ज्ञान-विज्ञान विमुक्तये

Peer Reviewed Referred and
UGC Listed Journal
(Journal No. 47100)

AN INTERNATIONAL MULTIDISCIPLINARY HALF YEARLY RESEARCH JOURNAL

ISSN 2279-0489

Volume-VI, Issue-II
February - July - 2018

PART - III

GENIUS

IMPACT FACTOR / INDEXING
2016 - 4.248 www.sjifactor.com

Ajanta Prakashan

CONTENTS OF PART - III

10. Challenges of Digital Payment System in India

Dr. R. B. Lahane
Assistant Professor, MSP Mandals, Deogiri College, Commerce Department, Aurangabad.
Mrs. Anuradha Phadnis
Research Student, Dr. BabasahebAmbedkarMarathwada University, Aurangabad.

Abstract

"*Digital payment* is a way of payment which is made through digital modes. In digital payments, payer and payee both use digital modes to send and receive money. It is also called electronic payment. No hard cash is involved in the digital payments. All the transactions in digital payments are completed online. It is an instant and convenient way to make payments."

Though, Digital financial services have benefits but pose privacy risks that harm consumers, merchants, markets, and nations alike. Some payments systems in India suffer from vulnerabilities because they were not prospectively designed on the basis of the 'privacy by design' principle. At the back-end, the centralized storage of data is risky. At the front-end, faulty capture devices enable data misuse. Across the middle mile, data is transmitted without strong encryption. Payment systems must be redesigned to prospectively protect privacy and use unbreakable encryption and open standards. Data privacy legislation and a strong market regulator are also necessary.

Through this paper an attempt is made to focus on challenges, like security concerns, equipment's, internet, and so, arise in different types of digital payment, be at grocer, in mall, at vendors, petrol pumps, shops, etc. Information is collected by secondary source by refereeing published data on websites, newspaper articles, some cases and surveys are mentioned, where customers had faced security issues and net connectivity problems in digital payment.

Keywords: Digital Payment, Digital financial services,

Introduction

Cash may no longer be king. While you wait for the serpentine queues at ATMs to peter out and currency notes of Rs. 100 denomination to become easily accessible again, the adoption of digital payment solutions is picking up at a furious pace. Everyone from the neighborhood vegetable vendor to the chai and bhelpuri-wala is embracing digital payment solutions to tide

over the cash crunch. Debit cards, e-wallets and other digital platforms are witnessing a surge in volumes. But are we fully equipped to make the switch to a less-cash society?

ET Wealth conducted an online survey to find out the level of adoption of digital payment solutions and user habits. The findings reveal that while people are getting comfortable with cashless payments, some mindset issues are holding back many from embracing the newer platforms. The findings also suggest that the usage habits of those who have taken to cashless modes could be exposing them to security threats.

Ease of Digital Transactions wins People

The online survey was conducted from 26 to 28 December. Some 663 respondents participated in it. Figures denote % of respondents.Most people are switching to digital payments for its sheer convenience.

Convenience over liquidity crunch: The government is going all out to encourage the adoption of digital payment platforms. It initially waived off the service tax on card transactions up to Rs 2,000 and announced discounts on purchase of petrol, diesel and railway tickets, among others, if paid for digitally. It is also pushing for a sharp cut in the transaction charges, levied by banks on merchants, on debt and credit cards.

More recently, the government launched two schemes, Lucky GrahakYojana and DigiDhanVyapariYojana, offering around Rs 340 crore in cash rewards to encourage digital payments between Rs 50 and Rs 3,000. It is also aggressively pushing UPI (United Payment Interface) and is expected to launch an app that users can download to transact across multiple banks. An upgraded, feature-rich version of the USSD (Unstructured Supplementary Service Data) platform, which allows banking transactions through feature phones without Internet connectivity, is also to be unveiled.

Those without mobile phones can now also transact digitally through Aadhaar based payments using just their fingerprints. E-wallet providers have also jumped at the opportunity. It is raining discounts and cash backs in this segment, which is attracting more users on these platforms. For instance, Free charge recently ran a two-day flat 100% cash back campaign on purchases like movie tickets, meals and online shopping. It claims that during this short window more than 3 lakh new wallets were created and volumes rose 15 times.

Others service providers such as Paytm and MobiKwik have also been lining up cashback offers. Banks are not far behind in promoting their debit and credit cards. Nearly nine out of the 10 respondents in our survey have been using debit or credit cards regularly since 9 November—

the day after the notes ban was announced. For higher payments, nearly three out of four respondents now prefer Internet banking and more than half use debit or credit cards and also cheques.

Limitations aplenty

Even as people adapt to newer, digital modes of payment, questions remain over the platform's operational aspects. The surge in digital payments that followed the notes ban has clearly overwhelmed the existing infrastructure. "As a nation, we are clearly behind on the preparedness to deal with this largescale move towards digital payments," admits Joy. There have been numerous reports of card transactions on PoS (Point of sale) terminals not going through owing to connectivity or server issues. E-wallet transactions have also not been smooth, with some customers complaining their wallet balance did not reflect the correct amount transacted. "Issues with network congestion and Internet connectivity have led to some delays in transactions going through and reflecting in the users' wallet balance," admits Gupta, explaining that the problem is a result of the sharp spike in transactions.

He assures users that there is nothing to be concerned about. "Digital payments are completely traceable and can be reconciled. Your money is safe and not going anywhere," he says. E-wallet platforms are constantly upgrading their systems to cope with the increased traffic. "Physical infrastructure supporting the digital payments needs to revisited and scaled up to cater to the next level of usage," says Mohan Jayaraman, Managing Director, Experian Credit Bureau, India. Merchant acceptance of digital payment platforms also remains a sore point. Shailaz Nag, COO, PayU India, says that both existing users and those yet to take to digital platforms remain confused with the different options available such as PoS terminal, ewallet, IMPS (Immediate Payment Service) etc.

Security issues: Concerns around the security of transactions and identity theft still prevent thousands from moving over to the digital payment platforms. Some 66% of the respondents in our survey said that security concerns remain their biggest worry. A cultural and mindset change is required to bring people on board and make them feel comfortable with digital payments, argues K.V. Karthik, Partner, Financial Advisory, Deloitte.

Experts insist digital payments platforms are fully secure provided the necessary precautions are taken by the user. "Cash can get stolen and you will have to bear the loss. However, if there is a fraud related to your debit/credit card then you have recourse. As per regulatory guidelines, the banks will investigate the case when you report a fraud and you will

get compensated in case it's not because of lapses on your part," points out Karthik. Most popular e-wallet platforms also comply with the latest security specifications and have added further layers of security, say experts.

However, the existing machinery for protection of consumers requires a huge revamp before consumers become comfortable with digital payments, says Jayaraman. "As more and more digital transactions move into the yet unregulated fintech space, proper fraud prevention, including device fingerprinting and consumer protection mechanisms, needs to be put in place. There is a definite need to improve the quality of the safeguards," he says.

However, service providers are taking steps for added protection. Freecharge, for instance, recently launched an e-wallet protection plan (at no added cost) for all its users, where the underlying wallet balance of all the customers will be insured up to a limit of Rs 20,000, as long as the user is transacting at least once a month. Other e-wallet platforms are also expected to follow suit.

Change in habits a must: What is clear is that users' habits related to online transactions and usage needs to undergo a drastic change. "This is a newer way to transact and it will involve a learning curve," insists Gupta. At the very outset, Karthik warns users not to reveal too many details on social media. "Nowadays users put up many personal details in the public domain through social networking platforms. If the profile is so widely available, it is not difficult for fraudsters to use it to their advantage," he warns.

Nag firmly believes the smartphone will increasingly become the hub for making payments, but users need to take necessary precautions—keep the Bluetooth switched off, install antivirus software on the smartphone and not download suspicious files from the Internet. "Most people today use antivirus software on their desktop computer or laptop, but ignore the smartphone. It is critical that the smartphone is also secured properly," says Nag.

Three out of five respondents in our survey admitted to not having installed an antivirus software on their smartphone. Even if your eWallet app is secure and trusted, you must be careful about other apps on the smartphone, which can potentially capture keystrokes or passwords being used for transactions. Most apps nowadays seek access to personal info stored on the smartphone including documents, media files, contacts, etc.

Users must be cautious when it comes to allowing access to information demanded by these apps. "Be wary of using apps asking for access to information that's not a must for the app to function," urges Karthik. This is where prominent anti-virus and anti-malware software can

come to the rescue. They scan the installed apps and flag potential risks, in case of apps asking for unnecessary permissions. Storing critical details on personal devices is another worrying habit.

For instance, one-third of the respondents admitted to allowing their smartphone or personal computer to store their billing or card details for easier future transactions. While this surely facilitates quicker payments, it leaves you vulnerable to hackers and identity thieves. "Habits like writing down the PIN on the back of the debit or ATM card or sharing details over the phone is like presenting someone with a blank cheque," warns Joy.

Similarly, you could expose yourself to risks, if you regularly access public WiFi through your smartphone or laptop. Three out of 10 respondents in our survey admitted to doing so at every opportunity. With all the financial information stored in the phone, losing or misplacing it is almost like losing your wallet. To ensure your critical data is secure, even when your phone is unattended or lost, the least you can do is enable the phone screen lock. You can further enhance the security by installing an app lock to protect apps with sensitive data.

As the government presses ahead with a cash to less cash to cashless economy, the success of the transition will depend on how the battle between bankers and hackers plays out. Bankers must upgrade and fortify their cyber defences as hackers attempt to pinch funds from banks or steal credit/debit card details of retail customers daily. If suddenly the easiest way to buy anything from soft drinks to cars is to use the mobile wallet, a few clicks of the mouse are all that is required to rob a bank.

True, in a country with 98% cash in circulation, electronic payments replacing cash will not be easy and will take time. But since demonetisation kicked off on November 8, digital payments have got a fillip. That has opened up more opportunities for cyber pickpockets to try and steal card details, PINs, mobile wallets and siphon off money. “India has been at the lower end of frauds as volumes were low. Now, I suspect that will change as digital payments volumes surge,” says R Venkatachalam, mana.

AkhileshTuteja, partner and global head of cyber security, KPMG says if the benefits of digital payments are exponential, so are the risks. India’s central banker itself flagged off concerns in this regard. In an October note, RBI deputy governor SS Mundra said one of the key targets by the attackers is the credential of the customers, as it provides the key to the ‘khazana’ (treasure). “Recent experience shows involvement of organised gangs and nation-state actors

fraud transactions is expected to reach $25.6 billion by 2020 up from $16.7 billion last year. "This means by end of the decade $4 in every $1,000 of online payments will be fraudulent," says Maiya. The 0.4% fraud transactions does not include money that could be stolen from compromised accounts.

Another study by Assocham-Pwc notes a surge of about 350% in cybercrime cases registered under the IT Act, 2000 between 2011 and 2014. MadhuSinghal, partner Khaitan & Company, says as it happens with other payments, there is a risk if user does not understand how e-payments work. "Just like losing a signed cheque leaf exposes a consumer to fraud, being negligent with passwords, card details could pose a risk in wallet or net banking transactions."

Types of Fraud

Singhal says there are three kinds of risks unique to e-payments. One, device related risk. If someone loses their mobile phone and there are no passwords protecting the phone or the app, money in an e-wallet could be compromised, or, leaving your accounts open when making payments from a public device. Two, risk from rights access. Connecting the e-wallets or other fintech apps with other apps like social networks could pose a risk of data leakage or a consumer unknowingly sharing information that should have been kept private. Three, negligence in sharing passwords or OTP (one time passwords) with others especially when using these modes publicly.

There are some other risks that are common to e-payments as well non-electronic payments — for example, giving away your account details to a third party. Provided the consumer takes basic precautions, the benefit of electronic payments far exceeds the inconvenience and transaction costs one would have incurred in other forms of payment, especially when the payment ticket sizes are small. Besides, downloading unverified apps and software can compromise security. Users should download apps with high ratings. Banking portals can get compromised as well. AltafHalde, managing director, Kaspersky Lab says, "HTTPs (the small 's' for secure) was always thought to be safe. But hackers can get here as well." Venkatachalam says problems can arise at both the bank and user end.

"While banks have to regularly update software and fraud detection systems, users should be aware of basics like changing passwords frequently, using unique passwords for different accounts (instead of the same for net banking, Facebook, Twitter)." The problem could be the hardware as well. Mobile chip maker Qualcomm's senior director for product management SyChoudhury recently raised concerns over hardware level security. "When you download a

having huge financial backing. On the other hand, the cost of orchestrating such attacks is coming down. There are several reports indicating availability of credentials of customers for sale in dark web, which is really scary."

The security threat notwithstanding, bankers prefer the shift to a digital payments system. A physical bank branch transaction is 50 times costlier than a digital transaction. And as volumes increase scale will ensure even lower costs of digital transactions. The government's push emanates from a desire to track the flow of money and check corruption and black money generation. The downside of a digital economy is that millions can lose money in seconds.

A single hack can ensure millions of accounts being compromised, as it happened in October when 3.2 million card details were stolen in a malware related security breach. These cards from customers of State Bank of India, HDFC Bank, ICICI Bank, Axis Bank and others, were used at ATMs. The stolen debit cards were used in China. The heist is still under investigation, but is almost forgotten in the scramble for a digital payments future.

Indeed, one of primary concerns over the rush to a digital economy, besides the challenge of drawing in swathes of people who do not even have a bank account, is the threat of cyber attacks. The government for now seems to be more focused on the second problem — goading people to embrace digital payments. On November 15, it announced a scheme to encourage digital payments between Rs 50 and Rs 3,000, offering around Rs 340 crore in cash awards for such transactions. The twin schemes, Lucky GrahakYojana and DigiDhanVyaypariYojana will be launched on December 25 and run by the National Payments Corporation of India (NPCI) for 100 days. NPCI is the nodal agency controlling e-transactions like Universal Payment Interface (UPI), USSD, NEFT and RTGS.

Mobile wallets are already experiencing a tremendous growth in transactions. The user base of the Chinese Alibaba-funded Paytm has climbed from 100 million to 170 million in a month. Likewise, sales of Point of Sales (PoS) machines have risen 200 times since November 8. "India is on the fastest track when it comes to growth of digital channels use in financial services. The troika of Jan-Dhan, Aadhaar and mobile is one of the catalysts in making it happen," says Rajashekara V Maiya, head, Finacle product strategy, Infosys.

The problem is hackers won't be far behind. According to the latest available data from RBI, 13,083 and 11,997 cases related to ATM, credit, debit card and net banking fraud were reported in 2014-15 and 2015-16 (up to December 2015). The October breach of 3.2 million cards was the single largest of its kind in India. Globally, Juniper Research says value of online

mobile banking app you don't know if it is using hardware security or not," he was quoted as saying in New Delhi on December 13.

Credit cards, debit cards, mobile wallets, net banking fall in two distinct buckets. Credit, debit cards work under Payment Card Industry (PCI) standards, reviewed every year. PCI DSS (Data Security Standards) are a set of instructions to store, process and transmit plastic transactions with details about firewalls configuration, storing passwords, information of users and so on. "If PCI is not adhered to, the card can be compromised," says Venkatachalam.

Card companies like Visa, Mastercard, Amex do this but banks want to control customer information and hence vulnerabilities can exist at their end. Net banking comes under electronic payment channels and the security protocols are released by Internet Engineers Task Force (IETF). When net banking started more than a decade back it worked with 40 kb encryption which went up to 64 kb and now 128 kb. "This is very good. But when you are dealing with variety of people with varying ability to transact digitally, the chance of a hacker getting the better of you increases," says Tuteja. Even if the network is robust (in India it is maintained by RBI with NPCI as nodal agency), the leaks could be at the banks end (software not updated) or the user end.

Basudev Banerjee, banking expert at Microsoft, says systems managing the links from origin to settlement of a transaction are robust and secured, yet probability of fraud exists at every stage—for example, buying a water bottle at a road side vendor via card or m-wallet, transmission of details to authenticate user to ok buy, completing the purchase with user getting a SMS or confirmation slip and reconciliation at the backend.

A hacker could get at any of the five stages— origin, transmission, transaction, settlement and reconciliation. To keep fraudsters at bay, Vishak Raman, senior regional director, India &Saarc, FireEye (a security software maker) offers a laundry list of precautions like unique passwords, typing out links in address bars instead of clicking on links, avoid exchanging sensitive information (even your birthday) over e-mail, enable two factor authentication if available and so on. KPMG's Tuteja.

Referring to above mentioned experiences, incidences, articles, surveys, cases, issues it is really a vital point of concern to think about security, equipment's and connectivity issues in Indian market for Digital Payment. Government and banks together have to come up with more concrete, accurate and fast process to handle such issues of customers.

References

1. https://upipayments.co.in/digital-payment/
2. http://www.orfonline.org/research/privacy-security-risks-digital-payments/
3. http://economictimes.indiatimes.com/articleshow/56269830.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
4. https://economictimes.indiatimes.com/tech/internet/as-india-braces-for-digital-payments-future-how-secure-are-banks-from-cyberattacks/articleshow/56073576.cms