IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 05-09
www.iosrjournals.org

QR Code based Authentication System for Banking

[1]Mr. Ashlesh Patel, [2]Mr. Pragnesh Patil, [3]Mr. Harsh Shah, [4]Mr. Nihir Shah, [5]Mrs. Ashwini Patil

[1,2,3,4]UG Student Computer Science, Thakur College of Engineering and Technology, Mumbai, India
[5]Assistant Professor Computer Science, Thakur College of Engineering and Technology. Mumbai, India

Abstract: *The main idea of our project is to build up a new system of banking and to overthrow the old system of using OTP's and instead use an inventive secure authentication method which utilizes a QR code; System which uses two way authentication by using a random number and registered IMEI number, acting as a token of authentication. As the information stored in the QR code is in encrypted format it is secured. QR code is scanned with the help of scanner in smartphone. The result generated by scanning a QR code is a combination of a random number which is generated by random number function and IMEI number registered by the user. If there is internet connectivity in the smartphone, the generated string is automatically entered in the login page and is redirected to the home screen of the banking page. If there is no internet connectivity in the smartphone, the encrypted string generated by the scanning of QR code gets decrypted and a new six digit pin code is generated which is to be entered manually by the user which then redirects to the home screen of the banking website. The objective is to develop an security system using a two factor authentication: a trusted device which will scan a QR code and act as a token and a password known by the user. Our aim is to enhance the security of the banking transactions and provide users with a convenient way of performing the transactions.*

Keywords: *QR code, IMEI number, authentication, AES algorithm, registration, encryption*

I. Introduction

A . Background

As most of the transactions in today's era is getting digitalized that fears the users of losing their credentials as we are still using the primitive measures of providing security. So there arises a need of providing more enhanced security measures to all these online transactions which will assure the user's information not getting tampered. Providing security by means of QR code is more efficient than password, fingerprints and face detection system. The QR code is a matrix which is an array of square modules arranged in a square pattern[1]. The three corners of the QR code forms a unique pattern that assists easy location of its position, size and inclination.

B . Problem Statement

The current system consists of OTP which is sent to user via SMS or email but email spoofing or man in the middle attack can occur. The password system provided security against unauthorized access but the evolution of different attacks like brute force dictionary attack 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 more efficient system which used a QR code instead of OTP but didn't solve the problem related to delivery of the code.

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 removes the problem of network spoofing, man in the middle and the delay in receiving the unique code.

II. Literature Survey

In the literature survey we did the survey of certain systems which are common used. The traditional password system fails to confirm the user identity as there is a threat of phishing of users credential. Using QR code will thus eliminate the problem of phishing as it uses user's registered IMEI number encrypted with a random number and then hashed to generate a string[2]. As a string is hashed, the attacker cannot retrieve the data in its original format. A variety of size of symbols is provided together with four levels of error correction which learns something new from each system.

Paper Name	Disadvantages
OTP Encryption Techniques in Mobiles for Authentication and Transaction Security	1. Most OTP systems are susceptible to real-time replay and social engineering attacks. 2. OTPs are also indirectly susceptible to man in the middle (MITM) and man in the browser (MITB) attacks.
SURVEY ON INFORMATION HIDING TECHNIQUES USING BARCODE	1. They Can Breakdown 2. Label damage. 3. Scratched or crumpled barcodes may cause problems
A Secure Credit Card Protocol over NFC	1. Security problems. 2. Sensitive data can be accessed if card is lost.

Table 1

III. Proposed Methodology

The ideology behind developing the system using the iterative model is that it will allow the software developers to take the advantage of previously developed versions of the system. The key steps in developing the system are to start with the implementation of the smaller essential modules and then as per the software requirements iteratively enhance the system. By using the current system, the developer can identify the flaws in the system and make improvements by providing new functionality to the system.

At each iteration, design modifications are made and new functional capabilities of the system are implemented. This process continues until the main objective of providing the finest security is achieved. The development consists of initialization step, Iteration step and the control list of the module to design a system which replaces the current OTP based system. The QR based authentication system lets the user input the password, if the user is authenticated then an encrypted string in the form of QR code is displayed on the screen.

The user gets authenticated if the encrypted string matches the IMEI number present in the database[3]. Designing a system for visually challenged people in which the person will be able to hear the code once the QR code is scanned. The visually impaired can enter the code via text-to-speech feature of the web application.

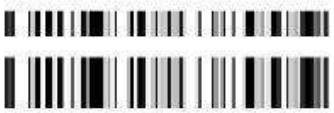

Figure I. Bar Code

Prior to QR code there were some primitive authentication techniques available namely Username and password, Barcode, Fingerprints, Face recognition. The security was compromised as the Username and password faced the problem of phishing and eavesdropping. The limitation with barcode is it can only store up to 20 digits so complex passwords cannot be generated using barcode. The crumpled and scratched barcode does not provide effective security.

The devices and the technology used for the Fingerprints and Face identity is not cost effective and it also suffers from accuracy problem. Thus to overcome from all the disadvantages of the existing system, QR code is introduced. QR code is Quick Response code. It was introduced in 1994 by Denso-Wave, a Japanese company subsidiary of Toyota. QR code can generate more complex passwords as it can store up to 4296 alphanumeric characters which comes over the disadvantage of the barcode. As it is a two-dimensional barcode, it can be read from any direction.

Figure II. 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 error correction, coding and the final message is structured. The second section decodes the QR Code image and displays the data contained in that QR code[4]. The decoding procedure starts with differentiating the black and white modules and then reorganizes the modules to obtain the decoded format information.

IV. Proposed System

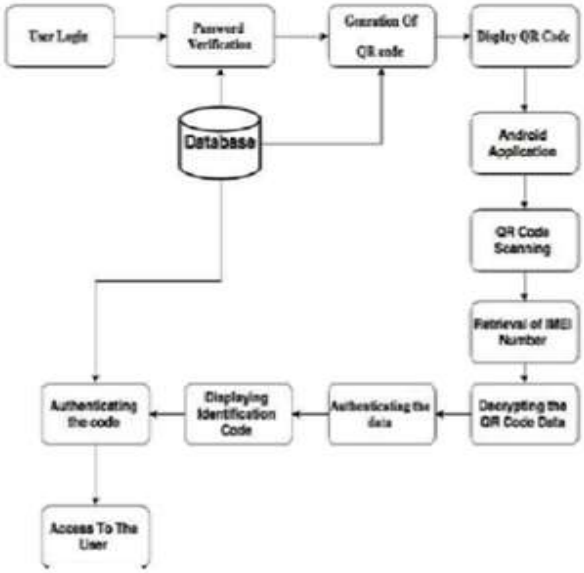

Figure III. System overview diagram

The following steps give the information on how to complete the registration process:- Firstly user would go into the registration section and submit the details like his/her username, Password, IMEI number of the phone. Once the data is validated it will be stored in the database. The data of the database server will produce the public key and private key and store it in the server.

After this, the user will proceed to download the application and install it on his/her phone. When user runs the application for the first time, the class files of public key and private are created and stored into the internal storage of mobile phone. In a registration if the user does not enter all the values like username, password, IMEI number, mobile number and email address then registration process will not get completed. Validation is most important part in the registration process; if validation is not successful then user will not be able to login.

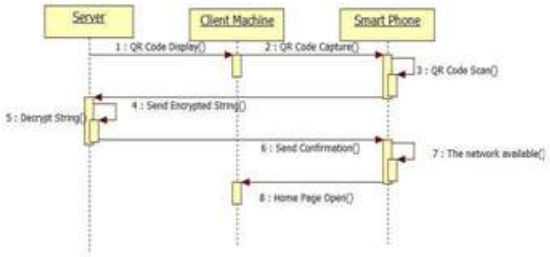

Figure IV. Registration system diagram

V. Implementation

A. Online Authentication System

This method is implied when the user's mobile has access to internet and is online, in which using the public key, random number and the IMEI number are encrypted forming a string. With help of this encrypted string, QR code is generated using QR code generation function. Once it is generated, it will be displayed on the client's machine and the client will scan this QR code with his mobile phone. As it is online mode, after scanning the generated string (combination of a random number and IMEI number) automatically enters the login page with help of the internet. If login is successful, the home page of banking website is displayed. So in

our system there is no real need of remembering the password. The user's public key is used to decrypt the string and also makes sure it exists in our transaction table with the random number and then modifies the row of the table. Then the server checks whether the IMEI is correct or not. If found correct, it assigns that IMEI to the legitimate user[5]. Once the login is successful, the transaction row is deleted and a new QR code image will be generated when the user wish to login again. Now the PHP session is created and when user finishes his transaction and logs off, the session is destroyed.

B. Offline Authentication System

This method is implied when the user's mobile doesn't has access to internet and is offline, in which authentication system, a unique six-digit number is generated using pin code generation algorithm which is formed by the encrypted string(IMEI number and random number). This unique code has to be entered manually on the login page with his username.

After the pin code is entered, the IMEI number is verified with the stored database by the server. If the number matches the database records then the user is a legitimate user and homepage of bank gets displayed and the timestamp is also checked. If the user does not login in the available timestamp of 5 minutes then the session is destroyed and the user won't be able to login.

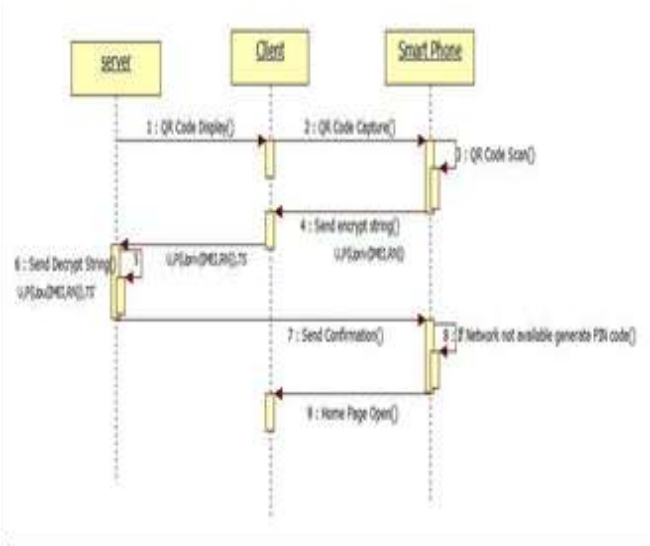

Figure V. Offline authentication

VI. Security

The QR code and the encryption algorithm provide a more powerful security to our system. It does not get vulnerable to the man-in-the-middle attack because the communication between the user and the server is always in the encrypted form. Username also cannot be reused again as it gets deleted after the user logs out of the system. Also for mobile application, person needs to have the password so that it can't be attacked by any other means. If the untrusted person knows to handle the internal storage then only the security problem is created. A phishing attack is possible on the mobile phone if we replace the application by some other application and the pass code also gets covered but it is still not possible if he does not own a certificate[6].
One of the key security feature in offline authentication mode is the timestamp, if user fails to login within the given time period then the login fails.

VII. Conclusion & Future Scope

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. 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 comfortably. We would like to use some advanced encryption and decryption algorithm, better than AES.

References

[1] Snehal.Kalbhor,Ashwini.Mangulkar,Mrs.SnehalKulkarni"Android App for Local Railway Ticketing Using GPS Validation".International Journal of Emerging Trends in Science and Tech.,IJETST-Vol-01,Issue-01,Mar-2014,Pages71-74.

[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 TrustedComputing,DOI10.1109,2012,Pages 638-643.

[3] Mrs.ShantaSondur, Ms.TanushreeBhattacharjee "QR-Decoder and Mobile Payment System for Feature Phone", VESIT,International Technological Conference(I-TechCON)-Jan.03(2014),Pages13-15.

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

[5] Dr.A.P.Adsul,GayatriKumbhar VrundaChincholkar, YogeshKamble, AnujaBankar "Automated Exam Process using QR Code Technology" International Journal of Application or Innovation in Engineering &Management,(IJAIEM)-ISSN 319-4847,Vol.3,Issue 4,April- 2014,Pages-296-298.

[6] Ben Dodson, DebangsuSengupta, 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).