A User Friendly Transaction Model of Mobile Payment with reference to Mobile Banking in India

Vibha Kaw Raina\textsuperscript{1}, U.S Pandey\textsuperscript{2} Munish Makkad\textsuperscript{3}

Department of Computer Science Birla Institute of Technology, Noida, India.
School of Open Learning Delhi University, India.
Department of Management, Birla Institute of Technology, Noida, India

Email: kawvibha@yahoo.com

Abstract

Mobile payments are the payments that are carried out through mobile devices in wireless environment. Mobile payment is considered as the accelerator of M-commerce. The internet and the mobile phone are basically two technological advancements that have created an impact on mobile payments. Using a variety of platforms and services mobile devices can perform many activities as compared to traditional payments. Mobile payments have also contributed to the banking industry. Which is a new activity in terms of mobile banking? Banking is an area that has extended by the use of wireless internet and mobile devices. Mobile banking is the symbiosis of technology and financial services. Despite of the convenience and business opportunities mobile banking and mobile payments are not used by people in India especially in the remote areas. This paper proposes a simple model of payment which takes into consideration the different modes of payment. This proposed work introduces alternative ways for providing mobile banking services aimed at Android O.S due to the use of mobile devices. The aim of the this work is to develop a model of payment that integrates with the financial services, including payment and banking ones, based on two primary capabilities: the use of computational resources of a trusted mobile device and the establishment of a user controlled channel with the customers bank. The proposed architecture is characterized bank-centric, since the bank acts consultatively, informatively and protectively or the end user and it offers flexibility, adaptability and continuous extendibility to open technologies. The
implementation of the proposed work is done in Android O.S with additional hardware in terms of Biometrics and NFC technology.

**Keywords**: Mobile Payment, POS, Payment Systems

I. Introduction

Although mobile payments and mobile banking is no longer a concept but a development entity, and that it has become a significant force of the economic development. Mobile payments are becoming more and more important with the increase of wireless services. Improved data transfer and the easier use of such services will also increase demand among end users. Mobile payments are payments for banking services, goods, and bills/invoices with a mobile device (such as a mobile phone, smart phone, or PDA’s) by taking advantage of wireless and other communication technologies (such as mobile telecommunications networks, or proximity technologies). Moreover, mobile payment must also abide by the security rules and regulations of the payment sector [1][2].

Mobile payments present several security challenges, including: confidentiality, authentication, integrity, authorization, and non-repudiation. The existing wireless payment systems can be classified into three types: account based payment systems, token-based payment systems, mobile POS (point of sale) payment, and mobile wallets payment systems [3]. But, the scenario of mobile banking in India is still in infancy. People are still not aware of mobile payments and still people face lots of dilemma in doing transactions and payments. People are not aware of the differentiation between internet banking and mobile banking. Especially in J&K, Uttarakhand and north areas like Tripura, Assam, Nagaland due to poor connectivity, erratic power supply, low income level of people and the remote locations of the states. Some of the payment systems used in rural India is Beam, Pay-as-you-go, Mchek, PayMate and UID projects in micropayments.

A. **Beam**: It is a micropayment service aimed at the non banked rural population of India. Beam distributes prepaid vouchers that one can purchase in the denomination of Rs100-1000 and load their account against the mobile number through SMS or IVR. [4] The strategy for the Beam seems to be a little confused. They claim of serving the rural crowd but the agency is targeting
the urban youth. A related opportunity in Beam could be micro-transfers, wherein the migrated rural crowd could use the service to transfer money.

B. **Pay-as-you-go**: This is a cell phone service and is applying to small scale solar energy systems. Simpa Networks partnering with solar manufacturing Selco India allows Hardware upfront customers, then purchase pay-as-you-go cards in increments of 50, 100,500 rupees which supplies them with a cable that they enter to unlock the solar system. Customers can also top off their account with their cell phones.[5] This cell phone payment system is focussed on providing the solar energy to the rural India, where the customer has to purchase cards to unlock the systems. This concept should have been integrated with the banking systems where the customers could directly recharge and access their accounts.

C. **Mchek**: It allows a cell phone to act like a debit card. It is a mobile based secure transaction platform that can be used for remote authentication, authorization and notification of payments from bank account using mobile phone. Its services are available to almost everyone who owns a mobile phone and a bank account. SIM cards from Airtel, Vodafone, TATA IndiCom; TATA DoCoMo comes with the Mchek application preloaded. [6] This acts as an wallet with limited functionality and usability.

D. **UID Project**: Introduced in Jan 2010 introduces micropayment platform in order to facilitate banking in rural India. The platform enables Business Correspondents (who could be a local departmental shop owner) act as micro ATM to conduct instant transaction. [7] This project is still under implementation not knowing the actual benefits as yet.

E. **PayMate**: PayMate offers mobile payments solutions through tie-ups with Banks, merchants and other financial institutions. It had partnered Essar’s mobile retail chain Mobile Store to offer mobile payment services, and Tata Teleservices and Corporation Bank to offer a mobile money transfer service, named Green. It also operates mobile payment service in Sri Lanka, Nepal and UAE. It also offers merchant mobile POS solutions in the US through transaction service provider-TSYS. Also, it is a mobile based loan repayment service that is extended to
remote rural villages in the Ganjam district of Orissa through Dhanei Kshetriya –Gramin Financial Services (KGFS) registered agents. [8] This mobile payment solution is not universal i.e. it can only be used by Essar and Tata Teleservices.

The remainder of this paper is organized as follows: Section 2 presents related work. Section 3 presents the proposed model. Section 4 presents Technical requirements of Android, Biometrics elements required to implement the proposed work and NFC technology for P2P transactions. Finally, in Section 5 we conclude with key points Section 6 presents Discussion.

II. Related Work

J. Ondrus has suggested [9] and identified different types of mobile payments considering the type of transaction and the location of POS and the number of entities involved in it. Further, Ondrus presented an assessment for future mobile payment systems in Switzerland[10]. Another mobile payment concept has been developed and realized together with the Pay box solutions in Germany (Pay box). A. Arun Gnana Raj and et al. [11] proposed a Mobile Payment Consortium System (MPCS) framework for Mobile Payment System. This framework was designed and well suited to the academic institutions of India to carry out payments and financial services in payment of fees by students from the customer’s bank to the institutions bank where they study using mobile device anytime, anywhere. SEMOPS [12] was developed in context of a European Union (EU) funded project and is regarded as one of the most advanced universal and open payment systems. The second phase of SEMOPS has been launched, in order to proceed with the market validation of the SEMOPS service. Yong Xu and et al. [13] gave a mobile phone based third party secured payment modes in China. Vahid Rahimian and Jafar Habibi [14] illustrated the use of MPaySmart that provides ubiquitous, instant, anytime balance inquiry of accounts, along with the payment of bills, prepaid top-ups, payment to merchants, etc in Tehran. Delic and Vukasinovic [15] presents a mobile payment system implemented by mobile telephony of Serbia. This system utilizes the general three layer architecture of application interface layer, core payment system layer and bank interface layer. Another work in this area is conducted by Saxena et al. [16] in which mobile payment system called
MMPS is proposed as a framework for offering EMV compliant secure mobile to mobile financial transactions. They have provided a general description of their architecture, along with schematic transaction flows. Apostolos Kousaridas et al. [17] developed a universal architecture (OFSA), in Greece that supports mobile payments and mobile banking, taking into consideration the third and the emerging fourth generation communication technologies. Interaction and cooperation between payment and banking systems, integration of existing technologies and exploitation of intelligent procedures provides the prospects for the development of open financial services architecture (OFSA), which satisfies requirements of all involved entities. Apart from research, there are several payment systems that are used from the commercial perspective and are used successfully. Mobile FeliCa [18] Mobile Suica is the two successful solutions launched in Asian market. PayPal, PayBox, Mobipay, Nokia Wallet and Vodafone’s m-pay bill are also well known solutions for payment. Mobey Forum, Mobile electronic transactions and Pay Circle presents a complete view of mobile payments with reference to banking systems and financial institutions. [19, 20, 21, 22]

A. Current Limitations:

Usability along with security is always a challenge in mobile payments. Several applications are available globally with either the insufficiency in usability or with security (as discussed above). Hardware and software providers for the mobile market, as well as mobile network operators (MNO) and financial service providers, have attempted to specify guidelines for such systems [36]. According to the Unisys Security Index, seventy one percent of the 13,296 [37] consumers surveyed in fourteen countries would not consider online banking or shopping via mobile devices due to security concerns. Less than ten percent of respondents currently employ mobile devices to perform money transfers, credit-card transactions or deposits [38]. Secure strategies are essential to convince mobile users and financial service providers to make use of mobile payment transactions. One may argue that with improving technology it is possible to transplant heavyweight security architectures to mobile devices. However, current top-end devices [39] are too expensive for people, from economically underdeveloped areas.
Another problem facing current two-party mobile payment systems lies in the mobile service technologies employed in payment transactions. The existing mobile payment systems are mostly based on the Short Messaging Service (SMS) or the Wireless Application Protocol (WAP) [40]. However, SMS and WAP have technical limitations that make security architectures very difficult.

III. Proposed Work

The proposed model gives the flexibility to perform any payment or transaction, where no external entity is involved other than the bank. This model is based on customer centric and bank centric approach which is useful for both the bank as well as the user. The model has the three levels of security to authenticate the user. The first step in the proposed model is to check the first level of security i.e. in the form of account number and password. After entering the account number and password the system checks the validity of the user credentials. If the user enters the right account number and password the system enters into second level of security otherwise again asks for the account number and password. After authenticating the first level the system asks for the second level of security which is the biometric template of the user. The system verifies the biometric template of the user with the stored biometric template in the database. If the user enters the valid biometric template then the system enters the third level of security i.e. barcode. The system asks for the scanning of the barcode of the phone through which the transaction takes place. After scanning of the barcode of the phone the system asks for the type of transaction. Then, the system proceeds and enters in to the mode of transactions/payments otherwise it will continue asking the valid set of credentials till the loop ends (three times). Since, this model is also used for P2P transactions and it uses mobile wallet it becomes necessary to ask for the security of mobile device. After entering the security credentials the model gets activated and the user can perform any kind of payment or transaction. For P2P transactions or POS transactions this model is to implement the NFC technology. There are two different modes proposed in this work. In the first one, the mobile user interacts with the bank of his choice and performs different transactions according to his requirements, where security measures have also been taken into consideration (i.e. Authentication
can be done by multimodal biometrics and Password). By implementing the security measures the user can protect the mobile device as well as the transactions. After meeting the security requirements the user is able to do any type of transactions given in the choice. The model provides the feature of IMEI check. IMEI is the unique equipment identification number that is given to customer by service provider. The advantage of this number is that the payment model can be used with respective devices. If the IMEI number of the devices matches the number stored in the device then only user can proceed for further steps. In the second mode, the transaction can be done by integrating with the different service providers (Airtel, Idea cellular, Vodafone, and BSNL)

Notations of the symbols:

Ano = Account number
Pwd = Password
B (i) =Biometric template
Barcode = BB1
Chg = Change password
Cb = Current balance
Opwd = Old password
Npwd = New Password
Cp = Confirm password
M= Number of transactions
P = 3 (Maximum limit for checking authenticated user)
Ccp = Credit card payment
Dcp = Debit card payment
Barcode =Barcode Payment
Mobile banking = mbanking
Op = Option
Int ch
Char op

Begin
Enter the ano and pwd /* this statement will check the account no and password in the in
The database*/

Step 1 for i= 1 to p do /* Maximum limit to check the authenticated user*/
Begin
Enter the biometric template = B (i)/* this statement will check the biometrics in the form of iris
Scan, fingerprint, face recognition the database.*/

Begin
Enter the Barcode = BB1/* this statement will check the barcode of the product or device used for
doing payments.*/

Step 2 for i= 1 to p do /* Maximum limit to check the authenticated user */
Begin
If correct then go to step 3 else show message “Retry” go to step 2
If second attempt also fails it will again go to step 2 and give the message “Last
Attempt” else go to step 3.
In the third attempt if the user fails the application is closed with the message “Login Or password incorrect” else go to step 3.

Step 3 for i= 1 to m do /* Menu */

Begin

. The menu shows mobile authenticated user the different options:

Op “a”= Current Balance
Op “b”= Funds Transfer
Op “b1”= Obapay /* Payment by wallet*/
Op “b2”= M-chek /* Payment by wallet*/
Op “b3”= Paymate /* Payment by wallet*/
Op “b4” =PayPal /* Payment by wallet*/
Op “c” =Update account
Op “d” = Credit Card Payment
Op “e” = Debit Card Payment
Op “f” = P2P payment
Op “g” = Change Password
Op “h” = Cheque Clearance form
Op “i” = Demand Draft Clearance Form
Op “j” = Barcode Payment
Op “k” = Home page of the website.

. If the mobile authenticated user option is <= j do else go to Op “k”

Op “a”: Current Balance Form

Begin

. Click on the current balance of the account
. Display balance
End /* End Current Balance Form*/

Go to Op “k”

Op “b” = Funds Transfer Form

Begin

. Enter Ano and amount to be transferred which is provided in funds transfer Form along with bank name.
. Click on submit button
. If transaction is successful go to Op “k” else Op “b” = Funds Transfer Form

End /*End of Funds Transfer Form */

Op “b1”= Obapay/* Payment by wallet*/

Begin

. Enter the account no of the wallet
. Enter amount to be paid
. If another transaction to be done go to Op”b1” else Op “k”

End /* End of payment by Obapay*/

Op “b2”= M-chek /* Payment by wallet*/

Begin

. Enter the account no of the wallet
. Enter amount to be paid
. If another transaction to be done go to Op”b2” else Op “k”

End/* End of payment by M-chek*/

Op “b3” = Paymate /*Payments by wallets*/

Begin
. Enter the account no of the wallet
. Enter amount to be paid
. If another transaction to be done go to Op”b3” else Op “k”
End/* End of payment by Paymate*/

Op “b4”= PayPal

Begin
. Enter the account no of the wallet
. Enter amount to be paid
. If another transaction to be done go to Op”b4” else Op “k”
End/* End of payment by PayPal*/

Op “c” = Update account

Begin
. Click on Update Account
. Records will be automatically updated
End/* End of Update account*/

Op “d” = Credit Card payment

Begin
. Enter Credit card number
. Enter CVV (Card Verification Value) number
. Enter OTP
. Confirm Payment
. If another transaction to be done go to Op “d” else Op “j”
End /* End of Credit Card payment*/

Op “e” = Debit Card Payment

Begin
. Enter Customer Id or User name
. Enter Account password
. Enter OTP
. Enter Payment Password.
. Confirm payment
. If another transaction to be done go to Op “e” else Op “k”
End /* End of Debit Card Payment*/

Op “f” = P2P payment

Begin
. Establish a connection with the POS
. Select relevant card
. Enter PIN
. Authorizes the debiting of a specified merchant provided with amount
. The Transaction is authorized or declined
. Go to Op “k”
End /* End of P2P Payment */

Op “g” = Change password Form

Begin
. Enter the Opwd
. Enter Npwd
. Confirm Password
. Click on the submit button
. If the screen displays password changed successfully click on Op “k” else go to Op “g”
End /* End of Change Password Form*/

Op “h” = Cheque clearance form

Begin
. Enter the Cheque number and Cheque date
. Click on submit button
. If screen displays successful clearance click on Op “k” else go to “h”
End /* End of Cheque clearance Form*/
Op “i” = Demand Draft Form
   Begin
   . Enter DDno and DD date
   . Click on submit button
   . If screen displays successful clearance click on Op “k” else go to Op “i”
   End /* End of demand draft form*/
Op “j” = Barcode Payment
   Begin
   . Enter Barcode of the product
   . Verify with the URL or website
   . Decode the barcode
   . Authentication request for Payment Process.
   . Confirm payment
   . If another payment to be done go to Op “j” else Op “k”
   End /* End of Barcode Payment*/
Op “k” = Home page of the website
IV. Android, Biometrics and NFC Technology:

A. Android: Android is a set of software including an operating system, a middleware and key mobile applications for mobile devices utilizing ARM processors. (Advanced RISC Machine and Acorn RISC Machine) (Reduced instruction set computer (RISC)). Open Handset Alliance, a consortium of 86 hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. Google releases the Android code as open-source, under the Apache License. The Android Open Source Project (AOSP) is tasked with the maintenance and further development of Android. As an operating system, Android is lightweight with full features. Android allows developers to program in the Java language, to control the device via Google-developed Java libraries, and to run on the Linux 2.6 Kernel. One of the more exciting and compelling features of Android is that third-party applications are executed with the same system priority as those that are bundled with the core system in Android. It provides developers not only software development toolkits and a well-formed library, but also a right to access to anything that the operating system can access.

According to the Android Open Source Project its goal is to create a successful real-world product that improves the mobile experience for end users. AOSP also maintains the Android Compatibility Program, defining an "Android compatible" device as one that can run any application written by third-party developers using the Android SDK and NDK, to prevent incompatible Android implementations. The compatibility program is also optional and free of charge, with the Compatibility Test Suite also free and open-source. [25, 26, 27, 33, 34, 35]

- Android (SDK):

The Android software development kit (SDK) is a collection of a comprehensive set of development tools. It includes a debugger, libraries, a handset emulator based on QEMU (Quick EMUlator), documentation, sample code, and tutorials. Currently supported development platforms include computers running Linux (any modern desktop Linux distribution), Mac OS X 10.5.8 or later, Windows XP or later. The officially supported integrated development
environment (IDE) is Eclipse using the Android Development Tools (ADT) Plugin, though developers may use any text editor to edit Java and XML files then use command line tools (Java Development Kit and Apache Ant are required) to create, build and debug Android applications as well as control attached Android devices (e.g., triggering a reboot, installing software package(s) remotely). Enhancements to Android's SDK go hand in hand with the overall Android platform development. The SDK also supports older versions of the Android platform in case developers wish to target their applications at older devices. Development tools are downloadable components, so after one has downloaded the latest version and platform, older platforms and tools can also be downloaded for compatibility testing. Android applications are packaged in .apk format (application package file) and stored under /data/app folder on the Android OS (the folder is accessible only to root user for security reasons). APK package contains .dex files (compiled byte code files called Dalvik executables), resource files, etc.

- **Native Development Kit:**

Libraries written in C and other languages can be compiled to ARM or x86 native code and installed using the Android Native Development Kit. Native classes can be called from Java code running under the Dalvik VM using the `System.loadLibrary` call, which is part of the standard Android Java classes. Complete applications can be compiled and installed using traditional development tools. The ADB debugger gives a root shell under the Android Emulator which allows native ARM code or x86 codes to be uploaded and executed. ARM or x86 codes can be compiled using GCC on a standard PC. Running native code is complicated by the fact that Android uses a non-standard C library (libc, known as Bionic). The underlying graphics device is available as a framebuffer at /dev/graphics/fb0. The graphics library that Android uses to arbitrate and control access to this device is called the Skia Graphics Library (SGL), and it has been released under an open source license. Skia has backend for both win32 and UNIX, allowing the development of cross-platform applications, and it is the graphics engine underlying the Google Chrome web browser. Unlike Java App development based on the
Eclipse IDE, the NDK is based on command-line tools and requires invoking them manually to build, deploy and debug the apps. Several third-party tools allow integrating the NDK into Eclipse and Visual Studio. [25, 26, 27, 33, 34, 35]

- **Android Open Accessory Development Kit:**

  The Android 3.1 platform (also backported to Android 2.3.4) introduces Android Open Accessory support, which allows external USB hardware (an Android USB accessory) to interact with an Android-powered device in a special "accessory" mode. When an Android-powered device is in accessory mode, the connected accessory acts as the USB host (powers the bus and enumerates devices) and the Android-powered device acts as the USB device. Android USB accessories are specifically designed to attach to Android-powered devices and adhere to a simple protocol (Android accessory protocol) that allows them to detect Android-powered devices that support accessory mode it can be move.

**B. Biometrics:** To maintain the security the proposed model needs additional hardware in the form of biometrics. Biometric identification systems(BIS) is based around a core Automated Fingerprint Identification System AFIS that offers full biometric integration – with the inclusion of fingerprints, palm-prints, facial images, descriptive data, signatures and documents. Known as multimodal biometrics (or ‘fusion’ technology), this approach optimizes the results of search queries, consequently achieving more accurate responses. Common BIS elements include:

- **Data Server** – a central repository (e.g. Oracle database) for storage and near-immediate retrieval of biometric identifiers, together with associated features and textual data (known as ‘descriptor’ data).

- **Work stations** – equipped with a camera and scanner to enable the capture, encoding and submission of finger/palm-print images, slap impressions, rolled fingerprint images, photographs, signatures and demographic information.
• Review stations – designed for the dedicated review and verification of search results, as well as match analysis.

• Live verification stations – allow the identification of individuals when the subject is present at the time of processing.

• Optional peripherals – portable and single-finger scanning devices, cameras, two/ten-print card printers, automated case management systems, web servers, application servers, mobile gateways, descriptor import/export modules.[28]

**C. NFC Technology**

For P2P transactions the proposed model requires the NFC technology. NFC is a short range and standardised (ISO 18092) wireless communication technology that adds contact less functionality to mobile devices including mobile phones and PDA’s (Personal Digital Assistants). Such devices can act both as a “contactless card” (based on its secure element ) and as a “contactless reader” and also operate in P2P mode with peer devices. The technology used in NFC is compatible with existing contactless infrastructure and NFC device offers three operating modes.

• Reader/Writer mode: In this mode the NFC device can read or write information such as URLs, SMS’s in a tag or smart card e.g. Smart posters applications. Here, users touch the device or a cell phone with the tag embedded in the poster, which triggers the transmission of a URL to the phone. The URL could be used to open the web browser without any human intervention.

• Card Emulation mode: In this mode the NFC enabled device emulates a contactless smartcard (ISO 14443). In this case there is a secure element embedded in the device where sensitive data can be stored in a safe place and value added services requiring a high level of security such as payment applications can be made available to the customers.
Peer-to-Peer mode: In this mode a connection is established between two NFC enabled devices and data can be exchanged between them. The NDEF (NFC Data Exchange format) is used to transmit data. This mode is standardized on ISO 18092.[29,30,31,32]

V. IMPLEMENTATION RESULTS:
The Proposed model has been implemented on Samsung Galaxy Tab2. The technical specifications of the mobile device are as under:

Features:
Emulator: Android 2.3 SDK
OS : AndroidOS, v4.0.3 (Ice Cream Sandwich)
Chipset : T1 OMAP 4430
CPU : Dual-core 1 GHz
GPU : PowerVR SGX540
Sensors : Accelerometer, gyro, proximity, compass
Messaging : SMS (threaded view), MMS, Email, Push Email, IM, RSS
Browser : HTML5, Adobe Flash
GPS : AGPS support and GLONASS
Java : Java MIDP emulator
USB : microUSB v2.0, USB On-the-go support

Data:
GPRS: Class 33
EDGE: Enabled
Speed: HSDPA, 21 Mbps; HSUPA, 5.76 Mbps
WLAN : Wi-Fi 802.11 a/b/g/n, DLNA, Wi-Fi Direct, dual-band, Wi-Fi hotspot
Bluetooth: v3.0 with A2DP, HS

Memory:
Card slot: microSD, up to 32 GB
Internal : 8/16/32 GB storage, 1GB RAM

General:
2G Network: GSM 850 / 900 / 1800 / 1900
3G Network: HSDPA 900 / 2100 - GT-P3100, HSDPA 850 / 900 / 1900 / 2100 - GT-P3105

Camera:
Primary : 3.15 MP, 2048x1536 pixels
Features: Geo-tagging, smile detection
Video 720p@30fps
Secondary: VGA
Display:
Type: PLS LCD capacitive touch screen, 16M colors
Size: 600 x 1024 pixels, 7.0 inches

Body:
Dimension: 193.7 x 122.4 x 10.5 mm
Weight: 345 g
Welcome to XYZ Corp.

I would like to:

- Check Current Balance
- Make Funds Transfer

Make Payment By: 

Credit Card Payment
Debit Card Payment

Your current balance is: 100000 INR

Click here to proceed!

Scanning your biometrics

Registered IMEI: 357952004387510
Phone IMEI: 357952004387510

Proceed
VI. Discussion:
The objective of the transactional model is to provide flexibility and user friendliness. Since this model is based on customer centric and bank centric approach that is useful for both the bank as well as the user. In addition, this model is a mobile payment application that can be used by the remote as well as rural India. This application provides the security features for transaction of money from the bank account. As this application works on different technologies, various features are being provided to the users. The biometrics helps in maintaining the security of the application. Only the verified user can use this application. The Account Number and PIN is stored in encrypted form with no chance of hacking the same. The application uses PKI infrastructure to maintain the encryption keys. Also barcode payment facility is provided to the users which lead to the authenticity of the products purchased with no cognitive energy. NFC technology used provides the instant transfer of money from the account without storing the money anywhere with no chance of threat to the transaction. From the banking perspective this application can be used for one and all types of banking transactions whether for credit payments, money transfer or getting electronic check book. In addition, this application has a facility to use the wallet present within it. In wallets the legal tender or currency gets converted into electronic money or tokens which are used for transactions. And above all, this application is only used for respective mobile devices i.e. this application asks for IMEI (International Mobile equipment Identity) number which is unique to every mobile device. If the IMEI number entered is correct than only the application gets activated.

VII. CONCLUSION:
The paper proposes a user friendly model of payment. This model provides the various modes of payments that are useful to the people in India especially the rural areas where the literacy rate is low. Technically the proposed work takes different challenges into consideration from implementation point of view. The scope of the proposed work is the combination of Android, Biometrics, NFC technology overcoming the technical limitations and the security considerations.
The proposed work is beneficial from banking perspective as Reserve Bank of India has proposed a regulatory framework for mobile transactions.

References:
Ms. Vibha Kaw Raina, pursuing PhD (Computer Science) is an Assistant Professor in Birla institute of Technology, Mesra; Ranchi (Extension Centre, Noida) has ten years teaching experience in the field of Computer Science and Management. She has done Masters In Computer management from University of Pune, and Post Graduation Diploma in Computer Applications from Brainware Software Developers, affiliated to University of Jammu. She is currently the member of ACM. 

She may be contacted at the following address:  
Ph : +91-98181-38800, Email Id : kawvibha@yahoo.com ;

Dr U S Pandey, PhD (Computer Science) is an Associate Professor in School of Open Learning, University of Delhi, Delhi having twenty years teaching experience in the field of Computer Science and supervising many research scholars in the field of Mobile Commerce, Artificial Intelligence, Expert System, Data Warehouse, Data Mining, e-learning and e-governance. Dr. Pandey has got published two books and many research papers. Dr. Pandey has worked as Professor & Director of VIPS affiliated to GGSIP University Delhi.

He may be contacted at the following address:  
Ph:+91-98911-11703, Email Id: us_pandey@hotmail.com
Dr. Munish Makkad, PhD (Finance), Department of Commerce, Delhi School of Economics, University of Delhi. M.Com, University of Delhi. Dr. Munish has over 35 years of experience in teaching, research and consultancy in India and abroad. He has co-authored and co-edited 4 books on accounting, and published several articles in the journals of repute. He has presented papers at national and international seminars/conferences. He is also member of team for developing study material for undergraduate programme of Indira Gandhi national Open University. Currently he is working as Professor of Accounting and Finance at Birla Institute of Technology, Mesra; Ranchi (Extension Centre, Noida).

He may be contacted at the following address:
Email Id: munishbit@gmail.com