Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2021); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:10, ISSUE:5(1), May:2021
Online Copy of Article Publication Available: www.ijmer.in
Digital certificate of publication:http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
DOI:http://ijmer.in.doi./2021/10.05.125
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 10th May- Publication Date:30th May 2021

A NEW APPROACH OF AUTHENTICATION: USING QR CODE AS A THIRD FACTOR

[1]Dr. V. S Narayana Tinnaluri, [2] Vyas Akondi, [3]M. Dinesh,[4]S. Pavani and [5]K. Havisha
[1]Professor, and [2,3,4,5] IV BTech Student
Department of Computer Science and Engineering
Satya Institute of Technology and Management
Vizianagaram, Andhra Pradesh, India

Abstract

In today's fast-paced environment, smart phone applications or web apps are widely used to support all of our needs, from market research to buying process and service research to service usefulness. The world is being transforming to digital era. In this view the application user data security is an important key prospect; towards Cyber-attacks. So, to overcome this type of situations, our focus is to implement a better security concerning, authentication factor. Already we have models like two factor authentication which is implemented using OTP, and advanced than two factor authentication in using, third factor by considering some of the parameters like user fingerprints, Iris etc... but in this case, the personal information of users needs to be maintained secure, it's one of the baggiest challenges as regards, cost effectiveness, storage and risk factor. The network protection is made up of a variety of protocols and guidelines set by the network administrator to prevent unauthorized access, changes to the network, and misuse of the network's resources. It is one of the most important and difficult domains in different fields where communication-based behaviors occur frequently and the need for data protection is strong. So, by view of all these existing challenges we are proposing a three-factor authentication model, as considering third factor a QR code. In our proposed model, we are planning to use a two-dimensional QR code generation by verifying authentication, which will be validated by the user.

Keywords: Security, 2FA, OTP, QR Code.

Introduction

Despite of wide use of current online system, it has many security issues as it's based on traditional password-based model, no mutual authentication between user and server which leads to threats like phishing(stealing passwords and using them for their purpose), intercepting communication lines, database hacking, etc... To make bank transactions or personal social logins more secure but also keeping them easy for user, following authentication system can be useful. For any type of bank websites or social media accounts or e-cart apps there will be user login which is the first factor of authentication. After that we implement an OTP validation page to validate the user. Even this is not secure because we can bypass the OTP using some professional cyber security tools like Burp suite.

QR Codes are 2-dimensional matrix bar codes originally developed for the automotive industry by a subsidiary of Toyota back in the mid-90s for the rapid decoding of information to track vehicle parts and components. The 2-dimensional QR Code consists of black square modules set on a white background. The format offered a very good mix of legibility and data storage capability. Compared with traditional bar codes (which can usually only encode 20 characters of information) QR Codes could encode significantly larger amounts of data (up to 7,089 numeric or 4,296 alphanumeric characters) that could be read rapidly in any 360° orientation. Also, compared with traditional bar codes, QR codes occupy significantly less space since data is stored both vertically and horizontally. So, for additional security we implement a QR based authentication or validation. The QR code will be allotted to the user at the time of registration. If this authentication is used for the purpose of bank transaction, it's better to give QR code in their bank pass book. If user lose his book, then user needs to intimate respective bank immediately so no cheating will be occurred. If this system is used in social media login, then the QR code will be sent to the user email for every login time.

will be sent to the registered mobile number. The user needs to enter his randomly generated OTP in the validation page for next page authentication. Where as in QR it may vary according to the purpose. After OTP validation QR validation page will be displayed.

To provide security for QR, the content in QR is encrypted content. Normal QR scanner will display the data which not original and the data is encrypted. This can only be validated by our system because we have only the decryption system included in the software. So webapp or mobile app can only validate the QR code. A mobile with a normal camera is enough to scan our QR code. Even webcam of Laptop is more than enough to read data in QR code.

Literature Review

Authentication

Despite its benefits, the Internet is subject to cyber thieves, hackers, and untrustworthy authorities, among other hazards. Unauthorized access, unprivileged activity, repudiation, and alterations of stored material are examples of such dangers. A crucial necessity for every Internet service is the implementation of solid solutions for validating an individual's identity before granting access to resources. In general, an individual must confirm his or her identification, and a credential that claims confirmation of the individual's identification is established. There are three sorts of variables that may be used to link an individual to a recognised credential [2]: ownership (something one has, such as a Badge), knowledge (something one knows, such as a password), and inherence (something one is, such as biometric data-fingerprint/iris pattern) are all concepts that may be used to biometric data. An authentication token is the exact proof that an individual offers to support each factor (the card, the password, or the fingerprint). A variety of suitable tokens may be used to enable several factors, from from basic passwords to information encrypted utilizing the public key infrastructure (PKI). Online security during the sharing of information on the Internet is still a key concern, according to empirical study on information quality delivery via the Internet application [3].

A) OTP

Authentication, the process of identifying and validating an individual is the rudimentary step before granting access to any protected service (such as a personal account). Authentication has been built into the cyber security standards and offers to prevent unauthorized access to safeguarded resources. Authentication mechanisms today create a double layer gateway prior to unlocking any protected information.

This double layer of security, termed as two factor authentication, creates a pathway that requires validation of credentials (username/email and password) followed by creation and validation of the **One Time Password (OTP)**. The OTP is a numeric code that is randomly and uniquely generated during each authentication event. This adds an additional layer of security, as the password generated is fresh set of digits each time an authentication is attempted and it offers the quality of being unpredictable for the next created session.

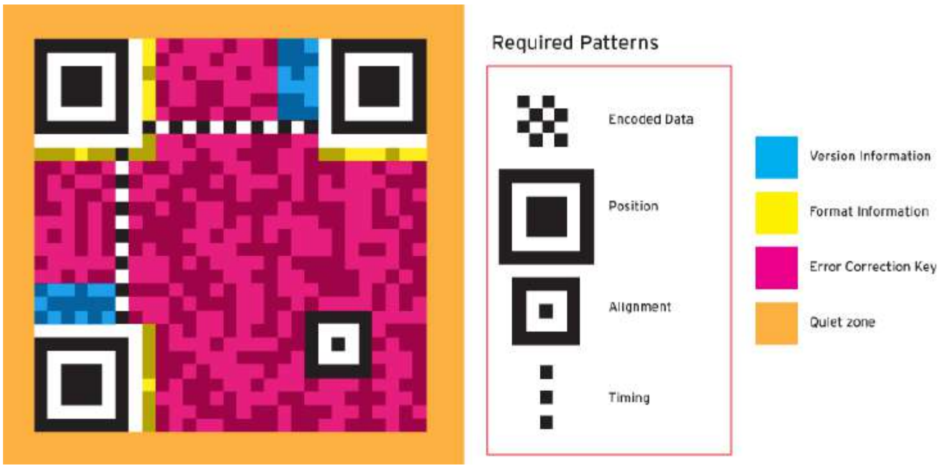
The two main methods for delivery of the OTP are:

1. SMSBased: This is quite straightforward. It is the standard procedure for delivering the OTP via a text message after regular authentication is successful. Here, the OTP is generated on the server side and delivered to the authenticator via text message. It is the most common method of OTP delivery that is encountered across services.

2. ApplicationBased: This method of OTP generation is done on the user side using a specific smartphone application that scans a QR code on the screen. The application is responsible for the unique OTP digits. This reduces wait time for the OTP as well as reduces security risk as compared to the SMS based delivery.

B) QR Code

QR is an abbreviation for Quick Response. QR Codes are 2-dimensional matrix bar codes originally developed for the automotive industry by a subsidiary of Toyota back in the mid-90s for the rapid decoding of information to track vehicle parts and components. The 2-dimensional QR Code consists of black square modules set on a white background. The format offered a very good mix of legibility and data storage capability. Compared with traditional bar codes (which can usually only encode 20 characters of information) QR Codes could encode significantly larger amounts of data (up to 7,089 numeric or 4,296 alphanumeric characters) that could be read rapidly in any 360° orientation. Also, compared with traditional bar codes, QR codes occupy significantly less space since data is stored both vertically and horizontally.

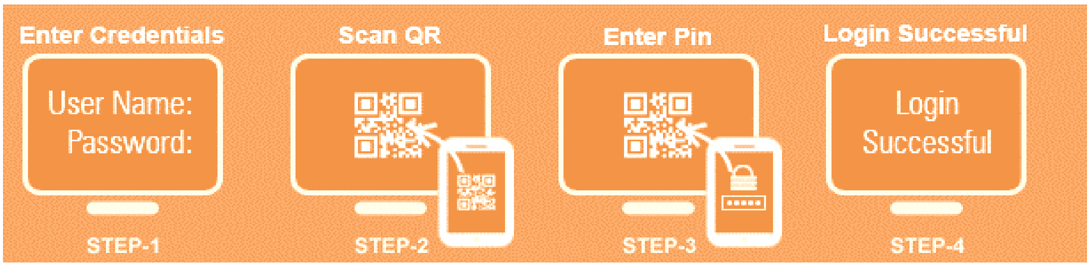


Position: The three position markers allow the QR code reader to quickly identify and orient that image in order to scan it.
Alignment: This detects any curvature or distortion to the code and allows the reader to make corrections as needed.

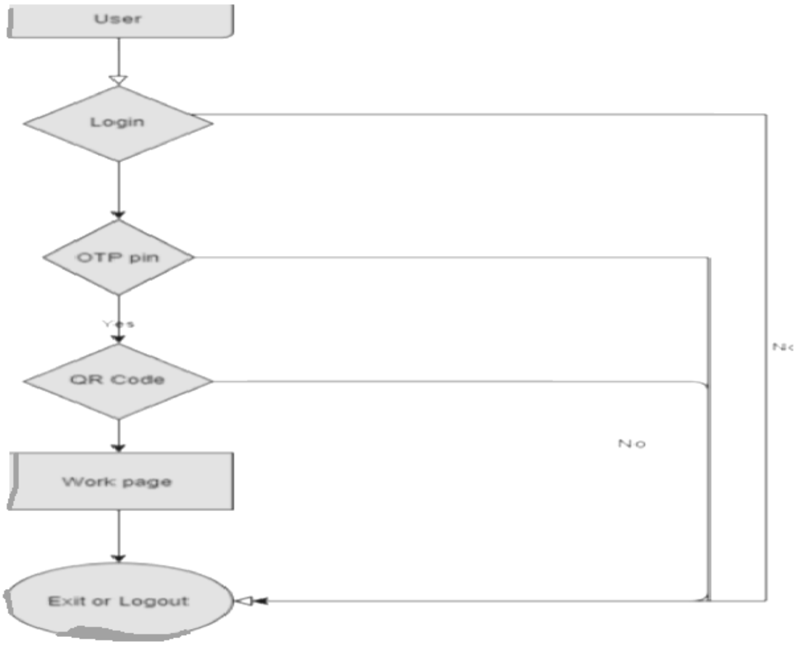
Timing: Determine coordinates for the scanner.
Version Information: Identifies the version of the QR Code. Different versions allow for different levels of data capacity and error correction.
Format Information: Contains information regarding the mask for the code and error correction.
Quiet Zone: These are the margins of the QR Code. It is recommended to leave 2-3 blocks of quiet zone to ensure an optimum scan.

Proposed Authentication System

The main objective is to create an online authentication system that is efficient, resilient, scalable, and simple to use. We introduce and evaluate the authentication strategy, which combines ownership factors (such as a mobile phone or a smartcard) with knowledge factors (OTP). The approach is based on a smart card and optical challenge response solution in which authentication is performed using a camera-equipped mobile phone. Using a form of knowledge-based authentication challenge to the user's smart phone rather than a code shown in clear language improves the scheme's security. Because to its simplicity of use, deployment, and cost effectiveness, this solution has a high usability. The user visits a website and logs in or registers. The user must now launch an app on their smartphone that is secured by a pin number and scan a one-time QR code that appears using the phone's main camera. The application then uses an out-of-band channel to connect with the server and offer verification of device ownership. The user serves as a link between the authorised device and the authentication entity in this scenario. A new user is required to create an account on the website. The user is prompted to submit login credentials, which include alpha numeric values as user choiced, and is then logged in using those credentials. The user's mobile device is then installed with the mobile application. For subsequent mobile authentication, the user must select a pin. The user account's list of devices now includes a mobile unique ID. When the user inputs their credentials in the browser from now on, a QR code will appear. When requested, the QR code is scanned and the PIN for the mobile application is entered. The user has successfully logged in if the QR and PIN are both valid.

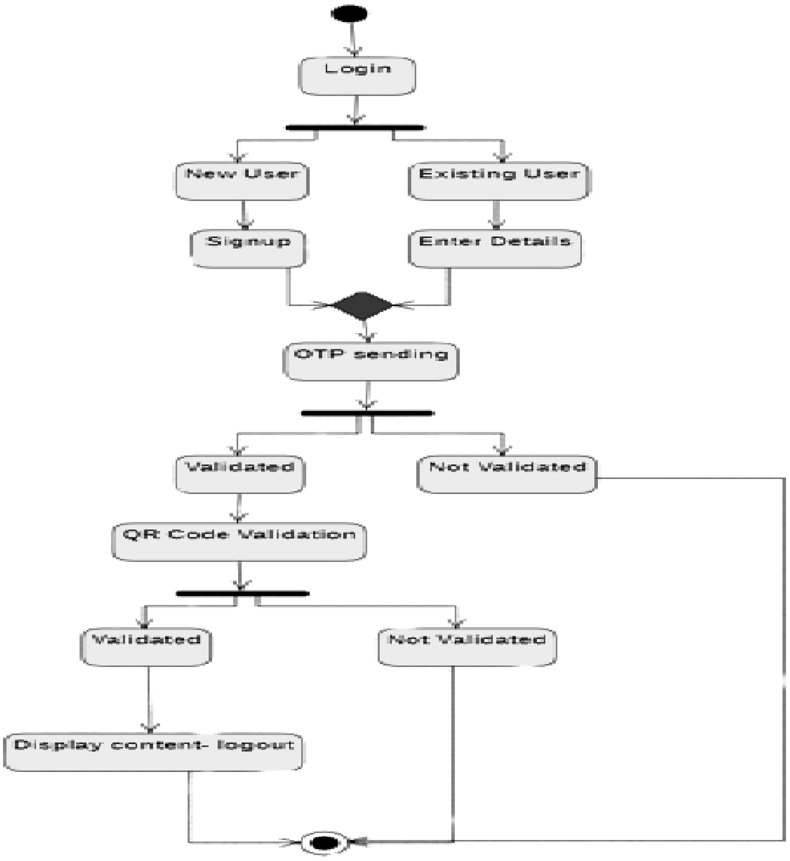


The flow representation and activity diagram which gives us clear vision about the process of authentication.



The above flow chart explains about how the system to be designed. The main steps involved in this system are user login – login validation, OTP – OTP Validation, QR code scanning – QR code validation, Displaying content page, Logout.

The Below Activity diagram show how the flow of work is going on. In the activity diagram, every validation step shows the validation failure steps also. So, there will be no confusion if any of the step is invalid.



Advantages in using the proposed idea

Robustness

- It is possible to make it available on all mobile platforms.
- In the event that the old phone is lost or altered, a secure handover to the new phone is required.

Secure

- In the event that the old phone is lost or altered, a secure handover to the new phone is required.
- Man-in-the-middle assaults have little chance of succeeding.
- The user authenticated to the server over mobile internet/GPRS, as opposed to the original Server to PC, QR originating channel, which resulted in increased security.
- The QR codes are created, which ensures that they are always unique and random.
- QR codes are 2D matrix codes with fast encryption and decryption speeds, as well as the capacity to store enormous amounts of data and repair errors.

Convenient

- There's no need for long, complicated usernames and passwords.

- In comparison to other second factor tokens and hardware, the mobile phone is more ubiquitous—almost everyone already has one.
- Unlike other options, there is no additional hardware expense.
- It's simple to set up and utilise.

Conclusion

This concept may be used to establish high levels of security in applications such as Net Banking, Online Shopping, and identifying counterfeit goods, among others. True random numbers are used to generate QR codes, which makes them incredibly distinctive and safe. The advantage of this method is that it eliminates the need for external hardware such as tokens and smartcards. These properties make it a very appealing alternative for future applications requiring second-level authentication. Every day, the digitalization process progresses in small steps. In this digital age, we need robust security provisions to protect our digital transactions and logins, which I believe our system will deliver. The user can only access his account with OTP and QR code authentication. Without the OTP and QR code, no one can access the user account.

References

1. Afrin Hussain, Dr. MN Nachappa, Author and Mentor respectively, Department of MCA, Jain University, Bengaluru, Karnataka, India, “E-Authentication System with QR Code & OTP”, International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 4 Issue 3, April 2020
2. Anna Vapen and NahidShahmehri, 2011. 2-clickAuth: Optical Challenge- Response Authentication Using Mobile Handsets.International Journal of Mobile Computing and Multimedia Communications. Volume 3, Issue 2, 1-18. DOI: 10.4018/jmcmc.2011040101URL: http://dl.acm.org/citation.cfm?id=2440583.2440584&coll=DL&dl=GUIDE&CFID=372999437&CFTOKEN=5481709
3. Gregory D. Williamson, 2006. Enhanced Authentication in Online Banking.Journal of Economic Crime Management. Volume 4, Issue 2.
4. Vittorio Bagini and Marco Bucci, 1999. A Design of Reliable True Random Number Generator for Cryptographic Applications. Cryptographic Hardware and Embedded Systems, First International Workshop, CHES’99 Worcester, MA, USA, August 12–13, 1999 Proceedings. Springer Berlin Heidelberg. 1717: 2014-218 DOI: 10.1007/3-540-48059-5_18 URL: http://link.springer.com/chapter/10.1007%2F3-540-48059-5_18
5. Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner and HaoZheng, 2003. Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts. Fifth International Workshop, Cologne, Germany, September 8–10, 2003. Springer Berlin Heidelberg. 2779: 152-165 URL: http://link.springer.com/chapter/10.1007%2F978-3-540-45238-6_13#page-1
6. Wen-Pinn Fang, 2011.Offline QR Code Authorization Based on Visual Cryptography. Seventh International Conference. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). 89-92. DOI: 10.1109/IIHMSP.2011.10 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6079541&url=htt p%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6 079541
7. Jonathan Wei and WeiQi Yan, 2012. Authenticating visual cryptography shares using 2d barcodes. IWDW'11 Proceedings of the 10th international conference on Digital-Forensics and Watermarking. Springer-Verlag Berlin, Heidelberg.7128: 196-210. DOI:10.1007/978-3-642-32205-1_17
8. RishabhKulshreshtha, AyushiKamboj, Sanjay Singh, 2012. Decoding robustness performance comparison for QR and data matrix code.CCSEIT '12 Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology.722-731. DOI: 10.1145/2393216.2393337
9. P. Preneel, V. Rijmen, and A. Bosselaers, 1998. Principles and Performance of Cryptographic Algorithms, " Dr.Dobb's Journal, Volume 23: 126 – 131. URL: http://www.drdobbs.com/algorithm-alley/184410756

Filename:	5
Directory:	C:\Users\DELL\Documents
Template:	C:\Users\DELL\AppData\Roaming\Microsoft\Templates\Normal.dotm
Title:	
Subject:	
Author:	Windows User
Keywords:	
Comments:	
Creation Date:	5/15/2021 12:19:00 PM
Change Number:	5
Last Saved On:	5/31/2021 9:45:00 PM
Last Saved By:	Murali Korada
Total Editing Time:	26 Minutes
Last Printed On:	6/2/2021 11:37:00 PM
As of Last Complete Printing	
Number of Pages:	5
Number of Words:	2,433 (approx.)
Number of Characters:	13,871 (approx.)