DSCI
PROMOTING DATA PROTECTION

PayPal

SECURING INDIA'S DIGITAL PAYMENT FRONTIERS

Contents

Foreword: DSCI and PayPal 5

Acknowledgement 7

Executive Summary 9

1. Background 11

2. Digital Payment Landscape: Snapshot 13

3. Fintech Revolution 14

4. Digital Payment Landscape 16

   4.1 Global 16

   4.2 Digital Payment Delivery Channels 16

   4.3 India 27

5. Technological Evolution and Threat Landscape: Global and India 28

6. Public Policies, Regulations, Standards, Frameworks 33

   6.1 India 33

   6.2 Global 38

7. Best Practices for securing the Digital Payment ecosystem 42

   7.1 Global 42

   7.2 India 51

   7.3 Security risks and Challenges: Digital Payment Systems 52

   7.4 Data Protection and Privacy Regulation in India 55

8. Fintech Future intertwined with Cyber Security 60

9. Recommendations 62

   9.1 Public Policy 62

   9.2 Enterprise Security 64

References 66

Glossary 69

Research Team 70

Table of Figures

Figure 1 Digital Payment Cyber Security Journey: India 13

Figure 2 Merchant-Presented Mode Transaction Flow 17

Figure 3 QR Code Payment Architecture 18

Figure 4 Samsung NFC Payment 19

Figure 5 Working of Andriod pay using NFC 20

Figure 6 UPI Architecture 22

Figure 7 Threat Landscape 29

Figure 8 Digital Payment Cyber Security Journey: India 34

Table of Tables

Table 1 Fintech Adoption - APAC, India and Developed Economies 14

Table 2 Public Policies Analysis - India 35

Table 3 Future Public Policies - India 37

Table 4 Risk and Challenges - Digital Payment Systems 54

Table 5 Fintech Future and Cyber Security 61

Table 6 Recommendations - Public Policies 63

Table 7 Recommendations - Best Practices 65

Foreword

Technological advancements in the digital payment ecosystem are changing our lives significantly and providing end consumers with speed, convenience, choice and savings. Undoubtedly, the Fintech revolution which has been sweeping the world off its feet has arrived in India as well, and it's growing stronger day-by-day. India, with a large share of 48% of the world's unbanked and financially underserved, clearly is a critical frontier for digital payments and Fintech Industry in general.

Over the last few years, the digital payment space has grown quite well in India with 400+ organizations working on creating and capturing value in online commerce. India's digital payment industry, which is currently worth around USD 200 Billion, is expected to grow five-fold to reach USD 1 Trillion by 2023, as per a report by Swiss financial services holding company, Credit Suisse. Digital payments present a huge opportunity for various digitization initiatives in the country. Furthermore, the Government's commitment "for creating the right environment for Fintech companies to grow in India" was reiterated by the finance minister during his budgetary speech in early February.

The flywheel effect created through Jan Dhan-Aadhaar and Mobile number (JAM) trinity, growth of the Fintech private sector, and proliferation of mobile phones seem to be spinning at an optimal speed right now. One of the key requirements for sustainable growth and adoption of Fintech solutions at last-mile touchpoints in rural parts of the country is 'trust'. A strong foundation based on resilient and secure infrastructure is one aspect that will define what role Fintech plays in accelerating India's economic development in the next five to ten years.

Technological advancements are enabling digital payment solutions providers to offer personalized experiences that are seamless and user centric. However, the same innovations are also being leveraged by malicious actors in the cyberspace to attack organizations as well as consumers to perpetrate fraud.

The risk perception survey that underpins WEF's Global Risks Report 2018 calls out Cyber Attacks and Data Frauds/Thefts as the predominant likely risks along with Extreme weather and Natural Disasters [1]. Inclusion of two cyber related risks, (cyberattacks and data theft) in the 'Top 5 global risks' for 2018 is a wakeup call for the world and India in particular. Malicious cyber activity pose threats at an individual, enterprise and country level. For instance, a recently released report by the Council of Economic Advisers to the US President estimates that cyberattacks cost the US economy between 57 and 109 billion USD in 2016 [2].

Considering that India is still at an early adoption stage of its digitization journey, it is absolutely critical that the right environment for digital payments include a comprehensive cyber security strategy supported by a robust framework to help all stakeholders involved in the ecosystem.

This report, a partnership between DSCI and PayPal is a joint endeavor to harness the experience and expertise in digital payments and cyber security and share key observations, learnings and recommendations in the Indian context.

While the study contains a concise summary of the evolving digital payment space in India, it also includes global perspectives on Fintech revolution as well as the impact of cyber security on various aspects of the industry. In addition to consumer best practices, key takeaways from the report include recommendations in the areas of public policy and enterprise security. Opportunities, threats and risks in digital payment space are further emphasized to stress the importance of a holistic cyber security framework. To find the right balance between enablement and protection, it is critical that a collaborative effort be undertaken to establish a comprehensive cyber security framework for digital payments in India. This paper outlines key components and recommendations to help accelerate such an initiative.

Emerging tools and technologies like cryptocurrencies, IoT, automation, machine learning, and analytics are redefining the future and Fintech is not immune to these advancements. The report serves as a ready snapshot of the Digital Payment Ecosystem, Threats and associated Cyber Risks, Policy, Regulatory Framework and some best practices. We hope this research report serves all stakeholders in their deliberations in evolving a robust cyber security and policy framework for securing and growing India's Digital Payment momentum.

Rama Vedashree
CEO
DATA SECURITY COUNCIL OF INDIA

Phoram Mehta
Head of Information Security, APAC
PayPal

Acknowledgement

We would like to acknowledge the efforts of various core members from IT, Banking and Government sectors who provided their valuable inputs and guidance throughout the study.

From the PayPal team, we would like to thank Nath Parameshwaran, Director, Corporate Affairs; and Mangesh Samant, Information Security Officer-India, for leading and executing this study.

A special acknowledgement to the DSCI team, Venkatesh Murthy, Mayank Lau and Amit K Ghosh for their efforts in pulling this report together.

On behalf of DSCI and PayPal, we would like to express our gratitude to all the individuals and firms for their valuable insights without which this report would not have been possible.

Executive Summary

Industry experts agree that the Fintech industry is entering its golden age and those paying attention are able to leverage its disruptive potential to transform entire nations. It is no coincidence that India, amongst the fastest growing economies in the world is banking on Fintech to be the catalyst for its vision for a connected and prosperous India 2.0. In Nov 2017, at Singapore Fintech festival, Arun Jaitley, Finance minister of India shared that reforms implemented by the government in recent years have brought "digitization of the economy to the centre-stage–the consequence of this has been that in the past one year, the number of digital transactions has almost multiplied by 100%, and new kinds of technologies, applications, instruments have been emerging...banks and government and Fintech companies have all been innovating and creating new payment gateways, and the mode by which India now spends its money has substantially begun to alter." He added that "this however is just the beginning".

Investments made in developing public digital payment infrastructure over the last few years are already showing results. UPI, has emerged as the fastest growing payment interface in the country and while domestic startups continue to grow at break-neck speed by leveraging these innovations, entry of the global players like Google, PayPal, and WhatsApp in India over the last few months speak volumes in regards to the opportunity, India offers in the Fintech space.

While India charts its own path full of new highs in its digital payments journey, it is critical that consumer trust and safety be treated as one of the highest priorities throughout the transformation cycle. From public policy to enterprise security and user best practices, it would require a long-term collaborative and concerted effort to maintain assurance around the availability, integrity and confidentiality of the environment.

The cybercrime threat landscape is evolving rapidly. It is global, persistent, ever evolving and requires that India establishes a strong foundation of security best practices, regulations and training to protect its Fintech sector from exploitation by malicious actors. More than 1.9 billion records were lost in the first half of 2017 over approximately 960 reported incidents. Of this India's share was 274,198,181 records over 15 reported breaches [3]. If this truly is the beginning, a robust cyber security framework has to be adopted to thwart this trend before it impacts business and economic growth in India too adversely.

DSCI and PayPal has conducted a study of the current state of cyber security for digital payment ecosystem in non-banking sector organizations. The study focusses on analyzing the following elements:

(I) India's journey in digital payments and its cyber security

(II) Threat landscape of digital payment ecosystem

(III) Digital payment ecosystem cyber security - public polices, regulations, standards and frameworks of major countries

(IV) Enterprise cyber security best practices

(V) Future trends

This study identifies various success factors to build a robust and resilient digital payment environment in India. The recommendations from this study would help strengthen the Fintech ecosystem and improve the cyber security posture of the digital payment landscape. Key recommendations include:

I. Establish a long-term strategy for managing the dynamic global cyber security environment and controlling cybercrime

II. Standardize data protection laws and cyber security frameworks for digital payments

III. Develop comprehensive regulatory guidelines on risk management technologies, payment security management and business continuity management

IV. Encourage threat intelligence sharing across the ecosystem

V. Establish a strong startup innovation program for cyber security and the Fintech sector

VI. Encourage public-private partnerships for cyber security education and workforce development

VII. Build a regulatory sandbox environment for cyber security testing

VIII. Incentivize companies to make cyber security and data protection a priority for Boards and C-Suites

The paper also contains detailed recommendations on public policy and enterprise security as immediate next steps to consider for key stakeholders.

Preparing for the impact of emerging technologies on the cyber security landscape and working towards achieving a balance between supporting innovation and protecting Indian Fintech industry, requires a strategic and collaborative effort between various public and private players. The time to begin these discussions, exploring possible solutions and implementing strong but flexible frameworks, clearly is now.

1 Background

The digital India mission envisioned by the Government of India is aimed at transforming the country into a digital economy. One major part of this larger program is a special focus on digital payments. The program on digital payments is envisioned with elements such as, extending banking facilities to underbanked, banking from anywhere, expanding the base of financial inclusion, creation of digital space flywheel opportunities with national identity program and establish enhanced transparency into the systems. Digital payments are becoming a key part of our daily lives and impacting society, business and the economy at large. India's digital payment industry, which is currently worth around USD 200 Billion, is expected to grow five-fold to reach USD 1 Trillion by 2023, as per a report by Swiss financial services holding company, Credit Suisse [4]. In India, as per a recent report by RBI, total digital payment transactions stood at 1.06 billion transactions for the month of December 2017 [5]. The Government of India is targeting to reach 25 billion digital transactions by the end of this fiscal year (FY2018). This significant growth, both globally and in India, warrants stakeholder's concerted efforts to envision robust cyber security and data protection policies. Such efforts would go a long way in enhancing the end-consumer trust in digital payment space and could potentially result in multifold increase in the digital payment market in India.

Innovative use of technology has enabled digital payment infrastructure and the creation of innovative products such as mobile wallets, i.e. prepaid payment instruments. The major technology capabilities which are responsible for this revolution are, but not limited to, Smart devices, Apps, Near Field Communication Protocol, QR Code and Mobile Wallets. It enables the end consumer to conduct commerce with ease, flexibility and from anywhere.

Mobile wallet providers belong to different sectors such as banking, telecom, pure play payment organizations and manufacturers of smart phones. The users are able to leverage the mobile wallets for services such as travel, ticketing, e-commerce, etc. Globally, mobile wallets have been existing for many years. M-PESA, a mobile phone based financial service was launched by Vodafone in Africa in 2007. Google launched its wallet in USA in 2011 and recently, in 2017 came out with TEZ application for mobile payments in India. PayPal launched its wallet in 1999. It has more than 227 million active users in 200 markets and supports over 100 currencies.

The private sector in India has taken a giant leap to drive digital payments adoption. At the same time, National Payment Corporation of India (NPCI) developed and introduced Unified Payment Interface (UPI) which provides 24x7x365 mobile payment platform for users to send and receive payments with a simple virtual payment address. This technology innovation was further augmented with the introduction of Bharat Interface for Money (BHIM) which has enabled high volume cashless payments through mobile phones.

The Indian Government's thrust on digital payments is making this space affordable and interoperable, which is benefitting end-consumers, businesses and digital payment sector at large. The total number of payment system operators in India stands at 91 till date, as per RBI report (Jan 2018). Mobile wallet transactions have risen 590.30% year-on-year as of Jan 2018. In 2016-17, as per the RBI Bulletin (Jan 2018), the prepaid payment instruments (PPI) transactions stood at 1.963 billion (volume) and INR

838 billion (in value) [6]. In India, the introduction of Unified Payment Interface (UPI) is also making a significant impact; as per NPCI, from FY-2017-18 (Apr'17 to Mar'18), transactions on this platform were to the tune of INR 509.62 billon (value) and 413.95 million (volume). Similarly as of Dec 2017, as per NPCI data, Aadhaar based transactions stood at 1900 million (volume) from Apr'17 to Mar'18 [7]. Retail digital payments leveraging NPCI platforms are also on the rise [8] [9].

As India rapidly transitions to a digital payment ecosystem, threats are also moving from cash to cyber and the nascent ecosystem is already facing sophisticated cyberattacks. As such, stakeholders may need more capabilities, processes, standards and best practices to detect, prevent or respond to advanced threats in the digital payment ecosystem. Recently a banking organization in India was hit by a cyberattack, it was discovered that INR 25 crore was pilfered from multiple accounts due to a bug in a digital payment application and also a mobile wallet organization suffered a loss of INR 19 crore due to vulnerabilities in its own online payment system.

Hence this warrants pertinent stakeholders to gear up, prepare and collaborate to provide secure and reliable prepaid payment instruments to the end consumers. This study is an effort to build a set of recommendations towards securing the emerging prepaid payment instruments ecosystem in India.

2 Digital Payment Landscape: Snapshot

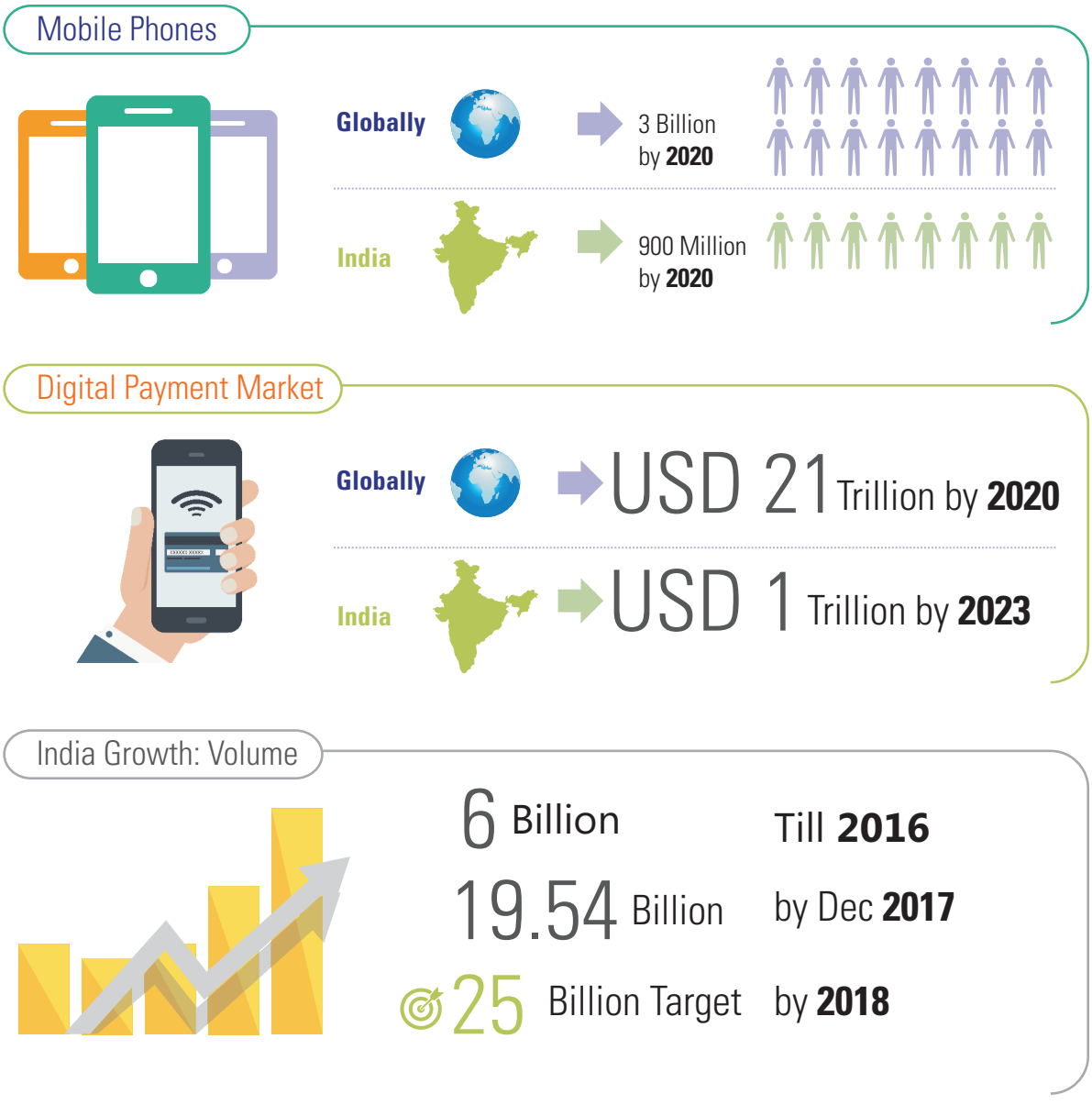


Figure 1 Digital Payment Cyber Security Journey: India

3 Fintech Revolution

The last few years have witnessed an unprecedented transformation with respect to the emergence of financial technologies. Tools and platforms are trying to disrupt the financial ecosystem globally. Earlier Fintech impacted only consumer payment landscapes i.e., enabling faster payments, removing hassles from processes for consumers, enabling frictionless commerce, making it more secure; and now it is expected that it may overhaul business operations end-to-end. The canvas of Fintech is becoming ever encompassing. Its emerging use cases are crowdfunding, peer-to-peer money transfers, data analysis, wealth management, cyber security and underwriting etc. These technologies are user friendly and designed to reduce costs of operations. Globally, Fintech innovators and financial service organizations are building collaborative business and co-creation models. The soul of these models is data availability from financial organizations to build financial technologies, i.e. access to data for Fintech developers which can be a boon to innovate next generation technologies or to leverage it for big data analytics.

Hence, it is imperative for India to learn and adopt global Fintech trends and technologies to align itself with global digital payment revolution. Emerging global Fintech trends are captured below as per different market adoption. The below analysis indicates alignment of synergies by Indian market to develop and adopt financial technologies at an expedited rate. India needs to gear up to accommodate these trends from a regulatory, technology, compliance and security perspective.

Trends		Asia-Pacific	India	Developed Economies
I.	Improving and simplifying financial operations	Growth	Early Adoption	Mature
II.	Leveraging virtual channels and self-service tools	Early Adoption	Early Adoption	Early Adoption
III.	Building products around costumer experience	Growth	Growth	Mature
IV.	Reaching and engaging customers	Mature	Early Adoption	Mature
V.	Cash Digitization	Growth	Exploration	Mature
VI.	Decentralization of operations via blockchain	Exploration	Exploration	Exploration
VII.	Peer to peer lending	Exploration	Exploration	Early Adoption
VIII.	Digital wallet adoption	Growth	Growth	Mature
IX.	Point of sales capabilities	Growth	Early Adoption	Mature
X.	Cross-border transfers	Early Adoption	Growth	Mature
XI.	Faster Payments	Growth	Growth	Early Adoption
XII.	Tokenization	Exploration	Exploration	Early Adoption

Table 1 Fintech Adoption - APAC, India and Developed Economies

The rise of Fintech revolution in India is characterized by trends such as, but not limited to, financial inclusion of larger population, demand of digital finances, smartphone adoption, government and regulator push, and collaborations by financial institutions. According to a report by an analytics company, Tracxn, there were 750 registered Fintech companies in India by 2017 of which 174 launched in the year alone. The challenges in India are similar to any other large developing nation, the big corporations are stringently regulated to push for Fintech revolution and emerging organizations are not regulated or propelled enough. Still the financial sector is moving in the right direction to construct an environment for financial services future and its cyber security. Initiatives such as Jan Dhan Yojana, Aadhaar and the emergence of UPI clearly mark the beginning of building a healthy Fintech ecosystem in India. As per a PwC report, India is expected to offer the highest expected return on investment on Fintech projects at 29% versus a global average of 20%. The key for Indian Fintech revolution lies in envisioning a conducive environment for all stakeholders which can promote innovation and faster adoption of financial technologies.

4 Digital Payment Landscape

4.1 Global

In recent years, a plethora of organizations have started emerging to deliver next generation product and services in the digital payment space. Both banking and non-banking organizations are capturing the essence of customer requirements at lightning speed and overhauling the value chain. This is primarily possible due to the accessibility of Internet and affordability of mobile technologies globally. As per a BCG report, the number of mobile internet users may reach to 3 billion by 2020 [10].

Rise of connected devices may lead to exponential growth in app purchases.

The future customer may transact via smart watches, smart cars and even smart apparel.

Smartphones today are equipped with capabilities such as enhanced processors, high capacity storage memories, NFC, high resolution cameras, etc. They are no longer only communication devices; rather they are becoming commerce enablers. Emergence of smartphones have enabled development of new payment technologies. Innovations such as, but not limited to, tokenization of card, NFC readers at merchant stores, biometric enabled transactions and interoperability of wallets are paving ways for the next generation financial world. The rise of non-traditional players such as Apple, Google, Samsung, Starbucks and Vodafone etc., clearly reflects that this space is no longer a monopoly of the traditional financial institutions. The future customer may transact via smart watches, smart cars and even smart apparel. The expectations from future digital payment modes include:

I. Simpler payment methods
II. Omnipresent merchant networks
III. Frictionless on demand payment options
IV. Customer friendly easy on-boarding and off-boarding provisions
V. Significant reduction in costs in performing digital transactions

Cyber security preparedness for the digital payment space warrants a concerted effort globally. It is helping is helping to enhance the Fintech revolution with help of stronger authentication options, robust data confidentiality & integrity mechanisms, and via building more transparency into the financial system etc. It is also ensuring assurance and foiling plans of malicious actors working towards the goal of duping organizations and consumers.

4.2 Digital Payment Delivery Channels

Prepaid Payment Issuers and banking institutions are focusing on developing products and services that can be delivered to its customers through multiple digital channels with mobile devices used predominantly for better user experience. Mobile devices provide an excellent opportunity for companies of all sizes to increase customer access to financial services and decrease costs. Although the risks from

traditional delivery channels for financial services continue to apply to latest digital payment channels, the risk management strategies may differ. As with other technology-related risks, management should identify, measure, mitigate, and monitor the risks and be familiar with technologies that enable digital payment channels.

The vulnerabilities in the IT systems or the process followed are continuously exploited by criminals. For instance, weaknesses related to software development may arise due to various factors like security not considered during development, patch management, configuration issues, etc. Users can be easily targeted since most of them don't have cyber security on their radar. So, while building the products, a holistic approach towards security without causing any inconvenience to the consumers need to be looked at.

This chapter intends to give the reader a view on different technologies used in the digital payment channels, opportunities created and associated vulnerabilities, and risks with the digital payment systems. The risks and controls addressed here are, however, not exhaustive.

QR Code

Quick Response Code (QR code) is a 2D matrix barcode that stores encoded information such as hyperlinks to website pages, app downloads, etc. To decode, users simply need to scan the QR code image using any device with built-in camera (e.g. smart phone) and QR code reader application installed.

Bharat QR code introduced by Govt. of India collaborated with Mastercard, American Express and Visa apart from RuPay. It is pertinent to note that Bharat QR code is enabling rapid rollout of digital payments acceptance infrastructure throughout the country, as it does not involve any upfront investment in Point of Sale (PoS) machines [11].

Working of QR tech [12]

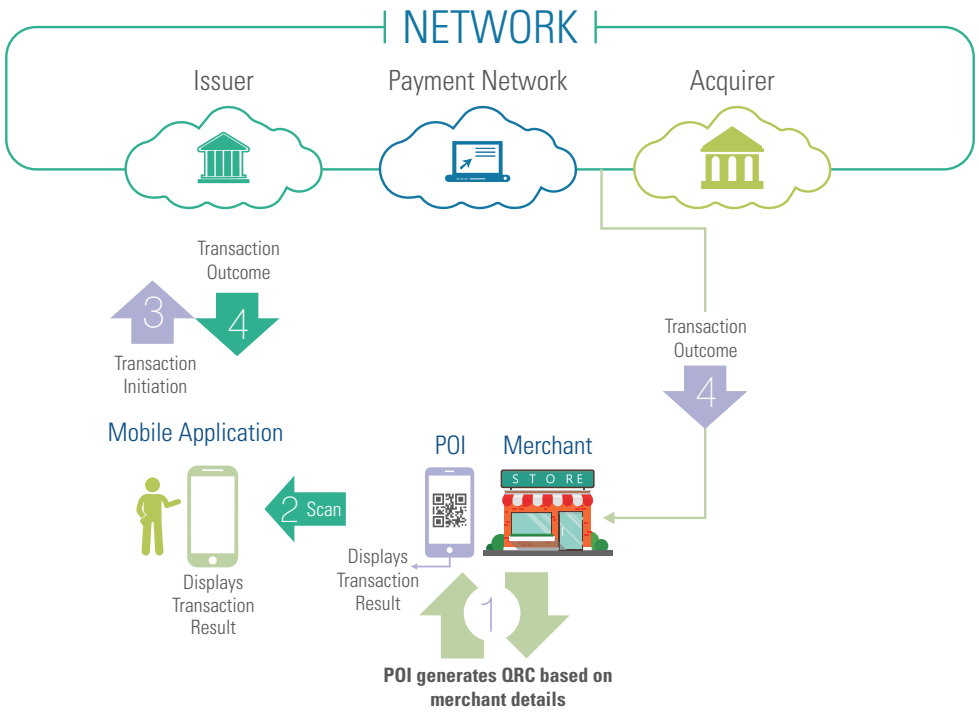


Figure 2 Merchant-Presented Mode Transaction Flow

Working of QR tech [12]

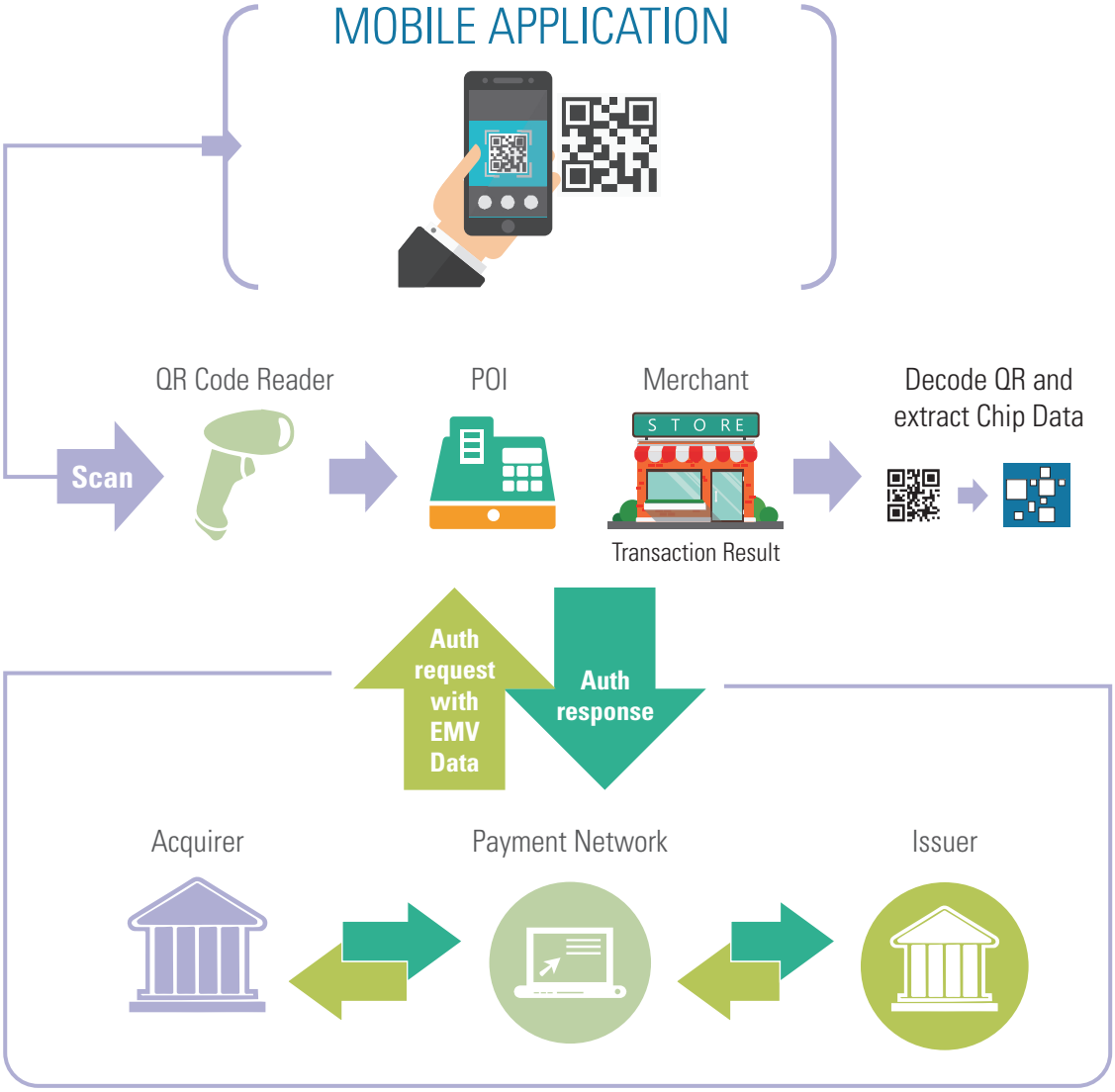


Figure 3 QR Code Payment Architecture

Threat vectors

- Criminals can simply prepare malicious QR codes and affix them over legitimate codes which may result in victims inadvertently making payments to a criminal rather a legitimate service provider.
- Victims may be enticed into scanning a QR code mimicking a legitimate brand, stealing their personal data, or to a malicious site that seeks to exploit their mobile device.
- Attackers generating a QR code for a shortened URL, redirecting to the phishing or malicious site [13].

Case Study

It was reported that about 90 million Yuan (USD 14.5 million) was stolen from people of South China through the fraudulent use of quick response codes which are often scanned for product identification and mobile platform access [14].

Key Learnings

It is very difficult for the consumers to verify the authenticity of the QR codes by casual observation. The payment providers should put efforts in educating the users about the possible misuse of QR technology and also incorporate technology to determine whether a QR code was generated by them or some other player [15].

As on the date of writing this report, there have been no reported instances of any Cyber security breach incidents related to use of QR code for performing money transfer/receiving in India.

NFC – Near Field Communication

Near field communication, abbreviated NFC, is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over a NFC compatible PoS device to send information without needing to touch the devices together or go through multiple steps setting up a connection [16].

Figure 4 Samsung NFC Payment

Working of NFC

NFC is a subset of RFID (radio-frequency identification), a technology that allows to identify things through radio waves.

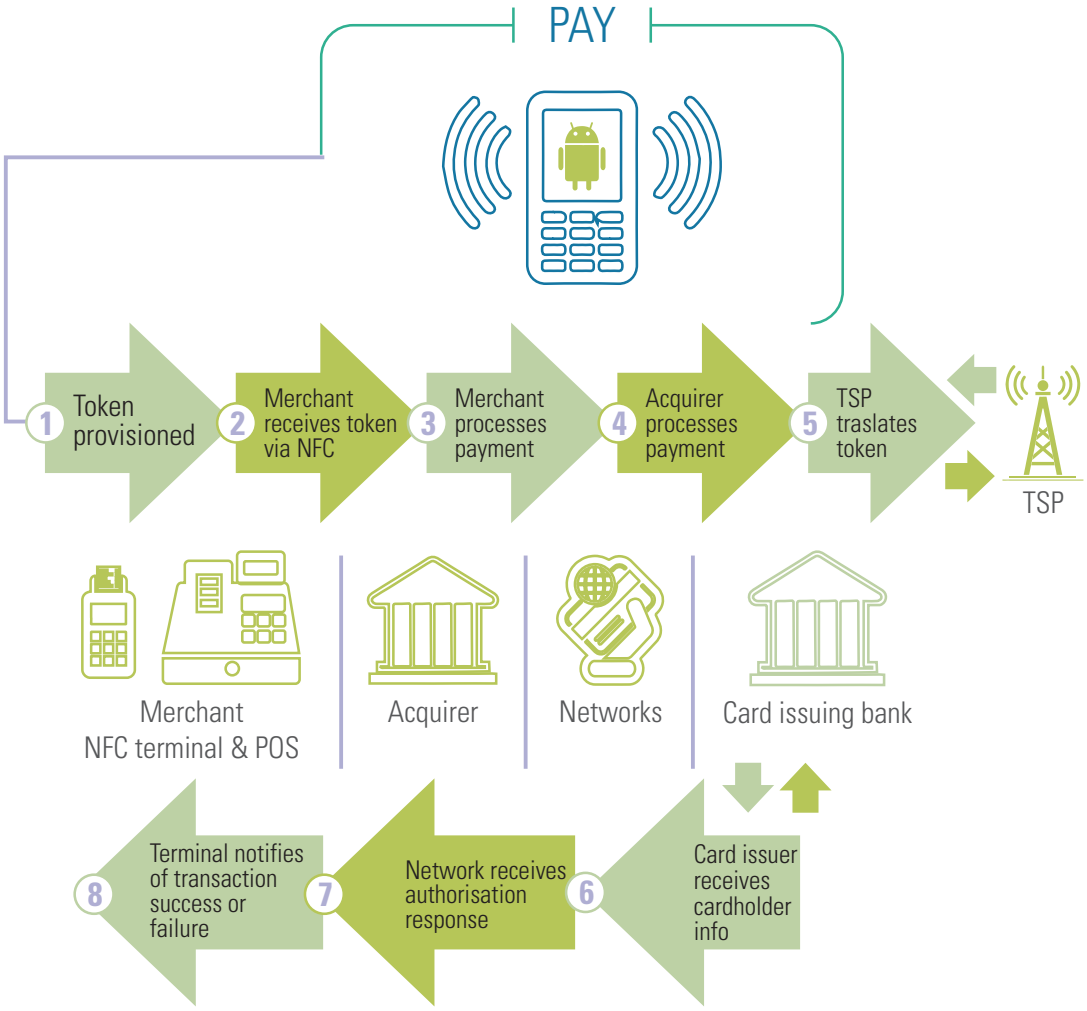


Figure 5 Working of Andriod pay using NFC

ICICI touch and Pay – NFC

The latest mobile payment solution 'Touch & Pay' of ICICI Bank enables to make secure contactless payments at retail stores using smartphones. This Touch & Pay feature on Pockets app simply lets the user to tap his/her smartphone at an NFC (Near Field Communication) enabled merchant terminal and make the payment through your linked ICICI Bank Debit/Credit Card.

NFC Threat vectors

- NFC communication protocol used by service providers may be vulnerable to interception, eavesdropping, and manipulation.
- An attacker can carry out data corruption by transmitting valid frequencies of the data spectrum that can interfere with the data transmission and can even block flow of information from NFC device.

Case Study

Australian police charged three men with compromising 45 bank accounts through the card emulation function used for mobile payments to make $1.5 million in fraudulent purchases across Sydney. Criminals exploited the Host Based Card Emulation, which is the fundamental component of NFC payments to emulate a credit or debit card and talk directly to an NFC reader. NSW Police identified a "sophisticated organized group" that it claims to have been porting mobile phones and compromising bank accounts through mobile payment applications [17].

Key Learnings

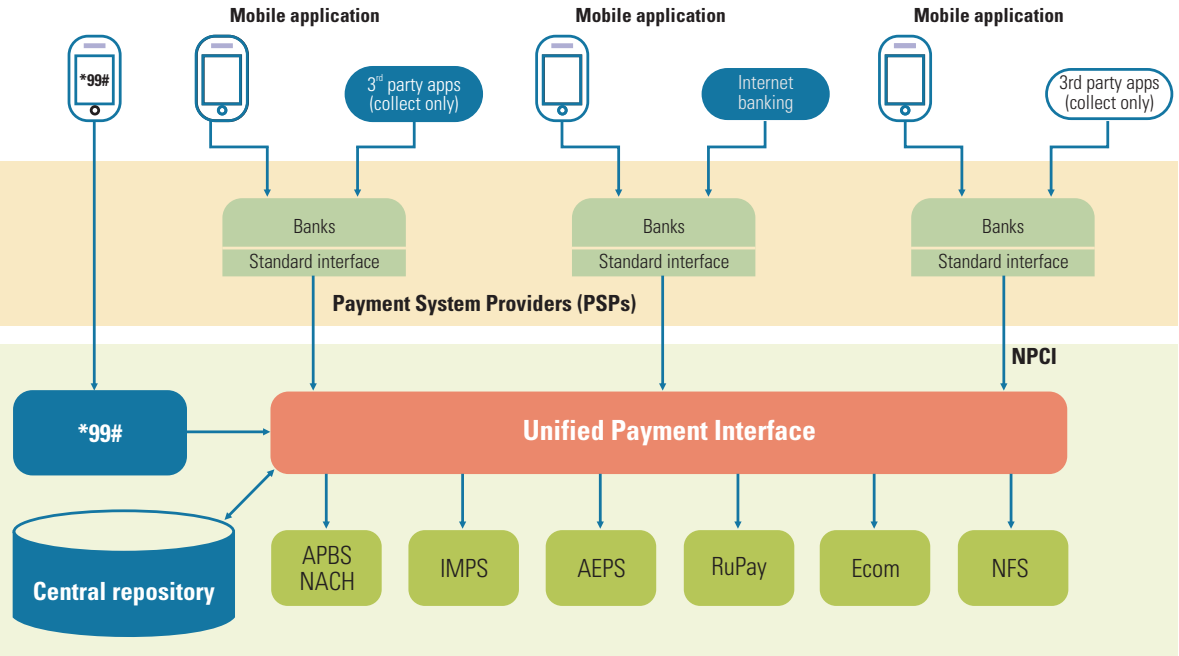
- Consumers should be aware about the apps that they are installing on their devices
- Apps should always be downloaded from trusted sources
- NFC should not be always ON: NFC usage should be configured in such a way that the app must ask the user to activate NFC when using

UPI – Unified Payment Interface

The Unified Payment Interface offers an architecture and a set of standard API specifications to facilitate online payments. It aims to simplify and provide a single interface across all NPCI systems besides creating interoperability and superior customer experience.

UPI – available in Two Modes	
Independent Mode – Bank developing a separate UPI app, and/or converting their existing mobile banking application to be extended to facilitate UPI services.	**Embedded Mode** – The UPI compliant app/module is embedded in other (merchant) apps by bank giving the binary/SDK to the merchant to integrate into their apps. Merchants may choose to include more than one UPI compliant app from different banks.

Working of UPI [18]



*99# NPCI USSD service code to access banking service via phone

Source: NPCI

Figure 6 UPI Architecture

Threat vectors

- The UPI application can be developed with customisation by a bank. There are risks involved around the third-party vendors who involve in the application development. If proper secure development practices are not followed, chances of exploitation of vulnerabilities are at higher side.

Case Study

A bug in UPI app costed Bank of Maharashtra 25 crore INR in one of India's biggest financial frauds [19]. The bug in the UPI app developed for Bank of Maharashtra allowed people to transfer money without having the necessary funds in their accounts. The accounts from which funds were pulled out as well as the accounts into which the money flowed into belonged to the group of swindlers. This fraud was committed by exploiting the vulnerabilities existing in the Bank of Maharashtra's UPI mobile application where there was a gap existing between bank's core banking system and UPI application.

Key Learnings

- In this case, the criminals didn't hack into the bank's IT system but they managed to pull out money with the old technique of identifying the bugs in the system. Institutions providing such services should perform application security audit to identify the bugs, which should be followed by the service providers on regular basis.
- There is a need for formulation and enforcement of proper regulations, ensuring proper testing, and certification of apps.

Mobile Wallets

A mobile wallet is a virtual wallet that allows the user to carry their credit card or debit card information electronically on their mobile devices. A smartphone or browser can be used to make purchases goods or even make merchant payments. Mobile wallets are categorized into four categories:

Wallet Type	Open Wallet	Closed Wallet	Semi-closed Wallet
Description	Allows a user to buy goods and services, withdraw cash at ATMs or banks and transfer funds. These services can only be jointly launched with a bank. Additionally, it allows its users to send money to any mobile number bank account.	Amount of money is locked with the merchant to place order, use in case of a cancellation or return of the order, or gift cards.	It does not permit cash withdrawal or redemption, but allows users to buy goods and services at the listed merchants.
Example(s)	M-PESA by Vodafone and ICICI Bank	Flipkart e-wallet	Paytm

Some wallets, such as Android Pay, Apple Pay, and Samsung Pay, are specific to the particular combination of software and hardware on certain devices and all seek to replace the use of traditional credit/debit cards with mobile phones [20].

Working of Mobile Wallets

Download the mobile wallet app (or it may be already built into your mobile device)

Add your credit card or debit card information to the mobile wallet

When you check out at participating merchants, access the mobile wallet and make payment

Threat vectors

- Malicious apps purporting to be banking apps
- SIM swap based attacks to obtain SMS based authentication for online banking taking place on a separate channel
- Phishing and Vishing attacks specifically targeting the mobile device
- Malware infecting the mobile device, compromising the legitimate use of the device and stealing credentials etc.
- Spoofed SMS messages to people purporting to be from their PSP to encourage them to call a compromised number or visit a malicious website

Case Study

Recently, an Indian digital wallet firm reported to police that an unknown fraudster carried out large scale fund transfer from his wallet account even though requisite funds were not available. This fraudulent action was possible because of a technical vulnerability existing in the payment system.

Key Learnings

- Unusual financial transactions should be monitored by the e-Wallet service providers which would prevent persistent attacks.
- The coding of application, if not securely done, may be prone to such attacks.

Mobile Money Transfer (Telco based)

Started as the transfer of airtime or bartering airtime with goods and services peer-to-peer transfer of money on telecom network is now one of the mainstream mobile money transfer instruments. This transfer can happen over SMS or use platform based USSD (Unstructured Supplementary Service Data) and IVR system.

Unstructured Supplementary Service Data (USSD):

USSD (Unstructured Supplementary Service Data) is a session based transmission protocol used by cellular telephones to communicate with the Telecom Service Providers (TSP). Unstructured Supplementary Service Data (USSD) is a capability built into mobile phones, much like the Short Message Service (SMS).

Threat vectors

- ***USSD Commands Request/Response Tampering*** – A malicious user can tamper with USSD command requests and responses through hardware and software interceptors leading to fraudulent transactions. Weak encrypted request and response messages are prime concerns in such threat vectors.
- ***USSD Request/Response Message Replay Attacks*** – When a phone is lost, an adversary may perform fraudulent transactions through an installed USSD application in absence of authenticating USSD request originator (e.g., by MSISDN, IMEI, PIN and unique Message Tracking ID).

Mobile Applications

Mobile applications are downloadable software applications developed specifically for use on mobile devices. Mobile financial applications are developed by or for financial institutions to allow customers to perform account inquiries, retrieve information, or initiate financial transactions. This technology leverages features and functions unique to each type of mobile device and often provides a more user-friendly interface than is possible or available with either SMS or Web-based mobile banking.

Threat vectors

- **Exploits**: They take advantage of design, code or configuration issues that cause unintended behavior of the application. Some common examples include SQL Injection (SQLi), cross-site scripting (XSS), buffer overflows, and various Secure Sockets Layer (SSL) and Transport Layer Security (TLS) manipulation attacks.
- **Abuse**: Abuse covers many non-exploit types of attack that primarily take advantage of business logic. This includes scraping, aggregating, account brute-forcing, scalping, spamming and other-often automated-scenarios.
- **Access violations**: These occur when an attacker or legitimate user takes advantage of weaknesses in the authentication or authorization policies of the app.
- **Fake Apps**: The adversaries may build fraudulent wallet applications and post it on the popular market places which users may use inadvertently and falling prey of it.
- **Rooted Device**: Usage of jailbroken devices may help criminals to easily bypass the security and steal user information.

Payment using wearables

From wristbands, fitness trackers and watches to jewellery and clothing, the potential of wearables technology is promising. Tap-and-pay wearables are slowly entering the market to provide customers with most comfortable payment options that is reliant on IoT.

Threat vectors

- Since IoT devices are connected to the Internet, they represent new targets for data exposure and attacks. They can be infected by a malware and be compromised by fraudsters or their communication could be intercepted (unauthorised access and use of the device, misuse and disclosure of personal information).
- The lack of usage and incentive of common standards in security such as encryption in IoT devices make them more attractive for attacks, and we are increasingly seeing new forms of extortions, botnet hacks, data theft and even physical harm. New potential use of technologies which could potentially serve as a new framework to facilitate processing of transactions or coordination of IoT could increase fraud if not properly secured.

Payment through Biometric Authentication

Biometrics of a person is used by service providers to identify and authenticate based on his/her biometric template that is stored in the device. In another example of how China is accelerating a cashless economy, Ant Financial launched the facial recognition payment service in a Hangzhou branch of KPro, the Chinese version of KFC, making it the world's first physical store where customers can use their face to make a payment.

The system works by using a photo ID of the customer, previously stored in the system, and scans their face for a match. The customer then simply inputs their phone number and the payment is accepted. Ant Financial uses the digital payment platform Alipay to allow its users to sign in using facial recognition [21]. Biometric authentication is increasing adopted by the companies using advanced technology for identity verification to improve their service to customers.

Behavioural biometrics: Unlike physiological biometrics, behavioural biometrics relate to your personal habits and unique movements. Whereas standard biometrics rely on a part of your body, behavioural biometrics use the unique way in which you do something to authenticate you. The main examples of this technology that are currently being developed analyse your gait (the way you walk) and your typing style (speed, keypad pressure, finger positioning and so on). Voice recognition technology is also sometimes classed as a form of behavioural biometrics.

4.3 India

Indian economy has traditionally been cash dependent. Two decades back, the main payment instrument and payment system that existed in the country was cheque and cheque clearing systems. After nearly twenty odd years of MICR clearing, the cheque truncation system (CTS) was introduced first in 2008. Moving further along the path of non-cash, non-paper payments; over a period of time, various systems have been put in place to meet the remittance requirements of different segments of users. With improvements in IT systems of banks and their core banking systems, integration of various delivery channels have been made possible. Online banking facilities are now easily available including payment

purposes. Taking advantage of this, an increasing number of payment facilities are being integrated through the mobile channel. For instance, customers can use their net banking application on their smartphone and send money on-the-go using IMPS or NEFT. The digital payment ecosystem is no longer a field belonging only to the banking sector. Non-banking organizations started emerging to deliver next generation product and services in the digital payment space [22].

With the emergence of various financial technology product and services, the digital payment landscape in India is witnessing unprecedented growth. The Indian government 'Digital India' initiative has emerged as one of the key catalysts. It is expected to enable awareness, availability and adoption of digital financial product and services at an accelerated rate. One of the key players emerging in this space are payment service providers (PSP) in India. A payment service provider is either a bank or a non-banking organization. PSP ecosystem includes PPI organizations also. They provide products such as digital mobile wallets or prepaid cards for end citizens to be leveraged.

As per the 'Vision 2018' document by RBI, a four pillar strategy has been devised for Indian digital payment industry. It includes a special focus on public policies, building next generation infrastructure, supervisory mechanisms and development of products & services. Further it is to be augmented by replacing cash payments, reducing digital payment costs and laying national optical fiber network to improve connectivity. The RBI vison document entails working on areas such as coverage, convenience, confidence, convergence and cost, for successful growth of the digital payment space in India. The demonetization decision helped in changing the outlook of end citizen in India towards adoption of digital payments. It enabled users to adopt new methods of commerce in cyber space with agility, trust and confidence. Indian digital payment space looks promising with initiatives such as, but not limited to, Aadhaar based transactions, JAM trinity, direct benefit transfers, and rise of Fintech technologies and with introduction of prepaid payment instruments. Taking a deep dive into India's journey in the digital payment space reveals following facts from various market reports.

India has the third largest Internet user base in the world with more than 300 million users. 100 million are only mobile Internet users

As per a KPMG report on Indian Fintech industry, the financial technologies software market is forecasted to touch USD 2.4 Billion by 2020 from USD 1.2 billion in the Financial Year (FY) 2016

Basis an ASSOCHAM report, e-commerce market revenue may grow to more than USD 30 Billion by 2020

For successful digital payment evolution, it is necessary for end users to have confidence and trust in the payment solutions. To maintain the end customer trust and confidence in the system, one requires a solid holistic cyber security framework covering regulatory and technological advancements. This is especially more important in the Indian context due to the factors such as (I) Large population which is not tech savvy may face challenges to secure their transactions (II) Lack of cyber security risks knowledge among masses (III) Sudden acceleration in adoption of digital payment channels. This puts a significant impetus on building a cyber security framework consisting of pertinent policies, regulations, best practices and standard operating procedures. The elevation for cyber security in digital payment space is required because the magnitude of risk for a user increases with digital payment systems adoption [23, 24].

5 Technological Evolution and Threat Landscape: Global and India

With the advancement of the digital payment space, organizations are able to provide endless product and services to the end consumers. At the same time, end consumers are at ease with the convenience provided by these platforms. One is able to execute transactions for every purchase from anywhere with minimal hassles.

The motive is to extract financial gain from either organizations or end consumers by duping them with new cyberattacks.

The evolution of digital payment infrastructure is exposed to ever rising and complex cyberattacks. The adversaries are constantly trying to identify vulnerabilities and gaps in the digital payment infrastructure and products of the organizations. The motive is to extract financial gain from either organizations or end consumers by duping them with new cyberattacks. Hence it is imperative for organizations to track and monitor cyber threats on continuous basis and also educate users on it.

Over the last few years, the technology landscape has been undergoing rapid changes. The advent of technologies like blockchain, machine learning, bots, cloud, crypto currencies, etc., are exploring development of new financial technologies. The business delivery and architectural models are changing due to these technological movements. Blockchain may overhaul how financial services firms operate, migrating from centralized to decentralized models of conducting business and operations. It may reduce the cost of various financial activities to near zero especially where it involves third parties; financial institutions may no longer face the millstone of operating costs due to the success of blockchain based digital payments.

Cloud delivery models bring advantages such as scalability, flexibility, agility and cost savings. The area in which financial sector is adopting cloud are card and mobile payment processing, core banking, human resources & talent management, and infrastructure as a service etc. It is expected that cloud technologies coupled with analytics, mobile technologies and big data, may allow financial institutions to extract real value from the data.

Improvements in algorithms and automation of financial activities may impact domains such as optimization of business processes, removing inefficiencies from operations, enhancing fraud and risk management, changing customer services models and application of virtual assistants instead of humans.

Another technological advancement which is making headlines in the digital payment sector is usage of Bots. Currently, its primary use is in the area of customer services because it delivers instant communication, optimizes costs, can be deployed across different delivery models, streamlines processes and reduces call load of business process management centers, etc. Together, these technological advancements are going to overhaul digital payment architectures and types of financial products which may get introduced in the market. The revolution has picked up in India with developments

such as proliferation of smart phones enabling rural consumers, introduction of zero balance account resulting in financial inclusion of larger population, Jan-Dhan scheme to check on leakage of subsidies. This may result in usage of technology and digital payment infrastructure by majority of the population. Hence it is critical to examine cyber threat landscape applicable globally and in India. The current threat landscape applicable to digital payment space are such as phishing, lack of user education, fake apps, etc., and futuristic threats may consist of attack on two-factor authentication and misuse of emerging technologies etc. Basis this study analysis, the threat landscape for digital payment sector ecosystem is described as follows keeping into consideration current and future technological evolutions in the realm of digital payments.

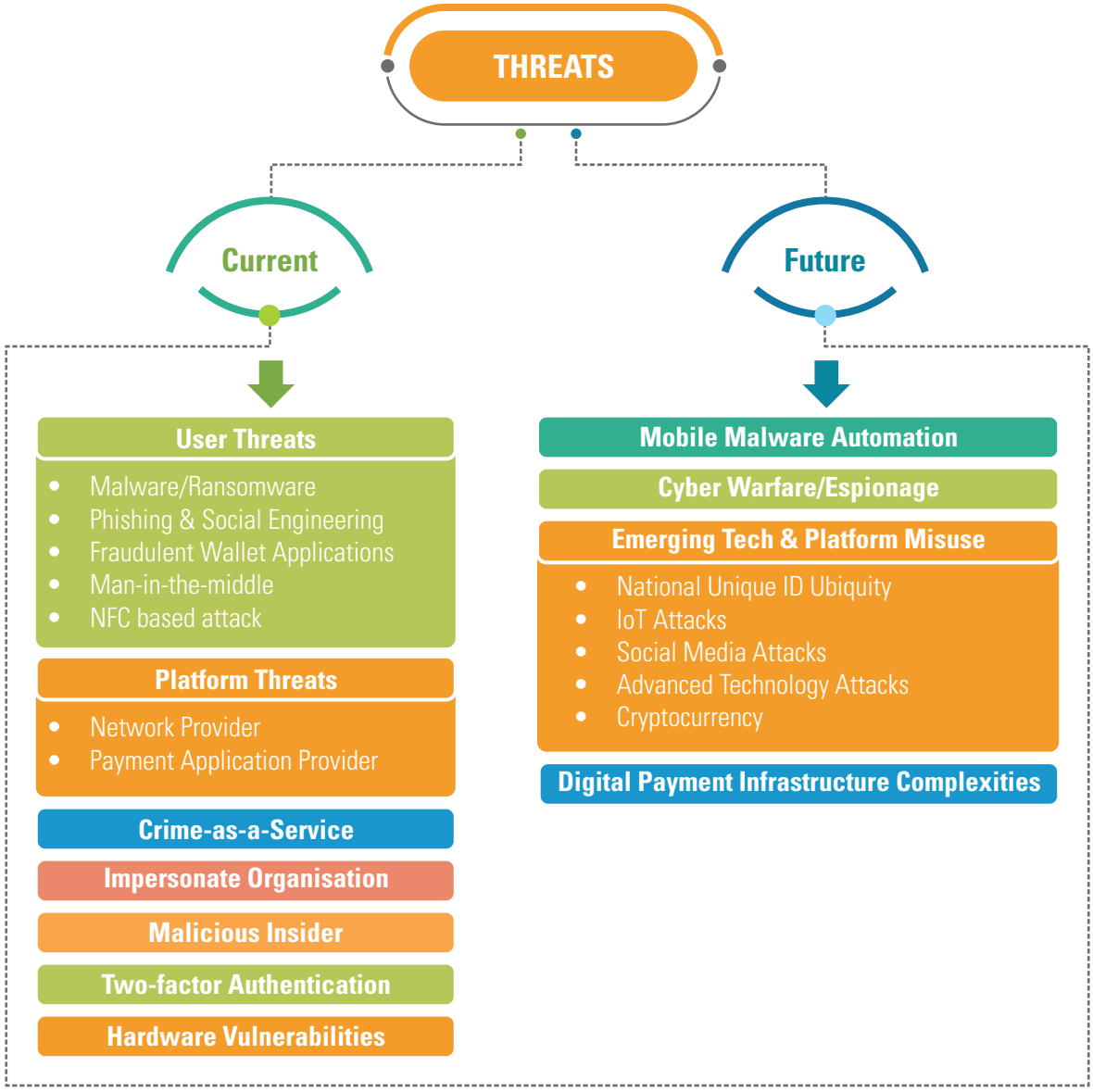


Figure 7 Threat Landscape

Current Threats [25]

- Users Threats
  - **Malware or Ransomware** Users unaware of malware infection in their devices carry out transactions, and then the malware is able to extract user credentials and share it with the adversaries. Leveraging their credentials, adversaries are able to conduct fraudulent transactions and draw off user finances or deny services and may be demand ransom for services continuation. For example, last year according to report by Kaspersky Labs, a new malware Xafecopy Trojan was detected in India which stole money through victims' mobile phones and it was cited that 40 % of this malware attacks were in India.
  - **Phishing and social engineering** are the most commonly used techniques to carry out cyber-attacks on the end users in the digital payment space. In phishing, deceptive link is sent to the user which appears legitimate and they are redirected to sites which belongs to cyber adversaries. The user without knowing about it transacts on it leading to loss of their credentials. Social engineers are everywhere navigating for opportunities either via telephonic conversations or well-crafted emails to fraud gullible users.
  - The adversaries may build **fraudulent wallet applications** and post it on the popular market places. There had been instances in which users transacted via illegitimate wallet applications instead of legitimate ones. Adversaries may also introduce backdoor or rootkit in the wallet applications to redirect user funds or gain information on user credentials to conduct frauds.
  - **Man-in-the-middle attack**. The communication layer of the transactions is vulnerable to cyber threats. In case of non-secure network implementation, adversaries are able to eavesdrop and fire a man-in- the-middle attack. With this method they can change the data packets integrity or obtain key information to conduct frauds against users.
  - **NFC based attack**: One of the most common concerns with NFC technology is that of eavesdropping. Eavesdropping occurs when a third party intercepts the signal sent between two devices. For example, adversaries might also pick up other personal information passed between two smartphones.
- Platform Threats
  - **Network Provider Threats**
    - When cyber attackers gain access to network providers' organizational infrastructure, it may compromise the end IT workforce token services used by them for work related activities. It is possible that the token information residing with the adversaries can be used to siphon of user finances or data to which the IT workforce had access.
    - Adversaries may flood network providers with plethora of ping or web requests which may appear as legitimate traffic. It may lead to **Denial of Services** as the functioning of the digital payment instruments may deteriorate or resulting in non-availability of the prepaid payment instruments.
  - **Payment Application Provider threats**

    A typical prepaid payment instrument consists of players such as payment application and infrastructure providers. The digital infrastructure of payment application provider ecosystem is to be protected against cyber threats. The threat landscape applicable on payment application provider is mentioned below.
    - Compromise of the user data
    - Token data leakage
    - Denial of Services attack on application providers infrastructure
    - Weak or insecure code
    - Immature web application
    - Denial of services

- Crime-as-a-Service
  - Organized cyber gangs may be given a bounty by the adversaries to dupe end users transacting on the digital payment ecosystem. The gangs may originate with defined product and services. This may lead to many systematic organized crimes in the cyber space.
- Impersonate Organizations
  - The current phishing techniques may get scaled to creating end-to-end fake online presence of the organizations to profit in billions as users may fall prey to it.
- Third Party
  - Organizations perimeters are getting blurred day-by-day, as more and more work is outsourced to third parties. The environment of third parties can also be responsible to introduce new cyber threats into the core operational environment.
- Malicious Insider
  - A disgruntled employee may cause havoc in an organization by stealing data, disrupting operations, inserting a backdoor in a financial services application or infrastructure based on the role he/she performs.
- Attacks on two-factor authentication
  - Techniques such as SMS or Biometrics are being leveraged as second factor of authentication for carrying out digital payment transactions. In future, large scale social engineering attacks may be launched to obtain OTPs or unauthorized access into systems to steal biometrics of end users.
- Hardware Vulnerabilities
  - Unpatched vulnerabilities of numerous hardware leveraged in digital payment ecosystem may get exploited to conduct frauds.

Future Threats

- Mobile Malware Automation
  - With the use of advanced techniques such as machine learning and AI, adversaries are developing malwares which can infect user devices surreptitiously in an automated way, with no human intervention.
- Cyber Warfare/Espionage
  - Nations are leveraging cyberspace as ground for cyber war; it may impact functioning of digital payment infrastructure at large.
  - Adversaries breaching organizations IT boundaries to steal corporate or R&D secrets, resulting in cyber espionage
- Misuse of emerging technologies and platform
  - **National Unique ID Ubiquity**: Mandating National Unique ID linking with every services in India may expand the user threat surface. As adversaries may get enticed to break into financial systems via National Unique ID.
  - **IoT Attacks**: Users of digital payments are adopting wearables such as smart watches to conduct commerce. These wearable devices are vulnerable to cyber threats such as acting as botnets in which they are used to conduct denial of services attacks without user knowledge.
  - **Social Media Attacks**: Social media integration with digital payments is getting prevalent. Users are using their social media profiles to login into payment applications. So, compromise of social media account details or identity theft may also result in digital payment frauds. The attack techniques of the adversaries may evolve to **avatar hijacking** from current identity thefts. This may get feasible due to increase of digital footprints of the next generation users. The adversaries may be able to clone an illegitimate digital avatar of the user in the cyber space. Organizations may not able to distinguish between real and fake avatars of the users.
  - **Advanced Technology Attacks**: Techniques such as artificial intelligence, machine learning and deep learning may increase complexities of cyberattacks and may automate them with minimum human intervention.
  - **Cryptocurrency**: Ransom demanded in cryptocurrencies which are untraceable may propel rise of cyberattacks on financial services and its users, with more motivation.
- Complexities in Digital Payment Infrastructure: With implementation of technology advancement in the products, integrating multiple services or components which may result in mesh of IT architecture, this may result in uncovered vulnerabilities in the system leading to cyber incidents.

6 Public Policies, Regulations, Standards, Frameworks

6.1 India

The current landscape in terms of cyber security public policies and regulations in India applicable to the digital payment space consists of the IT Act 2000, National Cyber Security Policy 2013 and RBI 2017 master directions for prepaid payment instrument organizations. The speed at which the digital payment space is changing in India with the introduction of new technologies and mass scale adoption, some of these regulations may require periodical review basis contemporary evolution of digital payment ecosystem, changes in cyber security, and data protection landscape. It has to be augmented with compliance guidelines and best practices.

Recently, the Ministry of IT and Electronics (MeitY), Government of India, has given administrative approval for the industry consortium 'Cyber Surakshit Bharat' intended to train the Chief Information Security Officers and IT officers of Central and State governments, Banks, PSUs, etc., to address Cyber security related challenges [26].

India is taking a giant leap in terms of adopting different modes of digital payment. The pillars which are warranted to safeguard organizations' and end citizen's interests are, but not limited to, robust cyber security public policies, regulations, standards and frameworks. The formulation of cyber security public polices is to happen in such a way that it fosters innovations and at the same time protects digital payment ecosystem against ever rising cyber threats.

As a country, India has taken some concrete steps to secure its digital payment landscape in the realm of public policies. An analysis of it is captured below after studying the following initiatives:

I. RBI Master Directions on Issuance and Operation of Prepaid Payment Instruments in India

II. MeitY Security Rules for Prepaid Payment Instruments

III. Medium Term Recommendations to Strengthen Digital Payments Ecosystem, Watal Committee Report

This analysis may help to further work on the future course in order to enhance our cyber security preparedness.

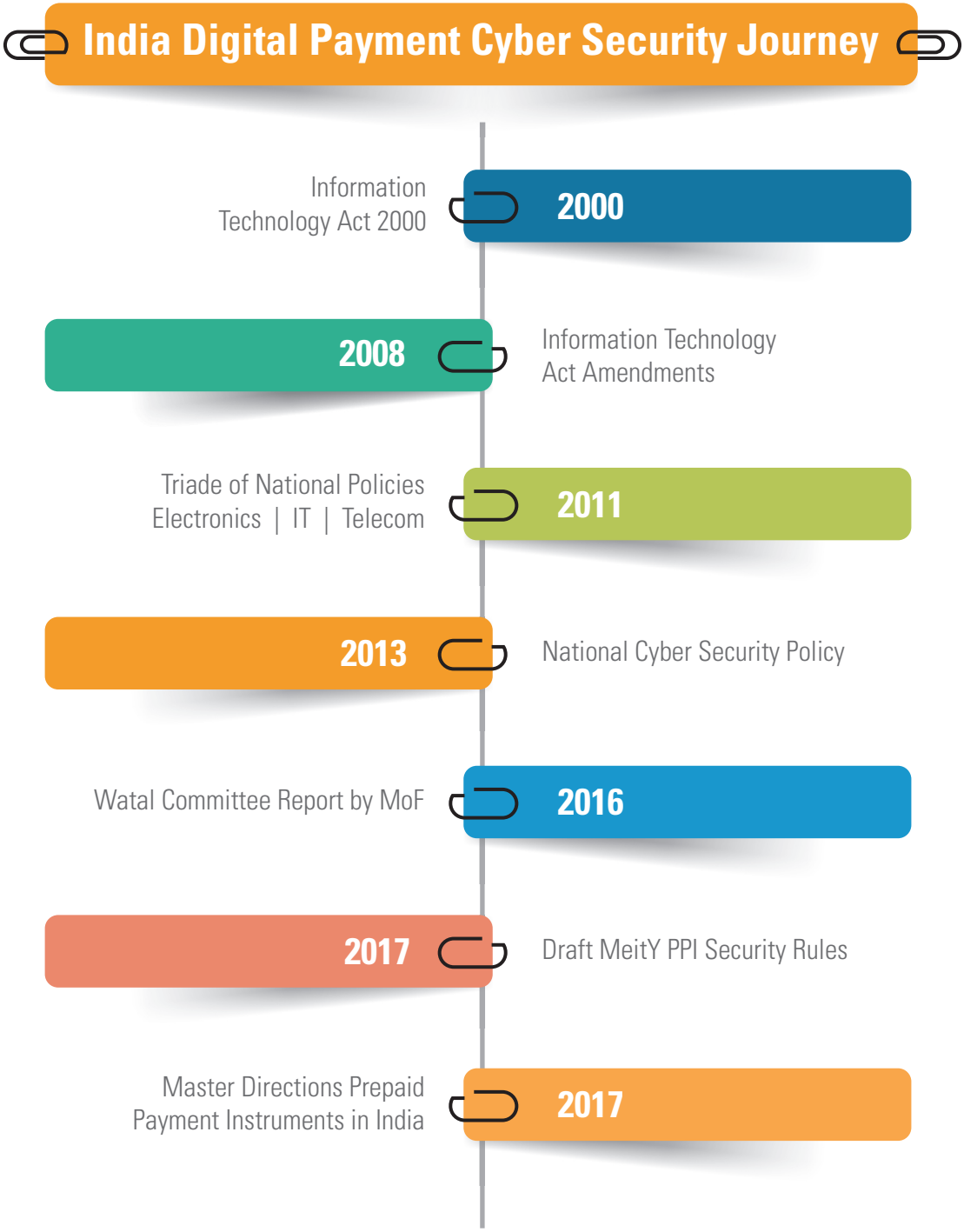


Figure 8 Digital Payment Cyber Security Journey: India

Learnings	Analysis
(I) RBI Master Directions on Issuance and Operation of Prepaid Payment Instruments in India [27]. • Section 15 stipulates security, fraud and risk management framework; Section 16 covers customer protection and grievance redressal framework and Section 17 entails system audit requirements. • Adequate information and data security infrastructure and systems for prevention and detection of frauds to be implemented by the PPIs with an emphasis on strong risk management system. • Requirement on a formal, publicly disclosed customer grievance redressal framework. PPI issuers shall create sufficient awareness and educate customers in the secure use of the PPIs and Report the frauds on a monthly / quarterly basis to the concerned RBI Regional Offices. • Establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. This is to be in place for reporting incidents to RBI & CERT-In. • Board approved information security policy and best practices on restricting multiple invalid attempts on account, velocity check on number of transactions, internal & external escalation mechanisms, MIS systems security, inactivity timeout failures, etc. • Process of determining customer liability in case of unauthorized / fraudulent transactions involving PPIs. • Minimum baseline requirements such as mobile app not to be installed on rooted or jailbroken devices, source code audit, integrated SoC Model, subscription to anti-phishing/ anti-rouge app services, disaster recovery services, etc.	• Mandatory security requirements from the regulator which is to be adhered by prepaid payment instruments organizations in India. This may enable trust in digital payment space for users to adopt digital payment channels at mass scale. • The requirements also provide a framework for the end users to submit their grievances and ensures protection of their transactions.
(II) Draft MeitY Security Rules for Prepaid Payment Instruments [28] • Mandates following process requirements such as, but not limited to, information security policy, privacy policy, and risk assessment, reporting of incidents, grievance redressals and adherence to security standards to be stipulated by MeitY. • Stipulate technological requirements such as, but not limited to, security of personal information, access to personal information, end-to-end encryption, traceability, retention of information, customer identification and authentication, etc.	• Mandatory prescriptive security requirements from the ministry which is to be adhered by prepaid payment instrument organizations in India. If stipulated, this may add to compliance burden and may impact the innovation space in digital payment ecosystem.
(III) Medium Term Recommendations to Strengthen Digital Payments Ecosystem, Watal Committee Report [29] • Make regulation of payments independent from the function of central banking. • Update the current Payments and Settlement Systems Act, 2007 to include explicit mandate for consumer protection including penalties and independent appeal mechanism, regulations on systemic risks, data protection and security and a process of regulatory governance.	• It consists of holistic recommendations from finance ministry committee to provide direction for overall digital payment space in India. It clearly articulates the importance of cyber security to propel digital payment adoption.

Table 2 Public Policies Analysis - India

Future Developments

The above journey in respect of public policies and regulations is limited to current evolution. This study also analyzed, at a high level, future developments in terms of public policies that may take place in the Indian context with respect to digital payment space. Few developments mentioned below may have a significant influence on how the space may evolve in terms of payments, security and commerce in general, in India.

Learnings	Analysis	Estimated Timeline
(I) Data Privacy Law [30] • The Indian Government has appointed an expert committee, headed by former Supreme Court judge B N Srikrishna, to build visibility on key issues with respect to data protection and to provide recommendation on these issues. • This may result in data privacy regulation for India. The future regulation on privacy may entail elements such as, but not limited to, defining liabilities of data controllers, data processors, requirements on data breach notification, and data protection measures for organizations to implement. The regulation is expected to cover organizations such as e-Wallets, payment gateways and pre-paid payment instruments, etc. The future regulation may have requirements on privacy by design which may bring significant changes in the development of financial technology products and services.	• The major outcome of the above committee activities may result in a data protection law in India. The stipulations in it which are work-in-progress such as, but not limited to, notice, choice, consent, usage limitation, stand on data localization, privacy policies, securing data, need of privacy impact assessment and protecting Indian citizen's fundamental right to privacy. • These new compliance requirements of future from data protection aspect may impact how organizations may build digital payment infrastructure and products to operate in this space. The future data protection law may also act as an enabler for end user to adopt digital payments with enhanced confidence and trust; as it is expected to provide assurance and grievance framework for the end citizens.	**2019**
(II) RBI Digital Payment Security Sub-Committees • The first sub-committee is on Mobile Banking and Security. It is studying various global security standards and protocols. The end outcome is to table best practices for mobile security for trusted banking (an enabler for digital payments in India) and promote its adoption across organizations in the country. This committee is focusing primarily on technology aspects and associated risks across all applicable stakeholders, specific issues needing regulatory attention with respect to mobile banking and security. Also to identify authorities/ institutions/stakeholder(s) in the mobile financial ecosystem that are in the best position to implement the measures as to be stipulated in the cyber security best practices report.	• The sub-committee's activities may result in cyber security guidelines on mobile banking and card payments. This can be a good start for digital payment organizations to understand regulator viewpoint from best practices implementation aspect. • Detailed guidelines from regulators prepared in consultation with industry helps organizations in building trust with end customers.	**2019**

Learnings	Analysis	Estimated Timeline
• The second sub-committee is on Card Based Payment and Security. This sub-committee is mandated to examine best practices in securing card based payments, identify gaps in current regulatory ecosystem, study the threats and solutions for PoS machines, compliance with extant standards, etc.		
(III) Protocol for e-Wallet Companies [31] • The Central Government of India is in discussion stage to explore stipulation of standard protocol for e-wallet companies on how to prevent and fight online financial frauds, in the advent of rise of digital payment space and associated cyber threats. It is also speculated that the government is exploring to formulate a 'Digital Payments Act' to regulate e-payments.	• Government stipulating a 'Digital Payment Act' which may also include cyber security requirements for digital payment organizations. It may add to compliance burden for the organizations in this space. • At the same time a dedicated holistic regulation which is to be supported by RBI master directions and data protection law of future may act as a factor of trust to propel digital payment adoption.	**2020**
(IV) Global Challenge for Cyber Security Workforce [32] The Ministry of Electronics and IT in collaboration with Cyber Peace Foundation (CPF) is planning to organize a global cyber challenge. The government's digital platform 'Mygov' has invited people to participate. The primary objective is to elevate the domain of cyber security; the challenge is to be based on numerous problem statements and participants may propose solutions resulting in an application or a product.	• Challenges similar to this on national level helps building capacity and capabilities in the realm of cyber security. Evolution of capabilities and skill building with the help of global platforms like these puts India, to lead from front in securing digital payment space globally. It also helps a nation to learn from companies which are not part of the Indian landscape. • This challenge can also benefit the space of digital payment security, as new protection solutions may emerge and it augments the skill building agenda of the country in the domain of cyber security.	**2019**
(V) Establishment of Financial CERT, India [33] An expert group has proposed the setting up of an independent Computer Emergency Response Team for Finance (CERT-Fin) to be the cyber warrior of the financial sector.	• CERT-Fin will be the key to ensuring a comprehensive cybersecurity framework for the financial sector, especially at a time when there has been a burst of activity in the Fintech space as India makes efforts to embrace a less-cash economy.	**2018-19**

Table 3 Future Public Policies - India

6.2 Global

The velocity with which the digital payment space is growing is to be noted. For its growth, secure enablement, promoting innovations and consumer protection from fraud, conducive and pragmatic public policies are warranted. This study analyzed few major countries' public policies, regulations, standards and frameworks from the viewpoint of cyber security and data privacy. Highlights of the different countries' study and learnings from it are captured below for reference.

Singapore

Singapore is leading the adoption of digital payment technologies and platforms globally. At the same time its public policies, standards and frameworks are aligned with the current ecosystem and visionary evolution. To govern the digital payment sector, i.e. prepaid payment instruments, they have released pertinent public policies such as (I) National Cyber Security Bill 2017 (still in draft stage and will be enacted in 2018), (II) Technology Risk Management Guidelines for BFSI Sector (III) Data Protection Law. Major learnings from its study are shared below [34] [35] [36].

Major Learnings

I. Appointment of dedicated cyber security commissioner to govern critical information infrastructure (CII) protection.

II. Designating BFSI Sector as critical information infrastructure which includes digital payment sector.

III. Cyber security incidents to be reported by CII owners to the commissioner of cyber security on regular basis.

IV. Inclusion of hefty penalties up to SGD 100,000 and 2 Years of imprisonment in case of noncompliance in respect of cyber security of CII.

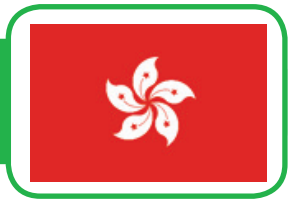
V. National cyber security bill proposes to license cyber security service providers and practitioners who intend to provide services and products to CII organization.

VI. Technology risk management guidelines include mandatory requirements in areas such as reliability, availability and recoverability of critical IT systems.

VII. During the development of data protection law, references were made to the data protection regimes of key jurisdictions that have established comprehensive data protection laws, including the EU, UK, Canada, Hong Kong, Australia and New Zealand.

VIII. The Personal Data Protection Commission (PDPC) published a "Guide to Securing Personal Data in Electronic Medium" and a "Guide to Managing Data Breaches".

Hong Kong



The journey of Hong Kong in terms of governing digital payment sector is marked with incremental changes. The central bank, i.e. Hong Kong Monetary Authority (HKMA) labelled prepaid payment instrument as stored value facilities (SVF). HKMA released licensing guidelines for SVF organizations assigning gravity to technology risk management, i.e. cyber security risks management in order to obtain licenses to operate. The licensing guidelines were introduced with the help of explanatory and practice notes pertaining with it. The Hong Kong data protection law also appropriately protects data subjects in the digital payment sector. Major learnings from its study are shared below [37].

Major Learnings

I. HKMA mandates appropriate risk management policies and procedures for managing the risks.

II. The HKMA attaches particular importance to the effectiveness of the applicant's technology risk management, payment security management and business continuity management.

III. The SVF licensee should perform a formal risk assessment.

IV. Conduct a comprehensive risk assessment before outsourcing.

V. HKMA assessment to include IT Governance & Technology Risk Management Process.

VI. Mandatory security controls on authenticity and traceability of payment & fraudulent transaction.

China

The governance landscape of China with respect to digital payment sector prepaid payment instrument organizations is limited to public policies such as (I) People Bank of China Regulation (II) Rules on the Administration of Payment Services Provided by Non-Financial Institutions. Major learnings from its study are shared below [38] [39].

Major Learnings

I. Prepaid payment service providers are not allowed to outsource their technology activities or processes pertaining to cyber or cyber security.

II. Chinese security and electronic authentication standards are mandated be used for digital certificate/electronic signatures by the payment service providers.

III. Three security methods are allowed to verify the customer's instruction; i.e. either password, the digital signature/electronic signature or a one-time password transmitted in a secured channel along with biometrics (such as fingerprint).

Australia

The Australian digital payment landscape has emerged as a forerunner for the rest of the world. Rather than following multiple paths to govern prepaid payment instrument organizations, Australia designated a single agency which is responsible to set requirements of cyber security and data protection for digital payment landscape. The Australian Payments Clearing Association Limited (APCA) is the designated authority. The data protection in the digital payment space is also governed with the help of Australian privacy principles and state data protection laws. Major learnings from its study are shared below [40].

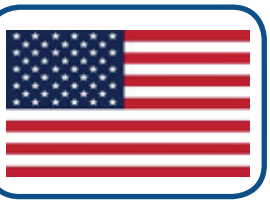
Major Learnings

I. APCA published best practice guidelines for card issuers in relation to third party mobile wallet security.

II. APCA published Payment Tokenisation Specification Technical Framework.

III. Tokenisation is not a mandatory requirement for transactions made using a third party digital wallet if the third party digital wallet includes security by design.

USA



The US approach to govern the digital payment sector is not based on designation of a single agency or a dedicated regulation for cyber security of prepaid payment instruments; rather a combination of different regulations and different agencies are responsible for it. Major learnings from its study are shared below [41].

Major Learnings

I. No single agency controls and governs digital payment cyber security.

II. Federal Reserve System, i.e. the national central bank primarily ensures the payment system remains stable and safe.

III. Financial CERT as an institution issued the prepaid access final rule, requiring prepaid access providers and sellers to file suspicious activity reports (SARs).

IV. Mobile Payment Industry Workgroup (MPIW) constituted to monitor evolving technology and potential threats to mobile payment participants.

V. The Office of the Comptroller of the Currency (OCC) published a paper on responsible innovation in the federal banking and digital payment systems that includes security and privacy innovations.

European Union (EU)

The European digital payment cyber security and data protection landscape is primarily driven by the agency called European Union Agency for Network and Information Security (ENISA) which is a center of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. The data protection regime is planned to be based on newly introduced GDPR regulation; to be enacted from May 2018. ENISA has released guidelines on Security of Mobile Payments and Digital Wallets. Major learnings from its study are shared below [42] [43].

Major Learnings

I. ENISA Guidelines have been prepared post assessing major wallet provider's product security.

II. ENISA Guidance focusses on minimum security measures; security payment chain; mobile OS security; risk management program.

III. Other areas in ENISA guidance includes detailed awareness for customers and merchants.

IV. Review of wallet providers to be conducted based on threat model which is provided by ENISA.

V. A single data protection law GDPR for member states focusing on hefty penalties in case of non-compliances. It also extends accountability to data processors other than data controllers in respect of data protection.

7 Best Practices for securing the Digital Payment ecosystem

7.1 Global

The pace of technological innovation in the finance sector has increased significantly in the recent years giving rise to new services and business models by banking institutions, technology companies and new startup organizations. Taking advantage of the most cutting-edge technologies, financial institutions have developed digital payment systems to bring the end consumers within the financial sector realm, attracting them with the most effective and efficient financial transactions. The secure and efficient operation of financial sector infrastructures is imperative for maintaining and promoting the financial stability and economic growth of the country. Digital payment systems can offer solutions to increase cost efficiencies, address the consumers' complex requirements with improved ability to perform financial transactions effectively and productively in lesser time.

The key motivations for the wide-scale adoption of technology by this sector includes:

- Provide convenience and improving the overall customer and provider experience
- Perform transactions from anywhere fading the geographical boundaries
- Making economic transactions cashless, thereby reducing of cost for both customer and payment service providers
- Reducing the operational costs and increasing efficiency in delivery

However, along with the above opportunities, there are wide range of entry points through which the digital payment systems could be compromised. The risks related to financial digitization may vary like availability of services (DDos attacks), Integrity and confidentiality of information (fudging of accounts, account spoofing, etc.). The convenience offered to customers with increasing technology adoption and its associated risks go together. The attacks on financial sector are increasingly becoming more advanced and sophisticated which are targeted to steal the enterprise/customer information. We have already witnessed many organized and sophisticated attacks like the recent Swift Global interbank series attacks in Bangladesh, Vietnam and Ecuador. Financial system resilience has now become an important concern to instill trust with customers.

Enterprises dealing with digital payments are putting in significant efforts in improving their security posture thereby trying to minimize the attacks on their systems. Achieving the objectives related to securing systems at various levels would also depend on various institutions/stakeholders to collaborate and work towards improving the security of the ecosystem. This would also help remove barriers to adoption through improving the perception of security.

Organizations need to keep track of the technological advancements in their payment delivery channels to derive into wide range of choices about how to balance usability and security, for example, customer-facing applications such as online or mobile banking must be in favor of usability yet must remain above a minimum acceptable level of security. On the other hand, the critical systems such as core banking need to strike a balance in favor of security.

It is imperative for entities in financial sector to establish and maintain an Enterprise security best practices/framework that is tailored to specific risks and appropriately informed by the national, international and industry standards and guidelines. Towards addressing the challenges, there are several Global Standards/Best practices/Guidelines currently available concerning Digital wallets, Mobile wallets, contactless payment communication technologies and mobile payment transactions. The focus of these are on application security architecture, secure design and development, security testing, digital forensics, etc., for stakeholders to adopt and implement. However, most of the standards/guidelines/ best practices are voluntary in nature and therefore, adoption and implementation has been varied and there is no uniformity in implementation to obtain assurance. In order to establish minimum assurance of trust and security, it would be important for the relevant regulators/stakeholders to prescribe some mandatory baseline security guidelines that has to be adhered.

Given the importance of digital payment systems, organizations should align themselves with leading standards, guidelines or recommendations, reflecting current industry best approaches in managing cyber threats, and incorporate the most effective cyber resilience solutions. The adoption of global standards and best practices can be categorized (not limited to) under the following broad categories:

I. Enterprise architecture principles, guidance and references

II. Guidance for Secure development, Implementation, deployment, testing and maintenance of application

III. Incident response and recovery

IV. Generic guidance by providing best practices for managing cyber security risks

The following sections provide a brief description of the above which can be adopted by stakeholders to ensure a secure ecosystem that can continue to provide the foundation for trustworthy and secure financial services.

I. Enterprise Architecture Principles, Guidance & References

Security Architecture and design of the digital payment solutions/products need more attention to avoid any sort of financial, operational or reputational damage through exploitation of weakness present in the systems. Mobile banking applications facilitate a customer to undertake a broad range of transactions from mobile devices that may include external devices like using a wearable accessory such as a watch. The digital payment transaction cycle involves hardware/software components on the device (operating system, application, and browser), network, intermediaries (gateways), backend services and users. Since vulnerabilities at any of the layers may potentially affect the security of transactions, it is imperative to evaluate the potential risks at each component level of the ecosystem while conceptualizing and designing the mobile banking applications. This would help in detecting the compromise either by the information provided by the device itself (e.g., via device attestation) or by data analysis performed on the transactions (e.g., by fraud detection monitoring process). Adoption of some form of Threat Modelling for identifying potential design vulnerabilities prior to implementation stage is one good practice in addressing the digital payment related risks.

There are diverse ways and opportunities existing for an attacker to compromise the security of the payment systems during each stage of the payment life cycle that includes customer enrolment, provisioning, credential change, payments, etc. Threat-modeling can be performed before a product or service has been implemented which can help ensure a thoroughly secure product or service design. While there are several approaches to threat modelling, their basic objective remains to ensure that applications are made secure by design. Few notable approaches are as follows:

1. **ISO 12812** is a five-part document that describes the requirements and implementation recommendations for mobile payments and focuses on the development of mobile financial services applications.

Part 1	General Framework	Provides an overview of what expectations the standard has for mobile financial service implementations
Part 2	Security and Data Protection	Provides requirements and recommendations for a framework to manage the security of mobile financial services
Part 3	Financial Application Lifecycle Management	Addresses lifecycle considerations, including roles and infrastructure for secure provisioning, credential authentication, terms of service, customer relationship, new features, and updates
Part 4	Mobile Payments to Persons	Specifies recommendations for the technical implementation of the generic architectures of the mobile payments-to-persons program
Part 5	Mobile Payments to Businesses	Focuses on mechanisms by which a person uses a mobile device to initiate a payment to a business entity

2. **The Open Group's (TOG) Mobile Management Forum (MMF)'s Secure Mobile Architecture (2014)**: The Open Secure Mobile Architecture (O-SMA) is a reference architecture to guide secure development of systems. The architecture focuses on communication over IP network, end-to-end-security, session security, standard device and network management, protection measures on devices, host identity security, data model, policy engine, location based security and network measurements.
3. **NIST Internal/Interagency Reports (NISTIRs) on computer security and privacy Draft 8144** (Assessing Threats to Mobile Devices & Infrastructure – Mobile threat catalogue), this document identifies threats to mobile devices and associated mobile infrastructure to support development and implementation. Threats are divided into broad categories, primarily focused on mobile applications and software, the network and associated infrastructure, mobile device and software supply chain, and the entire mobile ecosystem. Each threat as identified is catalogued alongside explanatory and vulnerability information wherever possible, and also applicable mitigation strategies. The Mobile threat catalogue is an on-line repository available for use which is being updated periodically with community involvement.
4. **Microsoft Threat Modelling (2016)**: This threat-modeling approach endorsed by Microsoft is called STRIDE which is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. STRIDE is a way to find a wide variety of threats using these easy-to-remember threat types. More important than fitting a threat to a category is using the model to help describe the threat and design an effective mitigation strategy.
5. **Draft Mobile Threat Model, OWASP** – this document is intended as an outline or checklist of items that need to be documented, reviewed and discussed when developing a mobile application.
6. **Top 10 design flaws and ways to avoid them by the Center for Secure Design (CSD) initiative of Institute of Electrical and Electronics Engineers (IEEE)**. CSD identified the top 10 design flaws and ways to avoid them. The CSD recommendation can provide valuable guidance to consider in the design of an application.

II. Guidance for Secure Development, Implementation, Deployment, Testing and Maintenance of Application

Secure Software Development Life Cycle (SSDLC)

Digital payment system providers should adopt secure coding practices and secure code reviews (both manual and automated) as the process of development itself may involve many third-party developers and technical components. Best practices from a secure mobile development perspective encompasses developer training, incorporating security in requirement gathering, design and coding (Threat modelling, Architecture review, Static Analysis), testing & release (Security Assurance-Dynamic Analysis) and maintenance (Vulnerability advisory monitoring and fixing). ENISA guidelines for secure development, OWASP standards for mobile application security verification, Android and iOS operating system specification and guidance, W3C best practices, application security testing guidelines by NIST and other organizations would provide guidelines for the development of applications.

The general practice of performing software testing to identify the security issues in the built system is no more effective, since identification of the number of critical issues would be too late or not discovered at all. It is imperative to integrate the security related activities across the Software Development Life Cycle (SDLC). The SDLC is a framework that defines the process used by organizations to build an application from its inception to decommission.

The Secure SDLC will help to discover and reduce vulnerabilities early, effectively building security in the system at the early stage of software development. This would also reduce the costs significantly in resolution of issues due to early detection of flaws/bugs present.

There are number of Secure SDLC models that are widely adopted. Following are few examples that are proposed for implementation.

MS Security Development Lifecycle (MS SDL) [44]: One of the first of its kind, the MS SDL was proposed by Microsoft in association with the phases of a classic SDLC. This document illustrates the core concepts of the Microsoft Security Development Lifecycle (SDL) and discusses the individual security activities that should be performed to follow the SDL process.

NIST 800-64- Security Considerations in the System Development Life Cycle [45]: The purpose of this guideline is to assist agencies in building security into their IT development processes. This should result in more cost-effective, risk-appropriate security control identification, development, and testing. This guide focuses on the information security components of the System Development Life Cycle (SDLC).

OWASP CLASP (Comprehensive, Lightweight Application Security Process) [46]: This is designed to allow the organizations to easily integrate its security related activities into the existing application development processes. Each CLASP activity is divided into discrete process components and lined to one or more specific project roles.

Standards/Guidelines related to Application Development:

- **Smartphone Secure Development Guidelines (ENISA):** The document is written for developers of smartphone applications as a guide for developing secure mobile applications and defending against mobile attacks
- **OWASP Mobile Application Security Verification Standard (MASVS) draft**: Intended for developers seeking to develop secure mobile applications
- **Android Application Security**: Provides tips, updates and resources, guidance on configuration, provide protection strategy, educates on how to use Android security services, etc.
- **iOS application security guidelines**: Provides best practices, information on APIs for security and their use, guidelines on the features devised for security, and practices on development and execution of code
- **PCI DSS, NIST & FIPS** Recommended Security Practices
- **BSIMM & OpenSAMM** Frameworks
- **Mobile Web Application Best Practices W3C Draft:** The guidelines are intended to aid in the development of rich and dynamic mobile Web applications for enabling a better user experience and warning against those that are considered harmful.

Security at Implementation Stage

As seen in the previous section, security is to be given due importance during the development phase of the application. But it may not show its effectiveness in the environment in which it is implemented. This often attributes to the issues in the deployment of the application. As digital payment application leverages many ecosystem components likely to be developed by third-party, hosted on the cloud or shared infrastructure, exchanging information etc., implementation level security would be critically important.

While implementing mobile application, the following aspects should be considered:

- Application deployment processes, deployment checks and tests and sign-off requirements
- Managing and maintaining versions of the code deployed in the production environment
- Product environment security, segregation from the rest of environments and access to assets in the product environment
- Security architecture, solutions, and controls deployed in the production environment
- Permissions, authentications and managing roles of the users access critical infrastructure assets
- **Apply coding and testing standards**: Coding standards help developers avoid introducing flaws that can lead to security vulnerabilities. For example, the use of safer and more consistent string handling and buffer manipulation constructs can help to avoid the introduction of buffer overrun vulnerabilities. Testing standards and best practices help to ensure that testing focuses on detecting potential security vulnerabilities rather than concentrating only on correct operation of software functions and features.
- **Apply security-testing tools including fuzzing tools**: "Fuzzing" supplies structured but invalid inputs to software application programming interfaces (APIs) and network interfaces so as to maximize the likelihood of detecting errors that may lead to software vulnerabilities.
- **Apply static-analysis code scanning tools**: Tools can detect some kinds of coding flaws that result in vulnerabilities, including buffer overruns, integer overruns, and uninitialized variables. Microsoft has made a major investment in the development of such tools (the two that have been in longest use are known as PREfix and PREfast) and continually enhances those tools as new kinds of coding flaws and software vulnerabilities are discovered.

- **Conduct code reviews**: Code reviews supplement automated tools and tests by applying the efforts of trained developers to examine source code and detect and remove potential security vulnerabilities. They are a crucial step in the process of removing security vulnerabilities from software during the development process [47].

Security Testing

It is important to perform security testing along with quality assurance (QA) tests to continuously integrate security into development. Specific and sometimes exhaustive guidance on security testing of mobile applications are OWASP Mobile Security Testing Guidelines, Mobile Security AppSec Verification, PCI-DSS Mobile Payment Acceptance Security Guidelines, etc.

i. **OWASP (Open Web Application Security Project)**: OWASP Mobile Security Project is a centralized resource from OWASP intended to give developers and security teams the resources they need to build and maintain secure mobile applications. It is a comprehensive guide on mobile risks, security checklists, and security testing guidelines, secure development and controls. A gist of secure mobile application development guidelines is given as below:

   - **Authentication and password management**: Set of controls used to verify the identity of a user, or other entity, interacting with the software, and to ensure that applications handle the management of passwords in a secure manner
   - **Code obfuscation**: Set of controls used to prevent reverse engineering of the code, increasing the skill level and the time required to attack the application
   - **Communication security**: Set of controls to help ensure the software handles the exchange of information in a secure manner
   - **Data storage and protection**: Set of controls to help ensure the software handles the storing and handling of information in a secure manner
   - **Payment related controls**: Set of practices to ensure the application properly enforces access controls related to resources which require payment in order to access premium content, additional functionality, improved support, etc.
   - **Server controls**: Set of practices to ensure the server-side program which interfaces with the mobile application is properly safeguarded
   - **Session management**: Set of controls to help ensure mobile applications handle sessions in a secure manner
   - **Use of 3rd party libraries/code**: Set of practices to ensure the application integrates securely with code developed by outside parties
   - **Mobile application provisioning/distribution/testing**: Set of controls to ensure that software is tested and released relatively free of vulnerabilities, that there are mechanisms to report new security issues if they are found, and also that the software has been designed to accept patches in order to address potential security issues

Application Security Maintenance

Security flaws may still exist in an application even after focussing on security features at the development stage. Routine security checks need to be planned along with the response plan that addresses the customer reported security incidents. The application and associated infrastructure need to be analysed for any possible security flaws before incorporating new features or any changes in the application. For proper authorization of the application, users need to be created with access privileges dependent on need to have basis. Proactively monitoring the security vulnerabilities in platform system software and embedded components and then initiating incident response and remediation, as appropriate, are crucial. Identifying security vulnerabilities using reputable sources for obtaining security information is a continuous cycle. Sources such as software vendor websites, the US National Institute

of Standards and Technology (NIST) National Vulnerability Database (NVD), and the CERT Common Vulnerabilities and Exposures (CVE) are reliable for vulnerability research and analysis. Inventory of all third-party frameworks/APIs that are used in the mobile application is helpful in robust implementation of security patches. Whenever any vulnerability becomes public, a corresponding security update must be done for the mobile applications that are using these vulnerable third-party APIs/frameworks. Database of all third-party frameworks/APIs that are used in the mobile application would be helpful to handle security patches. Whenever any vulnerability comes to public knowledge, a corresponding security update must be done for the mobile applications that are using these vulnerable third-party APIs/frameworks.

Disposal

The disposal stage is one very critical stage in the entire Software Development Cycle that is concerned with the disposition of the data, hardware and software. Security is not a one-time implementation during the development and delivery. The confidentiality of information can be compromised if the disposal stage is not planned properly. Some of the important concerns during this stage are as follows:

- For encrypted data, ensure long-term storage of cryptographic keys. Those responsible for archiving data will need to ensure that the ability to decrypt the data accompanies it. The Records Management section of your organization should be able to provide guidance in this area. In some cases, it may be required that the hardware (i.e. computer, media reader, and display device) accompany the system to ensure the technology exists at the time of retrieval. Future availability is the security concern here.
- Review the legal requirements for records retention. Consult with your records maintenance section regarding the preservation and retention requirements (if any) specified by the regulators and government. Prior to moving the documents to an archive facility, it may be necessary to stamp them with the appropriate sensitivity, or alternatively it may be appropriate to destroy (i.e. shred or burn) them. Confidentiality is a primary concern.
- A final disposal phase concern is sanitizing the media. Sanitizing can be done by overwriting, degaussing, or destroying the data on the storage media. Privacy and confidentiality are the concern of sensitive and/or personal data. Each organization should have a policy on proper disposal techniques and services.

III. Incident Response and Recovery

The NIST special publication 800-61 defines Incident as "Violation or threat of violation of computer security policies, acceptable use policies or standard security practices".

It is important to have an incident response team in this age of usage of counter-forensics tools by the criminals. Malware authors are spending more time researching anti-forensic techniques, especially when it comes to executing in memory only and virtual environment detection, to thwart both forensics and malware analysis techniques.

What incident response does?

- Confirm whether or not an incident occurred
- Provide rapid detection and containment
- Determine and document the scope of the incident
- Minimize disruption to business

Organisations need to define what a computer security incident means to your organization.

- If you don't have one, you should create one!
- It will establish the scope of what your IR team does

- Restore normal operations
- Allow for criminal or civil actions against perpetrators
- Educate senior management

A Handbook for CSIRTs has been published by the Carnegie Mellon University – SEI, clearly articulating the role of CSIRTs [48] and how they are to be set up. This document provides guidance on forming and operating a computer security incident response team (CSIRT). CSIRT services can be grouped into three categories:

(a) **Reactive services**. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.

(b) **Proactive services**. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.

(c) **Security quality management services**. These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

International Standards related to managing IT and cyber security incidents:

- **ISO/IEC 27002 Code of practice for information security controls**: Covers managing security incidents and wider business continuity issues, as well as backing up data
- **ISO/IEC 27035 Information security incident management**: Covers incident management in detail. A new version is under development which will have three separate parts. ISO/IEC 27035-1 will deal with principles; ISO/IEC 27035-2 will explain planning in advance of incidents; while ISO/IEC 27035-3 will deal with incident response.
- **NIST 800-61, Computer Security Incident Handling Guide**: Provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident
- **ISO/IEC 27037 Guidelines for identification, collection, acquisition, and preservation of digital evidence**: explains how to deal with malicious online activity
- **ACPO Good Practice Guide for Digital Evidence**: The best practice guide for handling digital evidence developed and published by the Association of Chief Police Officers.
- **ISO 22301 Business continuity management systems requirements**: Specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
- **ISO/IEC 27031** Guidelines for information and communication technology readiness for business continuity: It is the planning standard to help organizations ensure that their cyber systems meet their business continuity needs.

IV. Generic guidance by providing Best Practices for managing Cyber Security Risks

Below are Top 20 CIS security controls [49] for effective cyber defense that provide specific and actionable ways to defend cyberattacks.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Detailed information about individual controls may be found at https://www.cisecurity.org/controls/

Challenges in adopting global practices and/or standards – for various stakeholders (including end-consumers):

- Implementation and adherence to standards may delay the development and might impact the business potential
- Cost of investment, efforts, and resources required for implementation of standards and guidelines may prove detrimental to their adoption
- Enough capability and skills may not be currently available to work on the standards or guide implementation of these standards
- Diverse devices, technology components, players, and providers make mobile payment systems quite complex and interdependent. General standards may not include specific attention towards all the aforementioned elements. On the other hand, standard or guidelines that converge and integrate all components may not be interoperable.
- The mobile payment technology ecosystem is still evolving. There are many small and big players active in the ecosystem. It would be difficult to ascertain all possible issues and threats in case of evolving technology.
- Developers of the mobile application may not be aware of or skilled in or empowered to implement standards and guidelines. Although they may be aware of security capabilities provided by OEMs, there might not be proper incentives and governance to ensure developers are adhering to standards and best practices
- Infrastructure for testing of specifications of technologies and conformation of standards are limited in terms of availability

Following steps must be taken to ensure predictable, progressive and secure development of digital payment ecosystem:

- Awareness and outreach of global standards, guidelines, and practices evolving to influence mobile payment services
- Development of skills and expertise in the key standards that would shape mobile payment space
- Concerted efforts in increasing the country's participation in the standard making in mobile payment space
- Conducive regulatory ecosystem for adoption, implementation, and conformity testing against the standards

7.2 India

The Indian digital payment industry depends heavily on technology for providing cutting-edge digital payment products intended to offer better services to the customers. With the variety of actions taken by the Government and Reserve Bank of India, banking and financial system in India have proliferated exponentially in recent years. Financial inclusion, Pradhan Mantri Jan Dhan Yogna, Interbank ATM Transactions through National Finance Switch (NFS), Immediate Payment Service (IMPS), etc., have brought banking at customer's doorstep and customers are enjoying greater benefits [50].

Digital Payment providers need to take appropriate steps in defending against a variety of cybersecurity threats, primarily criminals gaining unauthorized access to systems, vulnerabilities existing in the systems being exploited for financial gain, crime syndicates/disgruntled insiders compromising business-related data for commercial gains, etc. The motive behind such actions may be to disrupt the operations, financial gain or even cause reputational damage to an organization. Based on the environment in which information systems are located and the type of information it is designed to support, attackers will have an interest in attempting to gain access to diverse types of information. Organizations need to have

clear understanding of which threats are most likely and most risky to their unique situation to develop and implement an effective Cyber Security strategy.

An enterprise-wide approach is critical to manage the multifaceted cybersecurity challenges because absolute cybersecurity is a myth. The approach should involve mitigation, avoidance and transfer risks posed by such threats. Companies need to establish and maintain an appropriate governance and cybersecurity risk management framework to address the risks related to their IT systems and processes.

To protect the interest of the public , the government makes rules and policies meant for assuring the data protection and privacy related to the information collected or processed by the service providers, while regulators like RBI set the framework to conduct the business. The cybersecurity best practices to be followed will have to integrate the elements of corporate security, rules & regulations along with the other essential elements like physical security.

The ecosystem that enables the digital payment services is a complex one posing various challenges in terms of managing security of enterprises and data protection. Several global standards/best practices/ guidelines are currently available concerning digital payment security architecture for stakeholders to adopt and implement.

The National Payment Corporation of India (NPCI) [50] in its whitepaper "Cyber Risk Management and 10 Essential Security tools" highlights the implementation of the following to improve the security of any financial institution: *For advanced controls on implementation in an enterprise cyber security environment, please refer Architectural principles, guidance and references (pg. 45)*

1. Firewall
2. Network Access Control (NAC)
3. Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)
4. Advanced Persistent Threat (APT) prevention
5. Anti-Virus / Anti Malware protection
6. Web Proxy & Content Filtering:
7. Security Incident & Event Management (SIEM)
8. Anti - Distributed Denial of Service (DDoS)
9. Data Loss Prevention (DLP)
10. Data Backup and Recovery Solution

Currently, due to lack of a single agreed standard or guidelines around the finance industry, each payment player can choose the standard/guidelines which suits his payment solutions to create a more secure and trusted solution eco-system.

7.3 Security Risks and Challenges: Digital Payment Systems

While the digital payment service providers continue their endeavor in providing new services and delivery channels that offer multiple potential benefits to their consumers, the exploitation options for criminals are also increasing. It is very important for the digital payment ecosystem to understand the threat vectors that come along with different payment methods and there is an urgent need to work together to find solutions.

This section of the report attempts to highlight some of the threat vectors associated with different payment methods and try to suggest few measures to mitigate the security risks.

Payment Method	Security Challenges	Security Tips for Consumers
QR Code	• QR codes are vulnerable to phishing. The attacker can gather information like victim's current GPS location, device IMEI number, SIM card data and other sensitive data • QR codes are easily infiltrated, manipulated to alter payee details, cause to introduce computer contaminant in the payer's mobile device. • Fake and malicious QR code can be easily pasted over the genuine one by fraudsters to divert the payment	• If the QR code looks like it was added on to marketing materials, do not scan it [51]. • Do not scan QR codes in the form of stickers placed randomly in public places as it might be from scammers testing out his/her malicious QR code. • If the QR code leads you to a website that request for your personal information, do not disclose anything until you have verified that the request is legitimate. • Install a mobile security application with antivirus, antispyware and web filtering abilities to protect your mobile devices [52].
NFC	• NFC communication protocol used by mobile payment wallet is vulnerable to eavesdropping, data corruption and manipulation, interception or man-in-the-middle attacks and NFC proxy relay attacks. • Malicious NFC tags may be embedded to the device for malicious operations. • Host Card Emulation (HCE) technique used for securing transactions may be vulnerable in the rooted devices. • Malware targeting NFC communication protocol can be used by criminals to steal sensitive information.	• Install updates and patches related to NFC on your device regularly. The vulnerabilities existing in the NFC are often fixed by the providers but, must be updated by the consumers. • Disable NFC if you are not using it- turning off unused networking features is a good rule of thumb to limit exposure to attackers. • If the NFC machine looks tampered with or there are any other suspicious items around it, don't use it.
UPI	• Compromise of device passwords • Unauthorized access to information stored in device • Misuse due to loss of device • Fake applications	• Strong passwords should be enabled on the user phones, tablets, and other mobile devices before mobile banking apps can be used. • Additional layers of security inherently provided by these devices should be used. • Bank account number or IPIN should not be stored on the user's mobile phone. • The user should report the loss of mobile phone to the bank to disable the user's IPIN and access to the bank's account through Mobile Banking app. • Mobile apps should be downloaded from trusted sources only.

Payment Method	Security Challenges	Security Tips for Consumers
Wallets	• Fraudulent transactions can be made if the mobile device falls into wrong hands. • Exploitation of mobile payment application vulnerabilities • Perpetual login to the e-Wallets are provided by many e-wallet providers that doesn't require password to be entered every time while using the application. .	• Do Not "Root" the Cell Phone – It would help criminals to easily bypass the security. • Enable Lock Screens – "Face Unlock," "Pattern," "PIN" and "Password" all will make difficult for physical access to the device by the criminals. • Enable Encryption – This will prevent even USB Debugging from bypassing the lock screen. • Maintain Device Up-To-Date – Ensure the device is current with the latest official software
MMT • USSD related issues [53]	• Fraudulent transaction can be performed by criminals through lost and stolen devices • Telecom-based money transfer is prone to command request/response tampering, message replay attacks, and server response malfunctioning • Unencrypted transmission over widely used telecommunications networks • SMS spoofing in which an unauthorized user sends an SMS message pretending to be from a different mobile number to mislead a consumer into providing sensitive information such as OTP, account information, transaction password, etc., to the fraudster	• Keep strong passwords for your phone • It is advisable for users to enable encryption, remote wipe abilities and antivirus software on the phone • Keep your SIM card locked with a Pin to avoid misuse. In case of loss or theft of the mobile device, contact your service provider to block the subscription of the SIM card [54] • Links in unsolicited text messages should not be opened • PIN should be changed periodically • User should be cautious of text messages from unknown senders, as well as unusual text messages from known senders
Mobile Apps	• Fake application security threats from App Store • Reverse Engineering • Credentials and Keys handling • 3rd party applications may host malicious Remote Administrative Tool (RAT) • Poor Authorization and Authentication	• The customer should update the Operating System on a regular basis, as soon as the OS provider makes an update available.

Table 4 Risk and Challenges - Digital Payment Systems

7.4 Data Protection and Privacy Regulation in India

The ability to protect sensitive information is often defined as Privacy, while protection is a security related component. The integrity and availability of information form the definition for data protection, privacy is much more granular, controlling who, what and when a specific data can be accessed. Banking institutions may have all the personal information of its customer to carry out the business; however data privacy allows access to information only when businesses requires it. It is important to note that in terms of business, privacy and security cannot be seen as one, there is an old saying "**You can't have privacy without security, but you can have security without privacy**".

Mobile applications collect personal information (e.g., name, account number, and other personal details) and track user activity through permissions implicit into the applications (e.g., SMS, location, camera, etc.). These data are also valuable to attackers and can compromise user privacy. Data protection principles are designed to protect the personal information of individuals by restricting how such information can be collected, used and disclosed. Financial related information demands an adequate data protection since the sensitive personal information includes financial information such as credit card, debit card and other payment instrument details; thus to that extent regulating their use, collection and disclosure.

Role of Intermediaries under the Indian law:

As per section 2(w) of Information Technology Act, 2000 (amended in 2008), "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

Mobile banking service providers are categorized as Internet intermediaries. Section 79 of Information Technology Act 2000 deals with the liability of the intermediaries. Mobile payment service providers fall in this category. Section 79 A of the act expects that the intermediary should observe due diligence while discharging its duty. The section also provides safe harbor protection to the intermediaries. The safe harbor protection would not apply if:

a. Intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of unlawful act

b. Upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

The intermediary conditions make mobile banking service providers liable for not adhering to the due diligence. The due diligence may be tested in court in case of a breach. The court, through a process of investigation and opinion of the experts, may take a decision with respect to liabilities of mobile banking service providers for lapses.

The Information Technology Rules, 2011 states that the body corporate should provide for clear and accessible statements of its practice and policies, type of personal data collected under Rule 3, purpose of collection and usage of such information and disclosure of information including sensitive personal data as provided in Rule 6. The body corporate shall collect sensitive personal data only when the information is collected for a lawful purpose and must be necessary for its purpose.

According to Rule 5 (3), while collecting information from the person concerned, he should have knowledge of the fact that the information is being collected, the purpose for which the information is being collected, the intended recipient of the information and the name and address of the agency collecting and retaining the information. The information so collected must be used ONLY for the

purpose for which it has been collected. The information provider shall be given opportunity to withdraw his consent at any point of time.

Privacy requirements under IT Act 2000:

Body corporate to provide policy for privacy and disclosure of information – the body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handles information of its customer, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who have provided such information under lawful contract.

Such policy shall be published on website of body corporate or any person on its behalf and shall provide for:

- Clear and easily accessible statements of its practices and policies;
- Type of personal or sensitive personal data or information collected under rule 3;
- Purpose of collection and usage of such information;
- Disclosure of information including sensitive personal data or information as provided in rule 6;
- Reasonable security practices and procedures as provided under rule 8

Definition of personal data

The Privacy Rules define the term 'personal information' as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, can identify such person.

Definition of sensitive personal data

The rules define 'sensitive personal data or information' to include the following information relating to:

- Password
- Financial information, e.g. bank account/credit or debit card or other payment instrument details
- Physical, physiological and mental health condition
- Sexual orientation
- Medical records and history
- Biometric information
- Any detail relating to the above clauses as provided to a corporate entity for providing services
- Any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics means the technologies that measure and analyze human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes. However, any information that is freely available in the public domain is exempt from the above definition.

Under the Information Technology Act, 2000 (amended in 2008), if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls

or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The rules created under this act further state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 'Press Note' issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they provide and also ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information must have the right to opt out (i.e. he/she will be able to withdraw his/her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

Security Requirements:

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. These practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement, 'reasonable security practices and procedures' to be adopted by any corporate entity comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Central Government. Presently, no such best practice codes have been approved by the Central Government.

Enforcement:

To ensure data protection by a service provider who has secured access to any material containing personal information about a person, discloses such information without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain to such a person, section 72A was inserted vide the amendments to the IT Act in 2009.

72A Punishment for disclosure of information in breach of lawful contract: Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Civil Remedies:

Section 43A primarily deals with all such contraventions resulting from the negligence on the part of the body corporate which is also identified as data processor and data controller. This section provides the redressal mechanism to any affected person to seek compensation from a body corporate which has been negligent in implementing and maintaining reasonable security practices and procedures and thus caused wrongful loss or wrongful gain to any such person. The affected person has two options:

a) To approach the Adjudicating officer, if the compensation sought is up to INR 5 crore, and

b) To approach the competent civil court, if the compensation sought is more than rupees INR 5 crore.

The Draft Information Technology (Security of Prepaid Payment Instruments) Rules 2017 framed under the powers conferred by clause (d) of section 10 and section 43A read with subsection (1) of section 87 of the Information Technology Act, 2000 (21 of 2000) also reiterates the need of PPI issuer having a privacy policy that is mentioned under Rule 4.

Rule 4 – Privacy policy: Every e-PPI issuer shall have in place and publish on its website and mobile applications, the privacy policy and the terms and conditions for use of the payment systems operated by it in simple language, capable of being understood by a reasonable person. The privacy policy shall include the following details, namely:–

- The information collected directly from the customer and information collected otherwise
- Uses of the information
- Period of retention of information
- Purposes for which information can be disclosed and the recipients
- Sharing of information with law enforcement agencies
- Security practices and procedures

Data Protection Best Practices

Sensitive payment data and personal data should be protected when stored, or processed on the mobile device.

a) Customer Information and account credentials should be secured against any possible identity theft, unauthorized access or modification. Proper controls for data classification and associated security controls should be put in place.

b) The minimum disclosure principle for collection and disclosure of personal information during business should be applied.

c) Sensitive data should be securely stored on the server instead of client-end device.

d) Sensitive data (including password, keys) should be stored/cache in an encrypted form or in an encrypted container.

e) Historical GPS/tracking or other sensitive information should not be stored on the device beyond the period required by the application. The information should not be stored in publically shared storage such as address book, media gallery, cache, temporary storage and audio files.

f) Deletion of sensitive personal data should be scheduled according to a maximum retention period.

g) Non-persistent identifiers, which are not shared with other applications, should be used, wherever possible - e.g. do not use the device ID number as an identifier.

h) Should ensure that no sensitive data can be accessed or modified by an unauthorized party through the contactless interface (e.g. Near Field Communication) of the mobile device.

i) Mobile Banking Application Providers should ensure that no sensitive payment data can be accessed on lost or stolen mobile devices.

j) Mobile Banking Application Providers should have the capability to disable the mobile payment application in handsets that, for example, have been lost, stolen or misused. Mobile Banking Application Providers should put in place specific end-of-life procedures with reference to components storing sensitive payment data (e.g. secure removal of user credentials stored in a handset chip or SIM card, secure SE destruction, etc.)

k) In order to mitigate cross-contamination risks, Digital payment service providers should ensure that no sensitive payment data related to payments, including authentication data such as a PIN, can be reused to make fraudulent payments in other environments.

l) Digital Payment Service Providers should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. They should also establish a procedure for reporting such incidents to management and, in the event of major payment security incidents, to competent authorities.

m) Digital Payment Service Providers should have a procedure for cooperating with the relevant law enforcement agencies on major payment security incidents, including data breaches.

8 Fintech Future intertwined with Cyber Security

Thinking about the future of Fintech takes us places where financial records may get verified by known/unknown stakeholders instantly; financial organizations may identify end customers with their pulse and travel habits; use various micro biometric indicators with minimal friction; machines and algorithms will take financial decisions on behalf of the customer; IoT devices will provide numerous financial services anytime and anywhere; etc. Contemporary Fintech products are designed in a way that the end customer is able to get contextual financial services. These scenarios also warrant cyber security preparedness well in advance; a world in which Fintech and Cyber Security are interlocked. The decisions which we take today on cyber security is going to pave a secure path for future Fintech revolution. Few global Fintech trends which may emerge in future are as follows with its probable impact on cyber security.

Global Trends	Purpose	Probable Impact on Cyber Security
I. Contact less payment leveraging protocols as NFC and Biometrics payments based on voices, ECG and body implants	• Auto-authentication of customer visiting bank branches and branch employees • Authentication of payment transaction on wallet/mobile app	• Threat surface may expand as new methods as NFC and biometrics may get leveraged for commerce
II. Artificial Intelligence and Payments using virtual assistants	• Financial advisory, Enhanced customer personalization • Automating wealth management services • Customer services and assistance • Account balance checking • Payment transactions	• Automation of financial decisions may get impacted because of non-secure coding practices • Security governance may become complex
III. Blockchain systems replacing current architecture of financial services	• Trade finance & Digital currency • Clearing & settlements and Forex deals • Digital identity of users and machines	• Organizations need to prepare for securing consensus protocol, defend against new attacks such as '51 % attack' and device a new model of security governance aligned to decentralization • New privacy requirements may emerge

Global Trends	Purpose	Probable Impact on Cyber Security
IV. Emergence of crypto currencies	• Anonymous Payments • Building Token Economy	• Tracking anonymous and encrypted payment trails may become arduous • Privacy legislations across globe may warrant a change
V. Plethora of non-conventional IoT devices participating in financial ecosystem as smart meters, automobiles, etc.	• Customer notification, Account information and basic banking tasks • Proactive services: identifying product problems before customers are aware • Provide augmented experience and intelligence	• Requirement of robust hardware security guidelines may emerge • Hardware threat surface may expand • Providing security for end user devices may get complex

Table 5 Fintech Future and Cyber Security

9 Recommendations

The recommendations are classified into two areas (I) Public Policy (II) Enterprise Security Best Practices. The public policy recommendations are strategic and tactical steps which India need to consider for securing the digital payment ecosystem. The enterprise security recommendations are best practices which can be implemented by digital payment organizations. These recommendations are derived based on a comprehensive secondary and primary research and analysis with respect to Indian context and global learnings.

The recommendations are arranged in order of importance mapped with categories such as high, medium and low. Further stakeholders are mapped against each recommendation who can be instrumental for its introduction, implementation and enforcement in India.

The legend to understand recommendations is depicted below.

Importance

Stakeholders as Mapped

9.1 Public Policy

Government has a key role to play in ensuring that the digital payment sector delivers expected growth in a secure and sustainable manner. To help build a strong foundation, its policies and standards will need to be dynamic, flexible and balanced. Technology advancements will enable new payments experiences but in parallel may accentuate the potential for cybercrime in India. Hence, it is critical that a comprehensive cyber security strategy should be developed with attributes like global collaboration, leveraging established best practices, support for awareness and innovation constituting a key part of the policies and regulations proposed in the digital payment sector.

Recommendations	Importance	Stakeholders
1. Develop a long term cyber security strategy in alignment with the vision and objectives for digital payments in India with consideration for the global and dynamic nature of the industry	★★★	
2. Establish standards and comprehensive guidelines for cyber security, fraud and technology risk management for the digital payment industry	★★★	
3. Develop a streamlined process with a single agency responsible for managing key aspects of regulations, enforcement, and education for security in the digital payment industry	★★★	
4. Establish a committee of subject matter experts from the Government and Industry to provide guidance to digital payment sector on cyber security	★★★	
5. Leverage and align with globally accepted cyber security frameworks to ensure India's digital payment industry is benchmarked with the global best	★★★	
6. Enhance data protection, privacy and security laws towards a productive balance between user safety and business growth. Establish strong baseline protection requirements but preserve global cross-border data flows through established principles and multilateral cooperation	★★★	
7. Encourage and establish strong public private partnership for trust, transparency and information sharing around threat intelligence (ISAC), incident reporting, best practices assessment and responsible disclosure (bug bounty)	★★★	
8. Actively defend the Industry against cyber /financial crimes by encouraging joint investigations with enterprises and intelligence agencies, quick action and broader law enforcement cooperation	★★	
9. Update standards and guidelines to reflect the changing landscape due to advancements like IoT, Artificial Intelligence, Machine Learning and Blockchain etc.	★★	
10. Invest in workforce development through partnerships with Academia and Industry, introduction of cyber security curriculum in schools, competitions and awareness events and other means	★★	
11. Build a regulatory sandbox environment approach that enables temporary, limited-scale testing of next gen digital payment products and services	★★	
12. Establish a cyber security innovation program to, nurture digital payment security startups, and applied research grants to constantly grow and strengthen the ecosystem	★★	

Table 6 Recommendations - Public Policies

9.2 Enterprise Security

As the global cyber security landscape continues to evolve, consumers as well as public institutions will be closely looking at steps taken by organizations to strengthen their security programs to minimize breaches and build user trust in digital payment channels. The following table includes some of these high priority recommendations that digital payment enterprises should prioritize for adoption. This study, apart from recommending short term measures also emphasizes the need for long term investment and efforts in improving security for the overall ecosystem.

Recommendations	Importance	Stakeholders
Design & Architecture		
1. Build a security program with strong foundations based on established cyber security frameworks and industry best practices to minimize unknown risks, enable measurement and progress overtime **E.g. PCI-DSS, NIST CSF, ENISA NCSS and ISO 27001-2**		
2. Deploy a strong & secure SDLC program to ensure that digital payment applications follow secure coding and development lifecycle practices **E.g. US-CERT SSF, OWASP S-SDLC, BSIMM and MSFT SDL**		
3. Employ a risk-based layered strategy for protecting data, defending the enterprise infrastructure and ensuring a secure customer experience **E.g. NIST RMF, ISO 27005, ISACA RISK IT and FAIR**		
Hygiene		
4. Build a state of the art cyber defense center or security operation center with SecOps, dynamic threat intelligence, data leakage prevention and incident response program etc.		
5. Establish a structured governance and risk management program with clear lines of defense, regular risk assessment and reporting to the board/ senior management		
6. Implement a comprehensive training and awareness program for information security and data protection, supporting skills upgrading for security team to help stay up-to-date with changing threat landscape and defense techniques. Channels of engagements can be such as quizzes, games and rewards/recognition which can help test effectiveness of the program		

Recommendations	Importance	Stakeholders
Monitoring and Testing		
7. Build a Vulnerability Assessment/Penetration Test program to monitor public facing web apps and other infrastructure. Also, include mobile apps, cloud/SaaS and partner endpoints based on risk management strategy		
8. Deploy Anti-virus/Anti-malware solution for end point security across the enterprise to detect and prevent compromise of user workstations, mobile devices and other system components		
9. Establish a cybercrime and threat investigation program to discover phishing websites, fake apps and social engineering attacks. Build detailed procedures for investigation and response in coordination with ISPs, law enforcement and other industry partners		
10. Implement prevalent industry encryption standards as per use cases for protecting data at rest or in transit		
Ecosystem		
11. Encourage active participation and partnerships with Industry and Government in research, standard building, threat intelligence sharing and development of frameworks etc., to help secure the overall ecosystem for enhanced consumer trust		

Table 7 Recommendations - Best Practices

References

[1] WEF, "http://reports.weforum.org/global-risks-2018/executive-summary/," WEF, 2018.

[2] Whitehouse, "https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/," Whitehouse, 2016.

[3] D. Reading, "https://www.darkreading.com/attacks-breaches/19-billion-data-records-exposed-in-first-half-of-2017/d/d-id/1329929?," Dark Reading, 2017.

[4] Credit Suisse, "Digital Payment Statistics," https://inc42.com/buzz/digital-payments-credit-suisse-report/, 2018.

[5] RBI, "Digital Payment Statistics," https://www.rbi.org.in/scripts/BS_ViewBulletin.aspx, 2017.

[6] RBI, "Payment Sector Growth," https://www.rbi.org.in/scripts/BS_ViewBulletin.aspx, 2017.

[7] NPCI, "Digital Payment Statistics," https://www.npci.org.in/statistics, 2017.

[8] RBI, "Digital Payment Statistics," https://rbi.org.in/Scripts/NEFTView.aspx, 2017.

[9] NPCI, "Digital Payment Statistics," https://www.npci.org.in/statistics, 2017.

[10] BCG, "Digital Payment 2020," http://image-src.bcg.com/BCG_COM/BCG-Google%20Digital%20Payments%202020-July%202016_tcm21-39245.pdf, 2016.

[11] "http://meity.gov.in/bharat-qr-code," [Online].

[12] EMVCo, "EMVCo_Merchant_Presented_QR_Specification_v1_0.pdf".

[13] cyberint. [Online]. Available: https://cdn2.hubspot.net/hubfs/2034462/Reports/CyberInt%20Report%20-%20QR%20Code%20Threat%20Landscape.pdf?utm_referrer=https%3A%2F%2Fblog.cyberint.com%2Fnew-research-qr-codes-threat-landscape.

[14] " http://www.chinadaily.com.cn/opinion/2017-03/02/content_28400890.htm," [Online].

[15] [Online]. Available: http://www.todayonline.com/tech/qr-code-scams-rise-china-putting-e-payment-security-spotlight.

[16] "http://nearfieldcommunication.org/about-nfc.html," [Online].

[17] "https://www.itnews.com.au/news/nsw-police-charge-three-men-with-15m-tap-and-go-fraud-460322," [Online].

[18] "https://www.npci.org.in/product-overview/upi-product-overview," [Online].

[19] "economictimes.indiatimes.com/articleshow/57921505.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst," [Online].

[20] "ENISA Security of Mobile Payments and Digital Wallets 2016".

[21] Gemalto, "Gemalto," [Online]. Available: https://www.gemalto.com/review/Pages/KFC-use-facial-recognition-for-payment-in-China.aspx.

[22] RBI, "RBI Speeches : https://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=1028," RBI, Mumbai, 2017.

[23] KPMG, "Digital Payment - Analysing the Cyber Landscape," https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf, 2017.

[24] RBI, "Payment and Settlement Systems in India: Vision-2018," https://www.rbi.org.in/scripts/PublicationVisionDocuments.aspx?Id=842, 2018.

[25] ENISA, "Security of Mobile Payments & Digital Wallets," https://www.enisa.europa.eu/publications/mobile-payments-security/at_download/fullReport, 2016.

[26] G. o. I. Meity, "http://meity.gov.in/writereaddata/files/Cyber_Surakshit_Bharat_Programme.pdf," [Online].

[27] RBI, "Master Direction on Issuance and Operation of Prepaid Payment Instruments," https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142, 2017.

[28] MeitY, "Draft MeitY Security Rules for Prepaid Payment Instruments," http://meity.gov.in/writereaddata/files/draft-rules-security%20of%20PPI-for%20public%20comments.pdf, 2017.

[29] Ministry of Finance, "Watal Report on Digital Payments," http://mof.gov.in/reports/watal_report271216.pdf, 2016.

[30] MeitY, "Data Privacy Law of India," http://pib.nic.in/newsite/PrintRelease.aspx?relid=169420, 2017.

[31] Economic Times, "Protocol for e-Wallet Companies," http://cio.economictimes.indiatimes.com/news/digital-security/government-plans-norms-for-e-wallet-firms-to-prevent-online-frauds/60774069, 2017.

[32] Indian Express, "Global Challenge for Cyber Security Workforce," http://www.newindianexpress.com/nation/2017/oct/07/government-to-hold-global-challenge-to-build-cyber-taskforce-for-india-1668336.html , 2017.

[33] I. Ministry of Finance, "FInancial Cert," http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf, 2017.

[34] Singapore Govt., "National Cyber Security Bill," https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en, 2017.

[35] MAS, "Technology Risk Management Guidelines," http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf, 2013.

[36] Singapore Govt., "Data Protection Law," https://www.pdpc.gov.sg/legislation-and-guidelines/overview, 2012.

[37] HKMA, "Regulations for SVF," http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf.shtml, 2016.

[38] KPMG, "Overview of China Cyber Security Laws," https://home.kpmg.com/cn/en/home/insights/2017/02/overview-of-chinas-cybersecurity-law.html, 2017.

[39] Davis Wright Tremaine LLP Shanghai Office, "Reality and Trend of China's Regulation on Payment Service by Non-Financial Institutions," http://documents.jdsupra.com/36992cc8-c91f-4bf7-97b7-ced97df80d7f.pdf, 2016.

[40] APCA, "Third Party Digital Wallet Security," http://www.apca.com.au/docs/default-source/guidelines/third_party_digital_wallet_security_industry_guidelines.pdf, 2016.

[41] Federal Reserve Bank of Atlanta, "Update on the U.S. Regulatory Landscape for Mobile Payments," https://www.bostonfed.org/-/media/Documents/PaymentStrategies/summary-of-mpiw-meeting-may-2014.pdf, 2014.

[42] ENISA, "Security of Mobile Payments and Digital Wallets," https://www.enisa.europa.eu/publications/mobile-payments-security/at_download/fullReport, 2016.

[43] EU Parliament, "GDPR," http://www.eugdpr.org/, 2016.

[44] Microsoft. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-8d258746bopq.aspx.

[45] NIST. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final#pubs-abstract-header.

[46] OWASP. [Online]. Available: https://www.owasp.org/index.php/CLASP_Concepts.

[47] Microsoft. [Online]. Available: https://msdn.microsoft.com/en-us/library/ms995349.aspx#sdl2_topic2_3.

[48] CMU. [Online]. Available: https://www.sei.cmu.edu/reports/03hb002.pdf.

[49] SANS. [Online]. Available: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf.

[50] NPCI. [Online]. Available: https://www.npci.org.in/sites/default/files/White-Paper-on-Cyber-Security-in-banking-Essential-tools-rev10.pdf.

[51] G. S. Online, "QR Code Security," IDA Singapore.

[52] " https://www.lifewire.com/how-to-protect-yourself-from-malicious-qr-codes-2487772," [Online].

[53] "https://blog.aujas.com/2011/05/31/mitigating-security-risks-in-ussd-based-mobile-payment-applications/," [Online].

[54] CERT-INDIA, "CERT-IN advisory notes for Cbyer security for digital payemnts.pdf".

Glossary

Term	Description
PPI	Prepaid Payment Instrument
RBI	Reserve Bank of India
NPCI	National Payment Corporation of India
INR	Indian Rupee
QR	Quick Response
UPI	Unified Payment Interface
BHIM	Bharat Interface for Money
USD	United State Dollars
PSP	Payment Service Providers
Cert-In	Computer Emergency Response Team- India
MIS	Management Information Systems
SoC	Security Operation Centers
PoS	Point of Sale
BCG	Boston Consulting Group
NFC	Near Field Communication
CII	Critical Information Infrastructure
EU	European Union
SGD	Singapore Dollars
CPF	Cyber Peace Foundation
MeitY	Ministry of Electronics & Information Technology
USSD	Unstructured Supplementary Service Data
UK	United Kingdom
PDPC	Personal Data Protection Commission
HKMA	Hongkong Monetary Authority
SVF	Stored Value Facilities
APCA	Australian Payment Clearing Association
SARs	Suspicious Activity Reports
MPIW	Mobile Payment Industry Workgroup
OCC	Office Comptroller Currency
ENISA	European Union for Network and Information Security
GDPR	General Data Protection Regulation
MoF	Ministry of Finance

Research Team

PayPal Team

Phoram Mehta
Head of Information Security-APAC, **PayPal**
Email: phmehta@paypal.com

Nath Parameshwaran
Director, Corporate Affairs, **PayPal**
Email: nparameshwaran@paypal.com

Mangesh Samant
Information Security Officer-India, **PayPal**
Email: masamant@paypal.com

DSCI Team

Venkatesh Murthy K
Deputy Director, **DSCI**
Email: venkatesh.murthy@dsci.in

Mayank Lau
Senior Consultant, **DSCI**
Email: mayank.lau@dsci.in

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: **www.dsci.in**

About PayPal

Fueled by a fundamental belief that having access to financial services creates opportunity, PayPal Holdings, Inc. (NASDAQ: PYPL) is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. Our open digital payments platform gives PayPal's 227 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, on a mobile device, in an app, or in person. Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying or getting paid. Available in more than 200 markets around the world, the PayPal platform, including Braintree, Venmo and Xoom, enables consumers and merchants to receive money in more than 100 currencies, withdraw funds in 56 currencies and hold balances in their PayPal accounts in 25 currencies.

For more information on PayPal, visit: **https://www.paypal.com/about**

For PayPal Holdings, Inc. financial information, visit: **https://investor.paypal-corp.com**

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 3rd Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries contact

P: +91-120-4990253 | E: info@dsci.in | W: www.dsci.in