E-Authentication System using QR Code and OTP

Miss. Shweta Kamble[1], Miss. Pooja Kendre[2], Miss. Ayesha Siddiqua[3], Mr. Deshpande G.R[4]

Students, Department of Computer Engineering[1,2,3]

Assistant Professor, Department of Computer Engineering[4]

Gramin Technical and Management, Nanded, Maharashtra, India

Abstract*: This paper proposes an authentication system that combines One-Time Password (OTP) and Quick Response (QR) code technologies to enhance security and user experience. The system generates an OTP and a unique QR code for each authentication attempt, which can be scanned using a mobile device to complete the authentication process. The QR code contains encrypted information about the user's identity and the OTP, which is verified by the server. The proposed system provides a secure, convenient, and efficient method for user authentication, which is crucial in today's digital world. An e-authentication system that uses OTP and QR code technology is a secure and efficient method for authenticating users in online transactions. This system combines the benefits of OTP and QR code technology to provide a two-factor authentication mechanism that is convenient for users and effective in preventing unauthorized access. This system aims to address the vulnerabilities of traditional username and password authentication by providing an additional layer of security through two-factor authentication. the system aims to prevent unauthorized access to online services and transactions. The system aims to provide a userfriendly and convenient authentication method that can be easily integrated into existing online platforms. It protect sensitive information and ensure that only authorized users can access online services and transactions*

Keywords: OTP generation, QR code

I. INTRODUCTION

This chapter gives the background of authentication system. The definition of The E authentication system using QR code and OTP is a project that aims to provide a secure and efficient way of verifying the identity of users for various purposes. The system uses QR codes and OTPs to authenticate users and prevent unauthorized access, fraud, and identity theft. The project is designed to be scalable, flexible, and easy to integrate with existing systems and technologies.

In today's digital age, online transactions have become an essential part of our daily lives, from online shopping to banking and other financial transactions. However, traditional methods of authentication, such as usernames and passwords, are becoming increasingly vulnerable to hacking attempts and identity theft. As a result, there is a need for more secure and efficient authentication methods

An e-authentication system that uses OTP and QR code technology is a two-factor authentication method that provides an additional layer of security for online transactions. OTP is a unique password that is generated for each authentication attempt and is sent to the user's registered mobile number or email. A QR code is a two-dimensional barcode that can be scanned using a mobile device to access encrypted information about the user's identity and OTP. Traditional authentication methods, such as usernames and passwords, are becoming increasingly vulnerable to hacking attempts and identity theft. Therefore, there is a need for more secure and efficient authentication methods. Traditional authentication methods, such as usernames and passwords, are becoming increasingly vulnerable to hacking attempts and identity theft. Therefore, there is a need for more secure and efficient authentication methods.

II. RELATED WORK

OTP (One-time password):

An OTP is a made mystery word which simply significant once. It is a consequently delivered numeric or alphanumeric series of characters that approves the client for a solitary exchange or login meeting. OTP security tokens are chip based savvy cards or pocket-size key dandies that produce a numeric or alphanumeric code to affirm admittance to the structure or string. This mystery code changes every 30 or 60 seconds, dependent upon how the token is planned. The

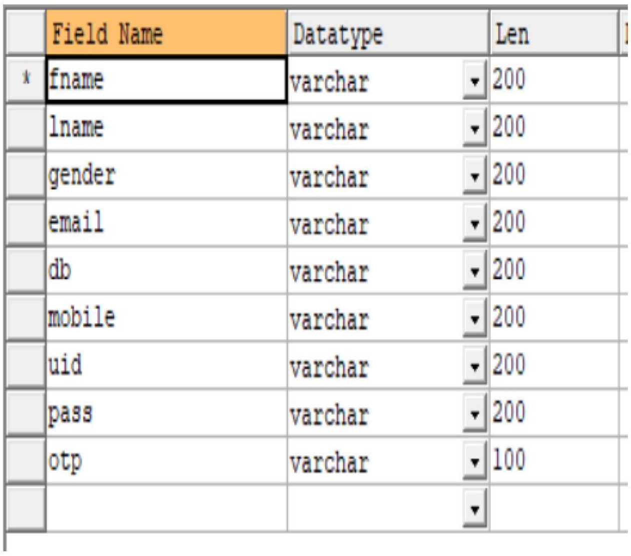
DOI: 10.48175/IJARSCT-14204

client is given a device that can make an OTP using a calculation and cryptographic keys. On the server side, an affirmation server can really look at the authenticity of the mystery key by having a comparable calculation and keys. In OTP-based approval procedures, the client's OTP application and the confirmation server rely upon shared insider realities. Characteristics for onetime passwords are delivered using the Hashed Message Authentication Code (HMAC) calculation and a moving component, for instance, time touchy information (TOTP) or an event counter (HOTP). The OTP values have second or second timestamps for more noticeable security. The one-time secret expression can be passed on to a client through a couple of channels, including a SMS-based text, an email or a serious application on the endpoint.

QR CODE:

A QR Code is a Matrix code and a two-layered standardized identification made by the Japanese affiliation Denso Wave. Data is encoded in both the vertical and flat course, thusly holding up to a couple on numerous occasions a larger number of information than an ordinary standardized identification. Information is gotten to by getting a photo of the code by using a camera (for instance combined with a cell phone) and dealing with the picture with a QR peruse.

TABLE



Field Name	Datatype	Len
fname	varchar	200
lname	varchar	200
gender	varchar	200
email	varchar	200
db	varchar	200
mobile	varchar	200
uid	varchar	200
pass	varchar	200
otp	varchar	100

DOI: 10.48175/IJARSCT-14204

This development has been around for longer than 10 years yet has become as a vehicle for backers to show up at cutting edge cell phone clients. Quick Response Codes, or QR Codes, are just old news new. Truth to be told, in Japan and Europe they have been utilized as a piece of advancing and moreover stock controlwhat's more, storing up all through the beyond 10 years. The security of one layered (1D) standardized identification is lower than 2D scanner tags. 1D standardized identifications are certainly not hard to examine by separating the lines and the spaces. Regardless, 2D scanner tags are difficult to examine an image plan by natural eyes. As to weightiness, one layered standardized identifications should yield along a solitary heading. On the off chance that the reason for a sweep line doesn't fit inside a reach, the information wouldn't be examined precisely. In any case, 2D standardized tags get wide extent of plot for examining. The critical differentiation between the two is the extent of information they can hold or share. Scanner labels are straight onelayered codes and can essentially hold up to 20 mathematical digits, but QR codes are two-layered (2D) lattice standardized tags that can hold 7,089 numeric characters and 4,296 alphanumeric characters, and 1,817 kanji.

III. SCOPE

Financial Services: This system can be used by banks, financial institutions, and payment processors to authenticate users accessing online banking and payment services.

E-commerce: Online retailers can use this system to authenticate users making purchases, ensuring secure payment transactions. ¬

Healthcare: Healthcare providers can use this system to authenticate patients accessing their electronic health records, ensuring secure access to sensitive medical information.

Education: Educational institutions can use this system to authenticate students accessing online course materials and exams, ensuring secure access to educational resources. ¬

Government Services: Government agencies can use this system to authenticate users accessing online services, such as tax filing, passport application, and social security services, ensuring secure access to sensitive information. ¬

Travel and Hospitality: Travel and hospitality industries can use this system to authenticate users booking reservations and making payments, ensuring secure transactions.

Online Gaming: Gaming companies can use this system to authenticate users accessing online gaming platforms, ensuring secure access to gaming resources.

V. HARDWARE REQUIREMENTS

- System: Pentium i5 Processor
- Hard Disk: 500 GB.
- Monitor: 15’’ LED
- Input Devices: Keyboard, Mouse
- Ram: 8 GB

VI. SOFTWARE REQUIREMENTS

- Operating system: Windows 10.
- Coding Language: HTML, CSS, JAVA, JS, JAVA SERVLET
- Tool: Eclipse IDE
- Database: MYSQL-8

VII. SYSTEM DESIGN

- **User Registration:** The first step in the authentication process is user registration. Users need to provide their basic information, such as name, email address, and mobile number, and set up their login credentials, such as username and password.

- **OTP Generation:** Once a user logs in, the system generates a One-Time Password (OTP) that is sent to the user's registered mobile number or email address. The OTP is a temporary code that is valid for a limited time and can be used to verify the user's identity.
- **QR Code Generation:** The system also generates a unique QR code for the user, which can be scanned using a mobile device to initiate the authentication process.
- **QR Code Scanning:** To authenticate using the QR code, the user scans the QR code using a mobile device, which launches the authentication process on the user's device.
- **OTP Verification:** The user enters the OTP received on their mobile device or email address into the system to verify their identity.
- **Authentication:** Once the OTP is verified, the system authenticates the user and grants access to the requested service or information.
- **Security Measures:** The system design incorporates security measures to protect against unauthorized access, such as rate limiting to prevent brute-force attacks, encryption to protect user data, and two-factor authentication to enhance security.

VIII. MODULESOF E- AUTHENTICATION SYSTEM USING OTP AND QR CODE

- **User Registration Module:** This module allows users to register for the service by providing their basic information, such as name, email address, and mobile number, and setting up their login credentials.
- **OTP Generation Module:** This module generates a One-Time Password (OTP) that is sent to the user's registered mobile number or email address.
- **QR Code Generation Module:** This module generates a unique QR code for the user that can be scanned using a mobile device to initiate the authentication process.
- **QR Code Scanning Module:** This module allows users to scan the QR code using their mobile device to launch the authentication process.
- **OTP Verification Module:** This module verifies the OTP entered by the user to authenticate their identity
- **Authentication Module:** This module grants access to the requested service or information upon successful authentication.
- **Security Module:** This module includes security measures, such as rate limiting to prevent brute-force attacks, encryption to protect user data, and two-factor authentication to enhance security.
- **Audit Trail Module:** This module maintains an audit trail of all authentication attempts, including successful and unsuccessful attempts, to enable monitoring and analysis of user activity.
- **User Management Module:** This module allows administrators to manage user accounts, such as adding or deleting users, resetting passwords, and disabling or enabling accounts.

VIIII. METHODLOGY

- **Surveys:** Surveys can be conducted to gather data on user requirements, preferences, and feedback on the e-authentication system. This could include questions about the ease of use, effectiveness, and security of the system.
- **User Testing:** User testing can be conducted to observe how users interact with the system and identify any usability issues. This could involve conducting usability tests, A/B testing, and user interviews.
- **Analytics:** Analytics can be used to gather data on user behavior, such as login attempts, authentication failures, and successful logins. This could help identify patterns and trends in user activity, and enable the system to adapt to changing user needs.
- **Logs:** The system can maintain logs of all user activity, including successful and unsuccessful login attempts, OTP requests, and QR code scans. These logs can be used for monitoring and analysis of user activity.
- **Feedback Forms:** Feedback forms can be provided to users to gather their feedback on the system. This could include questions about the user experience, security, and effectiveness of the system.

DOI: 10.48175/IJARSCT-14204

- **Interviews:** Interviews with users, administrators, and other stakeholders can be conducted to gather qualitative data on the system's effectiveness, usability, and security.
- **Case Studies:** Case studies can be conducted to gather data on specific instances where the e-authentication system was used. This could help identify areas for improvement and potential solutions to common issues.

X. CONCLUSION

In conclusion, an e-authentication system using OTP and QR code is a secure and efficient way of authenticating users for online services. The system offers an easy-to-use and accessible way for users to log in securely and reduce the risk of unauthorized access. The system's use of OTP and QR code technologies ensures that the user's identity is verified in a timely and secure manner. The system's design allows for flexibility, scalability, and ease of integration with other systems. The system also has potential applications in various sectors, including banking, e-commerce, and healthcare, where secure authentication is of utmost importance. Furthermore, the system can be customized to meet the specific needs of various organizations, making it a versatile solution for online authentication. Overall, the e-authentication system using OTP and QR code is a reliable and secure solution that has the potential to transform online authentication and provide users with a seamless and secure login experience.

REFRERNCES

[1]. Max E. Vizcarra Melgar and Luz M. Santander, "An alternative proposal of tracking products using digital signatures and QR codes," in Proceedings of the 2014 IEEE Colombian Conference on Communications and Computing, June 2014.

[2]. H. Bagherinia and R. Manduchi, "A Theory of Color Barcodes," in Proceedings of the IEEE Color and Photometry in Computer Vision Workshop, 2011.

[3]. M. S. B. Akila, B. Hema, "Secured Data Encoding Technique in High CapacityColor Barcodes for M-Ticket Application," in International Journal of Electronics and Computer Science Engineering, 2008.

[4]. Max E. Vizcarra Melgar and Mylene C. Q. Farias, "High Density ` Two-Dimensional Color Code," in Multimedia Tools and Applications, vol. 78, July 2018, pp. 1949–1970.

DOI: 10.48175/IJARSCT-14204