iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52175

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Cyber-Security in UPI Payments

Simran Kaur[1], Himanshu Mishra[2], Anuj Goyal[3]
Manva Rachna International Institute of Research and Studies

Abstract: ***Unified Payments Interface (UPI) is an innovative online banking system. Made in India has reached the peak of popularity ina short time wingspan. Growth in UPI alsoleads to higher data frequencies violate.***
Social engineering attacks are India's biggest security risk encountered duringconfinement (lockdown). Users of the Unified Payment Interface are Cyber criminals are easily enticed. These frauds are not due to default in the UPI systems or interfaces, but are tactics to deceive customers. By the way of phishing, vishing, or smishing. Social engineering attack techniques are planned to exploit users by utilizing significant UPI features such as "Collect Request", " Virtual Private Address, " or" QR Code." Reverse-engineering the UPI protocol through seven well-known UPI apps, this paper employs a principled methodology toconduct a thorough security analysis of theprotocol.
We find previously unreported design-levelflaws in the UPI 1.0 specification's multi- factor authentication that, when coupled with an installed attacker-controlled application, can result in serious attacks.
Even if a victim had never used a UPI app, the flaws in the attack's extreme version might have allowed a victim's bank account to be linked and emptied. Scalable and remotely executable attacks were possible. Most users blindly follow the instructions received through SMS or phone call and become a victim of cyber fraud. Analysis data collected from respondents reveals the grim fact that age or occupation has no impact on user behavior in response to technical attack techniques.
Keywords: UPI (Unified Payment Interface) Cyber crimes BHIM, DigiDhan, NPCI (National Payments Corporation of India) Cashless, Two factor Authentication

I. INTRODUCTION

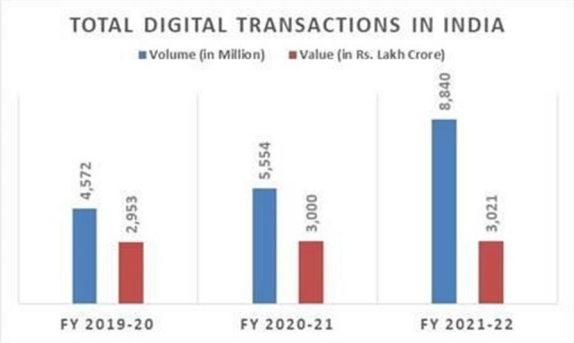
Following the demonetization of large currency notes in 2016 [2], payment appshave become a commonplace form of payment in India. The Indian Government actively encourages its citizens to use electronic payment methods. The Unified Payment Interface (UPI), which enables freeand immediate money transfers between bank accounts of different users, was introduced by the National Payments Corporation of India (NPCI), a consortium ofIndian banks, to facilitate digital micro- payments at scale. UPI transactions have a value of about $21 billion as of July 2019 [1]. On the other side, as UPI usage and transaction volume grow, customers are reporting an increased number of fraudulenttransactions. Transparency and tax revenuehave increased, corruption has decreased, and there are more opportunities for financial technology innovation thanks to theshift to digital payments. But as evidenced by cybercrimes committed by organised crime syndicates and rogue state actors, it has emerged at a time when threats to payment systems are becoming more and more serious. This paper is concerned with UPI's designflaws and how payment apps use it. Prior to this analysis, vulnerabilities in payment apps, particularly Indian payment apps, were uncovered [9, 48], and a PIN recovery bug was discovered in an Indian mobile banking service. These research, however, could not find any shared paymentinterfaces among the mobile apps. We are aware of no previous examination of a shared interface utilised by numerous payment apps. Such an investigation is crucial because, despite the adoption of other stronger security measures, security holes in them could affect users of numerous institutions and applications. We concentrate on the design decisions and security analyses of the unified payment interface utilised by many Indian payment apps. This paper reviews current policy measuresand cybersecurity standards, analyses India's payments industry and trends in cyberattacks on its payment infrastructure, maps the system's vulnerabilities and suggests ways to patch them.

II. DIGITAL PAYMENT SYSTEM

One of the major objectives of Digital Indiais to achieve “Fearless, Paperless, Cashless’’ status.
The Government of India has given the development of digital payments top priorityin an effort to formally integrate these services into every sector of our nation. Thegoal is to make seamless digital payment available to all Indian people in a way that ispractical, simple, affordable, rapid, and secure. In India, digital payment transactions have shown an unparalleled growth during the past three years. Prepaid payment instruments (PPIs), Immediate Payment Service (IMPS), Bharat Interface for Money- Unified Payments Interface (BHIM-UPI), and the National Electronic Toll Collection (NETC) system are among the simple and practical digital payment methods that haveexperienced significant growth and transformed the ecosystem of digital payments by increasing P2P and P2M payments.

Debit cards, credit cards, NEFT,and Real-Time Gross Settlement (RTGS), which are already common payment methods, have all experienced rapid growthat the same time.

BHIM-UPI has emerged as the preferred payment mode of users. The Government of India also launched the digital payment solution **e-RUPI**, a cashless and contactlessinstrument for digital payment which is expected to play a huge role in making Direct Benefit Transfer (DBT) more effective in digital transactions in the country. All these facilities together have created a robust ecosystem for a digital finance economy.



Source: pib.gov.in

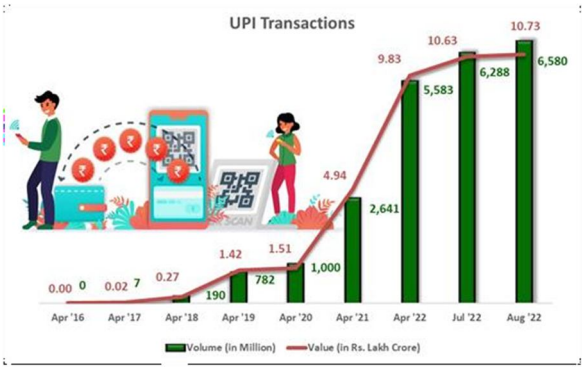
III. UPI: REVOLUTIONIZING DIGITALPAYMENTS

UPI has been termed a revolutionary product in the payment ecosystem. Launched in 2016, it has emerged as one of the most popular tools in the country for carrying out digital transactions.

The National Payments Corporation of Indiainvented the immediate payment system known as UPI (NPCI). It integrates different banking services, seamless fund routing, and merchant payments into one hood, powering several bank accounts into a single mobile application. On December 31, 2016, Prime Minister Narendra Modi introduced the BHIM-UPI App at the start of the "DigiDhan Mela" in order to improve andpopularise the interface even further.

UPI has made significant progress toward firmly setting India on the path to a cashlesseconomy and making digital payments a habit. With 346 banks operating live on the

UPI interface in August 2022 alone, 6.58billion financial transactions of over Rs. 10.73 lakh crores were completed.



Source: pib.gov.in

UPI currently constitutes well over 40% of all digital transactions taking place in India. It has given a boost to small businesses and street vendors as it enables fast and secure bank-to-bank transactions even for considerably small amounts. It also facilitates quick money transfers for migrant workers. The technology is convenient to use as it requires minimum physical intervention, making it possible to transfer money simply by scanning a QR code. UPI has also been a savior during the Covid-19 pandemic, with its adoption expanding rapidly due to its ability to allow easy, contactless transactions.

There is no doubt that India's digital payment landscape has changed in the present. In addition to the government's efforts, Indians have shown a strong propensity for embracing new technologies. India has emerged as a pioneer in the production of digital assets, which can serve as an example to many other countries, while some developed countries are experiencing issues owing to insufficient digital infrastructure for moving money to the accounts of their inhabitants.

Additionally, the Indian government is doingall possible to position India as a world leader in the field of digital payment systems and support it in becoming one of the most effective payment marketplaces inthe world. By providing transparent, safe, quick, and cost-effective procedures that are beneficial to the entire digital payments ecosystem, emergent fin-techs will go on to play a significant part in the further rise of digital transactions.

IV.CYBER ATTACKS IN UPI

Transactions were facilitated via UPI.

The risk has increased despite an increasein quick and transparent transactions. By demonstrating the allure of deceit and rewards, numerous forms of looting have been promoted. People that utilize UPI carelessly need to exercise prudence.

When utilizing this programme, certain simple but crucial information is needed. It is crucial to understand that receiving money does not require entering a UPI PIN. Only when sending money from the accountor when sending money to anyone else do you utilize the UPI PIN. This indicates that the UPI PIN is used to withdraw funds from the account. It's critical to keep in mindthat money isn't taken into consideration. Many con-artists construct misleading handles with names like NPCI, UPI, BHIM,etc. to trick people into divulging their account information through a bogus UPI app, which then leads to frauds. Many scammers prey on people who are unaware that one does not need to scan aQR code or enter the UPI pin in order to receive money on a UPI platform. To claim a prize, the hackers ask users to scan a QRcode and enter their UPI pin, which causes fraud on the UPI platform.[4]

Many unverified apps downloaded from theGoogle Play store can extract the phone information and tap all financial information available on the phone, leading to UPI frauds.

Fraudsters send unauthorized links through emails or SMSs to the users and once theyclick on such unauthorized links, frauds happen.[3] In order to avoid people from becoming victims of many of these frauds, digital literacy and UPI payment method educationare crucial, and the Indian government is always attempting to raise awareness among the populace

It is challenging to find a solution that satisfies both consumer privacy expectations and bank and regulatory surveillance requirements for fighting crime,preventing terrorism, and managing fraud and risk (FRM). With NUUP service, IMPS across all channels operated by using a Mobile Money Identifier rather than the complete bank account number. The NPCIdid not know which accounts were involved when transactions were routed through it. The NPCI had little personally identifiable metadata for transactions in which customers sent direct IMPS instructions to their banks via SMS (in plain text or encrypted) .

V. WAYS TO PROTECT YOURSELF FROMCYBERATTACKS

However, recent technological developments have simplified surveillance. While the UPI system guarantees end-to- end encryption, the payload is decrypted at each hop across the four parties. The Aadhaar number, device fingerprint (createdusing information like the Device ID, App ID,and IMEI number), IP address, operating system, application, bank account numbers,and GPS location of the user when making the transaction are all details that the NPCI can see because it controls the switch.

Theoretically, this data is intended to aid in the detection and prevention of fraud, but when combined with the data obtained from the NPCI's other services, a complete financial picture of the majority of non-elite Indians can be created. Aadhaar numbers are permanent and are kept on file by various UPI stakeholders, unlike VPAs, which can be issued again. Therefore, any data breach may have a long-lasting effect [5].

“There are multiple layers of security checksimplemented when any transaction occurs on a bank's mobile application using UPI. This is not just in between the user and the app but also between the banks, merchant and the UPI engine,” said Modi, who also advises banks globally on cyber risk management.[6]

A. Two Factor Authentication

Two Factor Authentication is known bymany names. Multi-factor identification. Two-step verification of the user. MFA. 2FA.All of them refer to choosing to take an additional step when reputable websites and applications ask you to verify that you are who you say you are. Here, two factor authentication can be done by setting upMPIN and a UPI pin that helps to make secure payments.

B. Don’t engage with fraudsters

Please don't continue if you are unsure of a phone number, the caller's identity, or the source of any information being shared. Be cautious of phone numbers shared on public websites, especially for restaurants orbars, as they might not be legitimate. Ensure the person's identity by checking it twice. Keep in mind that your bank will never request any private information from you over the phone or through a message.

C. Remember the Golden rule ofReceiving the Money

No PIN is necessary to receive money. On payment apps, scammers attempt to abuse the "request money" feature. They'll pretendto be interested in purchasing a product youmay have listed for sale online. Always keepin mind that you will NEVER be asked for a PIN if money needs to be credited to your bank account.

D. E mindful of payment requests and SPAM warnings

The UPI app will probably issue a spamwarning if it receives a request from an unidentified account. Pay attention to the option you are choosing, either "Pay" or "Decline." If you think a requestis fraudulent, kindly say no. Don't be fooled into thinking that by selecting the"Pay" option, you will receive money. Instead, money is transferred to the fraudster's account after you enter the UPI PIN.

E. Beware Of Counterfeit Apps Many Fraudulent Or Malicious Apps Try To

Trick you by appearing to be something else. The app will have a similar appearance to the original bank app and be simple to download. Your sensitive information will be shared with scammers ifyou unintentionally download and instal thefake app, giving them access to your account and enabling them to steal money.Watch out for fake banking apps like Modi Bhim, BHIM Payment-UPI Guide, Bhim Modi App, and BHIM Banking Guide that have been accused of stealing customer personal information under the guise of offering auseful service.

1) Never give a stranger your PIN.
2) Maintain your biometric recognitionand antivirus software installations.
3) Never click on links or emails fromunidentified sources.
4) Keep your bank updated with yourinformation.
5) Use trusted secure WiFi connectionsonly, avoid open ones.
6) Keep a close eye out for any suspicious activity on your accountand keep track of your financial transactions and bank account statements.
7) Immediately notify your bank if youdiscover anything strange.

VI. CONCLUSION

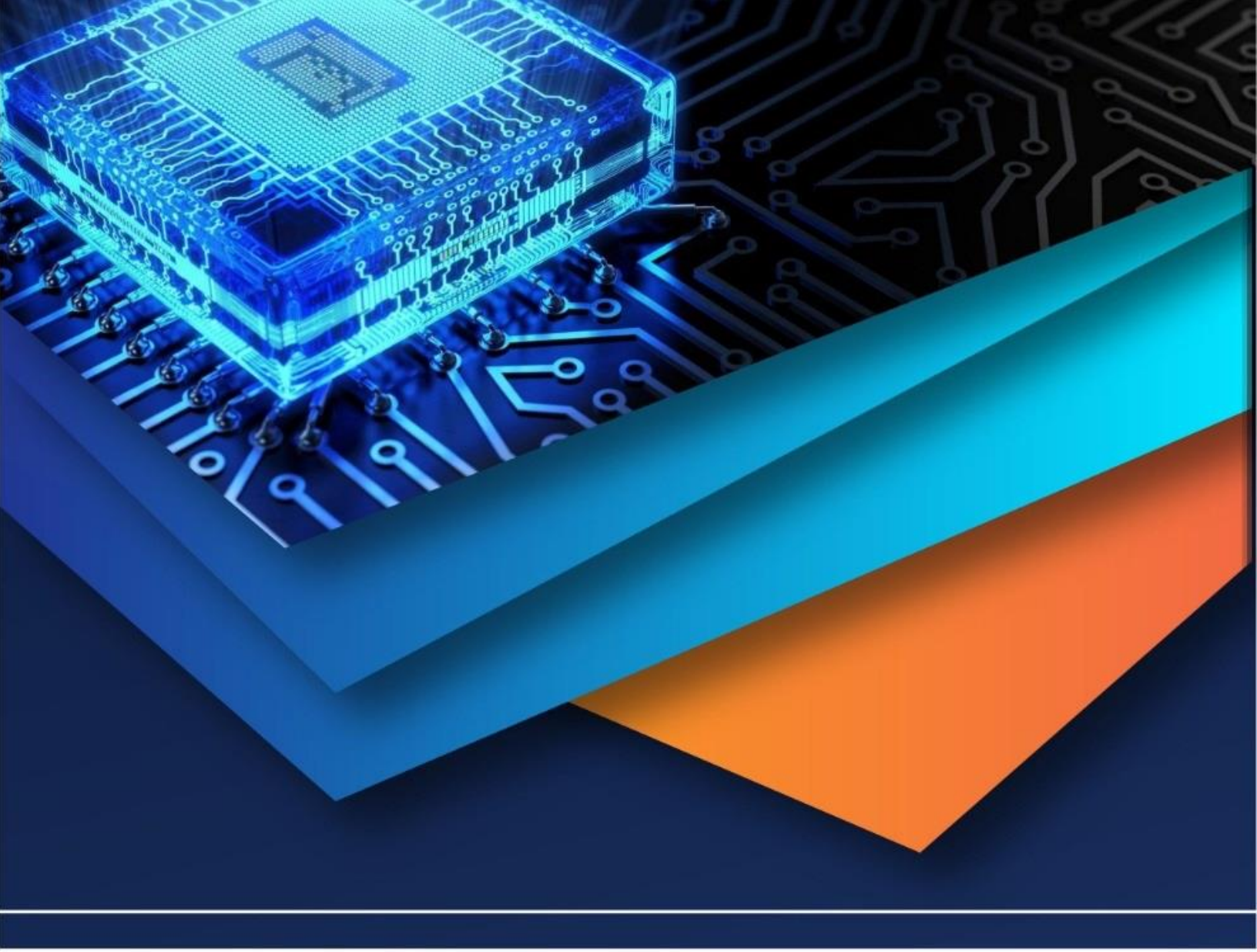
The fight against cybersecurity is never-ending. There won't be a permanent, conclusive solution to the issue anytimesoon.

The complexity of information technology systems, the inherent nature of information technology (IT), and human fallibility in making judgements about what actions and information are safeor unsafe from a cybersecurity perspective—especially when such actions and information are highly complex—are themain causes of cybersecurity problems.

There are no magic solutions—or even combinations of solutions—that can "solve the problem" permanently because none of these variables are likely to change in the near future. Cybersecurity threats also change over time. Intruders adapt by creating new tools and techniques to breach security as new defences are created to counter older threats. The incentives to undermine the security of installed IT systems increase as information technologyis more thoroughly ingrained in society. Withthe development of new information technology applications come new opportunities for criminals, terrorists, and other adversaries, as well as flaws that can be exploited by bad actors. The number of people who have access to the internet is growing, which increases both the potentialfor malicious actors as well as victims.

REFERENCES

[1] https://www.usenix.org/system/files/sec20summer_kumar_prepub.pdf
[2] Y. Kouraogo, K. Zkik, E. J. El Idrissi Noreddine, and G. Orhanou. Attackson Android banking applications. In 2016 International Conference on Engineering MIS (ICEMIS), pages 1–6, 9 2016.
[3] www.indiaherald.com/Technology/Read/994484611/Cyber-Attacks-on-UPI
[4] https://community.nasscom.in/communities/digital-transformation/fintech/upi-payments-top-security-issues-possible-way-arounds-an-opinion.html
[5] Unified Payment Interface: TowardsGreater Cyber Sovereignty | ORF (orfonline.org)
[6] https://www.csk.gov.in



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY