International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 6, Nov- Dec 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Digital Payments: Emerging Threats and Revamping Cyber Security Strategies

V. Swarnalatha, M.Com.,SET,
Lecturer in Commerce, SWR Govt. Degree College for Girls, Kalikiri, AP,India
Email: swarnalatha.m22@gmail.com

Abstract

The current National Cyber Security Policy was adopted under a prior regime and does not reflect policy priorities such as Digital India; the Smart Cities Mission; the push for digital financial inclusion; and next-gen technological movements, e.g. the Internet of Things (IoT) and artificial intelligence. Moreover, the capacity-building provisions of the policy were designed based on five-year targets (starting 2013). Even normatively, the NCSP appears incomplete as it does not address how Indian cyber- security strategies can be augmented by engaging the international community. While the NCSP refers to needs relating to greater bilateral and multilateral arrangements; greater cooperation with international law enforcement agencies, judicial systems and security agencies like CERTs; and creating mechanisms for technical dialogue -- these provisions have lacked specificity or defined processes to further such goals. Thus, it is now time for India to update its NCSP to reflect current technological and ecosystem realities, and provide special emphasis on challengesrelating to the international dimension of the cyberspace.

Key Words: Digital India, National Cyber Security Policy, Computer Emergency Response Team, Digital Payments Eco System, Cyber Space, Digidhan Mission.

Introduction

The term "digital payments" is used for both "online" and "mobile" payment systems. Some common payment and settlement options in India include interbank card (both debit and credit) networks, National Electronic Funds Transfer (NEFT), Real-Time Gross Settlements (RTGS), Immediate Payments Service (IMPS), the Unified Payments Interface (UPI), Aadhaar-Enabled Payment System (AEPS), Bharat Bill Payment System (BBPS), National Electronic Clearing Service (NECS), the consolidated National Automated Clearing House (NACH), Internet Banking, Mobile Banking, Unstructured Supplementary Service Data (USSD), and Prepaid Payment Instruments (PPIs) or "mobile wallets."

The scaling up of such modernised economies necessitates a simultaneous modernisation of legal, regulatory and institutional frameworks, and Indian decision-makers are cognisant of this. For instance, in 2017, the Supreme Court of India made a landmark pronouncement that an individual's right to privacy is a fundamental right under Article 21 of the Indian Constitution. The nine-judge bench categorically included informational privacy (relevant for internet/data economies) as a key constituent of this umbrella right.

The Indian government has outlined a target of creating a US$1-trillion digital economy by 2025. Digital payments are an important constituent of this target and a national payments mission ('Digidhan Mission') has been initiated

 ©IJSRED: All Rights are Reserved

under the aegis of the Ministry of Electronics and Information Technology. Such policy impetus has allowed the sector to continue its robust growth, clocking around 20.7 billion digital transactions in FY 2017–18, an 89.5 percent increase from the previous fiscal year. Moreover, as India's wider digital ecosystem continues to grow, there will be an increase in the adoption of digital payments. Key indicators in this regard include 560.01 million internet users; around 1.17 billion wireless users and around 404.1 million smart phone users. Extrapolating from these figures, India's digital-payments market is on paceto be a US$1-trillion proposition by 2023.

Objectives

1. To identify and evaluate the evolving cyber threats in digital payments
2. To Construct security frame works for digital payments
3. To secure the entire digital-payments ecosystem, which includes reviewing the efficacy of extant institutional and security frameworks.
4. To appraise the various moving parts within digital payments and broader policy making arenas.
5. To propose a forward-looking cyber-security strategy for the digital payments sector.

Digital Payments Eco System

In this context, the major supply-side market participants in India's payments ecosystem include:

- **Reserve Bank of India (RBI):** India's sole Large Value Transfer System (LVTS) operator; facilitates both NEFT and RTGS transactions
- **National Payments Corporation of India (NPCI):** India's sole retail payments system/ infrastructure provider, and controller of the National Financial Switch for ATMs
- **Payment Service Providers (PSPs) and Switch Providers:** These include banks, payment banks, mobile wallet companies, online payment gateway service providers, and card- network companies
- **Infrastructure Providers:** ATM network and White Label ATM Operators (WLAOs), Point-of- Sale (PoS) terminal providers, and mobile device providers
- **Other Supply-Side Participants:** Third-party vendors and network/connectivity providers

This list indicates disparate supply chain entry points for malicious actors to exploit. Multiple parties disaggregating digital payments value chains and managing financial data increases the complexity of financial networks and adds to potential cyber risks. This is further illustrated by open-card payment systems, which usually operate on the Four- Party Model, comprising the cardholder, the merchant, the merchant-acquiring bank and the card-issuing bank. Such systems must, therefore, be operated in a manner that engenders trustamongst customers.

The digital-payments ecosystem also includes demand-side participants, i.e. merchants and consumers. The figure below offers a map of the digital-payments landscape from the demand-side perspective

 ©IJSRED: All Rights are Reserved

The Emerging Threats in India's Digital Payments

As the ecosystem expands, Indian decision-makers must evaluate the evolving threat or incident matrix permeating the wider cyberspace. According to the 2018 Thales Data Threat Report, data breaches occur more often in India than the global average. As such, even at a global level, the number of cyber incidents targeting financial institutions continue to increase.

- **Rising Cyber Frauds:** Countries such as Brazil, Canada and Japan have explicitly highlighted identity theft and fraud in relation to 'Card Not Present' (CNP) transactions as a primary threat to their electronic payments frameworks. In India, "cyber fraud" in digital payments rose by around 25 percent (to 16,468 cases) in FY 2015–16. Moreover, during March–December 2017, the number of such cases for credit card, debit card, ATM, and net-banking transactions rose to 22,740. Other threats to digital payments include malware installations, phishing attacks, SIM Card Swap Attacks and unreliable devices.

- **Incidents with NPCI:** In March 2017, hackers took advantage of a bug in the UPI, leading to losses of around INR 250 million for Bank of Maharashtra customers. The NPCI initiallydenied any such breach.

- **Lessons from Other Sectoral Data Breaches:** The Indian e-commerce company Zomato suffered the world's sixth-largest data breach in 2017, compromising 17 million digital records. Exemplarily, Zomato disclosed the incident in a transparent manner and advised users to take specific mitigating action

Cyber Security Strategies

Any cyber-security policy—overarching or for payments—should incorporate the Strategies enlisted below:

- **Sunset Provision:** Similar to the UK government's National Cyber-Security Strategy (2016– 21), a new policy should only be applicable for a specific time period. Additionally, it should be subjected to periodic reviews to ensure that cyber-security efforts keep pace with technological advancements.

- **Standardisation:** Promoting "Security-By-Design," based on the ISO Common Criteria Product Assurance Certification (Singapore Cyber-Security Strategy, 2016).

- **International Dimension:** Countries such as Singapore and the UK tie up with international white-hat hackers, e.g. CREST, to set up penetration and accreditation facilities. Moreover, the US specifies that financial-sector security requires international cooperation (see FS- ISAC).

- **Capacity-Building Strategies:** The UK's strategy relies on market-driven solutions, such as cyber-risk insurance for SMEs, to adopt good cyber-security practices. The UK has implemented a citizen-facing capacity-building programme (Cyber Aware) and a cyber essentials platform to shield SMEs from low-level exploits. In the financial sector, the US' sectoral framework helps SMEs adopt appropriate cyber-security safeguards. The OECD espouses the benefits of introducing security labels to products and services to better inform the market and promoting cyber-security insurance markets.

 ©IJSRED: All Rights are Reserved

Cyber-security strategies must reflect the cross-border aspect of the cyber space. However, the current NCSP fails to provide specific strategies for effective international cooperation. It is important for India to effectively engage with international frameworks that enable cyber-crime investigation. At the same time, the government must recognise that traditional routes under Mutual Legal Assistance Treaty (MLAT) and Letters Regulatory frameworks remain inefficient.

Conclusion:

The Indian government has outlined a target of creating a US$1-trillion digital economy by 2025. Digital payments are an important component of this target and a national payments mission ('Digidhan Mission') has been initiated under the aegis of the Ministry of Electronics and Information Technology (MEITY). As this process continues, the security framework for the system of digital payments must be simultaneously constructed. One clear objective of the *Digidhan Mission* is to secure the entire digital-payments ecosystem, which includes reviewing the efficacy of current institutional and security frameworks. This report contextualises the various moving parts within digital payments and broader policymaking arenas to propose a forward-looking cyber-security strategy for the sector.

References:

1.Devi, S. (2019). Cyber Security In The National Security Discourse. World Affairs: The Journal of International Issues, 23(2).

2.Dilipraj, E. (2013). India's Cyber Security 2013: A Review. Centre for Air Power Studies, 97(14).

3.Dunn Cavelty, M. (2012). The militarisation of cyber security as a source of global tension. Center for Security Studies.

4.Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4).

5.Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in indian context. J. Comput. Inf. Technol, 8(5).

 ©IJSRED: All Rights are Reserved