International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

QR Code for Banking

Akul Desai

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 CODE, Banking, Banking security, QR Code with banking, Two Factor Authentication

1. Introduction

Now a day's 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. 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.

Figure 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 codeword's.

2. Existing Authentication Systems

The existing system consists of OTP which is sent to user via sms or email but email spoofing or man in the middle attack can occur. Hence user's security can be compromised. Our project uses the password as the 1st key of authentication and mobile phone as the 2nd key of authentication. Also it eliminates email spoofing, man in the middle attack and includes another level of security. Password Based Authentication paper studies and takes a careful look at this issue from the angle of philosophy and cognitive science. This paper has thrown light onto the philosophy of passwords and their study in connection with attacks. Although the points that were mentioned in this paper have been noted by different researchers at different times but there's no single place where the entire "password philosophy" has been defined. Merit of this paper is that it provides security to the users against unauthorized access. Demerits of this paper are that the passwords should be kept secured. They should not be such that they can be easily guessed and the password should not be very complex such that the user himself forgets what password he had set. Also the password may be compromised by Trojan programs on another system. OTP - Based Two - Factor Authentication Using Mobile Phones system proposes use of two factor authentication. It suggests sending of a randomly generated code to the user via email or SMS. Merit of this system is using forward hashing technique, attacks based on sending small challenges by intruders is eliminated. There is no delay in network while the second factor of authentication.

Demerit of this system is the user has to enter the data manually which is time consuming. Also the human interaction element makes the system prone to human error. Secure Login by Using One - time Password Authentication Based on MD5 Hash Encrypted SMS system, the developed login security system is using OTP that is encrypted with MD5 Hash, and the OTP is sent automatically to the registered user phone cell number. Merits of this system is that the time delay for active OTP is set up to 3 minutes. It is too short for hackers to possibly break the code and infiltrate the system. Also the use of MD5 Hash to encrypt a set of Student ID, Phone Number, and Timestamp (date and hour of access). Demerits of this system are that during every login request or transaction process, it is necessary to send an SMS - OTP from the bank to the user. This, in turn, will be costly to the bank with the consideration of statistics of bank's transactions. Also the message can be delayed causing the transaction to fail.

3. Problem Statement

The password system provided security against unauthorized access but the evolution of different attacks like brute force dictionary attack has made this system ineffective. An alternative of this system is given in form of a two factor authentication which uses password as the 1st factor and a randomly generated code as the 2nd factor. With advantages of this system also came the disadvantages for example spoofing of network, delay in delivery of the OTP, this system was replaced by an more efficient system which used a QR code instead of OTP but didn't solve the problem related to delivery of the code or QR. The new system we offer generates QR code which consist of the IMEI number and a 4 digit code. The 2nd factor of authentication is replaced by and android application installed on the registered phone. This system solves the problem of network spoofing, man in the middle and the delay in receiving the unique code.

4. Proposed System

To design a system which replaces the current OTP based two factor authentication system

The QR based authentication system lets the user input the password, if the user is authenticated then an encrypted string consisting of IMEI number of the user is displayed in the form of QR code.

The user uses his phone to scan the QR code and if the encrypted string is same as the IMEI number of the device the user is authenticated.

To design a system for visually impaired persons in which the person uses his phone to scan the QR code and after the scan is complete the code is spoken out.

The visually impaired can enter the code via text - to - speech to the web application.

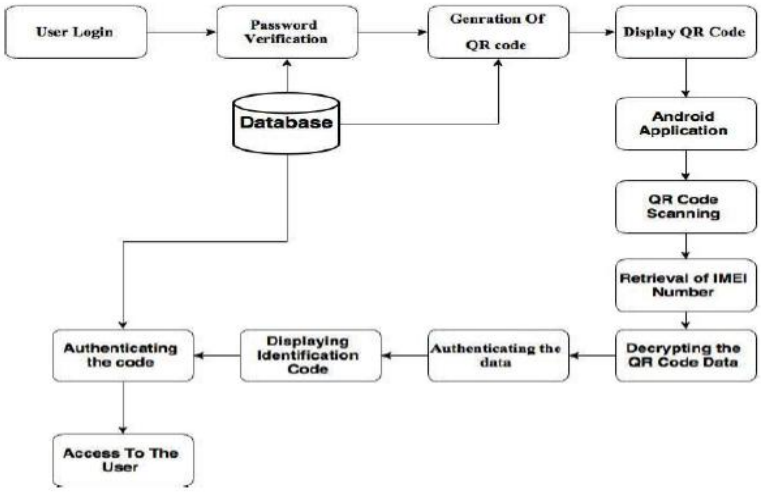

Figure 2: Architecture Diagram

5. 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.

6. Future Work

In future we would like to improve many aspects of our project. We would like to add voice input command feature to our website and android application. It will help the user to do his work comfortably.

Compliance with Ethical Standards

Disclosure of potential conflicts of interest Research involving Human Participants and/or Animals Informed consent

References

[1] Mr. Ashlesh Patel, Mr. Pragnesh Patil, Mr. Harsh Shah, Mr. Nihir Shah "QR Code based Authentication System for Banking" IOSR Journal of Computer Engineering (IOSR - JCE) - Conference on Recent Trends in Computer Engineering (CRTCE - 2018).
[2] Ambili M P, "E - Banking Security and Authentication using Multilevel QR" International Research Journal of Engineering and Technology (IRJET) - Volume: 08 Issue: 03 March 2021.
[3] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, "Online Banking Authentication System using Mobile - OTP with QR - code" Research Gate.
[4] Devendra Jadhav, Shivam Shinde, Krisha Shah "Secure Banking System Using QR Code Authentication" International Journal of Scientific & Engineering Research Volume 9, Issue 3, March - 2018.
[5] Amandeep Choudhary, Shweta Rajak, Akshata Shinde, SiddeshwarWarkhade, "Online Banking System usingMobile - OTP with QR - code" International Journal of Advanced Research in Computer and Communication Engineering – volume: 6 Issue: 4, April 2017.
[6] Brindha G, Gopikaarani N "Secure Banking Using QR Code" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3 Issue 12, December 2014.
[7] Aayushi Mishra "Multilevel Security Feature for Online Transaction using QR Code & Digital Watermarking" International Conference on Electronics, Communication and Aerospace Technology" IEEE - 2017.
[8] Peng - Cheng Huang, Yung - Hui Li, Chin - Chen Chang "Efficient QR code authentication mechanism based on Sudoku" Springer - Multimedia Tools and Application.