2025
ASIA-PACIFIC
COMMUNITY
MEETING

Evolving Payment Security Landscape of India & South Asia

PCI Security Standards Council®

Anuj Tewari

Cyber Risk Strategist

Senior Vice President

Axis Bank Pvt.Ltd.

AXIS B

PCI Security Standards Council

Evolving Payment Security Landscape of India & South Asia

A Comprehensive Analysis of Payment Products and Security Controls

Overview

The payment security landscape in India and South Asia has undergone dramatic transformation over the past decade, driven by digital adoption, regulatory frameworks, and emerging threats. This presentation examines the security controls implemented across various payment products in the region.

Key Highlights

- **Digital Payment Growth**: India processed over 13.2 billion digital transactions in FY 2024
- **Regulatory Evolution**: RBI, NPCI, SEBI, PFRDA, IRDAI and regional central banks have strengthened security mandates
- **Emerging Threats**: Sophisticated fraud schemes targeting mobile payments and digital wallets
- **Security Innovation**: Implementation of AI/ML-based fraud detection and biometric authentication

PCI Security Standards Council®

Market Overview & Growth Drivers

Market Dynamics

India Payment Security Market:
USD 3.96 billion (2024) → USD 9.62 billion (2030)
Growth Rate: 15.77% CAGR
Key Drivers: Digital payment adoption, regulatory compliance, fraud prevention

Regional Context

APAC Leadership: 23.76% global market share
Leading Countries: China, India, Japan, South Korea
Innovation Hub: Fintech security solutions driving growth

- Increasing Digital Fraud
- Evolving Cyber Threats
- Regulatory Compliance
- Data Protection
- Consumer Trust

PCI Security Standards Council

Regional Payment Ecosystem Overview

India's Digital Payment Infrastructure

Unified Payments Interface (UPI): 13.2+ billion transactions monthly
Immediate Payment Service (IMPS): Real-time fund transfers
RuPay Card Network: Domestic card scheme with 750+ million cards
Digital Wallets: Paytm, PhonePe, Google Pay dominating market
Digital Rupee: Central bank digital currency (CBDC)
Contactless Payment: Pay using near-field communication (NFC) technology

South Asian Payment Landscape

Bangladesh: bKash, Nagad mobile financial services
Sri Lanka: LankaPay, eZ Cash digital payment solutions
Nepal: Khalti, eSewa, Nepal Payment System (NPS)

UPI (Unified Payments Interface) Security Controls

Multi-Layer Security Architecture

- **Device Binding:** App installation linked to device IMEI
- **SIM Binding:** UPI PIN tied to registered mobile number
- **Biometric Authentication**: Fingerprint/face recognition for app access
- **Two-Factor Authentication:** UPI PIN + device authentication

Transaction Security Controls

- **Real-time Fraud Monitoring**: AI/ML algorithms detect suspicious patterns
- **Transaction Limits:** Daily / Monthly / Per transaction
- **Collect Request Validation:** Time-bound payment requests
- **Merchant Verification:** KYC compliance for merchant onboarding

Technical Safeguards

- **End-to-End Encryption:** TLS 1.2+ for all communications
- **Tokenization:** Card details replaced with unique tokens
- **API Security:** OAuth 2.0 and JWT token validation
- **Network Security:** Dedicated secure networks for payment processing

Credit & Debit Card Security Controls

EMV Chip Technology

- **Dynamic Data Authentication:** Unique transaction codes prevent cloning
- **Offline PIN Verification:** Secure PIN validation without network dependency
- **Application Cryptogram:** Transaction-specific security codes
- **Certificate-based Authentication:** Issuer and card authentication

PCI Compliance

- **PCI DSS:** People, Process & Tech Security
- **PCI PIN:** PIN Security
- **PCI HSM:** HSM Security
- **PCI P2PE:** Point to point encryption
- **PCI PTS:** Hardwares, Firmware Security
- **PCI MPOC:** Mobile Pyaments on COTS
- **PCI SPOC:** Software based PIN entry on COTS

Online Transaction Security

- **3D Secure 2.0:** Enhanced authentication with risk-based decisions
- **OTP Verification:** SMS/Email based one-time passwords
- **Device Fingerprinting:** Behavioral analytics for fraud detection
- **Velocity Checks:** Transaction frequency and amount monitoring

Regulator Mandated Controls

- **Additional Factor Authentication (AFA):** Mandatory for online transactions
- **Transaction Monitoring:** Real-time fraud detection systems
- **Merchant Category Code (MCC) Restrictions:** Limiting high-risk transactions
- **Chargeback Management:** Structured dispute resolution process

PCI Security Standards Council®

Mobile / Internet Banking Security Controls

Authentication Mechanisms

- **Multi-Factor Authentication**: Something you know + have + are
- **Biometric Login:** Fingerprint, face, and voice recognition
- **Device Registration:** Secure device binding with bank servers
- **Session Management:** Automatic timeout and session encryption
- **Virutal Keyboard, Captcha, Adaptive Authentciation:** Advance User authentciation

Transaction Security

- **Digital Signatures:** PKI-based transaction signing
- **Transaction Limits:** Tiered limits based on authentication strength
- Beneficiary Management: Pre-approved and verified payee lists
- Geo-location Verification: Location-based transaction validation

Mobile App Security

- **App Hardening:** Anti-tampering and reverse engineering protection
- **Certificate Pinning:** Preventing man-in-the-middle attacks
- **Root/Jailbreak Detection:** Blocking access on compromised devices
- **Secure Communication:** End-to-end encrypted channels
- **Containerizaton:** App Sandbox
- **Anti Malware Capabilties:** In mobile apps

Regulator Mandated Controls

- **RBI Guidelines**: Adherence to digital banking security standards
- **Data Localization:** Customer data storage within India
- **Audit Trail:** Comprehensive logging of all transactions
- **Incident Response:** Structured security incident management

PCI Security Standards Council®

Digital Wallet Security Controls

Account Security

- **KYC Verification**: Identity verification for full wallet access
- **Wallet Limits:** Transaction and balance limits based on KYC level
- **Device Authentication:** Secure device registration and management
- **Biometric Security**: Fingerprint/face unlock for wallet access

Transaction Controls

- **Real-time Monitoring:** AI-powered fraud detection algorithms
- **Velocity Limits:** Frequency and amount-based restrictions
- **Merchant Verification:** Comprehensive merchant onboarding process
- **Refund Protection:** Automated refund processing for failed transactions

Technical Security

- **Tokenization:** Sensitive data replaced with non-sensitive tokens
- **Encryption:** AES-256 encryption for data at rest and in transit
- **API Security:** Rate limiting and authentication for all APIs
- **Fraud Analytics:** Machine learning models for pattern recognition

Regulatory Adherence

- **PPI Guidelines:** Compliance with RBI prepaid payment instrument norms
- **Escrow Account Management:** Customer funds held in secure escrow
- **Reporting Requirements:** Regular transaction reporting to authorities
- **Grievance Redressal:** Structured customer complaint resolution

RTGS/NEFT Security Controls

System-Level Security

- **Dedicated Network:** INFINET for secure interbank communication
- **Message Authentication:** SWIFT-like message validation
- **Straight-Through Processing:** Automated transaction processing
- **End-to-End Encryption:** Complete message encryption

Operational Controls

- **Dual Authorization:** Multiple approvals for high-value transactions
- **Time-based Processing:** Defined settlement windows
- **Liquidity Management:** Real-time liquidity monitoring
- **Risk-based Monitoring:** Automated suspicious transaction detection

Regulatory Framework

- **RBI Oversight:** Direct central bank monitoring
- **Settlement Finality:** Irrevocable transaction completion
- **Audit Requirements:** Regular system audits and compliance checks
- **Business Continuity:** Disaster recovery and backup systems

Participant Security

- **Bank Authentication:** Strong participant verification
- **Transaction Limits:** System-wide and participant-specific limits
- **Reconciliation Process:** Daily settlement reconciliation
- **Fraud Reporting:** Structured fraud incident reporting

Cross-Border Payment Security

SWIFT Security Framework

- **Customer Security Programme (CSP):** Mandatory security controls
- **Message Authentication:** LAU (Local Authentication Unit) validation
- **Network Security:** Dedicated secure network infrastructure
- **Incident Response:** Structured security incident management

Correspondent Banking Controls

- **Due Diligence:** Enhanced KYC for correspondent relationships
- **Transaction Monitoring:** AML/CFT compliance systems
- **Sanctions Screening:** Real-time sanctions list checking
- **Regulatory Reporting:** Cross-border transaction reporting

Regional Integration

- **SAARC Payment Framework:** Regional payment system integration
- **Bilateral Agreements:** Country-specific payment arrangements
- **Currency Controls:** Exchange rate and currency conversion security
- **Cross-border Regulations:** Compliance with multiple jurisdictions

Emerging Technologies

- **Blockchain Integration**: Distributed ledger for transparency
- **Central Bank Digital Currencies (CBDCs):** Digital rupee pilot programs
- **ISO 20022 Migration:** Enhanced message format adoption
- **Real-time Cross-border Payments:** Instant international transfers

Regulatory Landscape & Compliance

Reserve Bank of India (RBI) Framework

- **Payment & Settlement Systems Act 2007:** Legal foundation
- **Master Directions:** Comprehensive guidelines for payment systems
- **Cyber Security Framework:** Mandatory security standards
- **Data Protection Requirements:** Customer data security mandates

Regional Regulatory Bodies

- **Bangladesh Bank:** Mobile financial services regulations
- **Central Bank of Sri Lanka:** Payment system licensing
- **Nepal Rastra Bank:** Payment service provider guidelines

Compliance Requirements

- **Know Your Customer (KYC):** Customer identification and verification
- **Anti-Money Laundering (AML):** Suspicious transaction monitoring
- **Combating Financing of Terrorism (CFT):** Terrorism financing prevention
- **Data Localization:** Customer data storage within jurisdiction

International Standards

- **Basel III:** Banking supervision framework
- **FATF Recommendations:** Financial crime prevention guidelines
- **ISO 27001:** Information security management
- **PCI DSS:** Payment card industry security standards
- **NIST CSF 2.0:** Cyber Security Framework

PCI Security Standards Council®

Emerging Threats & Challenges

Sophisticated Fraud Schemes

- **Social Engineering:** UPI fraud through fake customer service
- **SIM Swapping:** Mobile number hijacking for payment fraud
- **Phishing Attacks:** Fake payment apps and websites
- **Account Takeover:** Unauthorized access to payment accounts

Technology-Driven Threats

- **API Vulnerabilities:** Exploitation of payment system APIs
- **Mobile Malware:** Banking trojans and payment app targeting
- **Man-in-the-Middle Attacks:** Interception of payment communications
- **Deepfake Technology:** AI-generated voice for authentication bypass

Operational Challenges

- **Interoperability Issues:** Cross-platform payment integration
- **Scalability Concerns:** System performance during peak loads
- **Regulatory Compliance:** Keeping pace with evolving regulations
- **Customer Education**: Awareness about payment security practices

Regional Specific Challenges

- **Digital Literacy:** Varying levels of user awareness
- **Infrastructure Gaps:** Network connectivity and power issues
- **Regulatory Harmonization:** Inconsistent regional regulations
- **Cross-border Coordination:** International fraud investigation

PCI Security Standards Council®

AI/ML in Payment Security

Fraud Detection Algorithms

- **Anomaly Detection:** Identification of unusual transaction patterns
- **Risk Scoring:** Real-time transaction risk assessment
- **Behavioral Analytics:** User behavior pattern recognition
- **Network Analysis:** Identification of fraud rings and networks

Machine Learning Applications

- **Supervised Learning:** Historical fraud data for model training
- **Unsupervised Learning:** Discovery of unknown fraud patterns
- **Deep Learning:** Complex pattern recognition in large datasets
- **Reinforcement Learning:** Adaptive fraud prevention systems

Implementation Across Products

- **UPI Fraud Prevention:** Real-time transaction monitoring
- **Card Fraud Detection:** Purchase pattern analysis
- **Mobile Banking Security**: Login behavior monitoring
- **Digital Wallet Protection:** Spending pattern analysis

Challenges and Opportunities

- **False Positives:** Balancing security with user experience
- **Model Interpretability:** Understanding AI decision-making
- **Data Quality:** Ensuring accurate and comprehensive datasets
- **Regulatory Compliance:** AI governance and accountability

PCI Security Standards Council®

Future Outlook & Recommendations

Technological Evolution

- **Quantum-Safe Cryptography:** Preparing for quantum computing threats
- **Biometric Advancement:** Multi-modal biometric authentication
- **Blockchain Integration**: Decentralized payment security
- **IoT Payment Security:** Securing Internet of Things payments

Regulatory Development

- **Unified Regional Standards:** Harmonized payment security regulations
- **Open Banking Security:** Secure API standards for financial services
- **Digital Identity Framework:** National digital identity integration
- **Cross-border Regulation:** International payment security coordination

Industry Recommendations

- **Continuous Monitoring**: Real-time threat detection and response
- **Collaborative Defense:** Industry-wide threat intelligence sharing
- **Customer Education:** Comprehensive security awareness programs
- **Innovation Balance:** Security enhancement without user friction

Strategic Priorities

- **Invest in AI/ML:** Advanced fraud detection capabilities
- **Strengthen Partnerships:** Public-private security collaboration
- **Enhance Resilience:** Robust business continuity planning
- **Focus on User Experience:** Seamless security implementation

PCI Security Standards Council®

Key Takeaways

The payment security landscape in India and South Asia has evolved significantly with robust controls across all payment products. However, the threat landscape continues to evolve, requiring continuous adaptation and innovation.

Success Factors

- **Regulatory Leadership:** Strong government and central bank oversight
- **Technology Innovation:** Adoption of advanced security technologies
- **Industry Collaboration:** Coordinated approach to security challenges
- **Customer Awareness:** Educated users as the first line of defense