International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Card-on-File Tokenization – Issues, Technologies, and Innovations

Ms. Prachi Bansal[1], Prof. Dr. Surinder Singh[2]

[1]Research Scholar, Department of Commerce, Chaudhary Devi Lal University, Sirsa, Haryana
[2]Professor and Dean Faculty, Department of Commerce, Chaudhary Devi Lal University, Sirsa, Haryana

Abstract
Card-on-file tokenization has emerged as a critical technology in India's rapidly digitizing financial ecosystem, particularly following the Reserve Bank of India's (RBI) mandate prohibiting merchants from storing card details. By replacing actual card credentials with secure, context-specific tokens, tokenization significantly reduces the risk of data breaches and financial fraud, thereby enhancing digital payment security. This study conducts an extensive review of secondary research sources, including RBI circulars, academic literature, and domestic fintech case studies, to examine how tokenization is being implemented across the Indian payments landscape. The findings reveal that while tokenization has greatly enhanced consumer data protection, persistent challenges remain, including regulatory ambiguity, limited interoperability across platforms, and overreliance on centralized token vaults. Looking ahead, India's future tokenization frameworks may benefit from the integration of blockchain technologies, decentralized vaults, biometric-linked tokens, and quantum-resistant encryption models. These advancements could help create a more secure, inclusive, and resilient digital payments infrastructure tailored to India's unique regulatory and technological environment.

Keywords: - Tokenization, Card-on-File, Payment Security, Blockchain, Fraud Prevention, Digital Assets

Introduction

The digital payment landscape in India has seen rapid evolution over the last decade, driven by the widespread adoption of mobile wallets, UPI platforms, and e-commerce services. This growth has brought with it an increase in security risks, including data breaches and financial fraud. According to the Indian Computer Emergency Response Team (CERT-In), over **14 lakh cybersecurity incidents** were reported in 2022 alone, many of which targeted sensitive financial data (CERT-In, 2023).

To address these concerns, the **Reserve Bank of India (RBI)** issued a directive mandating **card-on-file (CoF) tokenisation**, prohibiting merchants and payment aggregators from storing actual card data beyond **October 1, 2022** (RBI, 2021). Instead, they must replace sensitive card credentials with unique, non-sensitive tokens — usable only within specific merchant contexts. This mandate aligns with global security practices but also addresses India-specific challenges such as **data localization**, **consumer consent**, and **merchant compliance**.

Tokenization not only reduces the surface area for attacks but also simplifies compliance with standards like **PCI DSS**, creating a more secure ecosystem for digital payments in India (Banerjee, Shukla, & Menon, 2022). The RBI's framework is both a regulatory safeguard and a technological driver for innovation in Indian fintech, enhancing user trust and securing digital infrastructure.

This paper aims to critically examine India's CoF tokenisation policy by analyzing RBI guidelines, domestic challenges, and technological adaptations within the Indian context. Through a review of secondary sources — including Indian academic publications, RBI circulars, technical whitepapers, and legal commentary — this study explores how India is building a robust, token-based payment security framework amid global and domestic pressures.

Literature Review

2.1 Tokenization Frameworks and Privacy Discontents (India-focused)

In India, tokenization has emerged as a central pillar in the RBI's strategy to strengthen payment security, yet it continues to face significant regulatory and operational challenges. Banerjee, Shukla, and Menon (2022) critically examined the Indian tokenization framework and pointed out that while the RBI's directive aims to eliminate storage of card details by merchants, gaps persist in areas like consumer consent, transaction reversibility, and coordination between issuing banks and third-party service providers. One core concern is the lack of interoperability — tokens generated with one merchant or platform often cannot be reused or ported, causing friction and inconvenience for users. Data localization mandates have further complicated this by requiring that token vaults and processing infrastructure remain within Indian borders, raising questions about scalability and cross-platform coordination (Basu, 2022). On the technical side, Indian researchers like Kashyap et al. have proposed AI-integrated frameworks that not only tokenize data but also predict fraudulent behavior before token issuance. These systems aim to create adaptive security layers suited to India's high-volume, low-margin transaction environment. Together, these studies emphasize that tokenization in India is not just about technology — it's deeply entangled with legal, infrastructural, and user-experience challenges.

2.2 Indigenous Innovations in Tokenization Technology

While India may not yet be a hub for tokenization-related patents like the U.S., indigenous innovation is thriving through platforms and partnerships driven by domestic fintechs and regulators. Indian players like **Razorpay**, **Cashfree**, and **Pine Labs** have introduced tokenization-as-a-service (TaaS) models to help thousands of small and medium-sized merchants integrate tokenization with minimal technical overhead. These models are especially tailored for India's fragmented and multilingual payment ecosystem, offering SDKs that work across devices and vernacular apps. The RBI has also authorized card networks such as **Visa**, **Mastercard**, and **RuPay** to act as Token Service Providers (TSPs), establishing a robust structure for token lifecycle management. Meanwhile, innovations around token refresh and dynamic expiry — such as time-limited tokens or those that automatically invalidate after usage — are being tested in collaboration with the **NPCI** and bank-led consortiums. Although these developments aren't formalized through patent filings, they reflect a rich undercurrent of homegrown ingenuity that aligns with India's fast-moving digital economy and policy imperatives.

2.3 Expanding Tokenization: Localized Use Cases and Emerging Solutions

Tokenization in India is extending beyond traditional card-based transactions into diverse and localized domains. One notable application has been in **UPI-linked credit card payments**, where tokenization ensures card details remain secure even as transactions are routed through mobile interfaces. Similarly, Indian fintechs are exploring tokenized voucher systems for use in **government subsidy disbursement**, **school fee payments**, and **public healthcare billing**. For instance, pilot projects in states like Telangana have used blockchain-linked token systems to ensure that medical reimbursements to low-income beneficiaries are tamper-proof and traceable (LiveMint, 2023). These efforts mirror global ideas, but with

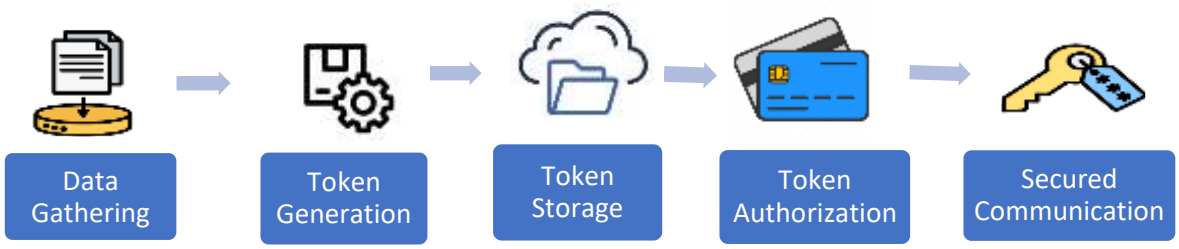
a uniquely Indian twist: solving logistical inefficiencies and corruption in welfare delivery through token-based mechanisms. Outside finance, researchers have also proposed tokenizing academic credentials to curb document forgery and streamline verifications across Indian universities (Rani et al. 2023). Such applications demonstrate that in India, tokenization isn't just about fraud prevention — it's becoming a tool for systemic accountability and trust-building.

2.4 Academic Perspectives and Blockchain Synergy in India

Indian academic institutions and blockchain consortia have started to seriously engage with the future of tokenization, especially in decentralized contexts. Researchers like Rani et al. (2023) have proposed frameworks where tokenized student records are stored on permissioned blockchains, allowing universities to securely verify degrees and exam results without manual paperwork or third-party background checks. In the financial domain, Granja (2024) and Royyuru et al. (2023) explored how blockchain can decentralize token storage, aligning with India's data sovereignty goals. Their models suggest a future where tokens are not stored in central vaults, but distributed across verified nodes — potentially linked to Aadhaar-verified digital identities. The **Indian Institute of Technology (IIT)** campuses have also conducted simulations on blockchain-enabled, tokenized microloans for rural markets, using dynamic smart contracts to release credit based on real-time repayment behavior. These experiments underline a shift in academic thinking: from tokenization as a security patch to tokenization as the foundation of transparent, decentralized, and inclusive digital ecosystems.

3. Technological Framework

Card tokenisation leverages advanced encryption techniques to replace card details with a token unique to each transaction. The process involves:



- **Data Gathering**: This is the process of safely and legally obtaining and preserving private credit card information. Credit card numbers, expiration dates, card verification value (CVV) codes, and occasionally even the cardholder's name and billing address are gathered when consumers use their credit cards to make purchases.
- **Token Generation:** This is the process of replacing sensitive credit card information with one-of-a-kind, useless identifiers known as tokens.
- **Token Storage:** After the token is generated, the token is safely kept in a token vault, which is a strictly regulated database. Without keeping the actual card information, this vault connects the produced tokens to the original credit card data. The saved tokens can only be accessed and interacted with by authorized persons and systems.
- **Token Authorisation**: It is used for subsequent transactions, ensuring seamless and secure payments (Visa, 2023).

- **Secured Communication**: This procedure makes sure that payment data is kept private and secure while it travels between the several systems and parties that handle the transaction.

4. Adoption Trends

India rapidly accepted tokenisation once it was put into place:

- **560 Million Tokens Issued:** Within a year after the mandate, more than 560 million tokens were produced. (RBI, 2023)
- **Transaction Volumes:** Tokenised transactions exceeding ₹5 lakh crore. (RBI, 2023)
- **Consumer Perception:** Enhanced trust in digital payments due to improved security (Visa, 2023).

5. Benefits of Tokenisation

- **Internal Protection:** Anonymous hackers are not just discouraged by tokenisation. Additionally, it shields private data from others associated with your company, such as suppliers, vendors, and workers. Only the payment processor is able to interpret randomly generated payment IDs.
- **Data Isolation:** In the unlikely scenario that one piece of data is compromised, other data remains secure because the secured data is no longer linked to customer or personal information (for example, customer names are stored independently from their date of birth, Social Security number, etc.). As a result, any compromised data is worthless and does not provide a security risk.
- **Reduced PCI scope:** Since tokenisation eliminates the need for retailers to retain sensitive consumer data, it makes it simpler for them to comply with PCI.
- **Online Protection:** Recently, EMV—chip-enabled credit cards that provide additional security—was adopted by all businesses. Customers must provide a signature or personal identification number (PIN) and the chip must be present for a transaction to be completed. Unfortunately, since the chip isn't physically present at the moment of purchase, this feature becomes outdated in the online world. Tokenisation, on the other hand, provides unmatched security for both online and offline transactions.
- **Compatible with Other Technologies:** In addition to credit/debit card , tokenisation also works with gift cards, NFC payments, ACH transfers, and Apple Pay; regardless of how customers choose to send and receive money, their data is protected.
- **Protection of Other Information:** By using tokenisation, merchants can safeguard a variety of financial and personally identifying data, such as employee files, patient records, email addresses, usernames, and passwords.
- **Cost-Effective:** In addition to being simple to execute, tokenisation is extremely economical. (Nisum, n.d.)

6. Discussion

6.1 Current Trends and Innovations in India

Tokenization in India is evolving rapidly, driven by the Reserve Bank of India's policy push and a booming digital payments ecosystem. The RBI's mandate on card-on-file tokenization has catalysed innovation across fintech companies, banks, and payment gateways. Companies like **Razorpay**, **Cashfree**, and **Pine Labs** are deploying tokenization APIs that enable real-time card masking and token provisioning, compliant with RBI guidelines. What's particularly Indian about these innovations is their scale and

inclusivity — they are built to handle millions of low-value transactions over diverse networks, including UPI and mobile-first platforms.

Blockchain is also starting to play a more experimental role in this landscape. The **National Payments Corporation of India (NPCI)** has explored blockchain frameworks for secure token storage within the **RuPay** and **UPI ecosystem**. While still in pilot stages, such distributed ledger-based models aim to eliminate single points of failure, thereby mitigating the risk of centralized token vault breaches. Meanwhile, AI is gaining traction in fraud detection: some Indian banks have begun integrating behavioral analytics to identify unusual spending patterns even before a token is issued, helping intercept fraud in real time (Kashyap et al., 2022). These innovations are still emerging, but they reflect a distinct movement: India's tokenization model is not just mimicking global tech, but crafting unique, scalable solutions that fit its own payment behavior and infrastructure.

6.2 Regulatory and Privacy Challenges in the Indian Context

Despite the forward momentum, India's tokenization journey is not without roadblocks. Regulatory clarity, while improving, remains a source of confusion for many stakeholders. Banerjee et al. (2022) noted that while the RBI's intentions were clear — to protect consumers by prohibiting the storage of card details — implementation left merchants scrambling. Small businesses especially struggled to adopt tokenization in time, citing inadequate technical support and a lack of readiness from banks. Issues around **interoperability**, **API integration**, and **data localization** have further complicated adoption.

India's **Personal Data Protection Act (PDP Bill)**, still evolving in its final form, introduces new layers of ambiguity. Token data — though anonymized — may still be considered personal data under some interpretations, making storage and transfer a legal grey area (Basu, 2022). Cross-border transactions further blur compliance boundaries, especially for international e-commerce platforms operating in India. In addition, while the RBI discourages centralized storage of card data, most tokenization infrastructures still rely on vaults maintained by large payment networks or processors. These vaults, if breached, could expose millions of token-to-card mappings — a structural vulnerability yet to be resolved. For India, the challenge is not just in designing secure systems, but in coordinating legal, technological, and operational standards across an extremely fragmented ecosystem.

6.3 Future Prospects for Tokenization in India

Looking ahead, the next phase of tokenization in India will likely center around **decentralization**, **biometric integration**, and **context-aware security models**. Indian researchers and blockchain startups are actively experimenting with **decentralized token vaults** — systems that store tokens across distributed nodes, making them harder to compromise and easier to audit. These innovations could align well with India's ongoing push for **sovereign digital infrastructure**, especially under initiatives like **India Stack** and **DigiLocker**.

Biometric-linked tokenization is also gaining interest. With India's vast **Aadhaar** infrastructure already in place, there's potential to fuse fingerprint or iris-based authentication with token issuance. In such systems, a token wouldn't just be tied to a device or merchant — it would be cryptographically linked to a unique biometric signature, offering unmatched security and eliminating risks from stolen devices or cloned apps (Karrothu et al., 2024).

Quantum-resistant tokenization, while still a long-term goal, is beginning to enter academic discussions in India as well. Institutions like **IIT Bombay** and **IISc Bangalore** are researching **post-quantum cryptography** models for future-proofing India's financial systems. Meanwhile, real-world applications

such as **tokenized welfare distribution via smart contracts** are being piloted by state governments and NGOs, offering transparent delivery of subsidies with zero leakage.

In short, the future of tokenization in India is not just about compliance — it's about building trust in a digital economy at a massive scale. The next generation of systems will need to be **context-aware**, **AI-enhanced**, **biometrically linked**, and **quantum-ready** — all within a regulatory landscape that protects consumer rights while enabling innovation.

Conclusion

There's no doubt anymore — tokenization works, and in India, it has become a foundational pillar in securing digital payments. It's no longer a futuristic concept but an everyday reality embedded in how we pay for groceries on mobile apps, subscribe to OTT platforms, or authorize card payments on e-commerce sites. Since the **RBI's CoF tokenization mandate** came into effect, millions of Indian card transactions now rely on this invisible shield that turns sensitive data into unusable tokens. As Banerjee et al. (2022) emphasized, tokenization hasn't just slowed down fraud — it has significantly narrowed the attack surface, replacing vulnerable card data with strings of context-bound characters that can't be reused or stolen with ease.

However, the journey is far from complete. India's digital economy is vast and diverse, and with it comes a tangled web of challenges. Differing interpretations of **data localization**, evolving **data protection laws**, and limited consumer awareness have complicated rollout and compliance. What works for large fintech giants may overwhelm small merchants. And without standardized technical frameworks across banks, processors, and merchants, fragmentation persists. Tokenization needs more than tech fixes — it needs **coordinated governance**, **industry consensus**, and **regulatory clarity** at every level. If not, we risk a future where some players overcomply and stifle innovation, while others fall behind and expose users to new vulnerabilities.

Looking forward, **India has a unique opportunity to lead globally** in building tokenized systems that are decentralized, inclusive, and resilient. Blockchain-based token vaults, like those being piloted by Indian researchers, could remove single points of failure and bring transparency to how token data is stored and accessed. Biometrics, especially when linked with India's robust Aadhaar infrastructure, could make token-based payments not just secure, but truly user-specific. And with **quantum threats on the horizon**, Indian institutions must begin investing in **quantum-resistant encryption**, preparing for tomorrow's risks before they become today's breaches.

At its core, tokenization is more than just a cybersecurity measure — it's a shift in philosophy. It says that your card data, your identity, your digital presence **belongs to you — not to platforms, processors, or hackers**. It's not perfect, and it's still evolving, but for India, it represents the best hope we have for building a digital payments infrastructure that is **trusted, scalable, and future-ready**.

References

1. Banerjee, S., Shukla, S., & Menon, K. S. (2022). The Tokenisation Framework and Its Privacy Discontents: Issues and Solutions. *NUJS L. Rev.*, *15*, 208.
2. Basu, P. (2022). Digital Transformation with Digital Assets-Tokenisation and Management by Technology Driven Processes. *The Management Accountant Journal*, *57*(6), 86-93.
3. Granja, E. N. C. (2024). Developing a Next-Generation Tokenization Framework to Secure Digital Payments.

4. Harraway, T., & Bekker, J. (2024). Voucher tokenisation using blockchain and smart contracts to support people in need. *South African Journal of Science*, *120*(11/12).
5. Karrothu, A., Mahesh, U., Bhanu, P., & Sahu, T. C. (2024, May). A Two-Factor Authenticated and Secure Credit Card System for E-Platforms. In *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 871-874). IEEE.
6. Kashyap, D. N., Naikade, K., Pandey, A. K., Sharma, N., Hashmi, S., & Pund, S. S. Enhancing Credit Card Data Security Using AI-integrated Encryption and Tokenization Framework.
7. Nisum. (n.d.). *White Paper: Tokenization: Credit Card Fraud Prevention, Beyond PCI Measures*. Nisum. https://www.nisum.com/nisum-knows/white-paper-tokenization-credit-card-fraud-prevention-beyond-pci-measures
8. Rani, P., Sachan, R. K., & Kukreja, S. (2023). Academic payment tokenization: an online payment system for academia utilizing non-fungible tokens and permissionless blockchain. *Procedia Computer Science*, *230*, 347-356.
9. *Reserve Bank of India - press releases*. (n.d.). https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=56503
10. Royyuru, V., Goodheart, R., Byers, L., Horton, T., Whalen, K., & Zhu, L. (2023). *U.S. Patent No. 11,748,744*. Washington, DC: U.S. Patent and Trademark Office.
11. *Visa Tokenisation Report forecasts six digital payment trends in India*. (2023). Visa. https://www.visa.co.in/about-visa/newsroom/press-releases/visa-tokenisation-report-forecasts-six-digital-payment-trends-in-india.html