UPI Based Mobile Banking Applications – Security Analysis and Enhancements

K. Krithiga Lakshmi[1], Himanshu Gupta[2], Jayanthi Ranjan[3]

[1]Amity School of Engineering and Technology, Amity University, Noida (India)
[2]Amity Institute of Information Technology, Amity University, Noida (India)
[3]Professor, Institute of Management Technology, Ghaziabad (India)
[1]krithigal@yahoo.com, [2]himanshu_gupta@yahoo.co.in, [3]jranjan@imt.edu

Abstract: **Technology advancements have reduced the cost of both a mobile device and data connection making it affordable to all. In parallel, mobile applications are also rising providing the quick, easy door-step solution(s) to one's professional and personal requirements. In the current trend of the digital and cashless economy, mobile-based app solutions are easy to use and ubiquitous, facilitating a wide range of banking financial services (pay/collect money etc.) and non-financial services (cheque request, account balance, view transaction history etc.). Mobile app revolution is also accompanied by many known and unknown security risks. Out of the various mobile banking applications, UPI (Unified Payment Interface) based apps are simple, reliable, centrally certified (by NPCI (National Payment Corporation of India)) and more secured. Study of UPI apps revealed the possibility of further security enhancements utilizing technological advancements to detect cybercrimes and fraudulent mobile transactions. This paper discusses UPI based mobile apps (architecture, transactions, features and security issues) and information security enhancement proposals w.r.t authentication and authorization.**

Keywords: **Mobile Banking; Security; Application Security; Information Security; UPI; USSD; Authentication; Authorization; Encryption; Financial Service**

I. INTRODUCTION

Mobile Banking service allows end user to perform remote banking transactions (both financial and non-financial) from his/her current location using the hand held mobile device anywhere-anytime. A variety of technology specific mobile banking solutions like IMPS (Immediate Payment Service), USSD (Unstructured Supplementary Service Data), SMS (Short Messaging Service) and UPI (Unified Payment Interface) [8] based app solutions (like BHIM (Bharat Interface for Money), GooglePay (Tez), PhonePe and Bank specific apps like SBIPay, AxisPay, iMobile, Mobile Money etc) are available to perform regular banking operations (like fund transfer, cheque request etc) and other payment [14,15] operations in m-shopping, metro card recharge, loan/credit card payment. Number of features and security level offered, varies with every application and are dependent on the mobile device capability, its operating system and internet connectivity. USSD and SMS based banking operations are suited to low end non-smart phone devices without internet connection. USSD service is offered in association with the Mobile Network Operators (MNO's). Though there are few security concerns in mobile banking applications, they are still preferred by everyone, because of its well-known advantages like fast, easy to use, convenient to pay bills, portable, available etc. Even banks promote mobile banking [1] as it helps to handle more customers with improved customer services at reduced operational cost without compromising on service quality. Banks also offer discounts, gifts etc., to promote mobile banking.

Following are some of the common terms used in mobile payment types.
VPA: Virtual Private Address. An address of the format <mobile number>@upi [6] used to transfer money using UPI App's. User can create multiple VPA's. UPI based fund transfer uses VPA internally to look up the account number.

IFSC (Indian Financial System code): It is a eleven digit code seen in cheque leaf used to identify the bank branches involved in money transfer.

MMID: Mobile Money Identifier. A unique seven digit code assigned to customers on registration to avail IMPS service as a beneficiary.
The paper contents have been organized in seven sections, with Section 2 on Evolution of Money and Payment Solutions, Section 3 on UPI Based Mobile Banking, Section 4 on Security Enhancement proposals, Section 5 on UPI vs other Parallel System, Section 6 on Conclusion and Section 7 on Future Scope of Work.

II. EVOLUTION OF MONEY AND PAYMENT SOLUTIONS

The evolution of money started with Barter scheme (i.e mutual exchange of goods and services) and have evolved over these years from coins to paper and plastic money (i.e cards). Fig.1 below shows the transitions in money evolution.

Fig. 1. Transitions in Money evolution

978-1-5386-9346-9/19/$31.00 ©2019 IEEE

Now in 21st century, it has advanced to currency less money transfer in the form of mobile payments and virtual currency. Even in mobile based payments, user has multiple options to choose from namely NEFT (National Electronics Fund Transfer), RTGS (Real Time Gross Settlement), IMPS (Immediate Payments Service), UPI, USSD and mobile wallets. Fig. 2 below shows the various options of mobile payment modes.

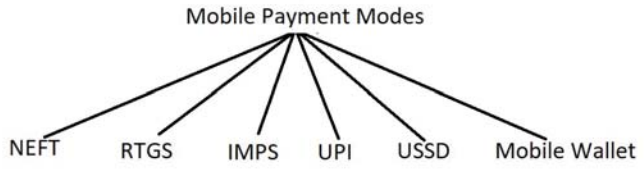

Fig. 2. Mobile Payment Modes

A. Mobile Payment Modes

Mobile payment modes are given below.

NEFT: Used to transfer fund from one account to another.

RTGS: Scheme for instant money transfer within 30 minutes. Unlike NEFT, RTGS processes the instructions immediately without delay.

IMPS: An instant payment system to transfer funds from one account to another using mobile. It is an initiative of NPCI.

UPI: UPI is the advanced version of IMPS. It is a mobile based payment mode where multiple mobile accounts can be managed using a single VPA. Allows fund routing and merchant payment. Uses UPI PIN to authenticate UPI fund transfer. It is built on IMPS infrastructure.

USSD: A mode of performing mobile banking transaction using *99#service codes.

Mobile Wallet: A secured way to carry credit/debit card information. Allows payment at stores via mobile phones.

Availability of more than one payment mode, facilitates the user to choose an appropriate mode depending on his/her device capability (smart/GSM phone), internet connectivity (online/offline), known/available confidential information (i.e Account Number/IFSC/MMID code/Mobile number/VPA and MPIN), fund transaction details including amount, day and time (i.e weekday/weekend and time of the day).

B. Comparison of Mobile Payment Modes

TABLE I below shows the comparison of various Mobile payment options.

TABLE I: MOBILE PAYMENT OPTIONS – A COMPARISON

Attributes	NEFT	RTGS	IMPS	UPI	USSD
Resource requirement	With/without Internet	With/without Internet	With Internet	Smart phone with/without Internet	GSM phone with/without internet
Fund Transfer Days	Monday-Friday (8am-7pm), Saturday (8am- 1pm)	Monday-Friday (9am-4:30pm), Saturday (9am- 2pm)	24 * 7 on all days of the year	24 * 7 on all days of the year	24 * 7 on all days of the year
Time required for Fund Transfer	Generally same day	Within 30 minutes	Instant	Instant	Instant
Information Required	Name, Account Number and Bank Name, IFSC code	Account Number and IFSC/MMID code and Mobile number	Account Number and IFSC/ Beneficiary's MMID code and Mobile number/Aadhar	VPA of recipient and MPIN	Account number and IFSC / MMID code and Mobile number
Fund Transfer Limit/day	No limit normally But ₹ 50,000 for cash transfer	Minimum is 2 lakhs	Upto 2 lakhs	Upto 1 lakh	₹ 5000
Transaction Amount and Charges	Upto ₹ 10,000 - < ₹ 2.50 + ST(Service Tax) 10,000 - 1 lakh – ₹ 5 + ST 1 lakh – 2 lakhs – ₹ 15 +ST Beyond 2 lakhs – ₹ 25	2 – 5 lakhs - < ₹ 30 Beyond 5 lakhs - < ₹ 55	Upto 1 lakh - ₹ 5 1-2 lakh - ₹ 15	Free of charge	0.50 paise

Attributes	NEFT	RTGS	IMPS	UPI	USSD
Limitation	Only on Bank working days	Both Account holder and beneficiary to be RTGS enabled Amount should be 2 lakh	Need to be online	Transaction amount only upto 1 lakh/day	MNO has to provide USSD support Account Number and IFSC Code/ MMID and Mobile number required for transfer

As NEFT/RTGS/IMPS requires Bank Account details, users prefer to use them in net banking using PC rather than using mobile. For transactions of 2 lakhs during banking hours, one may choose between NEFT and RTGS depending on affordable transfer time (i.e within 30 minutes or more but on same day). For offline/online transaction amount > 2 lakh, NEFT is the only option but, for offline transaction of smaller amount < ₹ 5000, one may choose among NEFT (only on working day), UPI and USSD (any day any time). For simple, free, secure, instant transfer of large amount (upto 1 lakh) any day-any time (online/offline) at ease without using confidential details (i.e Bank Account and IFSC number etc), UPI is the only choice. With low end non-smart phone device, USSD is the only available option. To conclude, every new payment mode overcomes the limitations of its earlier version and offers more features and use may choose one as per his requirements and resources

III. UPI BASED MOBILE BANKING

UPI is an instant payment system and uses the IMPS infrastructure at the backend. UPI is an outcome of mobile financial revolution drive towards cashless [12] economy.

A. UPI Objectives

It has been designed with the following key objectives.

- Simple, Secure Interface with one click 2 factor authentication based payment solution.
- Should be able to send/receive secured payment without sharing user's confidential information like Bank account number etc.
- Use the advanced features of mobile devices and provide an innovative solution with high security.
- Provide an integrated payment solution.
- Should be able to integrate with third party mechanisms to provide add more security.

B. UPI Architecture

The architecture of the UPI is given below in Fig.

Unified Payment Interface consists of architecture and a standard set of UPI API's [9,10,11,13] which are used to perform transactions (credit/debit). UPI payment transactions involves the following participants.

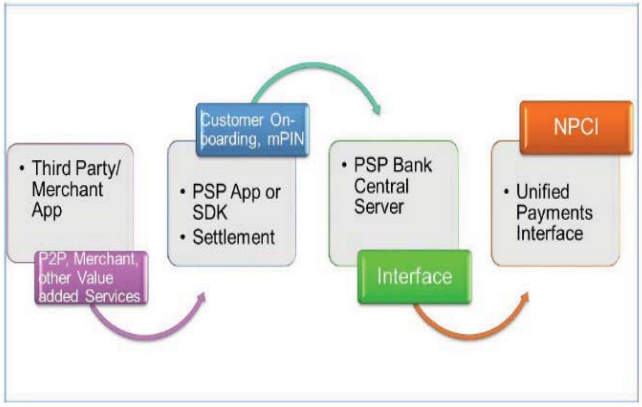

Fig. 3. UPI Architecture [9]

- **PSPs**: Refers to UPI Apps from Banks which are used to provide payment services to end user,
- **Banks**: Bank of customer.
- **NPCI**: Provides the UPI interface.

C. Transaction Types

UPI supports financial and non-financial transactions.

Financial Transactions:

- Pay Request - Customer initiated PUSH transaction to transfer funds to Beneficiary account using Account number/IFSC Code, Mobile No/MMID, Aadhaar Number etc.
- Collect Request - Customer pulls the funds from remitter using his VPA.

Non-Financial Transactions:

- Mobile Banking Registration
- OTP Generation
- Set/Update PIN
- Check Transaction Status

D. Transaction Flow

UPI transaction involves 3 phases (a one time Customer and Bank Account Registration [7] followed by push/pull transaction. Phase wise details ae given below.

Customer Registeration:

- Download and install UPI App.
- Create and send an PKI encrypted [2,3,4] SMS of device fingerprint (i.e about mobile number is bound with other device identities namely Device Id, App Id, IMEI number etc.[5]).
- Create VPA (It is a unique id of the format <name>@<bankname> and is used to map to the bank account number internally during transactions).

Bank Account Registeration:

- Register the bank accounts with app.
- Generate MPIN via OTP (need to provide last 6 digits of debit card number, expiry date along with generated OTP, once they are authenticated, app registers the user's MPIN with Bank .

Push/Pull Transaction:

Fig. 4 below show the transaction flow of pull request.

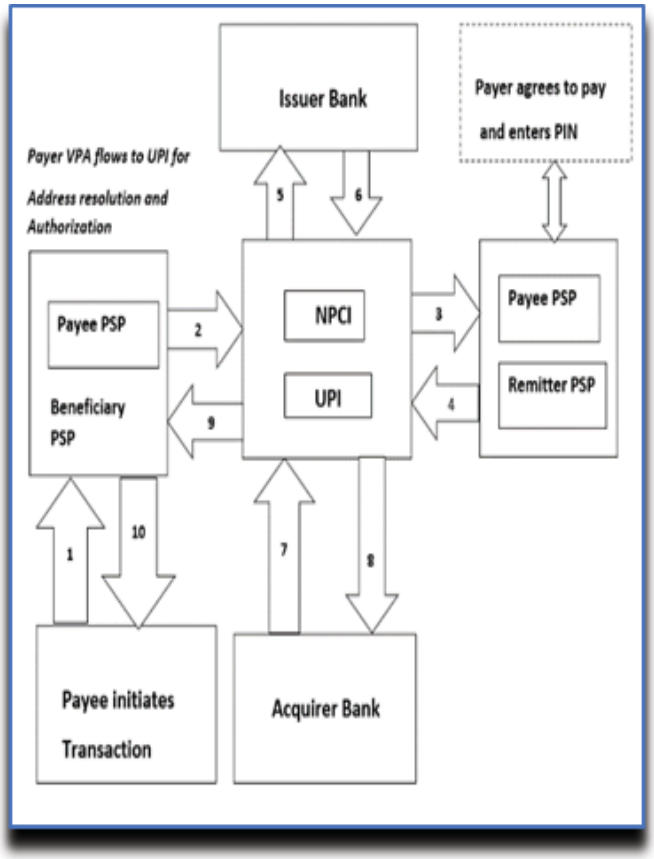

Fig. 4. UPI Pull Transaction

- Perform push using VPA or IFSC& Account number or Aadhaar.
- Perform pull by initiating collect request with VPA of payer as input and on authorization (by remitters PSP) followed by MPIN authentication (by Payee) the amount gets remitted in beneficiary's account.

E. Authorization

UPI uses 2F authentication as below.

- 1F – Device finger prints following mobile number transaction authorized by PSP.
- 2F – PIN/Biometrics authenticated by the UIDAI (Unique Identification Authority of India).

F. Advantages

- Simple and easy to use.
- Simple and Secured Multifactor Authentication (as it uses only VPA).
- Provides an integrated access to multiple accounts using a single VPA.
- UPI API's facilitates incremental and rapid app development. Simple, small and feature specific UPI API's facilitates innovations and exponential development of PSP applications.
- Addresses all challenges currently faced by other Non-UPI applications.
- Secured and Authentic as UPI App's by PSP's are audited and certified by NPCI periodically.
- No need to register beneficiary details for fund transfer.
- Security (i.e biometric/non-bio-metric) based on the Device capability.
- Provides biometric authentication involving finger/IRIS via third party application UIDAI (Unique Identity Aadhaar to all residents of India).
- Payments can be done using multiple identifiers namely VPA, Aadhaar Number, Account number & IFSC, Mobile number & MMID, QR Scancode.
- Payments as per RBI guidelines.
- Can be integrated with third party security tools/apps.
- Minimum infrastructure requirements.
- Can work with/without internet connectivity.

IV. SECURITY ENHANCEMENT PROPOSALS

The security threats and enhancement proposals in UPI based applications are given below in Table II.

TABLE II: UPI BASED MOBILE BANKING APPLICATION SECURITY ENHANCEMENT PROPOSALS

Security Threat/Issue	Proposed solution(s)
Low security in MPIN Update	• Currently in update of MPIN operation, it uses last 6 digits of the credit card number and expiry date alone for authentication and this will have to be enhanced as it can be remembered and misused by anyone. • Rather may prompt few pre-registered queries (let this be a subset of randomly chosen queries from a main set of queries which have been registered during Bank registration) and read and match the responses from the user. Only on 100% matching responses to all prompted queries, update the MPIN else terminate. • Also restrict the number of invalid MPIN update transactions to 3. Excess retries should block the VPA.
Fraud MPIN updates	• Currently, in case of MPIN failure, details are recorded in transaction log. In some bank applications, excessive MPIN update failures result in lock of UPI app and user will have to visit the bank branch. • As such MPIN failures may occur in case of misuse of stolen phone and in such cases, if any email is registered, then the user may be notified in such cases. • account Enhance the current UPI app to log failed MPIN update attempts with details
Fraud UPI transaction attempts using stolen phone	• If there is an email id registered, then in case of unauthenticated UPI transactions, an email alert can be sent to registered mail id.

Optional requirements as stated in RBI guidelines for UPI Apps, use of behavioral traits and artificial intelligence may also be explored for further security enhancements.

V. UPI VS OTHER PARALLEL SYSTEM

For UPI, the mobile wallet is the other parallel system. While UPI is more secured and is on a well-tested IMPS platform, mobile wallets apps are less secure, but technologically advanced and provide an easy user-friendly interface. Mobile wallet providers are expanding their market through promotional schemes and strategic tie ups with specific vendors. Mobile wallets are changing their business models and aligning it w.r.t to technology changes and market needs. They have also begun to partner with specific banks (For eg Freecharge with Axis etc). Hence both UPI and wallets shall co-exist while competing with each other in future.

VI. CONCLUSION

In this paper, we have discussed about the architecture of UPI based Apps, their transaction flow, authentication mechanism and its USP against other mobile banking payment solutions. Have identified few security issues and have proposed security enhancement solutions to deal with them (MPIN update transaction security issues and detection of fraud transactions related to MPIN update and UPI financial transactions). It is observed that inclusion of email alerts and additional fields in MPIN authentication shall enhance the security of existing UPI application. Also, there is a scope to include behavioral attributes and artificial intelligence to enhance security.

VII. FUTURE SCOPE OF WORK

As in this paper, some UPI issues have been identified and have discussed outline of their respective solutions, next step is to design, implement and evaluate the proposed solutions. For additional security enhancements, need to explore the optional requirements in RBI guidelines relevant to security for inclusion and use of Behavioral traits and artificial intelligence for authentication during UPI transaction.

REFERENCES

[1] Kelvin chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison, "Security of Mobile Banking", *Research Gate*, Jan. 2006.

[2] C.Narendiran, S.Albert Rabara, N.Rajendran, "Performance Evaluation on End-to-End Security Architecture for Mobile Banking System", *2008 1st IFIP Wireless Days*, IEEE, 2008.

[3] Gupta, Himanshu, Sharma, Vinod Kumar, "Role of Multiple Encryption in Secure Electronic Transaction", *International Journal of Network Security & its Applications*, vol. 3, pp. 89-96, Nov. 2011.

[4] Gupta, Himanshu, Sharma, Vinod Kumar, "Multiphase encryption: A New Concept in Modern Cryptography", *International Journal of Computer Theory and Engineering*, vol. 5, pp. 638-641, Aug. 2013.

[5] Nuril Anwar, Imam Riadi, Ahmad Luthfi, "Forensic SIM Card Cloning Using Authentication Algorithm", *International Journal of Electronics and Information Engineering*, vol. 4, pp. 71-81, June. 2016.

[6] Roshna Thomas, Dr. Abhijeet Chatterjee, "Unified Payment Interface (UPI): A Catalyst Tool Supporting Digitalization – Utility, Prospects & Issues", *International Journal of Innovative Research and Advanced Studies*, vol.4, pp. 192-195, February. 2017.

[7] Rahul Gochhwal, "Unified Payment Interface—An Advancement in Payment Systems", *American Journal of Industrial and Business Management*, vol.7, pp. 1174-1191, Oct. 2017.

[8] Radhika Basavaraj Kakade1, Prof. Nupur A. Veshne, "Unified Payment Interface(UPI) - A Way Towards Cashless Economy", *International Research Journal of Engineering and Technology*, vol.4, pp. 762-766, Nov. 2017.

[9] National Payment Corporation of India. (2016, Dec). "Unified Payment Interface Procedural Guidelines", [Online]. Available: https://www.npci.org.in/sites/default/files/UPI-PG-RBI_Final.pdf

[10] National Payment Corporation of India, "UPI Product Overview", [Online]. Available: https://www.npci.org.in/product-overview/upi-product-overview

[11] National Payment Corporation of India, (2016, Sep). "A step towards cashless economy -Unified Payments Interface (UPI)", [Online]. Available: https://ctconline.org/documents/income/14-9-16-Sanjay-Saxena-UPI-presntation.pdf

[12] Government of India, "Unified Payment Interface", [Online]. Available: http://cashlessindia.gov.in/upi.html

[13] National Payment Corporation of India, "UNIFIED PAYMENT INTERFACE API and Technology Specifications Version 1.0", [Online]. Available: https://github.com/AshishAgarwal2101/DCB-App/blob/master/NPCIUnifiedPaymentInterface.pdf

[14] National Institute of Rural Development and Panchayati Raj, "Unified Payment Interface THE FUTURE OF PAYMENTS", [Online]. Available: http://www.nird.org.in/nird_docs/cle9.pdf

[15] Nitinbhatia, (2018). "what is IMPS – Immediate Payment Servive", [Online]. Available: http://www.nitinbhatia.in/personal-finance/imps-immediate-payment-service/