CHALLENGES IN DATA SECURITY: DIGITAL PAYMENT LANDSCAPE IN INDIA

[1]Anupama Munshi [2]Dr. Vinay Kumar
[1]Assistant Professor [2]Dean Department of Computer Sciences and Applications
[1]Computer Sciences and Applications,
Jagannath International Management School,
New Delhi India.

Abstract: The Technological innovations and disruptions in the field of electronic exchange of financial transactions are shifting the gears of our lives meaningfully and providing the end consumers with speed, convenience, choice and savings. Certainly, the digital revolution which has been widespread in the world has reached India as well, and it's mounting vigorously day-by-day. Technical advancements are empowering digital payment solutions providers to offer tailored experiences that are smooth and customer centric. However, the same innovations are also being leveraged by nasty players in the cyberspace to attack establishments as well as customers to enact fraud. Since India is still at an initial implementation juncture of its digitization journey, it is absolutely essential that the right atmosphere for digital payments include an inclusive cyber security policy supported by a robust framework to help all stakeholders involved in the network. Annexation of two cyber related risks, (cyberattacks and data theft) in the 'Top 5 global risks' is a wakeup call for the world and India in particular. Malicious cyber commotion pose fears at an individual, enterprise and national level. As India rapidly switches to a digital payment ecosystem, dangers are also moving from cash to cyber and the emerging environment is already facing refined cyberattacks. This therefore demands appropriate stakeholders to be prepared and team up to provide protected and dependable payment instruments to the end consumers. In order to determine the right balance between enablement and security, it is crucial that a collaborative effort be embarked on to establish an inclusive cyber security framework for digital payments in India. This paper sketches key apparatuses and references to help fast-track such an initiative. Incipient tools and technologies like cryptocurrencies, IoT, computerization, machine learning, and analytics are redefining the future and digitization of finances is not resistant to these developments. This paper therefore serves as an equipped snapshot of the Digital Payment Ecosystem, Threats and associated Cyber Risks, Strategy, Regulatory Framework and some best practices. This research is an effort to figure out a set of approvals towards safeguarding the evolving digitized payment apparatuses network in India.This study identifies various success factors to build a robust and resilient digital payment environment in India.

***IndexTerms* - Digitization, Information Technology, Cybersecurity, Data theft, Privacy, Digital payments,**

INTRODUCTION

The mission of transforming the traditional economy of our country into a digital economy intended by the Government of India has a special focus on digital payments. The speed of transition to digital payments has considerably increased with the robust move towards cashless economy. The shift to digitization of finances is envisioned with components like expansion of banking facilities to underbanked, banking from anywhere, increasing the fundamentals of financial inclusion, establishment of digital space etc. Digital payments are becoming an essential part of our daily lives and are impacting society, business and the economy at large. India's digital payment industry, which is currently worth around USD 200 Billion, is predictable to grow five-fold to reach USD 1 Trillion by 2023, as per a report by Swiss financial services holding company, Credit Suisse. Pioneering use of technology has empowered the digital payment infrastructure and has boosted the creation of innovative products such as mobile wallets, and many other prepaid payment instruments. The key technological competencies that triggered this revolution are Smart devices, Apps, Near Field Communication Protocol, QR Code and Mobile Wallets and many more. The private sector in India has taken a huge jump to enhance digital payments implementation. Also adding to it, National Payment Corporation of India (NPCI) developed and presented Unified Payment Interface (UPI) which provides 24x7x365 mobile payment platform for users to send and receive payments with a simple virtual payment address. This was further amplified with the introduction of Bharat Interface for Money (BHIM) which has elevated bulk cashless payments through mobile phones. Therefore, the Indian Government's plunge on digital payments is creating space and also making it reasonably priced and interoperable, which is in turn helping end-consumers, businesses and digital payment sector at large. This strategic shift from the traditional system of cash economy to cashless one in a vast and diverse country like India wouldn't have been possible without numerous dynamics that impact the progress and propagation of digitalisation, including:

- A ground swelling mobile phone penetration.
- Minor cost of facility delivery.
- Banks encouraging online banking services to customers.
- Huge Unorganised sector in India coming in support of the digital economy.

Hence it is noticeable that in recent few years, a plethora of establishments have started evolving to provide next generation product and services in the electronic payment space. Both banking and non-banking sectors are seizing the opportunity of consumer needs at whirlwind speed and revamping the value chain. This is mainly possible due to the availability of Internet and affordability of mobile technologies globally. High end phones today are equipped with capabilities such as advanced processors, high storage memories, NFC, high resolution cameras, etc. They no longer function only as devices to communicate but are acting as commerce enablers. Modernizations in technology such as tokenization of card, NFC readers at merchant stores, biometric enabled transactions and interoperability of wallets are paving ways for the complete digitization of financial world. The escalation of non-orthodox actors such as Apple, Google, Samsung, Starbucks and Vodafone etc., undoubtedly echoes that this space is no longer a domination of the traditional financial institutions. In India initiatives such as Jan Dhan Yojana, Aadhaar and the arrival of UPI certainly mark the commencement of building a healthy digital payment ecosystem in India. According to a report by PwC, India is likely to offer the peak expected return on investment on digital finance projects at 29% versus a global average of 20%. The crucial part of Indian Digital financial revolution lies in foreseeing a conducive atmosphere for all participants which can encourage modernization and quicker acceptance of digitization of financial technologies.

DIGITAL PAYMENT ECOSYSTEM IN INDIA

The Digital payment system consists of payment transactions supported by the application of a wide variety of digital devices or in a digital mode such as credit/debit cards, mobile or internet based set ups, to send and receive money. This ecosystem comprises of buyer (consumer), supplier (merchant, service provider) and a Payment Service Provider (PSP) that allows handover of money from buyer to seller for the product/ service availed. The PSPs in India consist of both bank and non-bank players. These PSPs offer a diversity of digital payment modes – from the already existing ones such as National Electronic Funds Transfer (NEFT), National Electronic Clearing Services (NECS)/ Automated Clearing House (ACH), bank cards (credit, debit, pre-paid), internet banking, mobile banking to the upgraded ones such as wallets (PPIs), Aadhaar Enabled Payment System (AEPS), Immediate Payment Service (IMPS), UPI, Bharat Bill Payment System (BBPS), and now Aadhar Pay and India QR code. Some of the different technologies used in the digital payment channels are as:

Quick Response Code (QR code)

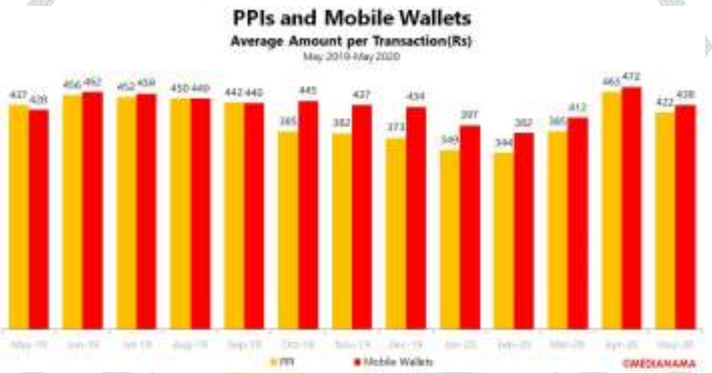
It is a 2D matrix barcode that stores encoded information such as hyperlinks to website pages, app downloads, etc. To decode, users simply need to scan the QR code image using any device with built-in camera (e.g. smart phone) and QR code reader application installed. Bharat QR code introduced by Govt. of India collaborated with Master card, 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.

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.

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.

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:



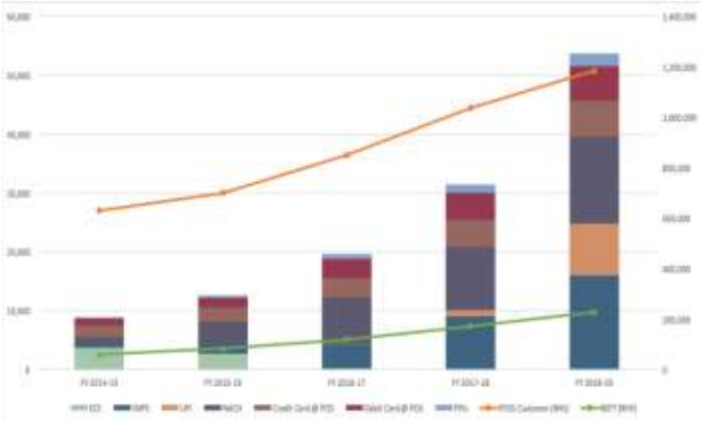
Mobile Wallet transactions

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.

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. Biometric authentication is increasing adopted by the companies using advanced technology for identity verification to improve their service to customers.

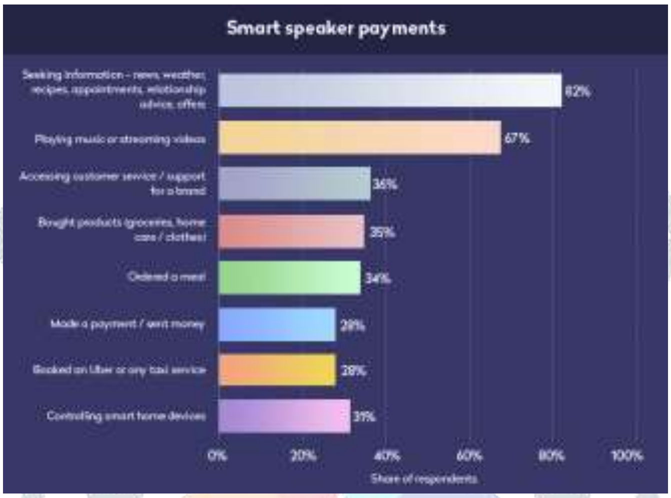
Behavioural biometrics: Unlike physiological biometrics, behavioural biometrics relate to your personal habits and unique movements. Whereas standard biometrics rely on a part of your body, behavioural biometrics use the unique way in which you do something to authenticate you. The main examples of this 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.



Status of Biometrics usage

Smart speaker payments

Home assistants or smart speakers allows its users to give voice commands to a speaker and receive a voice response in return. The user can give voice commands for various things such as getting weather updates, traffic update, ordering from Zomato or booking a cab from Uber.
Many giants have invested in the manufacturing of smart speakers. Amazon was the first one to come up with its first smart speaker in the year 2014. Google Home and Apple joined Amazon in the year 2016 and 2017 respectively. The speakers which evolved from the smart assistants were primitive in nature as they were restricted to just phone devices. However, with the growth of home automation, the smart speakers also started to go mainstream. Let's have a look at some stats to understand the smart speaker situation better. According to Statista, 35% of users use smart speakers for buying products like home care, groceries, and clothing. Interestingly around 28% of the people used smart speakers for sending money or making direct payments. This is not a huge portion as fewer amounts of people choose to make payments over smart speakers due to the security reasons. This concern over security is widespread as a press release from TNS found that around 74% of the users have security concerns for making payments over voice assistants. Moreover, they also said that they might stop making payments due to this concern.
Even after this, the future of smart speaker looks promising as big names like Amazon, Google, and Apple are investing to build their advanced smart speakers. Moreover, the stats also indicate a bright future for the smart speaker payments. BI has estimated that the usage of smart speaker will grow rapidly from 18.4 million users in 2017 to a whopping 77.9 million users by 2022.



DIGITAL EVOLUTION AND THREAT LANDSCAPE: GLOBAL AND INDIA
The past few years have therefore witnessed an extraordinary alteration with respect to the occurrence of digitization of financial services. Earlier Digital finance affected only customer payment landscapes i.e., allowing quicker payments, eliminating disturbances from processes for customers, permitting hassle free commerce, securing it and now it is expected that it may refurbish commercial operations end-to-end**.** The canvas of digital Finance is becoming ever encompassing. Its evolving use cases are crowdfunding, point-to-point money transfers, data analysis, wealth management, cyber security and underwriting etc. These technologies are user friendly and designed to reduce costs of operations**.** At a global level Fintech innovators and financial service companies are building concerted business and co-creation models. The intent of these models is data disposal from financial organizations to shape financial technologies, i.e. entree to data for digitization of finances which can be a boon to innovate next generation technologies or to leverage it for big data analytics. In India the rise of digital finance revolution is characterized by developments such as financial enclosure of vast population, demand of digital finances, smartphone adoption, government and regulator push, and collaborations by financial institutions. This earth-shattering growth, both globally and in India, merits stakeholder's concerted efforts to foresee robust cyber security and data protection policies. India needs to gear up to accommodate these trends from a regulatory, technology, compliance and security perspective. Such efforts would go a long way in enhancing the end consumer trust in digital payment space and could potentially result in multi fold increase in the digital payment market in India. The challenges in India are similar to any other large developing nation. As with other technology-related risks, governments need to identify, measure, mitigate, and observe the risks and be familiar with technologies that enable digital payment channels. The progress of digital payment set-up is wide-open to ever increasing and complex cyberattacks. The antagonists are constantly trying to identify susceptibilities and cracks 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 imperious for organizations to track and monitor cyber threats on continuous basis and also educate users on it and therefore it is essential to scrutinize 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**.**

Existing Cyber Threats

Malware or Ransomware Most of the naïve users are unaware of malware infection in their devices and when carrying out transactions, the malware is able to abstract user identifications and share it with the adversaries. Leveraging their credentials, adversaries are able to conduct deceitful transactions and draw off user finances. For example, a new malware Xafecopy Trojan was detected 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 regularly used techniques to carry out cyberattacks on the end users in the digital payment space. In phishing, a deceptive link is sent to the user which appears genuine and they are readdressed 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 routing for opportunities either via telephonic conversations or well-crafted emails to fraud innocent users.
The adversaries may also build fraudulent wallet applications and post it on the popular market places. There have been instances where in the users transacted via illegal wallet applications instead of legitimate ones.

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.

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.

Probable Future Threats

With the advent of new technologies involving machine learning and AI, challengers are developing malwares which can infect user devices covertly in an automated way, with no human intervention.

Cyber Warfare/Espionage; Countries 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. Securing India's Digital Payment Frontiers |

Mobile payments went viral. So did the threats to their security

The ubiquity of mobile devices is one of the key factors promoting digital payments. But the vast range of payment methods including e-wallets, payment apps (including P2P payment platforms), and NFC-based payments has only increased the number of threats. The most widespread are mobile malware, phishing attacks, data leakage at POS terminals, duplicating SIM cards, and physical theft.

An average cost of a phishing attack is $1.6 million for a mid-sized company.

Card-related fraud is not going to subside

According to The Neilson Report, global card fraud losses will exceed $35 billion in 2020. And it doesn't even matter if you carry your card around or keep it locked up in a safe. Card-not-present (CNP) fraud is conducted without the physical presence of a card as a result of malware or phishing attacks. Card-present fraud takes place at POS terminals and ATMs, where criminals intercept data when people make payments using contactless technology or even the comparatively obsolete magstripe. On top of that, there are cases of targeted attacks on specific institutions or stores (like Home Depot). In this case, the attacker's aim is to break into the payment system to gain payment card data and identity information

BEST PRACTICES FOR SECURING THE DIGITAL PAYMENT ECOSYSTEM

The assaults on the digital financial sector are gradually becoming more unconventional and sophisticated with the aim to steal the enterprise/customer information resulting in data theft and breach of privacy. These threats for digital financial transactions can arise from both the merchant side as well as the buyer side. During the period of 2018-19 alone, India recorded 1,477 instances of digital fraud. Therefore, it is imperative for all stakeholders to work in unanimity in order to negate these threats and ensure that digital payments work in a seamless manner. There are numerous gaps through which the digital payment systems could be compromised. The risks related to financial digitization may vary from (DDos attacks), compromising Integrity and confidentiality of data and information (fudging of accounts, account spoofing, etc.). Resilience of digital payment system has now become a critical concern to inculcate faith and trust in consumers. The enterprises dealing with digital payments are putting in substantial efforts in improvising their security apparatus therefore trying to minimize the attacks on their systems. Accomplishing the targets related to securing the digital payment systems at various levels also depends on various institutions/stakeholders to join forces and work towards improving the security of the ecosystem. This would also aid in eliminating obstacles to embracing the digitization through refining the perception of security. Given the prominence of digital payment systems, establishments ought to 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 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-modelling 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 that can be used to ensure minimization of cyber threats with regards to usage of mobiles and various other means of digital devices are as follows:

- Usage of self-defense techniques such as runtime application self-protection (RASP)
- Including dynamic integrity check
- Strong encryption of sensitive data on digital devices
- Implement device owner/user verification
- Use two-factor authentication when the risk is high
- Perform application penetration testing
- Test for authentication and authorization modes
- The card related security measures that can be applied are as; Use the 3D security authentication protocol based on the 3D model — acquirer, issuer, and interoperability domain — to secure digital transactions
- Tokenize users' sensitive data, substituting real cardholder data with randomized non-sensitive equivalents
- Deploy real-time anti-fraud solutions that make use of machine learning, automated workflows, customizable scenarios and rules, and guaranteed chargebacks
- Set blocking to limit the use of payment cards to specific channels or situations
- Provide geo-blocking
- Ensure strong customer authentication
- Perform annual risk assessments
- Following best security standards, policies and rules

Some of the essential apparatus for securing digital payments scenario in India can also be in the form of using innovative technologies such as;

Biometric authentication

Biometric authentication is an emerging trend currently, as Biometric authentication is a verification method which encompasses biological and structural characteristics of a person. These method includes fingerprinting scanners, facial recognition, iris recognition, heartbeat analysis, and vein mapping. With the escalation in the problems of identity theft and fraud, biometric authentication can become a reliable and secure option for all the digital payments. The statistics suggest the same. According to the industry data, by this year there will be more than 18 billion biometric transactions taking place every year. Biometric authentication is an exceptional and vital payment method as it integrates and provides precision, productivity, and security under a single package. Biometric authentication is a highly-secured strategy to adopt since it embroils an individual's unique features which obviously can't be fudged.

From cards to codes

Early on, the bank accounts were simply recognized by random combinations of unique digits present on card. However, the EMV technology (Europay, MasterCard, Visa) has gradually picked up and introduced customers with more computerized and secured mechanism for payment. The EMV technology is known for using codes that varies every time a transaction takes place. This use of temporary codes enhances the security in the bank accounts by leaps and bounds. Moreover, the future of plastic cards is bound to be overshadowed by cutting-edge payment services that offer more convenient and seamless methods of money transfer and store

Contactless payments

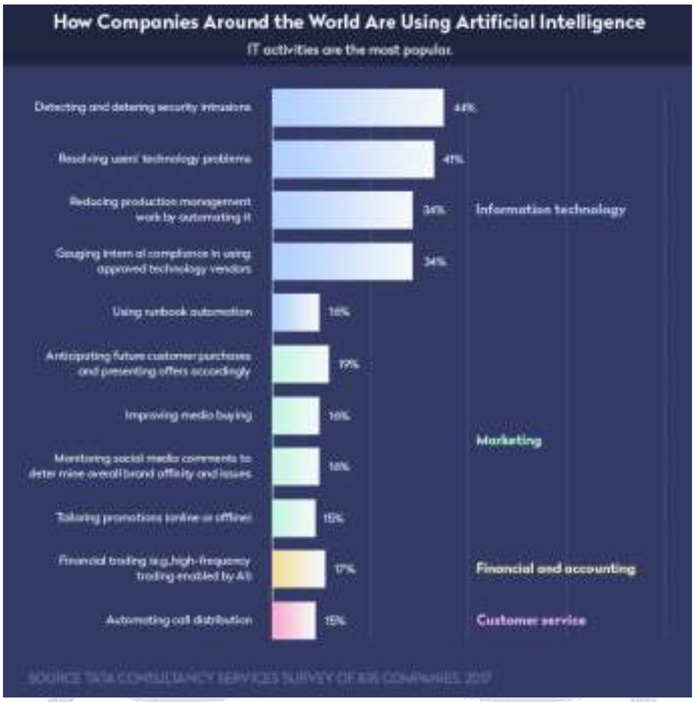
Contactless payments are yet another payment method which is innovative as well as secure way of conducting digital payments. As the name suggests, the contactless payment permits the consumer to simply wave their smartphone across the reader. This method of waving is quick as well as more convenient than inserting a card. Contactless payments are also swifter and more secure than the PIN technology as it transfers the encrypted data to the point-of-sale device instantaneously. Many companies like Samsung, Apple, and Google are already have their contactless payment system Samsung Pay, Apple Pay, and Google Pay respectively. To make payments, all a customer has to do is simply download the app, add card by entering card details, and then wave their phone across any reader. Contactless payments are possible with the NFC (near-field communication) technology. That's the reason why they are also termed as NFC payments. NFC payments are used in many countries. For example, in China it's used as a mode of payment in public transport. Similarly, in London the NFC payments is used in the bus and tube stations. In Japan this technology is used to provide information about the identity cards. UK finance represent a cluster of financial institutions and banks and it has predicted that around 36% of total payments will be made through NFC powered contactless cards by the year 2027.

Top-rated security powered by AI and Machine Learning

Security is the most crucial element whenever it comes to payment. People will always prefer using a payment method that has a high security. That's the reason why payment technologies won't be able to go forward without developing a top-grade security.

Banks receive a lot of customer details and payment data each day. And to detect all the possible threats within seconds, banks are now taking the help of machine learning. Machine learning is the first step you need to complete to achieve artificial intelligence. Banks continuously feed their software with different and new transactions. The software takes a set of limited transactions and learns to detect fraud transactions in real-time. As the software receives more and more transactions, it keeps getting better at identifying the fraud transactions.

The best example of this is when you receive a text from your bank asking if the transaction was done by you or fraudulent. This cautionary message helps the user and bank to prevent a major mishap. No human sends you these texts. A machine learning software is the one which sends all these texts to you.



SOURCE TATA CONSULTANCY SERVICES SURVEY OF 835 COMPANIES, 2017

Usage of AI in security of Digital Payments

CONCLUSION

In past few years, the digital payments landscape in India has come out of its shell. An amplified number of consumers in the country are now choosing to make digital payments for their consumption. This growth is being determined by divisions such as mobile wallets and buy now pay later (BNPL). According to KPMG, a leading consultancy, digital payments in the country are growing at a CAGR of 12.7%. This is a highly noteworthy figure which specifies the rapid growth of the industry. In this study we could gather certain concrete facts regarding digitization and security concerns in digital finances. Since finances, and the way we make payments have undergone several changes since time immemorial, these act as the key pointers of our progress as a species. The primitive methods indicated our primitive way of living. Similarly, the current payment methods powered by cutting-edge technology boast our technological achievements of today. Digitization of payments was a huge jump towards the goal to achieve an easy, convenient, fast, and secure payment method. Digital payment methods saw massive developments in the span of four to five years and we are about to see even more changes in the coming future. On the other hand, there are no limitations to security threats. That’s why establishments, governments, and tech giants all over the world must make collaborative efforts to set policies and standards for the payment industry. While international businesses seek a uniform and secure exchange of payment data, PSPs need global security benchmarks to take cues from. Security protocols and fraud prevention methods may differ from region to region, however the most reputable need to be discussed and implemented. Payment service providers along with other stakeholders have finally understood the emerging threats and their impending impacts. PSPs need to invest in suitable security and monitoring technologies, follow payment industry standards, and watch for updates. On top of that, promoting awareness of digital payment security is always a good idea. The price that one pays for a single mistake in digital payment security is very high, which in turn reflects that only experts and industry professionals can be entrusted with developing financial solutions regarding cyber frauds in digital transactions.

Over the last few years, the technology landscape with respect to digitization of finances has been experiencing hurried changes. The dawn of technologies like block chain, machine learning, bots, cloud, crypto currencies, etc., are exploring development of new financial technologies. The business distribution and architectural models are being updated continuously due to these technological movements. Block chain may completely refurbish how financial services firms function. Technology involving cloud delivery models bring benefits like scalability, flexibility, agility and cost savings. It is also expected that cloud technologies coupled with analytics, mobile technologies and big data, may allow financial institutions to extract real value from the data. Another technological progress which is making headlines in the digital payment sector is usage of Bots. Currently, its main use is in the area of consumer services because it delivers instant communication, augments costs, can be positioned across different delivery models, restructures processes and lessens call load of business process management canters, etc. Together, these technological innovations are going to overhaul digital payment architectures and types of financial products which may get introduced in the market. The study also suggested that there is an increasing Demand for Mobile Point of Sale which can act as a groundbreaking technology as it liberates the merchants from their bricks-and-mortar locations and in-store payments. The mPOS technology also makes a mammoth alteration in the payment process of a store by making it more restructured and flexible by switching the central checkout areas with sales staff equipped with mPOS devices. mPOS is surely going to be trending digital payment technology and stats suggests the same. According to Business Insider, there will be around 27.7 million mPOS devices operational by the year 2021. This number is huge as compared to 3.2 million in the year 2014. With regards to the cyber threat landscape in India our study shows that innovative technologies like AI and Machine learning are taking a center stage in optimizing the security solutions in digital payments. In addition to these advance technologies like contact less payments and biometric authentication will also play a major role in ensuring that the digital payment landscape in India is secure although a lot needs to be done in order in terms of creating awareness, gaining trust and improvising the IT infrastructure in India so that there is a total tectonic shift from offline to online payments. Digital payments are future. In coming years, we will see payment methods transitioning from physical cash to the digital payment methods. Before the transition concludes, many new trends will appear and disappear. These trends will play a vital role in shaping our future payment methods. Many of the mentioned trends will also play a major role in that process.

ACKNOWLEDGEMENT

I am are deeply indebted to my guide Dr. Vinay Kumar, my organization JIMS Kalkaji, my colleagues and all the people involved in this survey for supporting us throughout in this study. Thanks a lot everyone for their kind support.

REFERNCES

1. D.Reading, “https://www.darkreading.com/attacks-breaches/19-billion-data-records-exposed-infirst-half-of-2017/d/d-id/1329929?” Dark Reading, 2017.
2. Credit Suisse, “Digital Payment Statistics,” https://inc42.com/buzz/digital-payments-creditsuisse-report/,2018.cyberint
3. 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-andscape.
4. “http://www.chinadaily.com.cn/opinion/2017-03/02/content_28400890.htm,”
5. http://www.todayonline.com/tech/qr-code-scams-rise-china-putting-epayment-security-spotlight.
6. https://www.npci.org.in/product-overview/upi-product-overview,” economictimes.indiatimes.com/articleshow/57921505.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst,”
7. ENISA Security of Mobile Payments and Digital Wallets 2016”.
8. Gemalto, “Gemalto,” [Online]. Available: https://www.gemalto.com/review/Pages/KFC-use-facialrecognition-for-payment-in-China.aspx.
9. RBI, “RBI Speeches: https://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=1028,” RBI, Mumbai,2017.
10. KPMG, “Digital Payment - Analysing the Cyber Landscape,”
11. https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf, 2017.