Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 15 Issue 01, 2026

A Study on Transaction Tools Used in Online Applications: Trends, Challenges, and Opportunities

[1]Vivek Kumar Soni, [2]Krishanu Gharami, [3]Priyansh Ratre, [4]Saumya Chandrakar
[1,2,3,4] Department of CSE SSIPMT, Raipur, Chhattisgarh, India
[1]vk.soni@ssipmt.com, [2]krishanu.gharami@ssipmt.com, [3]priyanshratre@ssipmt.com, [4]saumya.chandrakar@ssipmt.com

Peer Review Information

Submission: 29 March 2026
Revision: 17 April 2026
Acceptance: 21 May 2026

Keywords

UPI, API, Digital Wallets, Card Payment Gateways

Abstract

This study is for the transaction tools that determine the integrated delivery of online applications for digital wallets, card payment gateways, and also aggregators; account-to-account rails unlike UPI and open banking APIs. The paper explores the evolution of real-time payments, tokenization, and risk- based multi-factor authentication, and how market dynamics, regulations, and developers' ecosystems impact adoption. The trends in instant payment adoption, cross-rail interoperability, and API-Driven integration-based adoption patterns have been synthesized from authoritative sources and public statistics. It further analyzes the security compliance challenges that still exist in production environments, these include API authoriza- tion gaps; inconsistent 3-D Secure flows; fragmented standards adoption; and the operational cost of PCI DSS v4.0. This work postulates a comparative framework that spans security controls, latency, availability, interoperability, and standards conformance, and the developer experience, enabling structured evaluation across tool classes. The study identifies areas such as privacy- preserving fraud analysis, tokenization-first architectures, ISO 20022-native developer tooling, and standards-aligned sandboxes for predictable SCA and error semantics as fruitful niches where opportunities are found. The results are summarized into tables and graphs to show adoption patterns, control coverage, and implementation trade-offs. Lastly, such paper presents prescriptive and readily implementable recommendations for improvement of security posture, reduction of friction, and acceleration of reliable integrations in modern transaction ecosystems to engineering leaders and stakeholders.

Introduction

Integrated digital transactions weave the connecting tissue of the online economies, encompassing consumers, merchants, financial institutions, and fintech with interoperable architecture that should perform security, speed, and frictionless experience. Typically, the current formulation of these systems comprises four pillars: digital wallets for tokenized and device- bound payments; card payment gateways [1, 2, 3]; aggregators of worldwide acceptance with standardized dispute regimes; and account-to-account rails (notably India's UPI) for real- time push payments at scale [4, 5, 6]; and open banking APIs that enable consented initiation and data access for new financial services. Engineering choices across these pillars: authentication patterns, token management, data models, and error semantics directly shape measurable conversion rates, fraud outcomes, operational resilience, and compliance viability.

Recently, adoption has shifted dramatically toward real- time payments and a mobile-first experience. UPI in India stands out as an example of how standardized interfaces, interoperable architecture, and layered ecosystem roles can be created for fast, comprehensive growth while also achieving robust customer authentication through app/device binding and risk controls at the PSP and scheme levels. Concomitantly, the entire globe sped up the transition to ISO 20022 - an even richer, structured messaging standard which facilitates better reconciliation, analytics, and regulatory reporting [7, 8, 9]. On the card side, EMV 3-D Secure version 2.x upgraded customer authentication according to the concept of data- rich, risk-based step-ups that are much better at balancing security and conversion than previous versions. Although these changes herald positive developments, they now also bring twists of new complexities in integration: disparate APIs, uneven adoption of standards, and splintered user journeys across regions and channels.

Security and compliance are paramount. The PCI DSS v4.0 advances expectations about identity, logging, scoping, and continuous control validation within card-data environments, casting organizations to more disciplined security engineering [10, 11, 12]. The APIs of open banking and payments usually traverse multiple vendor and cloud boundaries. Permanent risks include broken object authorizations, poor token life- times, and mismanaged shadow endpoints [13, 14]. Mean-while, fraud patterns evolve across channels and devices so that even on tight latency budgets, they require a streaming detection pipeline that can adapt to drift but also satisfy explanation and fairness expectations for risk operations and regulators [15, 16, 17].

This paper analyzes current trends, giving three impor- tant contributions to the needs in the real world. First, it will address large-scale ecosystem developments across pay- ment methods such as wallets, payment gateways, account- to-account transfers, and open banking APIs so that adoption and functionality can actually build together. Second, it will highlight the secured compliance, compatibility, and user ex- perience challenges that still hamper the large-scale reliability of these systems in practice. Third, it introduces a way of comparing different tools and provides clear guidelines, based on real-world operations and the standards set by industry bodies, that will help teams select and use transaction tools optimally aligned with their risk tolerances, user experience goals, and legal requirements. Findings are laid out in tables and charts such that adoption appears to progress, how con-trols are established, and trade-offs involved to engineering managers, product leaders, and compliance officers.

Literature Review

Transaction technology scholarship traverses the depth tran- sition from card-based models, to tokenized, mobile-first, and instant account-to-account schemes, which always emphasizes assurance and conversion through time. Early works were re- volving around cryptographic protocols, terminal security, and acquirer-issuer messaging, while the latest studies investigated ecosystem-scale properties such as end-to-end authentication journeys, interoperability, and regulatory compliance across jurisdictions. Surveys of mobile and web highlight the recur-rent trade-off between stronger controls and consumer friction resulting in risk-based authentication whereby contextual data is used to step-up only when actually warranted. This most clearly spells out in EMV 3D Secure v2.x where merchants provide richer data to issuers thereby enabling improved authorization accuracy and reduced abandonment as compared to v1.0 in properly integrated environments.

A detailed reference of UPI's research for real-time retail payment on a national scale involves architectural analy- ses that describe well-defined ecosystem roles (payer bank, payee bank, PSPs, switch), standardized APIs, and strong customer authentication anchored in app/device binding and per-transaction confirmation. Security assessments in earlier versions had indicated attack vectors at the mobile application level such as secure credential stores and resistance to reverse engineering, which informed the more stringent implementa- tion guideline and wider adoption of device attestation and tamper checks. The collective body of work within UPI is indicative of co-evolution between protocol design and app hardening with PSP-level monitoring to secure the fast growth. Fraud detection literature testifies to a transition from rule engines to supervised and unsupervised machines up to hy- brid machine learning means [18, 19, 20]. Public dataset benchmarking (IEEE-CIS, ULB credit card data, PaySim synthetic mobile money) often indicates ensemble approaches will lead single learners in precision-recall trade-off delivery when class imbalance and cost sensitivity are incorporated into the solution. More recent contributions have tended to emphasize the operationalization of such models in streaming

pipelines where they have to deal with aspects such as concept drift, monitoring, population stability indices, feature drift, and calibration checks to ensure performance remains valid after deployment. The need for increased explainability appears to grow, with recent research proposing SHAP/feature attribution and constrained models for auditing in regulated environments. Adapted perpetuation gave rise to the accompaniment of security and compliance frameworks. PCI DSS v4.0 for- malizes objective validation and advocates for individualized approaches, which strengthen identity, tracking, and continual control verification. Empirical studies associated more mature PCI programs with reduced breach risk, but these benefits were barracked by compliance costs and operational complexities particularly for SMEs and long-tail merchants. Meanwhile, ISO 20022 migration holds promises in rich structured mes- sages for enhanced reconciliation, AML screening, and ana- lytics. Some impediments to implementation include legacy integration, inconsistent timelines in migration processes, and
the necessity to coordinate cross-border.

Open banking and API security research highlights recur- ring weakness gaps, such as broken object-level authorization, inadequate mutual TLS and key rotations, delicate token lifecycles, and ungoverned shadow endpoints. Possible miti- gations will include: thorough threat modeling tied to OWASP API risks; schema-first design with contract testing; gateway enforced fine-grained authorization; and runtime protection with anomaly detection for consent and payment initiation flows. Furthermore, studies emphasize the importance of con- formance test suites, certification regimes, and production-like sandboxes for predictable developer onboarding.

Such is now the experience of a developer—the systemic determinant of the reliability of a system and time-to-market. Comparisons show that consistent error taxonomies of failure, high-fidelity sandboxes, robust SDKs, and reference flows for consent/SCA and 3DS contribute meaningfully to time shrinkages in the integration process as well as reduced incidents rates. In short, the literature seems to be conclusive that resilience to high-conversion transaction systems does not hinge solely on cryptography or authentication primitives but is largely dependent on cohesive ecosystem.

Research Methodology

The study is a mixed-methods design that involves a struc- tured review of evidence, quantitative analysis of authoritative indicators, and a comparative evaluation framework for the four dominant transaction tool classes: digital wallets; card gateways/aggregators; account-to-account (A2A) rails (e.g., UPI); and open banking APIs. The derived results are intended to be generalizable across ecosystems and actionable for engineering, product, and compliance teams.

Scope and research questions: The methodology seeks to address the following three questions: (Q1) What use and interoperability trends describe the contemporary transaction tools across markets? (Q2) Which security and compliance controls influence risk and conversion outcomes the most? (Q3) Where are the possible greatest high-leverage opportu- nities to improve the fraud defense and developer experience but without unacceptable delay or cost?

Data source: The primary quantitative evidence is from the official portal and dashboard of the scheme, such as national payment statistics, UPI product/monthly metrics, and anything that captures volumes, values, participant counts, and cadence (daily/monthly). Security and compliance references were drawn from the PCI DSS v4.0, EMV 3-D Secure v2.x, and ISO 20022 materials regarding message standard and migration consequences. For innovation analysis, public fraud datasets (IEEE-CIS, ULB credit card, PaySim) also inform feasibility of ML approaches under class imbalance and streaming con- straints. Signals regarding developer experience come from audits around documentation, SDKs, error taxonomy stability, and fidelity of sandbox as reported by major providers.

Variable extraction and normalization: A consistent schema captures comparable variables across tool classes: adoption (thereby volume growth, geographic spread), security con- trols (MFA/biometrics, tokenization, device binding, logging), interoperability (adherence to standards, message richness, cross-border readiness), developer experience (API stability, semantics of error, SDKs, sandbox quality), and performance (authentication/authorization latency bands, availability SLOs, dispute/chargeback processes where relevant). Time-series in- dicators are normalized to monthly equivalents where neces- sary to enable trend visualization.

Comparative framework and scoring: Each class of tools will be assessed against the schema at the level of one to five per criterion (1 = minimal, 5 = best-in-class). Scoring depends in part on documented standards requirements, published oper- ational behaviors, and ecosystem characteristics (e.g., built-in device

binding for wallets/A2A and dispute regimes for cards). Analysis procedures: Trends are depicted using line charts (e.g., monthly volumes of A2A), stacked bars and checklists summarize the control coverage and developer experience factors. Sensitivity analysis is performed regarding changes in scores based on different assumptions (e.g., stricter SCA requirement or partial adoption of ISO 20022).

Results

Adoption and usage: Time series analysis of official scheme statistics shows that account-to-account (A2A) transactions grow continuously, with volumes, and values increasing month on month with merchant enablements and improved applica- tion user experience. Daily series indicate there are cycles around salary credits and festive periods, implying that real-time payments are embedded in routine and seasonal com- merce to an extent. Digital wallets remain popular within app ecosystems, particularly for subscriptions and in-app pur-chases. Card-not-present (CNP) continues to be relevant in assisting cross-border e-commerce and is already fortified with dispute/chargeback protections.

Authentication and conversion: From the perspective of bedecked authorization accuracy and curtailed abandonment liability, EMV 3D Secure (3DS) v2.x is a galaxy away from v1.0 since the merchants would supply enriched context and the onus of risk policy optimization would lie with issuers. Wallets and A2A flows enjoy device binding and biometrics, creating much lower friction for returning users and merchants. However, these buckets for user experience issues remain confusingly fragmented; issuer challenges by device type differ with contexts from app vs. browser; step-up prompts can be mistimed; and user recovery can be hampered by inconsistencies in error semantics. The overwhelming consen- sus is that strong authentication must be applied to ensure high conversion when flows are implemented and monitored consistently.

Interoperability and standards: Migrating to ISO 20022 enhances the richness of data for reconciliation, AML, and analytics, but the benefits come with an uneven mix of timeline for legacy integration and regional mandates. For the open banking ecosystem, clearly defined profiles, certification suites, and sandboxes that mimic the production environment correlate with faster onboarding with fewer incidents. When messages' semantics or models of consent diverge, the cost for developers in integration rises as time-to-market elongates, indicating the necessity for schema first APIs, stable error taxonomies, and reference flows.

Security posture: PCI DSS v4.0 adoption enhances identity, logging, and continuous validation inside card processing envi-ronments, with the mature programs reporting fewer security incidents correspondingly. API security remains a recurrent weak point: common findings include broken object-level authorization, weak token lifecycles, insufficient MTLS, and unmanaged shadow endpoints. Effectively bringing a fit be- tween design-time controls (threat modeling, contract testing, least-privilege scopes) and runtime defense (enforced via rate limiting, anomaly detection, inline authorization decisions, and continuous posture monitoring) is vital.

Fraud analytics opportunities: Benchmarking indicates that ensemble ML approaches, calibrated thresholds, and drift- aware monitoring can maximize recall given false positives particularly in situations where latency budget and cost-of- error are explicitly modeled. Privacy-protecting measures (to-kenization, feature hashing, and federated learning) can help minimize data exposure while still providing useful signals for risk scoring. On the ground, better results are achieved when models tie into event-driven architectures, feedback mechanisms to enforce quality of the labels, and explicit operator-centric tools meant for overrides/investigations.

Support for decision making with reference to tables and graphs: The comparative matrix clarifies that wallets and A2A rails excel in low-friction authentication and device binding (high security/UX scores), card gateways lead in dispute management and global acceptance, and open banking APIs offer consented initiation.

Table 1: Comparative Matrix (Scores 1–5)

Dim.	Wallets	Cards	A2A	OB APIs
Security				
Overall	4.5	4.0	4.5	4.0
MFA/Bio	5.0	4.0	4.5	4.5
Token/PCI	4.5	4.5	4.0	4.0
API/AuthZ	4.0	4.0	4.0	3.5
Interop				
Overall	3.5	4.5	4.0	4.0

Std Conf.	3.5	4.5	4.0	4.0
ISO20022	3.0	4.0	4.0	4.5
DevEx				
Overall	4.0	4.0	3.5	3.5
Docs/SDKs	4.5	4.0	3.5	3.5
Sandbox	4.0	4.0	3.5	3.5
Perf				
Overall	4.5	4.0	4.5	3.5
Latency	4.5	4.0	4.5	3.5
Avail.	4.5	4.0	4.5	3.5

Table 2: API DevEx Checklist

Criterion	**Wallets**	**Cards**	**A2A/OB**
Docs (refs/guides/examples)	√	√	√
Errors (codes/causes/fixes)	√	√	√
Sandbox (flows/webhooks/limits)	√	√	√
SDKs (langs/updates/samples)	√	√	√
Versioning/Deprecation	√	√	√
Auth (OAuth2/MTLS/scopes)	√	√	√
Webhooks (retry/signature)	√	√	√
Rate limits/Backoff	√	√	√
Observability (status/SLOs)	√	√	√
Support (SLA/forums/issues)	√	√	√

Conclusion

Online transaction ecosystems are converging toward real-time rails, richer structured messages, and authentication models that balance assurance with conversion. However, the reality of deployment remains constrained by uneven stan- dards uptake, fragmented API practices, and recurring security weaknesses at the authorization and integration boundaries. This paper translated those dynamics into a comparative framework that integrates adoption metrics, security and com- pliance controls, maturity of interoperability, and quality of developer experience, offering a practical lens for selecting and integrating wallets, card, A2A rails, & open banking APIs.

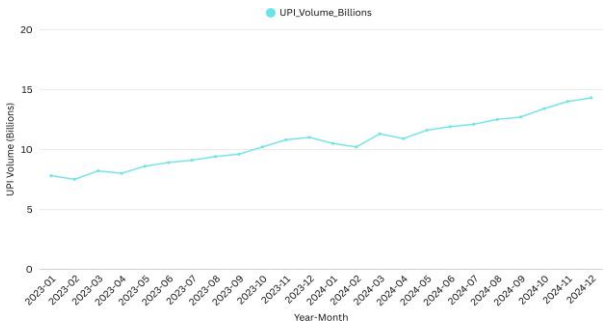

Fig. 1: Monthly A2A/UPI Transaction Volume Trend.

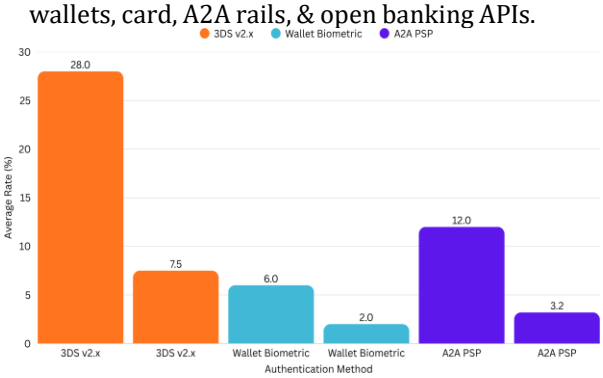

Fig. 2: Authentication Flow Friction by Method

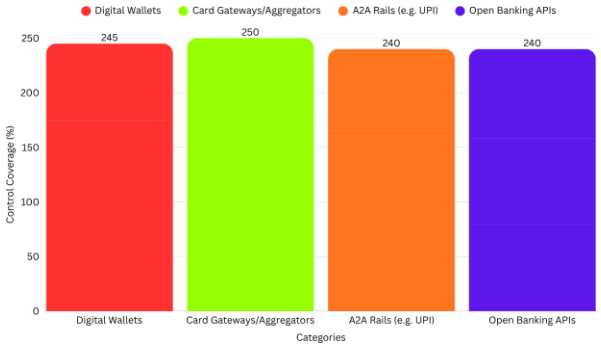

Fig. 3: Security Control Coverage by Tool Class.

The results point to priority moves with the highest return: standardize EMV 3DS v2.x flows with merchant–issuer data sharing, adopt tokenization-first data paths to limit sensitive exposure, harden API authorization with least-privilege scopes and MTLS, and invest in ISO 20022 native tooling that normalizes semantics across providers. Combined with aggregation drift awareness, fraud analytics, and strong op- erational monitoring, these actions increase security posture while minimizing friction.

Progress from here depends on disciplined engineering and cross-ecosystem coordination: publish stable schemas and error taxonomies, run high-fidelity sandboxes, and measure latency and challenge rates as first-class reliability metrics. Organizations that execute on these fundamentals will deliver faster, safer, and more reliable payments while preserving the trust essential to digital commerce at scale.

References

National Payments Corporation of India, "UPI: Product Booklet," Mumbai, India: NPCI, 2025.

National Payments Corporation of India, "Unified Payments Interface (UPI): Product Statistics and Monthly Metrics," Mumbai, India: NPCI, 2025.

National Payments Corporation of India, "UPI Monthly Metrics (Daily Trends)," Mumbai, India: NPCI, 2025.

Reserve Bank of India, "Database on Indian Economy (DBIE): Pay- ment System Indicators," Mumbai, India: RBI, 2025.

Bank for International Settlements, Committee on Payments and Mar- ket Infrastructures, "Red Book Statistics: Payments and FMIs Data Portal," Basel, Switzerland: BIS-CPMI, 2025.

EMVCo, "EMV 3-D Secure: Specification and Program Information (v2.x)," 2025.

ISO 20022 Registration Management Group, "ISO 20022: Universal financial industry message scheme—Overview," Geneva, Switzerland: ISO 20022, 2025.

SWIFT, "ISO 20022 for Financial Institutions: Focus on Payments Instructions," La Hulpe, Belgium: SWIFT, 2025.

Open Banking Ltd., "Directory Sandbox: UK Open Banking Testing Environment," London, UK: OBIE, 2025.

Solomon, D., IEEE DataPortTM. Innovate, 2025.

PhonePe, "PhonePe Pulse: India Digital Payments Data Repository and API," Bengaluru, India: PhonePe, 2021–2025.

Fitzgerald, A., What's new in PCI DSS 4.0? key updates explained. Secureframe, 2024.

Mohmmed, Asmaa A.; Rahma, Abdul Monem S.; and AbdulWahab, Hala Bahjat (2024) "Digital Wallets Evolution: Navigating Challenges, Innovation and the Future Landscape," Al-Qadisiyah Journal of Pure Science: Vol. 29 : No. 1 , Article 4.

PwC India, "The Indian Payments Handbook 2024–2029," New Delhi, India: PwC, 2024.

PCI Security Standards Council, "PCI DSS v3.2.1 to v4.0: Summary of Changes," Wakefield, MA, USA: PCI SSC, Mar. 2022.

R. Khan, M. M. Rathore, and A. Paul, "Security in next generation mobile payment systems: A comprehensive survey," IEEE Access, vol. 9, pp. 123456–123490, 2021.

Lucas, Yvan & Jurgovsky, Johannes, Credit card fraud detection using machine learning: A survey, 2020.

S. Kumar, V. Sharma, A. Kumar, and P. K. Jain, "Security analysis of Unified Payments Interface and payment apps," in Proc. 29th USENIX Security Symp., 2020, pp. 1–20.

Vesta Corp. and IEEE Computational Intelligence Society, "IEEE-CIS Fraud Detection Dataset," 2019.

Addison Howard and Bernadette Bouchon-Meunier and IEEE CIS and inversion and John Lei and Lynn@Vesta and Marcus2010 and Prof. Hussein Abbass, IEEE-CIS Fraud Detection, 2019.

European Central Bank, "Card fraud statistics and trends in digital payments"

World Bank Group, "Digital Financial Services: Challenges and Op- portunities for Emerging Economies", World Bank Publications, Wash-ington, DC, USA, 2023. ECB Statistical Data Warehouse, Frankfurt, Germany, 2024.

OWASP Foundation, "OWASP API Security Top 10 – 2023", OWASP, 2023.

McKinsey & Company, "The Future of Digital Payments: Real-Time, Open, and Embedded

Finance" McKinsey Global Payments Report, 2024.

NIST (National Institute of Standards and Technology), "Digital Iden- tity Guidelines (SP 800-63 Rev. 4)", U.S. Department of Commerce, Gaithersburg, MD, USA, 2023.