

ISSN 0974-763X

# **SOUTH ASIAN JOURNAL OF MANAGEMENT RESEARCH (SAJMR)**

Volume 13, No. 1

January, 2023



**Chhatrapati Shahu Institute of Business  
Education & Research (CSIBER)**

(An Autonomous Institute)

University Road, Kolhapur-416004, Maharashtra State, India.

# SOUTH ASIAN JOURNAL OF MANGEMENT RESEARCH (SAJMR)

ISSN 0974-763X

(An International Peer Reviewed Research Journal)

Published by

**CSIBER Press, Central Library Building**

**Chhatrapati Shahu Institute of Business Education & Research (CSIBER)**

University Road, Kolhapur - 416 004, Maharashtra, India

Contact: 91-231-2535706/07 Fax: 91-231-2535708 Website: [www.siberindia.co.in](http://www.siberindia.co.in)

Email: [sajmr@siberindia.co.in](mailto:sajmr@siberindia.co.in), [sibersajmr@gmail.com](mailto:sibersajmr@gmail.com)



## ■ *Chief Patron*

**Late Dr. A.D. Shinde**

## ■ *Patrons*

**Dr. R.A. Shinde**

Secretary & Managing Trustee

CSIBER, Kolhapur, India

**CA. H.R. Shinde**

Trustee Member

CSIBER, Kolhapur, India

## *Editor*

**Dr. R.S. Kamath**

CSIBER, Kolhapur, India

## ■ *Editorial Board Members*

**Dr. S.P. Rath**

Director, CSIBER, Kolhapur

**Dr. Francisco J.L.S. Diniz**

CETRAD, Portugal

**Dr. Paul B. Carr**

Reent University, USA

**Dr. T.V.G. Sarma**

CSIBER, Kolhapur, India

**Dr.C.S.Kale**

CSIBER, Kolhapur, India

**Dr. K. Lal Das**

RSSW, Hyderabad, India.

**Dr. Nandkumar Mekoth**

Goa University, Goa

**Dr. Gary Owens**

CERAR, Australia

**Dr. P.R. Puranik**

NMU, Jalgaon, India

**Dr. Rajendra Nargundkar**

IFIM, Bangalore, India

**Dr. Yogesh B. Patil**

Symbolis Inst. Of International Bsiness, Pune, India

**Dr. R.M. Bhajracharya**

Kathmandu University, India

**Dr. K.V.M. Varambally**

Manipal Inst. Of Management, India.

**Dr. B.U. Dhandra**

Gulabarga University, India

**Dr. K.N. Ranbhare**

CSIBER, Kolhapur, India

**Mr. S.H. Jagtap**

CSIBER, Kolhapur, India

**Dr. Pooja M. Patil**

CSIBER, Kolhapur, India

## ■ *Type Setting & Formatting*

**Mr. S.Y. Chougule**

# South Asian Journal of Management Research (SAJMR)

Volume 13, No. 1

January, 2023

## C O N T E N T

---

### Editorial Note

- Electoral Democracy and Citizen Life Satisfaction : The Mediating Role of Public Trust**  
**Deribe Assefa Aga**, Department of Public Management, Ethiopian Civil Service University, Addis Ababa, Ethiopia 1 – 14
- The Influence of Organizational Culture on Employees' Commitment in Civil Service Organizations: The Cases of Selected Cities in Ethiopia**  
**Terefe Zeleke**, Ethiopian Civil Service University, Addis Ababa, Ethiopia 15 – 34
- Determinants of Structure Plan Implementation: Perception of Residents in Sebeta City, Next-door of Addis Ababa, Ethiopia**  
**Degu Bekele**, College of Urban Development and Engineering, Ethiopian Civil Service University, Addis Ababa, Ethiopia 35 – 44
- Social Networking and Public Participation As A Vital Entry Elements for Improving Municipal Governance and Service Satisfaction: Evidence from Ethiopia**  
**Dr. Meresa Atakltiyand Dr. Kanchan Singh** 45 – 60  
College of Urban Development and Engineering, Ethiopian Civil Service University, Addis Ababa, Ethiopia
- A Case Study On The Environment Management System of Bauxite Mine**  
**Dr.A.R.Kulkarni** , Prof. & Head, Dept. of Env't. Mgt.  
Chhatrapati Shahu Institute of Business Education And Research, Kolhapur, Maharashtra, India 61 – 69  
**Shri. Mainak Chakraborty**, Vice President & Head of Mines & **Shri. V.K.Chauhan**, Gen.Manager Mines, Hindalco Industries Ltd.
- Security Model for Banking Domain Based on Cardless QR Code Transactions**  
**Dr. Vaishali P. Bhosale**, YCSR, Shivaji University, Kolhapur, India 70 – 85  
**Dr. Poornima G. Naik**, Department of Computer Studies, CSIBER, Kolhapur, India  
**Mr. Sudhir B. Desai**, YCSR, Shivaji University, Kolhapur, India
- Behavioral Health Integration for India's Pediatric Population for Social Workers**  
**Kennedy L. Paron**, College of Health Solutions, Arizona State University, USA 86 – 102
-

---

<b>State of Solid Waste Management Challenges as Exacerbated by COVID-19 Pandemic Related Littering in Addis Ababa City Administration.</b>	
<b>Markos Sintayehu Metaferia</b> , College of Urban Development & Engineering , Department of Environment & Climate Change Management, Ethiopian Civil Service University,AA, Ethiopia.	103 – 122
<b>Challenges for Teachers in E-education Transformation at Yangon University of Education</b>	
<b>Nay Mar Soe</b> , Professor & HOD Department of Chemistry, Yangon University of Education, Myanmar	123 – 127
<b>The Effects of Organizational Culture on Employee Commitment as Mediated by Job Satisfaction in Addis Ababa City Administration</b>	128 – 143
<b>Zewdie Zakie Koyira</b> , Consultant at Leadership, Policy & HR training Center, Ethiopian Civil Service University, Addis Ababa, Africa	
<b>Interrogating the Non-Anthropocentric Claims of African Environmental Ethics</b>	144 – 149
<b>Egbeji, Patrick Odu</b> , Department of Philosophy and Religious Studies, Faculty of Arts, Nasarawa State University, Keffi, Nigeria	
<b>Building Human-Environmental Friendly City Through Linking Ecological Research and Social Science</b>	150 – 156
<b>Chali Etefa Taye</b> , Ethiopian Civil Service University, Addis Ababa, Ethiopia, Africa	
<b>A Study on the Potentiality of Sustainable Ecotourism In Dawei and Myeik at Tanintharyi Region</b>	157 – 165
<b>Tin Aung Lwin</b> , Department of Economics, Yangon University of Education, Myanmar	
<b>Analysis of Bandish, Aalaps and Taans of Raga in Indian Classical Music Using N-grams</b>	166 – 171
<b>Omkar Barve</b> , Department of Computer Studies, Chhatrapati Shahu Institute of Business Education and Research, Kolhapur, Maharashtra, India	
<b>Akhtar Mohammad Shaikh</b> , Department of Electronics, The New College, Kolhapur, Maharashtra, India	
<b>Effective Use of Human Asset in Higher Education By Using ICT</b>	172 – 179
<b>Nivas Mane</b> , Research Scholar, Dept of commerce and Management, Shivaji University, Kolhapur, Maharashtra, India.	
<b>Dr. C.S. KALE</b> , Chhatrapati Shahu Institute Of Business Education & Research,, Kolhapur, Maharashtra. India	

---

# Security Model for Banking Domain Based on Cardless QR Code Transactions

**DR. VAISHALI P. BHOSALE**

Yashwantrao Chavan School of  
Rural Development,  
Shivaji University,  
Kolhapur, India

**DR. POORNIMA G. NAIK**

Department of Computer Studies  
CSIBER,  
Kolhapur, India

**MR. SUDHIR B. DESAI**

Yashwantrao Chavan School of  
Rural Development,  
Shivaji University,  
Kolhapur, India

---

**Abstract:** In the modern digital era, traditional banking is slowly becoming obsolete and is being replaced with mobile banking which has resulted in improved customer service in a banking sector. Convenient banking enables the customer to perform the financial transactions from anywhere at any time irrespective of the time zone and the geographical location where the customer is located. At the same time mobile apps are growing to be more and more power day by day offering a wide range of services to the end users. This prevents a customer from physically visiting the bank of availing different services. However, all this does not come for free. There is a cost involved. Convenience comes at the cost of security breaches. If the proper security measures are not taken care of in the design of mobile app it will have adverse effects which can prove to be costly in the long run. In the current research the authors have designed a model for secure banking solution based on QR Code transactions and QR Code based wallet. The encryption key is selected with an objective of key space minimization. The different RBI norms are integrated into the model to render it acceptable by any authorized bank. The layered security model is designed to address various security vulnerabilities that might creep in during transaction processing.

**Keywords:** ATM, Authenticity, Card-less Cash, Confidentiality, Integrity, Mobile Banking applications, QR code.

---

## 1.0 Introduction

The innovation of a mobile banking app has eliminated the need for physically visiting the bank by enabling the execution of any financial transaction such as inter or intra bank funds transfer, UPI, e-Passbook, bill payments and ticketing, mini account statement, branch locator, ATM locator etc. remotely irrespective of time zone and geographical location with a single button click. Hence the customers can reach their respective banks virtually through their mobile phones. In the COVID-19 pandemic situation financial transactions using Mobile Banking Apps became more popular (Varsha Agarwal 2020, Singh et al 2017).

## 2.0 Literature Review

There is lot of research currently being actively carried out in integrating security with banking solutions. Most of this work focuses on card-based transactions. For standardizing the mobile operations and securing the transactions RBI has brought out a set of operating guidelines to be adopted by all banks which are interested in rendering their services through their mobile apps. After downloading and installing a mobile banking app on mobile device, users can perform various financial transactions (Parul Deshwal 2015, Reshma S. et al 2017, Mirjana P. B. et al. 2020). Newly added services include one of card-less cash transactions. Several banks have launched the 'Card-less Cash Withdrawal' facility in their ATMs. Customers can withdraw cash securely and conveniently from ATMs. This facility can be used only on the respective bank's ATMs. iMobile by ICICI also allow Cash withdrawal at the local shop. Around 5 lakh local shops avail this facility. No other bank has this facility of card-less cash withdrawal at local shops. HDFC allow card-less cash withdrawal using net-banking facility. Option of providing QR based card-less ATM cash withdrawal service is also made available by SBI using YONO Lite App (Calin-Mihai Istrate 2014, Khaled Aldiabat et al 2019, Saprikis, V. et al. 2022).

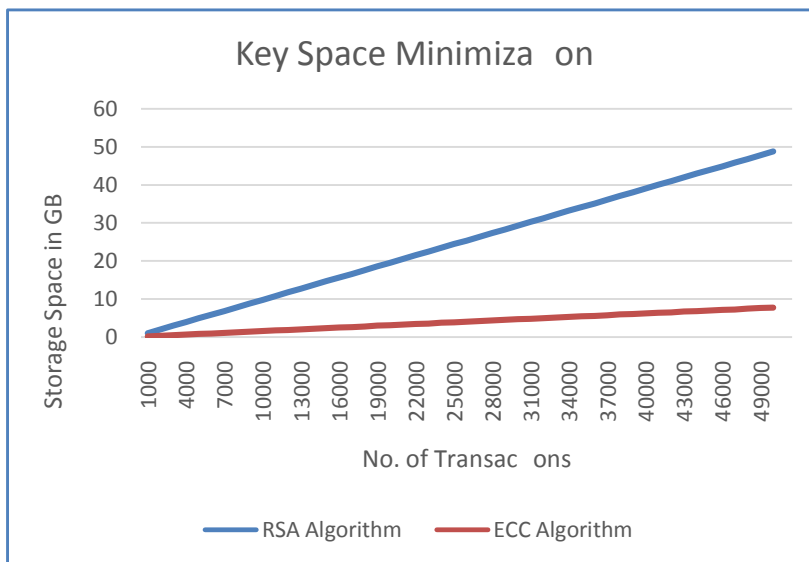
### 3.0 Design of a Model for Secure Banking Transactions based on QR Code

The current research is divided into the following phases:

**Phase 1:** Selection of Encryption key with an objective of keyspace minimization.

In the current research authors employ asymmetric key encryption based on Public Key Infrastructure (PKI) for securing a QR Code in which a public/private key pair is generated by the sender. Either of the key can be used for encrypting the message. The message which is encrypted using public key can only be decrypted using the corresponding private key and vice-versa. For asymmetric key encryption RSA algorithm based on modular arithmetic is a good choice. However, as recorded in history on two occasions RSA algorithm has been compromised for the key sizes of 256 bits and 512 bits. Hence the only secure and reliable key size is 1024 bits. The same security can be achieved using Elliptic Key Cryptography (ECC) for the key size of 160 bits. Hence there is a huge reduction in key space by ~84% if RSA algorithm is replaced with ECC algorithm. As the no. of transactions grow exponentially, it would result in huge preservation of key spaced as depicted in Fig 1.

Fig 1. Key Space Minimization



A word of caution. None of the encryption algorithms existing today are quantum immune. If the quantum computers are realized in future, the entire crypto system is going to break and the entire crypto system needs to be redefined. The active research is being conducted in both these areas of quantum computing and security implications of quantum computing. The solution is based on N-

dimensional lattice theory.

**Phase 2:** Integration of few prominent RBI norms in the model implementation.

This phase focuses on few prominent RBI norms employed during the implementation of the mobile banking app:

1. Frequent connections to the bank server must be avoided.
2. Technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity and non-repudiation.
3. All mobile banking transactions involving debit to the account shall be permitted only by validation through a two factor authentication.
4. Proper level of encryption and security shall be implemented at all stages of the transaction processing.

All the above mentioned RBI norms have been taken care of in the model design.

The first RBI norm is taken care of employing disconnected database architecture. A typical user can possess more than one account with the bank. First time the user connects to the banking

server all the pertaining data is pulled from the database and stored on the client-side in the form of different DAO (Data Access Object) classes conforming to Plain Old Java Objects (POJO). All the processing will take place on the client side and the subsequent connection to the bank server is only established for updating the data to the server.

Most of the high level languages such as Java, Python etc. support security APIs and packages for incorporating authenticity, integrity, validity and non-repudiation into the model implementation. This addresses the second RBI norm.

Most of the banking applications use multi-factor authentication (at least two-factor authentication) for authenticating the user. Authentication refers to proving the identity of the user. There are three categories of authentication:

**Category 1:** What the user knows : - It could be password, pin etc., which is confidential and known to only that user and is remembered by the user.

**Category 2:** What the user has : - It could be any gadget which the user owns, such as credit card, debit card, hardware token, software token, or any device which is owned by the user.

**Category 3:** What the user is :- It refers to the biometric identity of the user such as iris, finger prints or facial recognition of the end user.

For multifactor authentication, two different authentication mechanisms from at least two different categories are to be selected. For example, banking applications employ authentication mechanisms from first two categories, username/password combination, and OTP which has been sent to the registered mobile of the user.

The model is based on PKI infrastructure employing public/private key pair for securing transaction at all stages of its processing which takes care of RBI norm 4.

### Phase 3: Working of Model

Fig 2 shows the sequence diagram for the generation of QR Code.

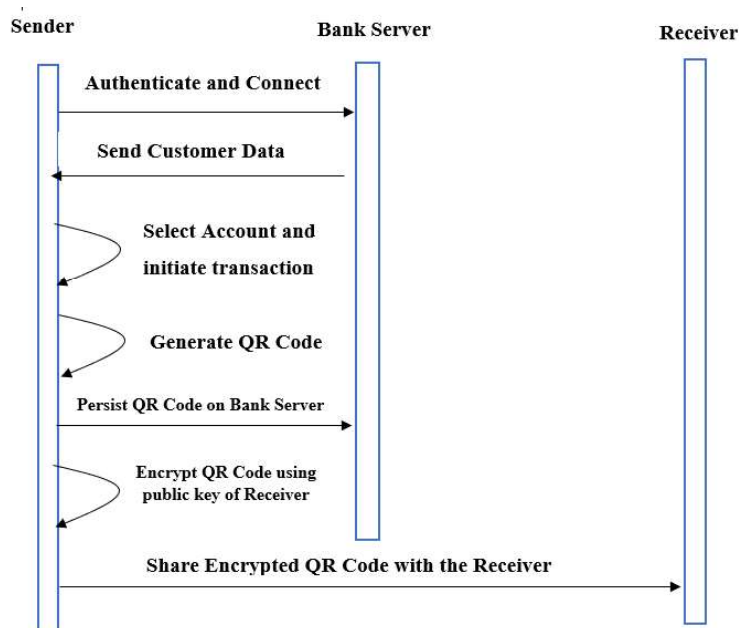


Fig 2. Sequence Diagram for QR Code Generation

We will consider a scenario where A wants to transfer some amount to B. For the execution of the transaction smoothly the following pre-requisites should be met:

- Both A and B must be account holders of the bank since the model deals only with the intra bank transactions.
- A must perform the transaction from his registered mobile device.

## Generation of QR Code

The prominent steps involved in the generation of QR code holding the transaction information are depicted below:

- A sends a connection request to the bank server using his registered mobile device.
- On proper authentication with the bank server, the connection is established.
- A enters the transaction details, on successful validation of transaction data (account type, amount, balance) OTP is generated by the system for 'withdraw' transaction and sent to the registered mobile device of user A.
- A's mobile device retrieves OTP from the system and generates the QR code. If the user A is operating from another device, the transaction is aborted.
- A will request public key of B and encrypts the QR code using public key of B.
- The QR code encrypted with the public key of B is shared with B. This is another level of security. If the QR code of B is compromised and a hacker gets an unauthorized access to the QR code, he will not be in a position to decrypt it since the corresponding private key is owned by B.
- The unencrypted version of the QR code is also stored on the bank server.

The data stored in a QR Code for 'withdraw' and 'deposit' transactions is shown below:  
For Withdraw transactions:

### Withdraw Transaction

- Customer ID
- Customer Name
- Account ID
- Date and Time of Server when the QR Code is generated
- Amount
- Unique 10-digit Transaction ID

For Deposit transactions:

### Deposit Transaction

- Customer ID
- Customer Name
- Account ID
- Date and Time of Server when the QR Code is generated
- Amount
- Denominations
- Unique 10-digit Transaction ID

The validity of the QR Code generated by the system is 6 hours. Encashment request can be generated and send to the cashier by the customer by using the above system generated QR code at any time within 6 hours of generation of QR code

The naming convention used for QR code generated by the system is 'qrcode\_year\_month\_day\_hour\_min\_sec.png' where date and time correspond to the date and time when the QR code is generated as depicted in Fig 3.

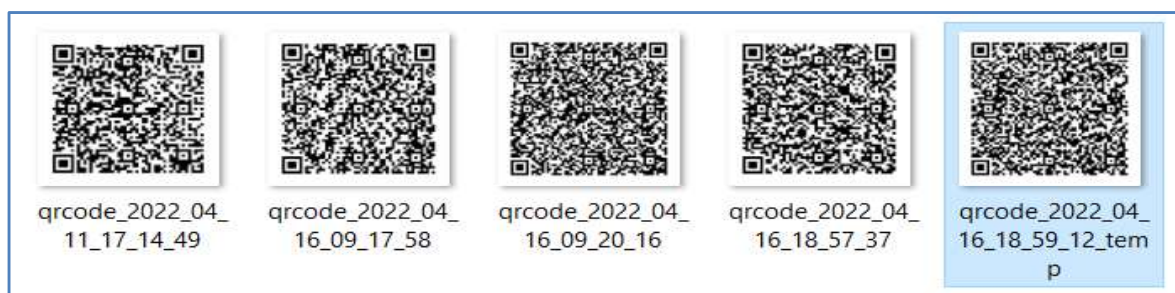


Fig 3. QR Codes Generated by the System

The above data is encrypted using the private key of the sender and is then concatenated with the public key of the sender before storing in QR code.

**QR Code Data  $\rightarrow$  Public key of sender + E {Cust\_id + cust\_name + account\_id + date and time on server + amount + denominations + trid (10 digit)} Private key of sender**

Let D represent the QR code transaction data.

**$D = \text{Cust\_id} + \text{cust\_name} + \text{account\_id} + \text{date and time on server} + \text{amount} + \text{trid (10 digit)}$**

**Doubly Encrypted QR Code = {Public Key of A + E(D) Private Key of A } Public Key of B**

**Phase 4:** Design of layered security model.

- Both the sender and the receiver must be account holders of the bank.
- The sender can initiate the transaction and generate the QR Code only from his/her registered mobile.

In the current security model, the following securities are addressed during transaction processing:

1. **Validation of MAC Address :** When the cashier sends the connection request to the bank server, the MAC address of the cashier's machine is retrieved and sent along with the request to the bank server. Bank server maintains a list of allowed MAC addresses of the cashier's machine. The MAC address of the cashier initiating the transaction is looked up in the MAC table and if it is present, then the connection is accepted else is rejected. This is the first level of security which prevents a hacker from initiating the transaction from his machine.

2. **Authenticity** - QR Code is generated by the system : A copy of QR Code generated by the system is stored on the bank server. The naming convention used for the generated QR Code is

**<QRCode\_year\_month\_day\_hour\_min\_sec>**

where, year, month, day, hour, min, sec refer to the timestamp when the QR Code was generated. As a first security check, the date and time when the QR Code was generated by the system was retrieved from the QR Code and was compared to its filename.

If the first security check passes, then the second security check was initiated which retrieves the transaction id from the QR code and compares it with the transaction id of the QR code stored on the bank server. If both match, it is guaranteed that the QR code is indeed system generated.

**3. Integrity-** QR Code data is not tampered with since its generation: For verifying the integrity of QR Code data, the SHA-2 hash of the data stored in the scanned QR code is compared with the SHA-2 hash of the data stored in the bank server. If the two match, the integrity of QR Code data is proved which means the QR code data is not tampered since it is generated.

**4. Validity** - QR code is begenerated before six hour : To prove the validity of QR code, the date and time when the QR code is generated was compared with the time at which the transaction is processed. If it is less than 6 hours, then the QR code is declared as valid else is invalid.

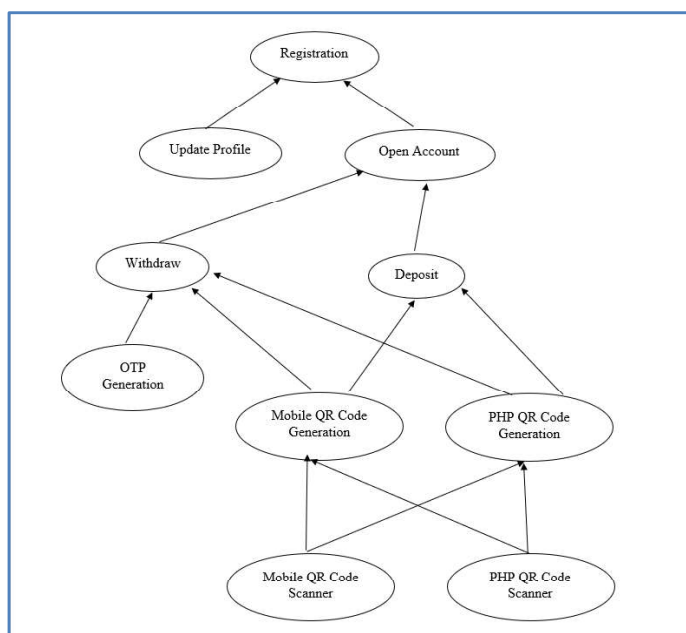
**5. Non-repudiation** - QR code is decrypted using public key of sender : If the QR code data can be decrypted using the public key of the sender which is stored in QR code, it proves that the QR code has indeed been generated by the sender.

**6. Double spending problem** - Transaction table has trid as primary key : Since trid is a primary key in transaction table, duplicates are not allowed which automatically takes care of double-spending problem.

Each layer is a micro service rather than monolithic system to account for distributed banking database where data processing is distributed. If a bank adopts storing the data in a distributed database, it would be cumbersome and time consuming to process the transactions employing the systems based on monolithic systems.

Modules Designed in the System and Module Dependency Diagram.

The system comprises of the following discrete modules.



1. Registration Module
2. Update Profile Module
3. Open Account Module
4. Withdraw Module
5. Deposit Module
6. OTP Generation module.
7. Mobile QRCode generation module.
8. PHP QRCode generation module.
9. Mobile QRCode Scanner module
10. PHP QRCode Scanner module.

The dependency between different modules is depicted in Fig 4.

Fig 4. Module Dependency Diagram

**Phase 5:** Processing Encashment Request by the User B. : Fig 5. shows sequence diagram for transaction processing.

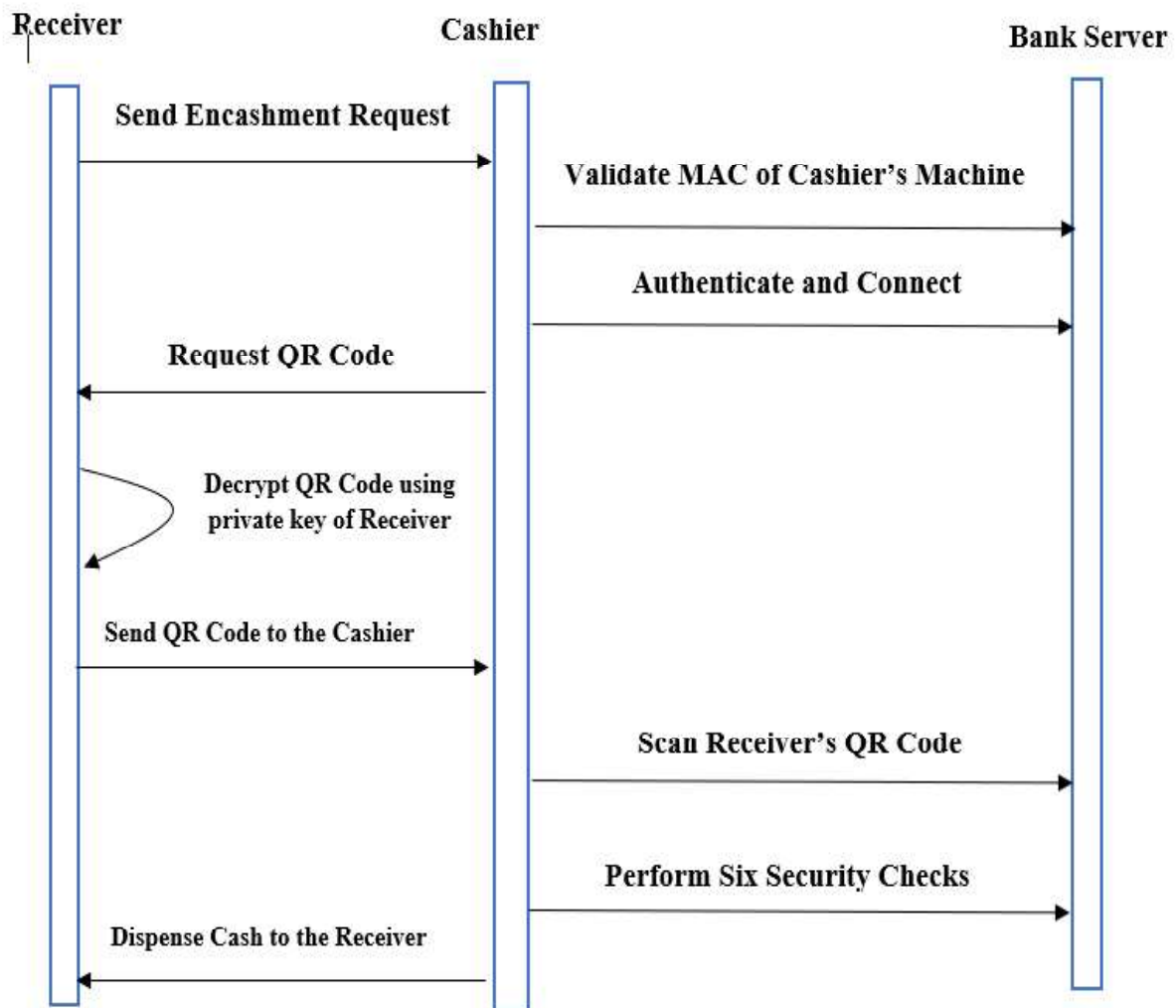


Fig. 5. Sequence Diagram for Transaction Processing

When the user B wants to encash his QR code within six hours of its creation, decrypts the QR code using his private key. B visits the bank physically and requests encashment to the cashier. The prominent steps involved in processing the transaction are depicted below:

- The cashier sends a connection request to the bank server.
- The bank server validates the cashier's machine from where the request is generated by retrieving the MAC id of the cashier's machine.
- On successful validation, cashier is prompted for username/password pair.
- On successful authentication, cashier is connected to the bank server for initiating the transaction.
- Cashier scans the QR code which performs several security checks are performed as depicted below:
  - Validity of QR Code
  - Integrity of QR code
  - Non-repudiation
  - Double spending of QR Code
- On successful security checks, the requested cash will be handed over to B.

**Phase 6:** Possible QR Code hacking attempts and proposed solutions : QR Code Hacking Attempts

Suppose A is a sender and B is a receiver

1. Hacker will generate a fake QR code by studying the data stored in it. Two cases arise:  
Case 1: Hacker is an account holder and has not performed any transaction which means the public key will not be available on the server. Hence the transaction will be aborted.  
  
Case 2: Hacker is an account holder and has performed at least one transaction which means the public key will be available on the server. Corresponding transaction id is not present and hence the QR Code is fake and as such will be rejected.
2. H Requests B for QR Code. Data is encrypted using private key of H. B Uses public key of H to decrypt QR Code data. Changes the amount, encrypts it using his private key and replaces public key with his own public key.

Data present in original QR Code

public key of B  
E(D) Private key of B

Data present in tampered QR Code

public key of H  
E(D') privatekey of H

3. Hacker tries to change the date and time of the server recorded in QR Code. : Hash of scanned QR code does not match with the version of QR code stored on server and hence integrity fails
4. Double spending problem.: Double spending problem is genuinely addressed by making the unique transaction id generated and stored in the QR code is declared as a primary key in the transaction table which means not duplicates are allowed.

The layered security model consists of security header consisting of six bits corresponding to six security checks as depicted in Fig. 6.

Successful Validation of MAC Address of Cashier Machine	1	0	0	0	0	0
Non Repudiation	1	1	0	0	0	0
Authenticity of QR Code	1	1	1	0	0	0
Integrity of QR Code Data	1	1	1	1	0	0
Time Validity of QR Code	1	1	1	1	1	0
Double Spending Problem	1	1	1	1	1	1

Fig 6. Layered Security Model with Security Header

3 level authentication system has been explored by different researchers (Velasiri Dwarakamayi Amareswari et al 2021). Multi-layer security model has been designed and implemented by the authors to keep track of different security vulnerabilities. In the above layered security model, each layer updates a 6-bit header and sends it to the next layer. At the end of the sixth layer, the 6-bit header encapsulates the various security checks performed at each layer. Bit 1 indicates a security check is passed and 0 indicated the failure of security check. For example, the following six bit header indicates that the QR code is indeed generated by the sender, the request is indeed

generated by the cashier, the QR is system generated and QR code data is not tampered. However, the QR code is generated before six hours and hence is invalid. Hence the transaction is aborted. Transaction is successful if all the bits in the security header contain 1.

1	1	1	1	0	0
---	---	---	---	---	---

**Phase 6:** Designing QR Code based wallet : The work can be extended to create a QR code based wallet since each QR code is associated with a monetary value. The wallet contains the public/private key pair along with the QR codes shared by the senders.

Description of Different Activities Employed in Software Implementation

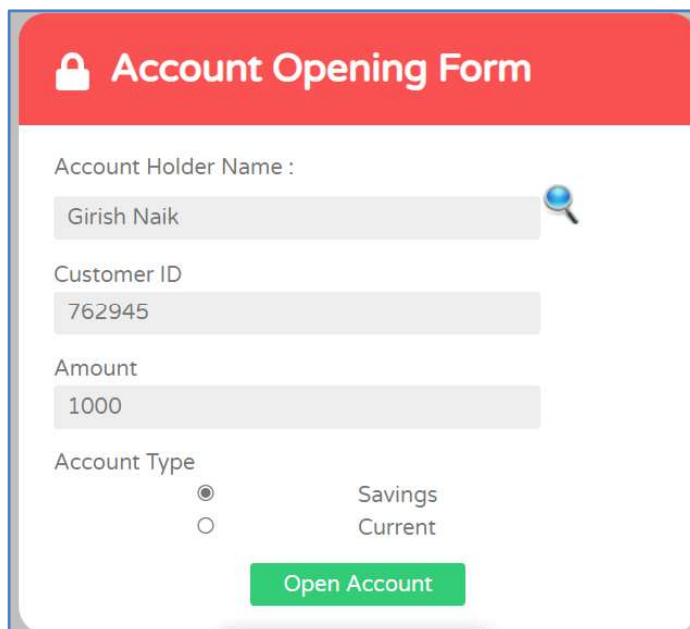
Sr. No	Name of the Activity / Class	Description	Name of the Layout File
1.	HomeActivity	Launcher Activity containing main menu.	activity_home.xml
2.	MainActivity	Displays Login Form for authenticating the user.	activity_main.xml
3.	Customer	POJO class for storing customer information of logged in customer	N/A
4.	Account	POJO class for storing account information of logged in customer	N/A
5.	AccountActivity	Asynchronous task for invoking PHP script for creating account of user on bank server.	N/A
6.	AccountOpenActivity	Generates a random account no. and starts AccountActivity for creating account of user on bank server.	activity_open_account.xml
7.	CashierDashboardActivity	Displays cashier dashboard	activity_cashier_dashboard.xml
8.	CustomerDashboardActivity	Displays dashboard for customer.	activity_customer_dashboard.xml
9.	CustomerRegisterActivity	Persists customer registration information on PHP bank server using Asynchronous task.	N/A
10.	DepositActivity	Generates request for deposit transaction.	activity_deposit.xml
11.	ErrorActivity	Displays error page for authentication failure.	activity_error.xml
12.	IntegrityFailureActivity	Displays error page on integrity failure.	activity_integrity_failure.xml
13.	LogoutActivity	Logs out the currently logged in user from the system.	activity_logout.xml
14.	MobileQRGenerateAct	Generates a QRCode for the requested	activity_mobile_gene

	ivity	transaction and stores it in documents/qrcode folder in a mobile.	rate.xml
15.	OperationActivity	Displays a screen for performing withdraw/deposit transactions.	activity_operation.xml
16.	OTPActivity	Generates OTP for multi factor authentication.	activity_otpactivity.xml
17.	PerformTransaction	Asynchronous task for executing transaction on bank server using PHP from mobile.	N/A
18.	PHPQRGenerateActivity	Generates QRCode for withdraw/deposit transaction on the server.	activity_phpqrgenerate.xml
19.	ProfileUpdateActivity	Updates the profile of the customer	
20.	QRCodeActivity	Displays the transaction information for customer verification and allows the user to navigate to customer dashboard.	activity_qrcode.xml
21.	QRGenerateActivity		
22.	QRReadActivity	Reads the data of the QRCode scanned by the user on mobile.	activity_qrread.xml
23.	RegisterActivity		activity_register.xml
24.	SigninActivity	Asynchronous task for connecting to bank PHP server for checking the authentication of the user. If the user is successfully authenticated, pulls the customer and account data and stores it in POJO classes Customer and Account array. (Since a single customer can have multiple accounts).	N/A
25.	TransactionActivity	Invokes an asynchronous task for performing transaction on the PHP bank server.	activity_transaction.xml
26.	TransactionFailureActivity	Displays a screen on failure of a transaction.	activity_transaction_failure.xml
27.	TransactionSuccessfulActivity	Displays a screen on success of a transaction.	activity_transaction_success.xml
28.	UpdateProfileActivity	Updates the profile of a logged in customer.	activity_update_profile.xml
29.	WithdrawActivity	Performs withdraw transaction.	activity_withdraw.xml

**Task / Activity Mapping Table**

Task	Role	Activity Flow
Launch App	Customer Cashier	HomeActivity
Customer Registration	Customer	RegisterActivity
Profile Updation/ Change Password	Customer	UpdateProfileActivity
Authentication	Customer Cashier	MainActivity SignInActivity
Perform Transaction	Customer	OperationActivity WithdrawActivity/DepositActivity OTPActivity MobileQRGenerarionActivity PHPQRCodeGenerationActivity QRCodeActivity
Execute Transaction from mobile	Cashier	QRReadActivity TransactionActivity TransactionSuccessfulActivity/TransactionFailureActivity
Signout	Customer Cashier	LogoutActivity

#### 4.0 Results and Discussions



The model presented above is partially implemented employing proven cutting edge technologies, HTML5, CSS3, jQuery as presentation tier technology, java as middle tier technology, MySQL as backend and PHP for server-side processing. Fig 7. shows the account opening form for the user.

Fig 7. Opening Account with the Bank

On opening the account with the bank and on successful authentication, the customer dashboard is displayed as shown in Fig 8.

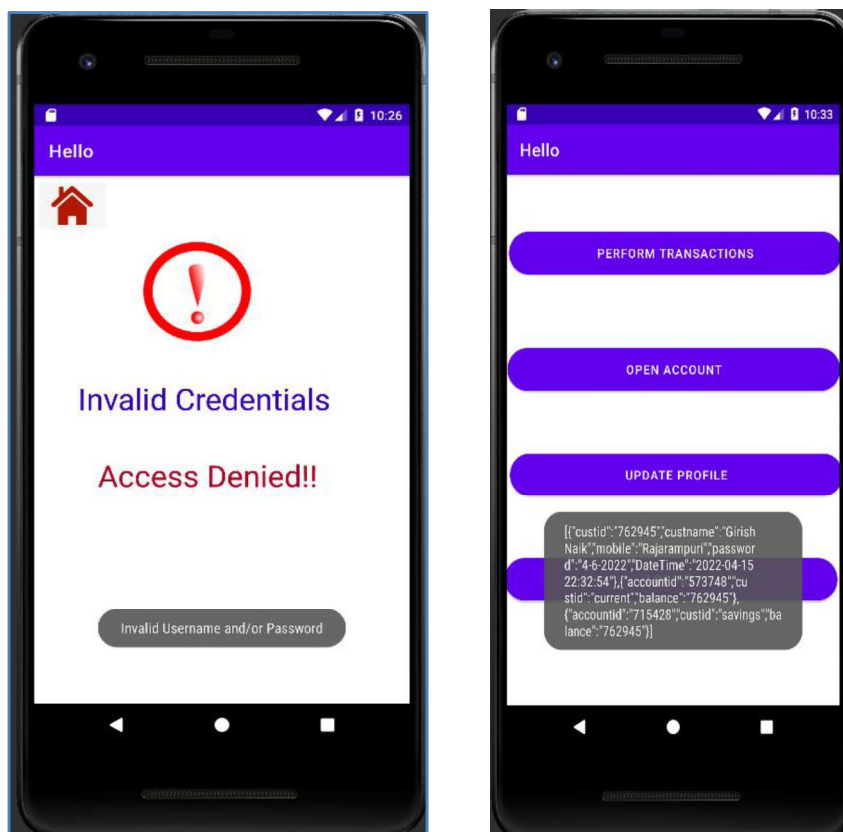


Fig 8. Authentication and Customer Dashboard

Fig 9. shows updating the profile by a customer .

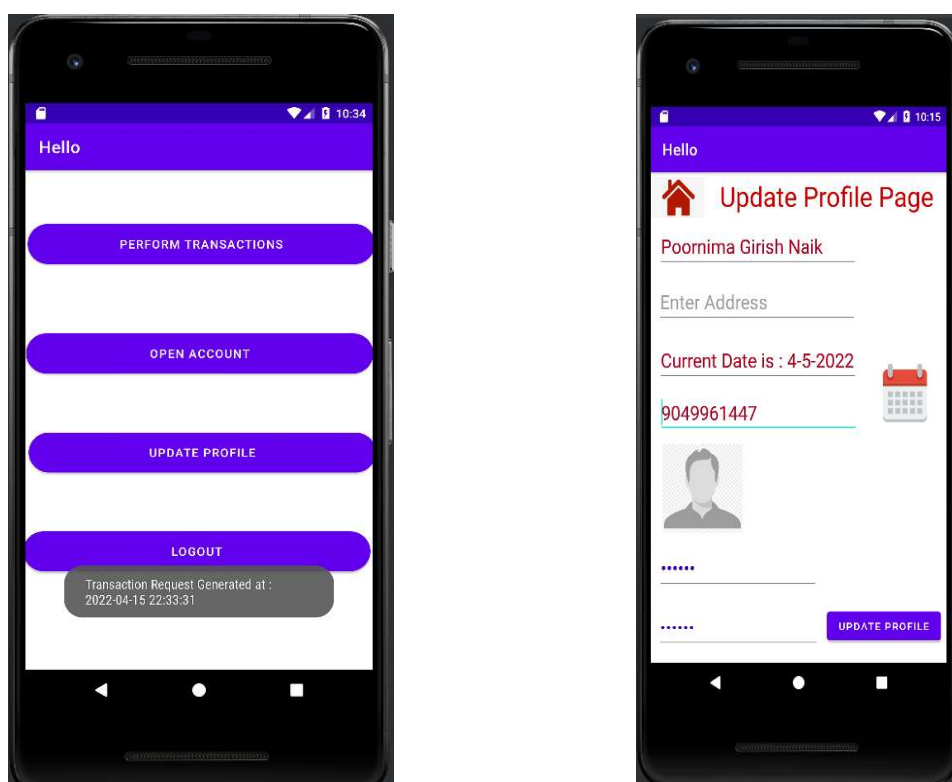


Fig 9. Updating Customer Profile

A customer can have multiple accounts with the bank. On successful authentication, all accounts are displayed on the client screen from which the user can select the account and the transaction operation. The data stored in the QR code is shown in Fig 10.

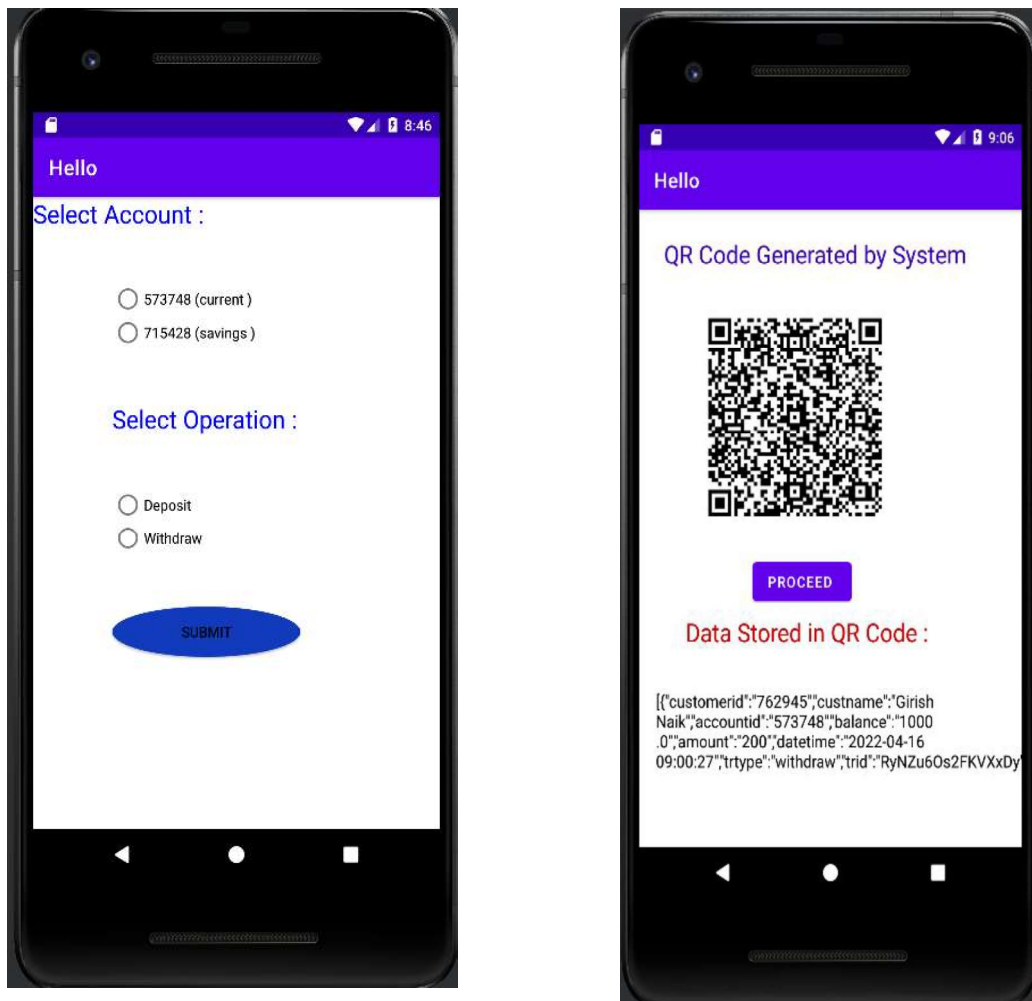


Fig. 10. Transaction Processing and QR Code Generation.

For the withdraw transaction, the OTP generated by the system is retrieved and QR code is generated as depicted in Fig 11.

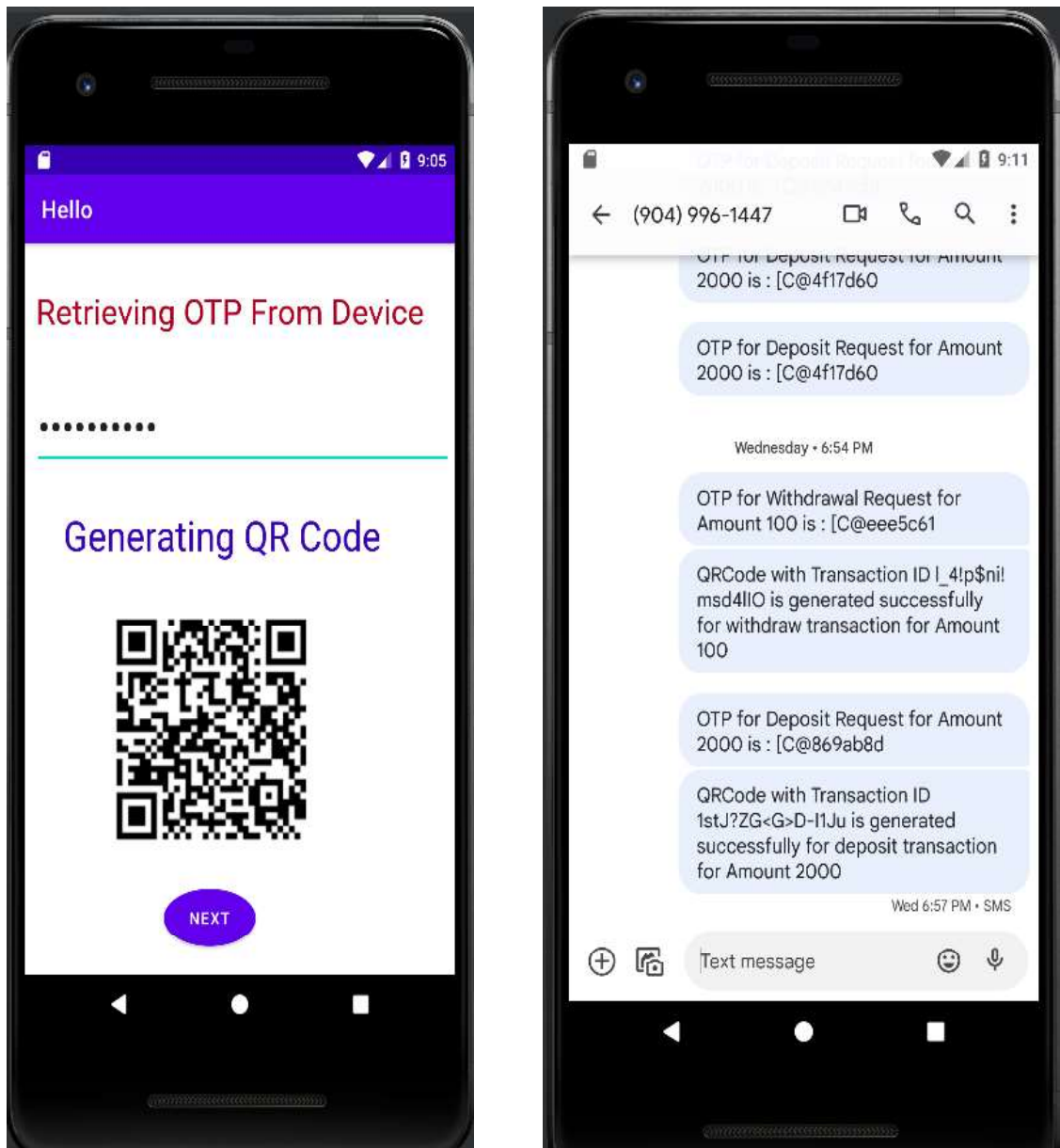


Fig 11. OTP Generation and Retrieval

For deposit transaction, the denomination information is entered as shown in Fig 12.

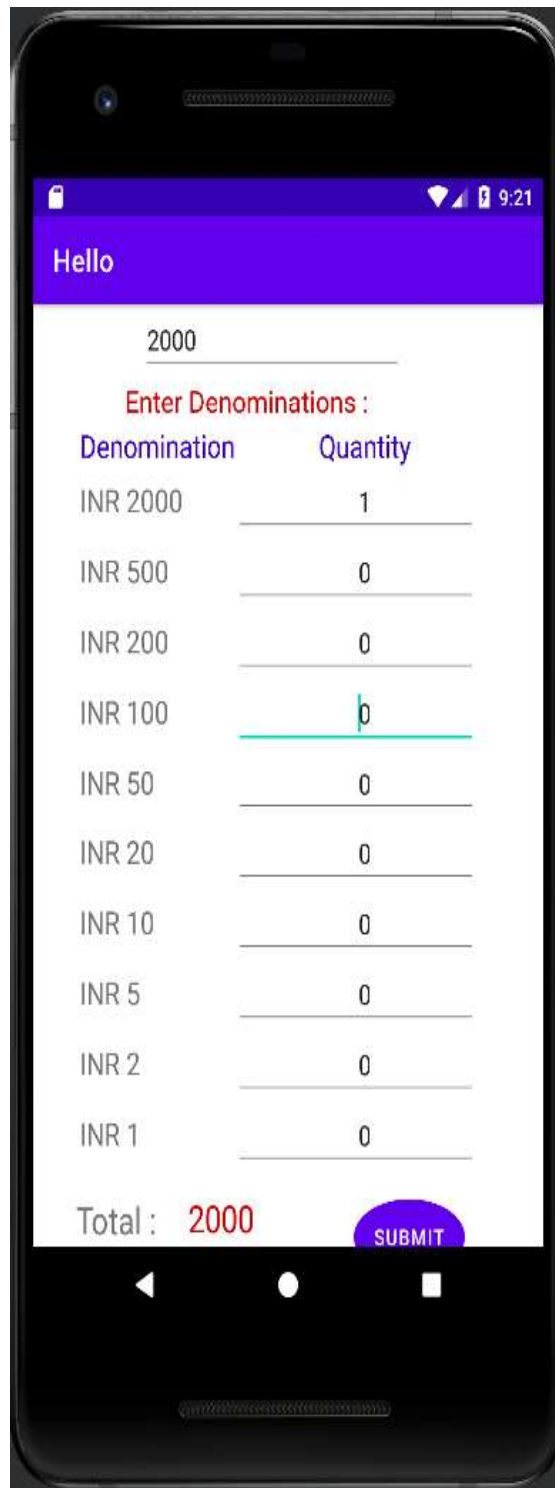


Fig 12. Denomination Information for Deposit Transaction

## 5.0 Conclusion and Scope for Future Work:

Card-less cash is an alternate and convenient option for cash withdrawal. Card-less cash withdrawal has made no compromise in security and banking norms. In spite of this it is not very popular due to its various limitations. In the current research, authors have designed a model for secure QR code transactions in N-tier applicable architecture. The model aims at providing a cost-effective solution for performing banking transactions. The prototype of the model is developed employing currently available server-side and client-side technologies. 6-level security checks are

performed to render the model highly secure and robust. The possibilities of QR code hacks are presented and the solutions are proposed. Double spending problem is tracked.

As a future amendment to the current research, the encryption algorithm can be replaced with the most robust ones which are quantum immune. The current model focuses on intrabank cash withdrawal by physically visiting the bank. Deposit transactions can be performed remotely. As a future enhancement the model can be updated to account for both intrabank and interbank fund transfers in virtual mode without the customer physically visiting the bank.

#### **Acknowledgment:**

Authors are grateful to The United Western Bank's Late R. N. Godbole Chair, Department of Commerce and Management, Shivaji University, Kolhapur for the financial support in the form of 'Minor research project Scheme 2021-22'.

#### **References:**

- Dr. Varsha Agarwal et al.(2020)**, 'A Study on Growth of Mobile Banking in India During COVID-19', *Palarch's Journal Of Archaeology Of Egypt/Egyptology*, Vol. 17, No.6, ISSN 1567-214x ,.
- Singh et al.(2017)**, 'Consumer preference and satisfaction of M-wallets: a study on North Indian consumers', *International Journal of Bank Marketing*, pp. 944-965.
- Dr. Parul Deshwal (2015)**, 'A Study of Mobile Banking in India', *International Journal of Advanced Research in IT and Engineering*, ISSN: 2278-6244, Vol.4, No. 12.
- Reshma S. et al. (2017)**, 'Awareness of E-Banking Services among Rural Customers', *International Journal of Innovative Science and Research Technology*, Vol. 2, Issue 4.
- Mirjana P. B. et al. (2020)**, 'm-Banking Quality and Bank Reputation', *Sustainability*, Vol 12, No. 4315, DOI: 10.3390/su12104315
- SIX Group Ltd Report publication: QR Code:** The Innovative Way to Withdraw or Deposit Cash without a Card.
- Khaled Aldiabat et al.(2019)**, 'The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry', *International Journal of Interactive Mobile Technologies*, Vol. 13, No. 2.
- Saprikis, V. et al.(2022)**, 'A Comparative Study of Users versus Non-Users' Behavioral Intention towards M-Banking Apps' *Adoption, Information 2022*, Vol. 13, No. 30. DOI:<https://doi.org/10.3390/info13010030>.
- Calin-Mihai Istrate ( 2014 )**, 'Cardless Withdrawal System for Mobile Banking Applications', *Journal of Mobile, Embedded and Distributed Systems*, Vol. VI, No. 1, ISSN 2067 – 4074.
- RBI Report available at <https://www.rbi.org.in/scripts/ATMView.aspx?atmid=86>
- Velasiri Dwarakamayi Amareswari et al.( 2021)**, 'Card less ATM Using 3-Level Authentication System', *International Journal of Advanced Research in Computer and Communication Engineering*, Vol.10, Issue 2.
- <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MC177DF24D0B0964448286BC682385CDA1F3.PDF>

\*\*\*\*\*