Two Way Authentication for Banking Systems

Nupur Shinkar[1], Sanket Sonje[2], Shubham Kamble[3], Pranav Pardeshi[5], Prof. Pooja Dhule[5]

[1,2,3,4](Student, Department of Computer Engineering, MMCOE, Pune, India)
[5](Department of Computer Engineering, MMCOE, Pune, India)

***Abstract**:- The basic idea of our project is to build a new banking system and reduce old systems use OTP and instead use a security verification method that uses the QR code. System which uses two-way authentication using Random Numbers and IMEI Signed Signs of Verification. Since the information stored in the QR code is encrypted, it is protected. The QR code is scan with the help of scanners on smartphones. The results generated by scanning QR codes are a combination of the random number generated by the random number function and the number of IMEIs registered by the user. If the internet connection in smart phone is on then user will automatically get inserted into the login page and forwarded to the home screen of the bank page. The goal is to develop a security system that uses two-factor authentication: a trusted device will scan the QR code and act as a known signal and password. Our goal is to increase security bank operations and provide customers with easy access to operations.*

Key words: - *QR codes, online privacy, mobile security, secured authentication, smartphone*

1] INTRODUCTION

1.1] Background

Most of the current transactions are digitized, users are scared of losing their important data. We still use the first safety measures. This requires delivery of greater security measures for these Internet operations will ensure that user information is not getting tampered. Securing QR code works more effectively than password, fingerprints, and face detection system. The QR code is a matrix that is an array of squares. The three points of QR code form the only model that can easily scale and size.

2] PROBLEM STATEMENT

The present system has an OTP that is sent to users via text message or email, but email spoofing or man in the middle can occur. The password system provides security against unofficial access, but the evolution of various attacks, such as violent attack, does make the system ineffective. This system option is provided in two identities that use the first-factor password, and the randomly generated code is a second factor. There are many advantages of this system but it also comes with some disadvantages. For example, a fraudulent network late delivery of OTP. This system has been replaced with an efficient system that uses the QR code instead of OTP but does not resolve the code issue. The new system we offer provides a QR code with an IMEI number and a 4-digit code. The second verification factor is replaced by the Android app installed on the registered phone. This system eliminates the problem of man in the middle and the delay in obtaining a unique code.

3. Literature Review

Table1.Literature Review

Sr.No.	Paper Name	Gap Identified
1.	OTP encryption techniques in mobiles for authentication and transaction security.	Most OTP systems are susceptible to real-time replay and social engineering attacks.
2.	Survey on information hiding techniques using QR barcode	They can breakdown Label damage. Scratched or crumpled barcodes may cause problems
3.	Authentication and transaction verification using QR codes with a mobile device	Use of QR code for transaction process instead of login is not safe and secure

3. Proposed Methodology.

The ideological development of the system using the iterative model is that it will allow the developers to take advantage of earlier versions of the system. Important steps in development of the system should start with the application of a small module and then make changes according to the system requirements are by using the current system, developers can identify errors in system and improve it by providing new functionality.

In doing this, the design changes were made, and new system functions were created. This process continues until the ultimate goal of ensuring the best security is achieved. Mostly, Development consists of, initialization steps and system design module control lists that replaces the current OTP system. The QR authentication system allows the user to log in by using password if the user is identified, the encrypted string in the form of the QR code is displayed on the screen. A user gets logged in if an encrypted string matches an IMEI number in the database.

***Fig.1**. barcode*

Before the QR code, there were some advanced verification techniques, such as user names password, barcodes, face recognition, fingerprint. Security is compromised as passwords faced the problems of hacking. The code limit is that it can only save up to 20 digits therefore complex passwords cannot be created by using the code. Barcode which are scratched, does not provide any security. Devices and technology used for fingerprints and face identities suffers from a problem of accuracy.

Therefore to reduce all the drawbacks of previous security system QR code is made. QR code is a Quick Response code. It was introduced in 1994 by a Japanese company subordinate –Danso-Wave. The QR code can produce more complex passwords because it can hold up to 4296 alphanumeric character. Since it is a two-dimensional barcode, can be read from any direction.

***Fig.2**. QR code*

There are two parts to this system. Section in which input data is converted into QR code is known as encoding section. Data analysis and encoding is performed in this then it is followed by error correction, coding and the final message is organized. Decoding is second stage where decoding of QR code image is done and whatever data it contains is displayed the decoding technique starts with distinguishing the black and white modules and then rearranging the modules to achieve the decoded format information.

4] Proposed system

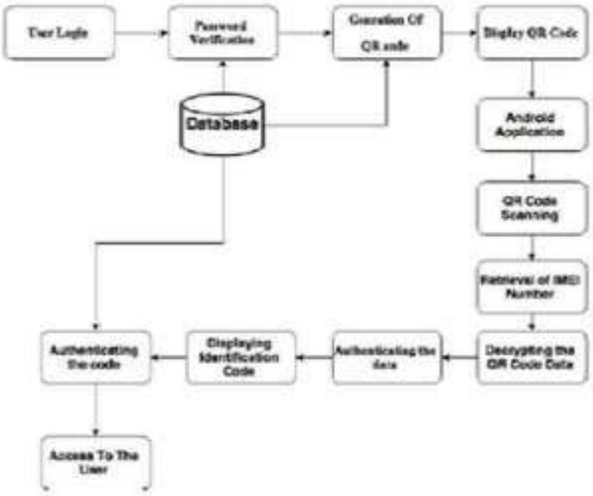


***Fig.3**. Flow Diagram*

The steps in above diagram provide information on how to complete the registration process: -At first user will sign up for registration by submitting details such as his username, password and IMEI number. When the data is verified it will be saved in the database. Then public key and private key will be generated by the data in the data server and they will be stored in the server.

The user will continue to download the Application and install it on his phone. When a user executes the application for first time, public and private key files are created and saved internal storage of mobile phones. When registering, if the user does not enter all values as user names, IMEI number password, phone number, and email address then the registration process will be failed. Validation plays an important role in the registration process; if validation unsuccessful then login of user is not possible.

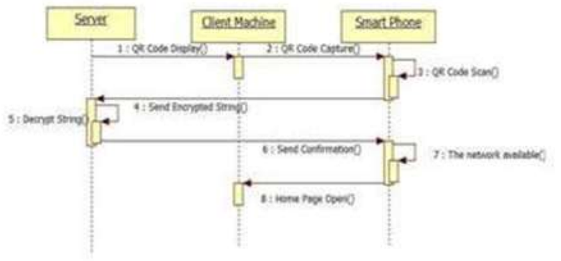


Fig 3.Registration process diagram

5] IMPLEMENTATION

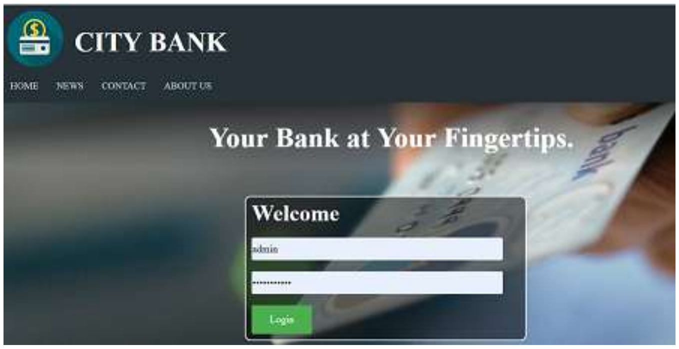
This system is implied when your (user) mobile phone has the internet and is online where string is formed by doing encryption of random number, public key and IMEI number. With this help of this string QR code is obtained by using the QR code generating function. Once it is produce, it will be shown on client's machine and clients will scan this QR code with their mobile phone. Since its online mode, after scanning, the generated string user directly enters into login page by using internet. If there is successful login, the customer home page of the bank website is displayed. So in our system, we do not need to remember the password. The user's public key is used to decrypt the string and also ensure that it is in our transaction table with random number, and then modification of the line are done in the table. Server, then check whether IMEI is valid. If it is found valid, then the login is successful. After successful login, the transaction row is removed and a new QR code appears when the user wants to sign in again. Now, PHP sessions are created and when the user is finishes his/her task, the session is destroyed.

6] SECURITY

The QR code and encryption algorithms provide powerful security for our system. It does not get susceptible to the man-in-the-middle attack because the message between the user and the server is always in the encrypted form. Also, for a mobile app, one has to have a password so they cannot be attacked by anyone in any other ways. If the people who are untrusted know how to work on data storage, the security issue is created. Phishing attacks are possible on mobile phones if we replace apps with others app.

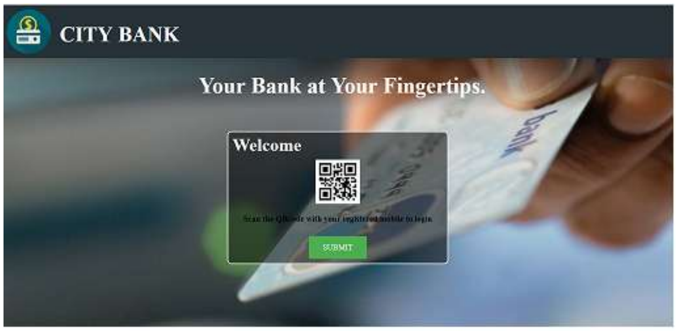
Result:-

Screenshots



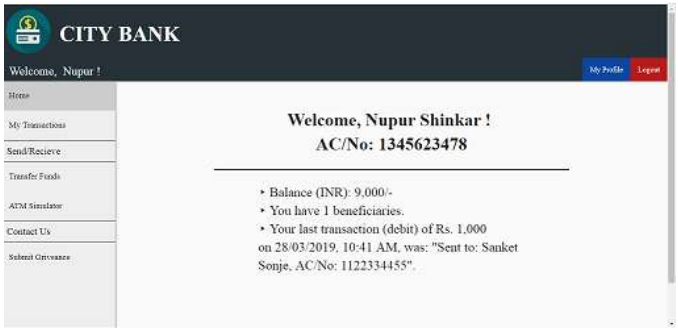
admin

1.Home Page.



Scan the QRcode with your registered mobile to login.

2.QR code**.**

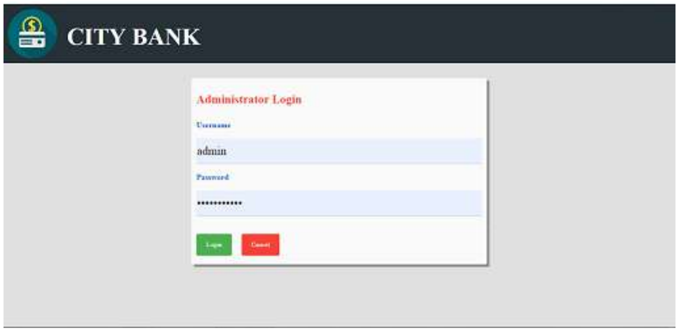


Welcome, Nupur !

Welcome, Nupur Shinkar !
AC/No: 1345623478

- Balance (INR): 9,000/-
- You have 1 beneficiaries.
- Your last transaction (debit) of Rs. 1,000 on 28/03/2019, 10:41 AM, was: "Sent to: Sanket Sonje, AC/No: 1122334455".

3.Login Succsess.



Username
admin
Password
•••••••••••

4.Admin Page.

Conclusion: - This system gives additional security with the traditional way of online authentication of banking; which contains username and password. On the other hand, by adding QR code authentication, the security measures for banking are improved. Two factor authentications are measured in this system. With the help of this QR code, security is improved during the login of the specific bank. Depending on the authentication only the client will be able to achieve the transaction. In future we would like to add voice input command feature to our website and android application. It will help the user to do his work easily. We would like to use some advanced encryption and decryption algorithm, better than AES.

Refernces:-

[1] T. Purnomo, Y. S. Gondokaryono and C. Kim, "Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure," 2016 6th International Conference on System Engineering and Technology (ICSET), Bandung, 2016, pp. 194-198. doi: 10.1109/ICSEngT.2016.784964

[2] S. Khairnar and R. Kharat, "Online fraud transaction prevention system using extended visual cryptography and QR code," 2016 International Conference on Computing Communication Control and automation (ICCUBEA), Pune, 2016, pp. 1-4. doi: 10.1109/ICCUBEA.2016.7860061

[3] S. Istyaq and M. S. Umar, "Encoding passwords using QR image for authentication," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2016, pp. 818-823. doi: 10.1109/NGCT.2016.7877523

[4] 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

[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] SomdipDey, B. JoyshreeNath and C. AsokeNath “OTP Encryption Techniques in Mobiles for Authentication and Transaction Security” Institute of Information Systems Argentinierstrasse -2009.

[7] Jawahar Thakur, Nagesh Kumar “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis ” International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011).