Cyber Resilience & Digital Payment Security Controls

Non-bank Payment System Operators

AI Perspectives & Challenges

Dr. Srinivas Yanamandra
Professor of Practice (Visiting), IDRBT

December 2025

Brief Profile

- **Qualifications**
  - Cost Accountant from ICWAI (2000)
  - Chartered Accountant from ICAI (2001)
  - Doctor of Business Administration (DBA) from Manchester University UK (2013)
- **25 Years of Regulatory Compliance expertise (Banks / Fintech)**
  - Indian Banks - ICICI Bank (2003-14), IDFC First Bank (2015-16)
  - International - BRICS New Development Bank (Shanghai, China) (2017-22)
  - Fintech - Paytm (2022-25)
- **Professional Highlights**
  - TEDx Speaker (2020 / 2023) / Winner of CA Global Achiever Award from ICAI (2019)
  - Visiting Fellow - Cambridge Institute for Sustainability Leadership (2019)
  - Chevening India Cyber Security Fellow - Cranfield University, UK (2025)
- **Academic Engagements**
  - Research Fellow - Indian School of Business, Hyderabad (since 2020)
  - Non-Resident Senior Fellow - Dhirubhai Ambani School of Law (since 2025)
  - Visiting Professor of Practice - IDRBT (since 2025)

Agenda

Non-Bank Payment System Operators

AI & Payment Innovation

AI & Cyber Security

Conclusion

Bank-dominated Payment Systems

Traditionally banks dominated the payment systems in the country

Introducing new ways of making the payments at their own pace - cheque truncation, internet banking and plastic money.

Food for
Workshop Discussion !!!



Cheques



Net-Banking



Cards

Challenges

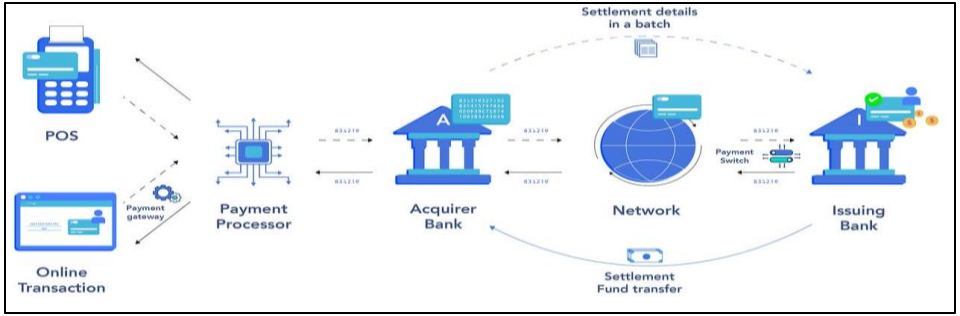
- Accessibility
- Availability
- Affordability

While innovations did happen through banks, it did not meet demand for micro-payments in a big way

Non-Bank Payment Aggregators

Specialized set of licensed players regulated by RBI in Payments space

PAs enable merchants to accept payments by connecting them to the customers' payment instruments & broader financial infrastructure.



Online | Offline | Cross-Border

Food for Policy Discussion !!!

Technology

- PoS Machines - Repurposed
- Payment Gateways
- Payment Soundboxes

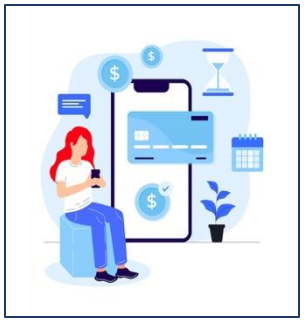
RBI Guidelines mandate requirements for onboarding / settlement of merchants

CyberSec Perspectives

Developments in payments eco-system shifts the focus towards Cyber security

Owing to the way payment companies are facilitating open finance requirements of customers / merchants

Food for
Classroom Discussion !!!



APPs



APIs



APKs

Cyber Resilience

- Technological Resilience
- Operational Resilience
- Financial Resilience

Motivated by external elements such as organized cyber crime and CRINGE factors

Agenda

- Non-Bank Payment System Operators
- **AI & Payment Innovation**
- AI & Cyber Security
- Conclusion

Applications (APPs)

Mobile apps are currently enhancing the payments experience at the end of customers

Artificial intelligence features are at the core of customer payment experience.

Food for
Classroom Discussion !!!



eCommerce



PPIs



TPAPs

AI Integration into APPs

- Liveliness Checks
- Behavior Biometrics
- Adaptive Authentication

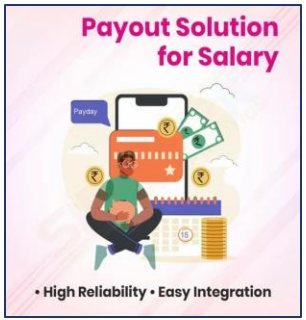
Providing personalized payment experience and security issues for customers

Application Programming Interfaces (APIs)

APIs facilitate payments experience at the end of merchants / corporates

Drastically reducing the need for merchant / corporate to interact with the banks on a day-to-day basis

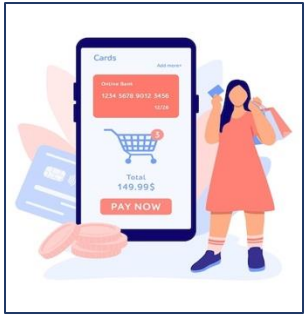
Food for Classroom Discussion !!!



Salary Processing



Reward Points



POS Financing

AI integration into APIs

- Payment Orchestration
- Dynamic Checkouts
- Agentic Commerce

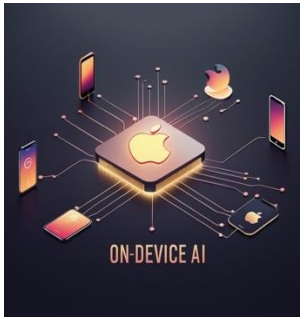
Raising new threat vectors and new supply chain vulnerabilities

Android Packages (APKs)

APKs are the packaged files used to install Android apps, like IPA files on iOS

The scripts of AI files are embedded in the SDKs and are delivered to the mobile applications via APKs

Food for
Classroom Discussion !!!



On-Device Models



SDKs



APKs

AI Integration using APKs

- AI Contextual Autofill
- AI Smart Nudges
- AI Without Internet

APKs can be vulnerable if their code, libraries, or permissions are tampered with or poorly secured

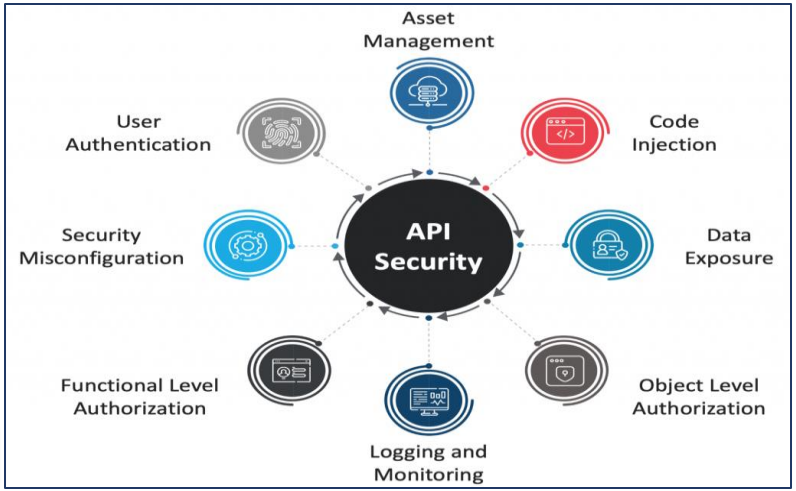
Agenda

- Non-Bank Payment System Operators
- AI & Payment Innovation
- **AI & Cyber Security**
- Conclusion

Emerging monitoring requirements for preventing misuse of APIs

How are API risks handled in the organization?

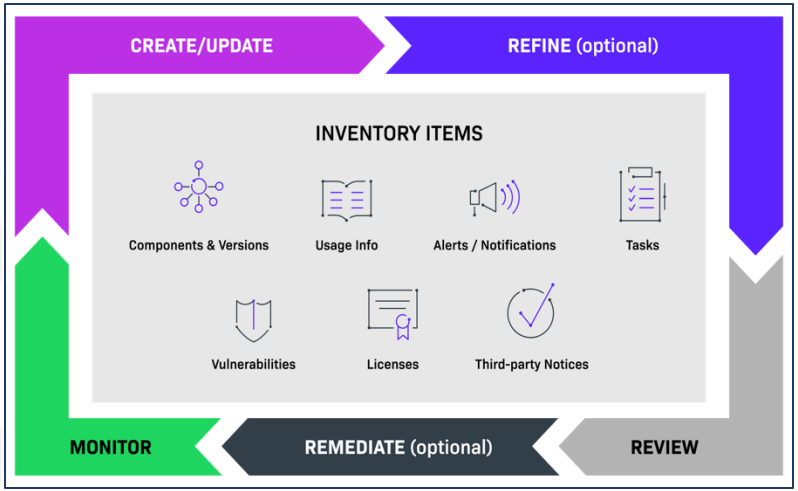
- Finding balance between agility & vulnerability
- Accounting for API inventory
- Formalizing the API due diligence process
- Instituting API controls (e.g., Throttles)
- Case-in-point: *RBI Guidelines on APIs*



Evolving Bill-of-Material (BOM) requirements for deploying APKs

How is AI deployment tightened with Bill-of-Materials (BOM)?

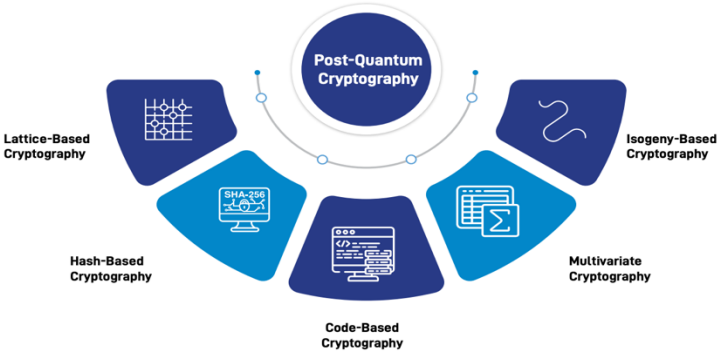
- Model Components & Dependencies
- Data Sources & Provenance
- Infrastructure, Compute & Operations
- Risk, Safety, Governance & Compliance
- Case-in-point: *CERT-IN Regulations / IT Tools*



Embracing Post-Quantum challenge to encryption in APPs

How are cyber risks assessed from PQC standpoint?

- Current classical computing (KEM / DSA) (S / AS)
- Quantum Threat Horizon (RSA / ECC)
- Paths to PQC - Physics (QKD) / Maths (non-QKD)
- CARAF (existing IT) & Rapid Swap-Out (future IT)
- Case-in-point: *SEBI CSCRF Guidelines*



Ref: RBIH Whitepaper: *Securing the Indian Banking Sector in the Age of Quantum Computing Migrating to Post Quantum Cryptography*

Agenda

- Non-Bank Payment System Operators
- AI & Payment Innovation
- AI & Cyber Security
- **Conclusion**

Conclusion

Non-Bank Payment System Operators		
TPAPs	PPIs	PAs

Channels for AI Impact		
APPs	APIs	APKs

Monitoring Risks		
APIs	BOM	PQC

Thank You

Stay connected:

dryanamandra@icloud.com

+91 98215 09192