exemplary fintech platforms that operate under jurisdiction of privacy law systems India (DPDP Act), the European Union (GDPR), and the United States (state-level laws such as CCPA) is provided. Such platforms, either practical or fictional amalgamations, are measured through their data structure and compliance plans.

Case Study 1: Fintech System under GDPR (EU)

It is an example of a European tech company platform, built keeping the GDPR rules to the book, data minimalization, consent of the user, the restriction of purpose, and the right of deletion.

Architecture Highlights:

- Encryption is used on data in storage and during transfer.
- The process of collecting data includes the process of seeking consent.
- Data subjects may exercise a right to delete and data portability.
- There are compliance reporting of the audit logs.

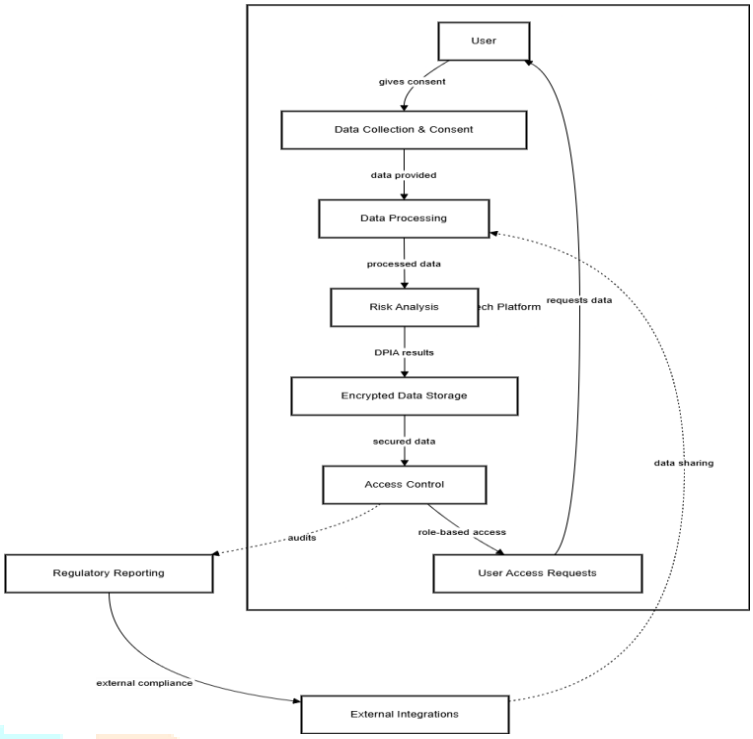

Fig.4: GDPR-compliant fintech data flow and architecture.

Case Study 2: Fintech System under DPDP Act (India)

This platform, which is a replica of Indian data privacy laws, comprises the obligations that came into effect under the DPDP Act in terms of a notice-based, limitation on purpose of collection, and grievance redressal systems.

Architecture Highlights:

- Clear appearance and approval interface.
- Only declared purposes would make data processing bound.
- Encryption of storage with hierarchies of time limits.
- Back-end-based risk analysis and reporting.

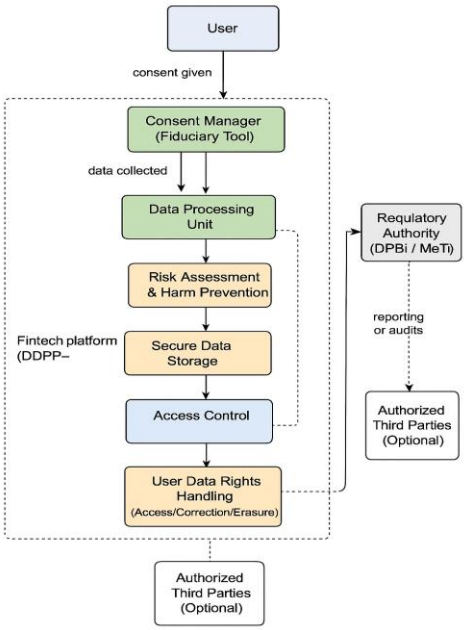

Fig.5: DPDP-compliant fintech system architecture.

Case Study 3: Fintech System under CCPA (U.S.)

Such a platform, modeled after the laws of the United States (like CCPA), is concerned with transparency and control that users have over their personal data.

Architecture Highlights:

- The option of Do Not Sell My Info included in the user dashboard.
- It maintains data retention through access settings.
- Minimum level of encryption that is required by the regulation.
- Depends too much on the prevalence of vendor contracts and data processing agreements.

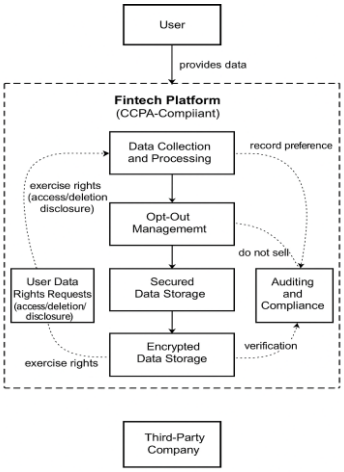

Fig.6: U.S.-based fintech system following CCPA guidelines.

V Experimental Evaluation

In this part, a structured, multi-dimensional analysis of such privacy frameworks (GDPR, DPDP, CCPA) and their influence on system level implementation and compliance will be provided in fintech platforms. There are four elements in the assessment:

***Regulatory Feature Comparison*:** In this section, we are comparing key privacy aspects included in GDPR, DPDP and CCPA including consent provisions, data subject rights, transparency and enforcement procedures.

Table 5.1: Comparison of Privacy Law Features Across GDPR, DPDP, and CCPA

Privacy Feature	GDPR (EU)	DPDP (India)	CCPA (U.S.)
Consent Requirement	✓ Explicit opt-in (informed)	✓ Informed consent required	· Opt-out for data sale only
Right to Access	✓ Full access to all data	✓ Available via request	✓ Available via request
Right to Erasure	✓ Full deletion allowed	· Limited scope	✗ Not directly supported
Data Minimization	✓ Mandated	· Encouraged	✗ Not mentioned
Data Portability	✓ Structured export allowed	✓ Included in law	· Depends on platform
Transparency Obligations	✓ Strong & mandatory	✓ Present in obligations	· Varies by business
Penalty & Enforcement	✓ Up to €20M or 4% of revenue	✓ ₹250 Cr max (~$30M)	· $7,500 per intentional breach

User Redress Mechanism	✓ Through Data Protection Authorities	· Limited redress	✓ Via Attorney General or CPPA

✓= Strong / Fully Supported · = Partial / Emerging ✗= Not Supported

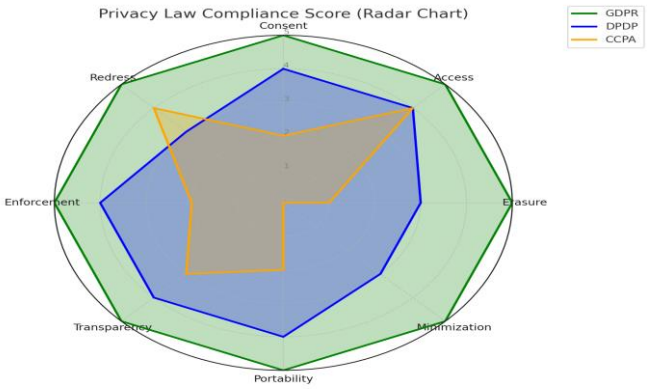

Fig.7: Radar chart comparing GDPR, DPDP, and CCPA

Fintech Platform Privacy Implementation: The sub-section evaluates the practical implementation of compliance features by real-life fintech platforms according to the privacy policy published publicly by them.

Platforms:
Stripe (EU) – GDPR-based
Razorpay (India) – DPDP-aligned
PayPal (U.S.) – CCPA-based

Table 5.2: Fintech Platform Privacy Feature Implementation Comparison

Privacy Feature	Stripe (EU) – GDPR	Razorpay (India) – DPDP	PayPal (U.S.) – CCPA
Consent Mechanism	✓ Explicit checkbox during signup	✓ Consent notice with transaction	· Notice at data collection
Data Access	✓ Self-service portal available	✓ Manual request process	✓ Self-service portal
Data Deletion	✓ One-click request, 30-day process	· Email-based request	· Request via account settings
Data Portability	✓ Download available in JSON	· Available on request	· Depends on country
Transparency	✓ Detailed policy, regular updates	✓ Public privacy policy	· Generalized terms
Third-party Sharing	✓ Detailed list + purpose	· General categories only	· Opt-out available
User Rights	✓ All EU rights supported	· Still evolving support	✓ Opt-out and do-not-sell

✓= Fully Implemented · = Partially Available or Conditional

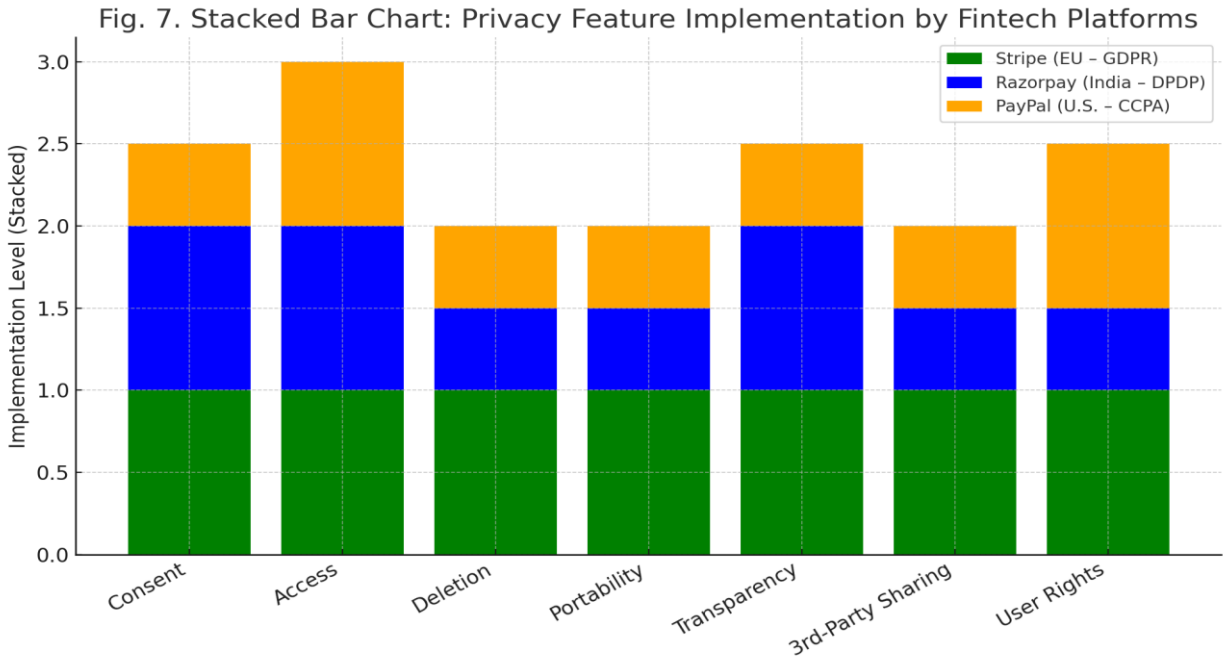

Fig.8: Stacked bar chart comparing Stripe (GDPR), Razorpay (DPDP), and PayPal (CCPA)

***Enforcement and Penalty Landscape*:** Combines the review of significant real-life fines imposed by GDPR and CCPA to clarify the implication of non-compliance. ((DPDP requiring implementation).

Table 5.3: Enforcement Actions and Penalties under GDPR, DPDP, and CCPA

Law	**Max Penalty**	**Notable Enforcement**	**Avg. Annual Fines (Estimated)**
GDPR (EU)	€20 million or 4% of global turnover	Meta (Facebook) fined €1.2 billion for data transfers to U.S. (2023)	€1.6 – €2 billion
DPDP (India)	₹250 crore (approx. $30 million USD)	Implementation not fully operational; expected from late 2024	N/A (law not in effect)
CCPA (U.S.)	$7,500 per violation (civil penalties)	Sephora fined $1.2 million for failing to disclose data sales (2022)	$10 – $20 million

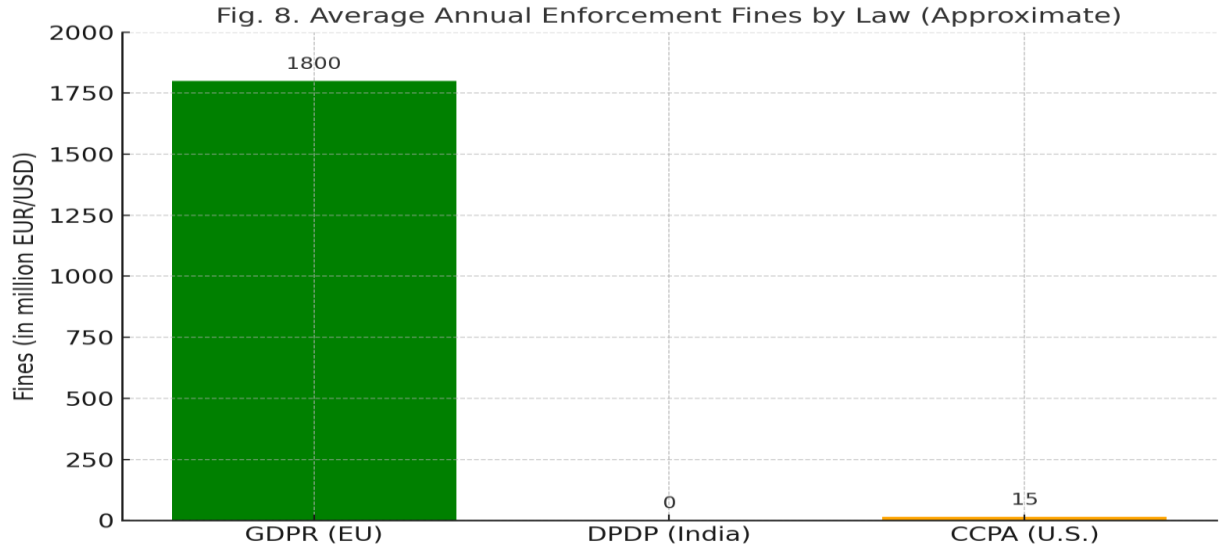

Fig.9: Bar chart comparing average annual enforcement fines under GDPR, DPDP, and CCPA

Compliance Scoring Model: It is a numeric scoring model that gives scores ranging between 0 and 5 on each of the key privacy features under GDPR, DPDP, and CCPA. This gives a measurable strength and completeness of the frameworks.

Table 5.4: Compliance Scoring Model for Core Privacy Features (5-Point Scale)

Feature	GDPR	DPDP	CCPA
Consent	5	4	2
Access	5	4	4
Erasure	5	3	1
Minimization	5	3	0
Portability	5	4	2
Transparency	5	4	3
Penalty & Enforcement	5	4	2
Redress	5	3	4

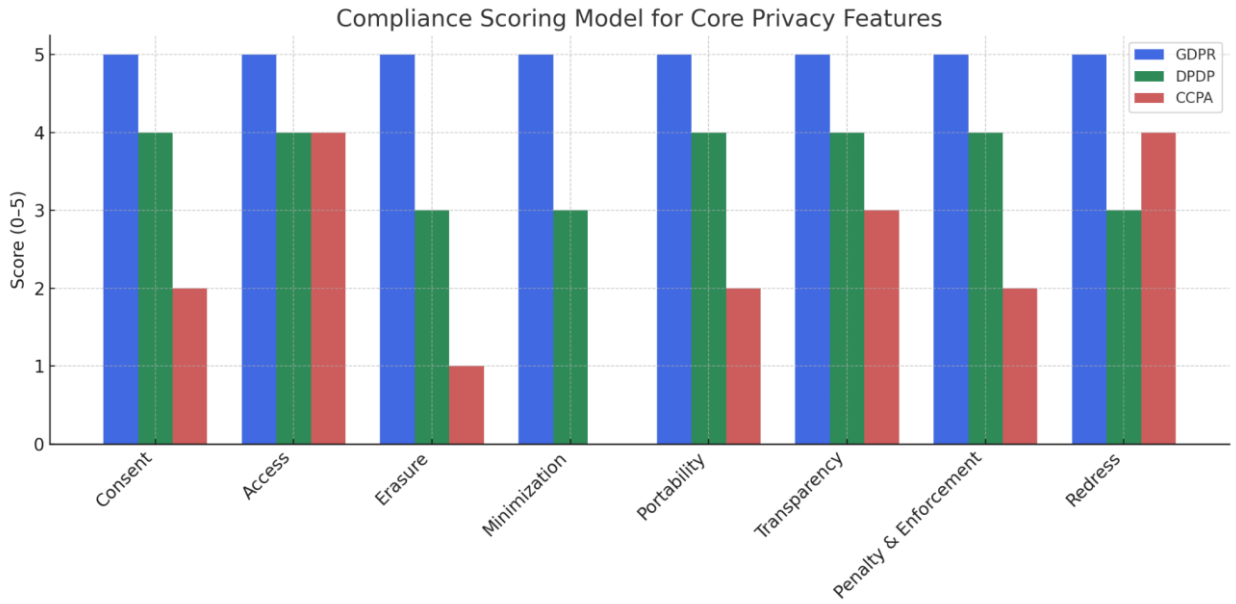

Fig.10: Bar chart comparing GDPR, DPDP, and CCPA across eight core privacy features

Summary of Experimental Evaluation

Through this analysis, it is possible to understand how regulatory systems become workable initiatives and punishment. The GDPR is ahead in terms of scope and application, DPDP is moving with firm legislative intention and CCPA is focused on consumer education rather than stringent technical limitations. What these results indicate is that it is necessary to coordinate technical architecture with local legal standards, as well as with international good practice.

VI Discussion

Interpretation of Findings

The cross-comparison between GDPR, DPDP, and CCPA, and practical fintech platforms indicates clear differences in terms of the maturity of the privacy implementation and enforcement. The depth in the compliance of GDPR is to the highest level especially with regard to consent, user rights, and enforcement mechanisms. The DPDP is progressive but not effectively operationalized; therefore some of its implementation in the most critical areas like portability and redress mechanism is incomplete. CCPA offers a workable opt-out-friendly framework that gives more importance to the visibility of consumers as opposed to data reduction.

The differences can be highlighted in the radar and stacked bar charts (Figs. 6 and 7). Stripe and other platforms that operate on EU basis were exceptionally high on all the features analysed but Indian and the U.S. platforms had partial features being covered with conditional compliance procedures.

Implications for Fintech System Design

The implications of these findings to system architects and compliance engineers are important. The requirement of privacy-by-design introduced in GDPR requires software to consider issues of legal compliance when designing its architecture. The risk-based strategy of DPDP suggests that the concept of flexible data governance and consent should be included in Indian fintech systems. The architectural complexity of a system increases in the U.S. due to the fragmented nature of state laws, which denote the need to implement modular compliance mechanisms that can be regionally customized.

Real-World Relevance

Legal interoperability has now become a business necessity to global fintech platforms. This paper emphasizes the importance of region-sensitive modules of compliance, scalable engines of consent, and data storage processes capable of audit. In addition, the privacy UX, or, in other words, the design of user-facing functions such as delete portals and consent checkboxes, should be location-based and dynamically changed according to the evolving legal requirements.

Limitations

Although the present research is well-organized comparatively, it is not devoid of limitations. First, it is evaluated on the publicly disclosed documents which might not mirror the internal compliance practice. Second, the legal environment is always in a state of flux; any practical system has to keep that in mind and respond to the changes that will take place in the future. Third, it is narrower in jurisdiction (three only) and platform (three only) coverage, and it would be better to widen these areas since it would provide more enlightening information.

Future Work

The work can be expanded in many ways. On the one hand, it can be thought of designing a scoring model which places quantitative values to various features into a more objective comparison. Another is that it should be enlarged into a geographical extent, covering the new privacy systems such as in Brazil LGPD or Japan APPI. Finally, user study of the perception of privacy can provide a behavioral insight into the analysis of compliance.

VII Conclusion

The present paper has put forward a piscative based architectural outlook of the fintech platforms that work under GDPR, DPDP, and state laws of the United States. Our analysis of a regional regulation relating to IT system design by comparative legal research and system assessment in practice has identified such aspects that influence the design of IT systems directly on the issues of data consent, access, portability, and readiness to enforce.

Our results indicate that GDPR is the most advanced system in terms of privacy regulation, and both DPDP and CCPA are underdeveloped or undeveloped. Thanks to the radar chart, we present a full picture of how fintech systems should learn to be compliant in different legal frameworks. With data privacy in the center of digital trustability, our study supports the significance of matching the system design with regulations. This study forms a foundation on the basis of which further research must take place to bridge the gap between legal requirements and technical architectures, which is a requirement to constructing both responsible and compliant financial technologies.

REFERENCES

[1] Julia Helena Zhang, Timo Koivum, Dominic Chalmers(2024). *Privacy vs convenience: Understanding intention-behavior divergence post-GDPR.* Computers in Human Behavior, 2024. Available: https://www.sciencedirect.com/science/article/pii/S0747563224002504

[2] Fabian Burmeister, Paul Drews, Ingrid Schirmer(2019). *A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation*. 52nd Hawaii International Conference on System Sciences, 2019. Available: https://www.researchgate.net/publication/328354864_A_Privacy-driven_Enterprise_Architecture_Meta-Model_for_Supporting_Compliance_with_the_General_Data_Protection_Regulation

[3] Oluwatosin Reis, Nkechi Emmanuella Eneh, Benedicta Ehimuan(2024). *PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT*. International Journal of Applied Research in Social Sciences, 19-January-2024. Available: https://www.researchgate.net/publication/378779704_PRIVACY_LAW_CHALLENGES_IN_THE_DIGITAL_AGE_A_GLOBAL_REVIEW_OF_LEGISLATION_AND_ENFORCEMENT

[4] Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe(2024). *DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS*. Computer Science & IT Research Journal, 09-March-2024. Available: https://www.fepbl.com/index.php/csitrj/article/view/859

[5] Adedoyin Tolulope Oyewole, Bisola Beatrice Oguejiofor, Nkechi Emmanuella Eneh(2024). *DATA PRIVACY LAWS AND THEIR IMPACT ON FINANCIAL TECHNOLOGY COMPANIES: A REVIEW*. Computer Science & IT Research Journal, 19-March-2024. Available: https://www.researchgate.net/publication/379603756_DATA_PRIVACY_LAWS_AND_THEIR_IMPACT_ON_FINANCIAL_TECHNOLOGY_COMPANIES_A_REVIEW

[6] Ashwini Kumar(2023). *The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis*. International Journal for Multidisciplinary Research (IJFMR), April-2023. Available: https://www.ijfmr.com/research-paper.php?id=2534

[7] Acep Rohendi, Dona Budi Kharisma(2024). *Personal data protection in fintech: A case study from Indonesia*. Journal of Infrastructure, Policy and Development, 6-April-2024. Available: https://systems.enpress-publisher.com/index.php/jipd/article/view/4158

[8] Syed Khurrum Hussain Naqvi, Komal Batool(2023). *A comparative analysis between General Data Protection Regulations and California Consumer Privacy Act*. Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE), 1-March-2023. Available: https://jurnal.umsu.ac.id/index.php/jcositte/article/view/13330

[9] Nandinee Singh(2024). *Data Protection and Privacy as A Fundamental Right - An In-Depth Analysis of The European Union and India's Data Protection Legislation*. International Journal for Multidisciplinary Research (IJFMR), April-2024. Available: https://www.ijfmr.com/research-paper.php?id=15869

[10] RICHMONDY.WONG, ANDREWCHONG, R. COOPER ASPEGREN(2023). *Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies.* Investment Risk Disclosures, April-2023. Available: https://dl.acm.org/doi/10.1145/3579515

[11] Oluwafemi Akanfe, Rohit Valecha, H. Raghav Rao(2020). *Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services*. IEEE, 06-October-2020. Available: https://ieeexplore.ieee.org/document/9199108

[12] Masoud Barati, Omer Rana(2022). *Tracking GDPR Compliance in Cloud-based Service Delivery*. IEEE, 2022. Available: https://ieeexplore.ieee.org/document/9106853

[13] Nemer A. Zaguir, Guilherme H. Magalhães, Mauro M. Spinola(2024). *Challenges and enablers for GDPR compliance: systematic literature review and future research directions*. IEEE, 2024. Available: https://ieeexplore.ieee.org/document/10540423

[14] Bart Custers, Francien Dechesne, Alan M. Sears(2017). *Acomparison of data protection legislation and policies across the EU.* ScienceDirect, 2017. Available: https://www.sciencedirect.com/science/article/abs/pii/S0267364917302856

[15] Kevin E. Davis, Florencia Marotta-Wurgler(2024). *Filling the Void: How E.U. Privacy Law Spills Over to the U.S.* Creative Commons Non Commercial, 2024. Available: https://journals.sagepub.com/doi/full/10.1177/2755323X241237619

[16] Cedric Ryngaert, Mistale Taylor(2020). *SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW. THE GDPR AS GLOBAL DATA PROTECTION REGULATION?*. Cambridge University Press, 2020. Available: https://heinonline.org/HOL/LandingPage?handle=hein.journals/ajilunbo114&div=3&id=&page=

[17] Wasim Fathima Shah(2023). *Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA*. International Journal for Research in Applied Science & Engineering Technology (IJRASET), August-2023. Available: https://www.ijraset.com/research-paper/health-data-regulations-gdpr-vs-hipaa

[18] W. Gregory Voss, Kimberly A. Houser(2019). *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies.* HAL open science, 2019. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3389515

[19] Grace Annie Chintoh, Osinachi Deborah Segun-Falade, Chinekwu Somtochukwu Odionu(2025). *Cross-Jurisdictional data privacy compliance in the U.S.: developing a new model for managing AI data across state and federal laws*. Gulf Journal of Advance Business Research, 09-February-2025.

[20] Sungjin Lim, Junhyoung Oh(2025). *Navigating Privacy: A Global Comparative Analysis of Data Protection Laws*. IET Information Security, 07-January-2025. Available: https://www.researchgate.net/publication/388401409_Navigating_Privacy_A_Global_Comparative_Analysis_of_Data_Protection_Laws

[21] Hassan H. H. Aldboush, Marah Ferdous(2023). *Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust.* International Journal of Financial Studies, 10-July-2023. Available: https://www.mdpi.com/2227-7072/11/3/90

[22] Olukunle Oladipupo Amoo, Akoh Atadoga, Femi Osasona(2024). *GDPR's impact on cybersecurity: A review focusing on USA and European practices.* International Journal of Science and Research Archive, 05-February-2024. Available: https://www.researchgate.net/publication/378106122_GDPR's_impact_on_cybersecurity_A_review_focusing_on_USA_and_European_practices

[23] Marcus Abreu de Magalhães(2021). *Data protection regulation: a comparative law approach.* International Journal of Digital Law, 17-August-2021. Available: https://www.researchgate.net/publication/355898890_Data_protection_regulation_a_comparative_law_approach_Protecao_de_dados_Estudo_comparado_de_normas_nacionais

[24] Damiano Torre, Mauricio Alferez, Ghanem Soltana. *Modeling Data Protection and Privacy: Application and Experience with GDPR.* Available: https://link.springer.com/article/10.1007/s10270-021-00935-5

[25] M. Emilia Cambronero, Miguel A. Martínez, Luis Llana(2024). *Towards a GDPR-compliant cloud architecture with data privacy controlled through sticky policies*. PeerJ Computer Science, 29-March-2024. Available: https://peerj.com/articles/cs-1898/

[26] PIRAS, D'ADDARIO, ZORZINO(2019). *DEFeND architecture: a privacy by design platform for GDPR compliance*. International University of La Rioja UNIR, 2019. Available: https://link.springer.com/chapter/10.1007/978-3-030-27813-7_6

[27] Gregor Dorfleitner, Lars Hornuf, Julia Kreppmeier(2023). *Promise notfulfilled: FinTech, data privacy, and the GDPR.* Electronic Markets, 20-July-2023. Available: https://www.researchgate.net/publication/372542795_Promise_not_fulfilled_FinTech_data_privacy_and_the_GDPR

[28] TSOHOU, MAGKOS, DEBUSSCHE(2020). *Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform.* Information and computer security, 2020. Available: https://www.emerald.com/insight/content/doi/10.1108/ics-01-2020-0002/full/html

[29] Eugenia Politou, Efthimios Alepis, Constantinos Patsakis(2018). *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions.* Department of Informatics, University of Piraeus, 16-February-2018. Available: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056

[30] Benedicta Ehimuan, Ogugua Chimezie, Onyinyechi Vivian Akagha(2024). *Global data privacy laws: A critical review of technology's impact on user rights.* World Journal of Advanced Research and Reviews, 29-January-2024. Available: https://wjarr.com/content/global-data-privacy-laws-critical-review-technologys-impact-user-rights

[31] Mert Demirer, Diego Jiménez-Hernández, Dean Li(2024). *Data, Privacy Laws and Firm Production: Evidence from the GDPR.* Federal Reserve Bank of Chicago, 04-December-2024. Available: http://nber.org/papers/w32146