ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Secure Authentication Method using QR Code for Banking

Dr. A. P. Adsul[1]
Information Technology
Sinhgad Institute of Technology and Science
Savitribai Phule, Pune University
India

Anuj Shukla[2]
Information Technology
Sinhgad Institute of Technology and Science
Savitribai Phule, Pune University
India

Juhi Sinojia[3]
Information Technology
Sinhgad Institute of Technology and Science
Savitribai Phule, Pune University
India

Rohit Sinkar[4]
Information Technology
Sinhgad Institute of Technology and Science
Savitribai Phule, Pune University
India

Sheetal Jagtap[5]
Information Technology
Sinhgad Institute of Technology and Science
Savitribai Phule, Pune University
India

Abstract: ***This work contributes in the design and implementation of an inventive secure authentication method which utilizes a QR code; an open source proof-of-concept authentication system that uses a two-factor authentication by combining a password and a camera-equipped mobile phone, acting as an authentication token. QR code is extremely secure as all the sensitive information stored and transmitted is encrypted; however it is also an easy to use and cost-efficient solution. In the QR code a complex password is stored. Smart phone is used for scanning the QR code. The code is scanned with the QR code scanner. Scanning result generate one string which is the combination of IMEI number of a phone which is register by the user and the random number, where random number is generated by the random number function. If the network is available on the smart phone then that generated string is automatically entered into the login page and homepage of bank is open. Otherwise six digit pin code is generated and it has to manually enter in the login page and home page of bank is open for transactions. In a modern world where we are able to do almost everything on-line (banking, shopping, communicating, storing and sharing personal information...), it is nowadays a critical matter to be able to access these services in the most secured manner. Indeed, as viruses and cracking methods become more complex and powerful by the day, the available security techniques must improve as well, allowing users to protect their data and communications with the maximum confidence. The aim is to develop an authentication method using a two factor authentication: a trusted device (a mobile phone) that will read a QR code and that will act as a token, and a password known by the user.***

Keywords: QR (Quick Response) code, IMEI, QR, RN, TS.

I. INTRODUCTION

Now a days almost all the things we are able to do online (like banking, shopping, communicating) and in this the challenge is that while doing this things online our information is not get damaged.[3] Indeed, as the method of cracking the security code get more complex and powerful. There is need to develop more powerful security application. These powerful applications allow user to work on untrusted computers confidently. This work is based on the two way authentication system. In this the QR code provides security. QR code is the Quick Response code [5]. The existing system having security methods such as password, username, figure prints, and face detection. But in these methods security is not up to the mark, so there is need to develop such security system which provides high security.

The recent interest in the use of visual tags in everyday life is a natural consequence of the technological advances found in

modern mobile Phones.[2] The QR code is a matrix consisting of an array of nominally square modules arranged in an overall square pattern, including a unique pattern located at three corners of the symbol and intended to assist in easy location of its position, size and inclination. A wide range of sizes of symbols is provided together with four levels of error correction. Module dimensions are user specified to enable symbol production by a wide variety of techniques.

Fig. 1: Structure of QR code

There are two sections in this system. In the encoding section conversion of input data to a QR Code symbol takes place. In this the data analysis and encoding is done then after Error correction coding the final message is structures. Following the Module placements in matrix with masking another section is the Decode section. This section contains decoding of the input QR Code image and displays the data contain that QR code. The decoding procedure starts with the reorganization of black and white module then Decode format information. Following the determination of version of QR code and releasing Masking. Then restoring of data and RS codewords follows the Error detection and then decode the Data codewords.

II. PROPOSED FLOW

The system is basically divided into three modules:

1) Generation of QR code

2) Banking System

3) ATM System

1) Generation of QR code:

QR code comprised of following patterns: finder pattern, timing pattern, format information, alignment pattern, and data cell. Use of QR code ensures that data will be decoded by legitimate user only as decoding device will be required to decode it. The figure 2 shows the structure of QR code

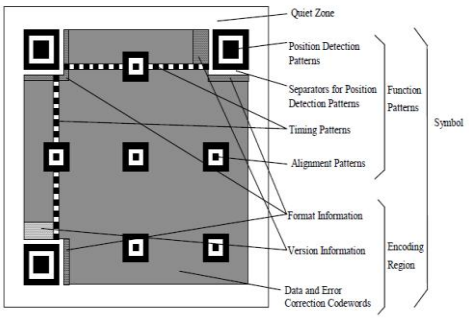

Fig. 2 Structure of QR code

All four sides of the QR code are surrounded by the quite zone border. QR code consisted of function patterns and encoding regions.The localization of QR code gets help from finder patterns of its most marked feature. Obtain the approximate region of QRcode, and implement coarse positioning for QR image according to the finder patterns. According to the located QR code,

obtain the version number determine the size of QR code. Data and error correction code words ensures that the OR code will be read successfully if some portion of it is damaged.

2) BANKING SYSTEM [6],[7]:

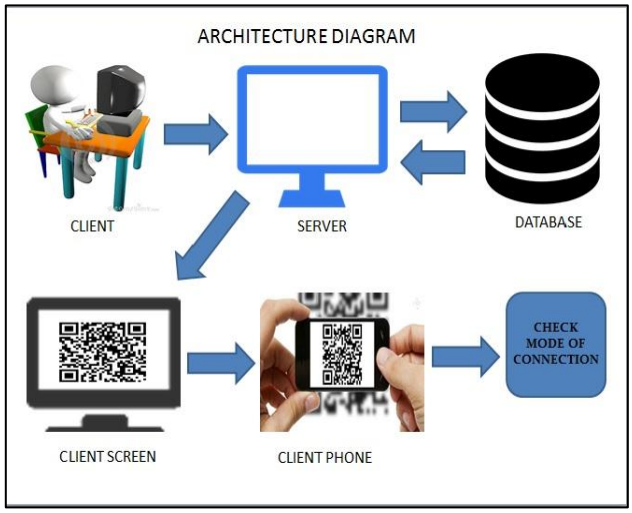

Fig.3: Architecture of Banking System

The figure 3 shows the architecture of banking system. In this the client fills up the details of bank account and submits it to the bank employee. The employee stores all the details into the system. Bank then sends an OTP to the client. The client then proceeds for the verification process and once the verification process is finished the client is said to change the password [6].

The client when relogins the system with the username and new password generated by the client, it sends request to generate QR code. Once the request is sent to the server it generates QR code which will be displayed on the client's machine. The client then scans the QR code with the mobile with the help of [Random no + IMEI no] which will be stored in the system database. It is then said to check the mode of connection.

2.1. Online mode :

The figure 4 on the next page shows the online mode of authentication. As shown, in this First IMEI number and random number are encrypted using the public key. This encrypted string generates the QR code using the QR code generation function which is present in java. Now this QR code image is display on the client machine. User scans this QR code using mobile phone. After scanning, in online mode means net is available on phone the generated string (IMEI number and random number) is automatically get entered into the login page. After successful login the home page of the bank is get open.

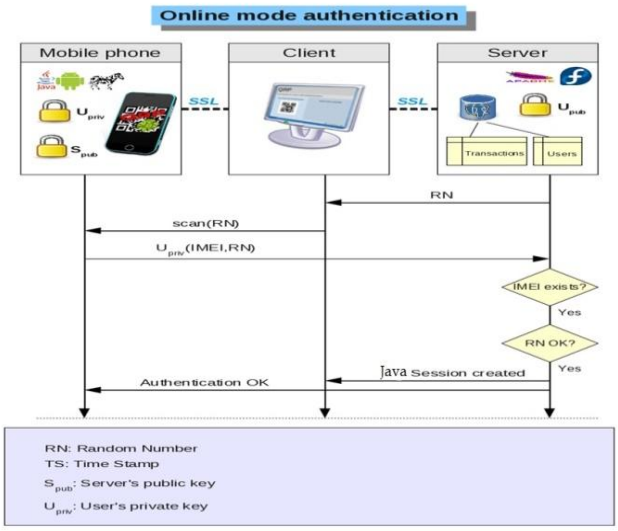

Fig.4: Online Mode of Authentication

Hence in this system there is no need to remember the password which is the combination of your IMEI number and the random number. The server decrypts the string using the user public key and verifies that a row exists in the transactions table with our random number and then accordingly updates the row of transaction table. Subsequently the server checks that the IMEI is correct or not and assigned that IMEI to the correct user. If the login is get successful the transaction row is deleted. It means every time the generated QR code image is different. Now the PHP session is created and when user gets logoff the session is destroyed.

2.2. Offline mode:

Figure 5 illustrations the architecture of offline mode of authentication. In this if the phone detects that the Internet cannot be accessed within specified time period then, Using pin code generation algorithm, a unique six-digit number is generated from the encrypted string (IMEI number and random number).

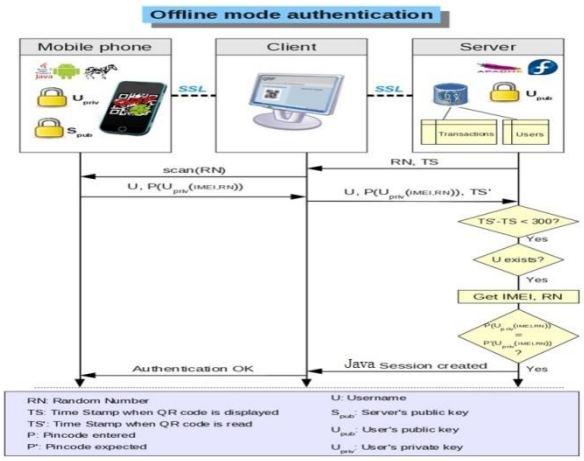

Fig.5: Offline Mode of Authentication

User has to enter this pin code on login page manually with respect to username. For entering the pin code the keypad is available on screen. So there is no need to enter the pin code using systems keypad. This system provides more security at this point. After entering the pin code server verify the IMEInumber of user which is stored in the database. If the IMEI number is present then user is valid and then homepage of bank is gets open. The timestamp is also checked. If the random number is generated before the 10 minutes ago then session is destroyed. Hence the user is not able to login.[1][7].

3) ATM SYSTEM:

The ATM architecture diagram of ATM system is shown with figure 6. In this module the additional security to the user has been provided in terms of QR code authentication. Here the client enters into ATM centre to transfer the money from one ATM card to another ATM card for which he has to enter his own PIN number to authenticate himself.

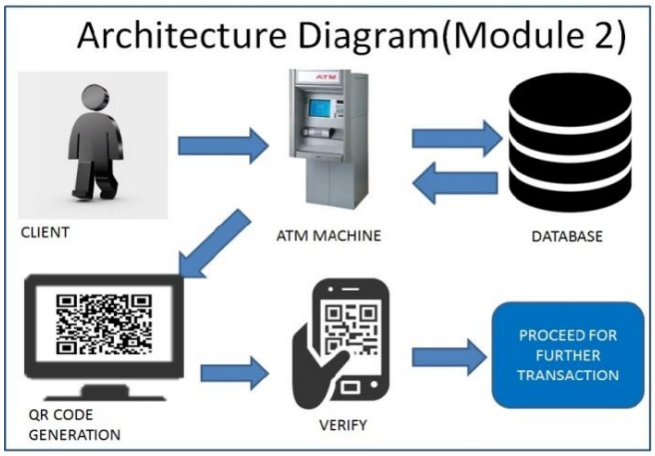

Fig.6: Architecture diagram of ATM System

Afterwards ATM machine checks his PIN with the database; if the PIN matches then he is given authentication. After authentication he proceeds towards money transfer option. For transferring money from one ATM card to another ATM card, he has to enter his own ATM number then the amount to be transferred and at last he has to enter the ATM number of the other person. After entering the second account number the pop up message is shown to confirm the transfer by manually confirming the given information of the other person. In this system extra measures have been provided to prevent silly mistakes. The security is in the form of QR code authentication. The QR code will be displayed immediately after hitting the next button at the transfer level. By scanning that QR code we will get the recipient's information on the screen of our mobile phone. After the verification of the information on our mobile phone the transaction will be processed else declined.

III. System Implementation

This section gives the details about the implementation of the banking system and ATM system with respective website front end and application back end.

A) Website Front End: 1.) Banking System

In the banking system three different forms are designed to provide the required information by the user.

i) Login Page

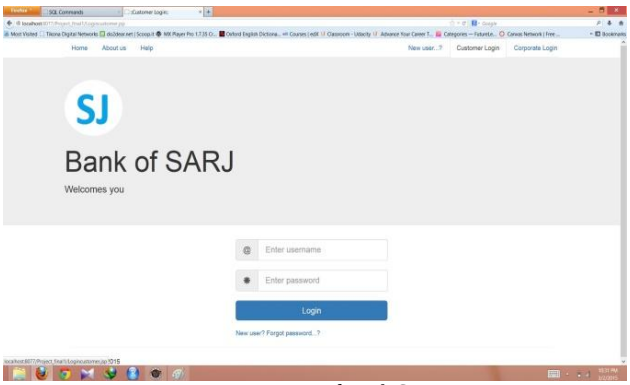

Fig.7: Login Page of Bank System

Figure 7 shows the login page for client**.** The client is said to login with the username and password i.e. OTP at first time login.The client then proceeds for the verification process and once the verification process is finished the client is said to change the password. The client when relogins the system with the username and new password generated, it sends request to generate QR code.

ii) QR code scanner

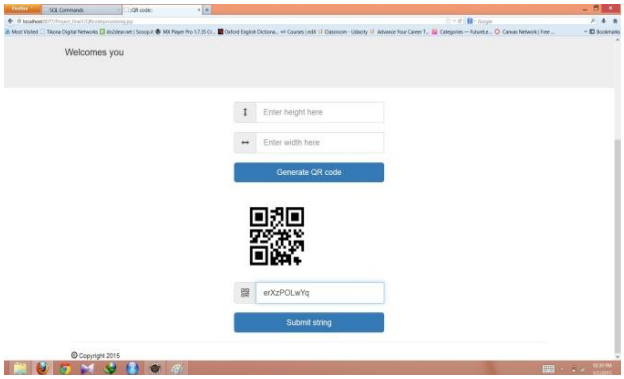

Fig.8: QR Code Scanner for Bank System

Once the request is sent to the server it generates QR code which will be displayed on the clients screen. Figure 8 shows the particular form designed for it. The client then scans the QR code with the mobile with the help of [Random no + IMEI no] which will be stored in the system database.

iii) Transaction

The client then proceeds further for the transaction process by entering the details and amount. Subsequently proceeds for the other banking process likewise. The figure 9 depicts the form designed for transaction process of bank.

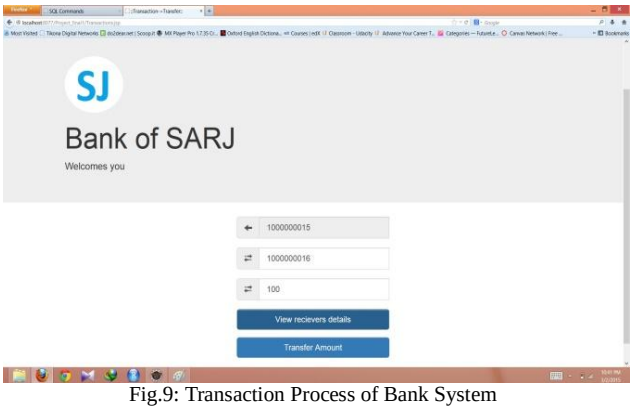

Fig.9: Transaction Process of Bank System

2) ATM System

Similar to the bank system different form are also designed for the ATM system to acquire information from the client.

i) Login

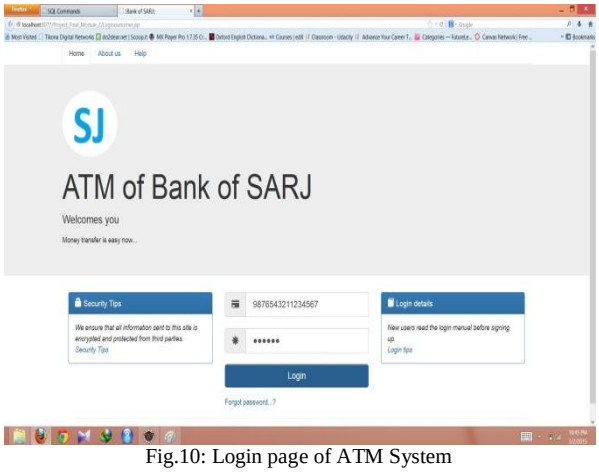

Fig.10: Login page of ATM System

With this login page the client able to enter the account no. and the password for the process of the withdrawal of money. The figure 10 shows the field detailed of it.

ii)Transfer

After authentication the client proceeds towards money transfer option. Figure 11 presents details about money transfer. For transferring money from one ATM card to another ATM card, the client has to enter his/her own ATM number then the amount to be transferred and at last he has to enter the ATM number of the other person. After entering the second account number the pop up message is shown to confirm the transfer by manually confirming the given information of the other person.

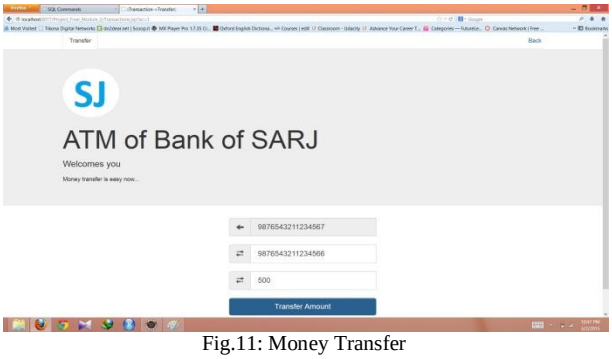

Fig.11: Money Transfer

iii)QR Scanner

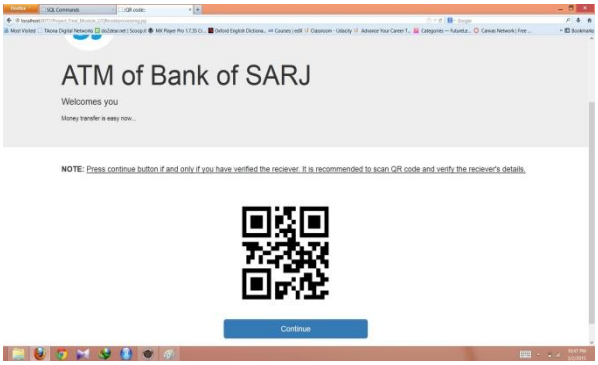

Fig.12: QR scanner for the ATM System

Once the request is sent to the server it generates QR code which will be displayed on the screen. The client then scans the QR code with mobile. Figure 12 gives the exact glance of the QR code page to be scanned.

B) Application Front End: 1)QR code scanner

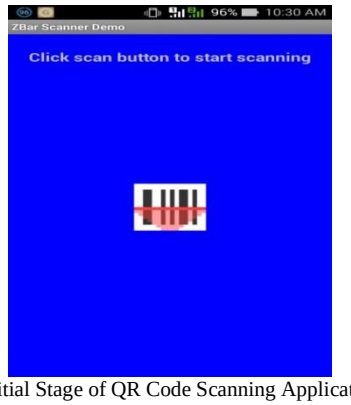

Fig.13: Initial Stage of QR Code Scanning Application

QR code is said to be scanned with the above scanner type of the content application stored in mobile. Figure 13 specifies it.

2) Display Result

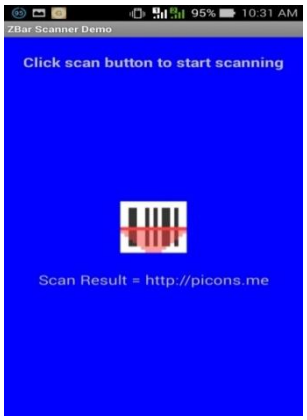

Fig.14: Scanning of the QR Code and displaying the result

After the scanning is said to be carried away then random no. string is said to be generated, which is said to be useful in the further process thus providing security measures into the system. It is shown with figure 14.

IV. CONCLUSION

This work provides additional security with the traditional way of online authentication of banking; which includes username and password. However, by adding QR code authentication the security measures for banking are enhanced. Two factor authentications are considered in this system. With the help of this QR code security is increased during the login of the particular bank. Depending on the authentication only the client will be able to perform the transaction.

ACKNOWLEDGEMENT

This research paper cannot be considered complete without mentioning Prof. Dr. A. P. Adsul. We wish to express true sense of gratitude towards her valuable contribution .We are grateful to her for his constant encouragement and guidance in the fulfillment of this activity.

References

1. SnehalKalbhor, AshwiniMangulkar , Mrs.SnehalKulkarni"Android App for Local Railway Ticketing Using GPS Validation". International Journal of Emerging Trends in Science and Technology,IJETST-Volume 01,Issue- 01, March-2014,Pages 71-74.
2. Fu-HauHsu,Min-HaoWu,Shiuh-JengWANG, "Dual-watermarking by QR-code Applications in Image Processin".9th International Conference on Ubiquitous Intelligence and Autonomic and Trusted Computing,DOI 10.1109,2012,Pages 638-643.
3. Mrs.Shanta Sondur, Ms.Tanushree Bhattacharjee "QR-Decoder and Mobile Payment System for Feature Phone", VESIT,International Technological Conference(I-TechCON)-Jan. 03 – 04(2014), Pages 13-15.
4. SomdipDey, B. JoyshreeNath and C. AsokeNath "A New Technique to Hide Encrypted Data in QR Codes" Institute of Information Systems Argentinierstrasse -2009.
5. Dr. A. P. Adsul, Gayatri Kumbhar, Vrunda Chincholkar, Yogesh Kamble, Anuja Bankar "Automated Exam Process using QR Code Technology" International Journal of Application or Innovation in Engineering & Management, (IJAIEM)-ISSN 2319-4847,Vol.3,Issue 4,April- 2014,Pages-296-298.
6. Ben Dodson, Debangsu Sengupta, Dan Boneh, and Monica S. Lam "Secure, Consumer-Friendly Web Authentication and Payments with a Phone", International Journal of Applied Engineering Research, ISSN 0973-4562, Vol. 8, No. 17 (2013).
7. SadafShaikh, GayatriShinde, MayuriPotghan, TazeenShaikh, RanjeetsinghSuryawanshi "Android Urban Railway Application with Quick Response Code Ticket" International Journal of Advanced Research in Computer Science and Software Engineering,ISSN:2277 128X,Vol.4,Issue 3,March 2014,Pages 1184-1187.
8. Jiejing Zhou, Yunfei Liu, Amit Kumar "Research on Distortion Correction of QR Code Images" ISSN:0976-8491, IJCST,Vol. 3,Issue-1,Jan-Mar 2012,Pages 415-420.

