IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

E-Authentication System Using OTP & QR Code

[1]Harsh Sharma, [2]Gautam Kumar Singh, [3]Raj Kumar, [4]Panaag Bhushan, [5]Chaman Kumar

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor

[1]Department of Information Technology,

[1]IIMT College of Engineering, Greater Noida, 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 user-friendly 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.

INTRODUCTION

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.

FACTS AND STATISTICS

- Two-factor authentication (2FA), which includes the use of OTP and QR code, can reduce the risk of account takeovers by up to 99.9%
- According to a report by Cybersecurity Ventures, the global cost of cybercrime is projected to reach $10.5 trillion USD annually by 2025, making it a significant concern for businesses and individuals alike.
- A survey by Ponemon Institute found that 64% of respondents experienced a phishing attack that resulted in a data breach, highlighting the vulnerability of traditional username and password authentication methods.
- The use of biometric authentication, such as fingerprint scanning and facial recognition, is increasing, with the market projected to grow from $17.2 billion in 2020 to $36.6 billion in 2025.
- A study by Google found that using two-factor authentication can prevent 100% of automated attacks, 99% of bulk phishing attacks, and 66% of targeted attacks.

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.

IDENTIFICATION OF NEED

The need for an e-authentication system using OTP and QR code technology arises from the limitations and vulnerabilities of traditional authentication methods, such as username and password. Here are some of the reasons why this system is needed:

Weak Passwords: Passwords are often the weakest link in online security, as users tend to choose weak and easily guessable passwords, or reuse the same password across multiple accounts, making them vulnerable to hacking and data breaches.

Phishing Attacks: Phishing attacks are a common tactic used by hackers to steal login credentials by tricking users into entering their login information on fake websites or through malicious emails.

Identity Theft: Identity theft is a growing concern in the digital age, as hackers can use stolen login credentials to gain access to sensitive information and perform fraudulent transactions.

Regulatory Compliance: Regulatory bodies require organizations to implement strong authentication methods to protect sensitive information and comply with data protection regulations.

User Experience: Traditional authentication methods can be cumbersome and time-consuming, leading to frustration among users and increasing the likelihood of security breaches due to shortcuts taken by users to bypass security measures.

Increasing Cyber Threats: The frequency and sophistication of cyber-attacks are increasing, making it imperative for organizations to implement stronger authentication methods to protect against data breaches.

SYSTEM DESIGN

1) **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.

2) **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.

3) **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.

4) **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.

5) **OTP Verification**: The user enters the OTP received on their mobile device or email address into the system to verify their identity.

6) **Authentication**: Once the OTP is verified, the system authenticates the user and grants access to the requested service or information.

7) **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.

MODULES OF E-AUTHENTICATION SYSTEM USING OTP & 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.

METHODOLOGY

a) **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.

b) **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.

c) **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.

d) **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.

e) **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.

f) **Interviews**: Interviews with users, administrators, and other stakeholders can be conducted to gather qualitative data on the system's effectiveness, usability, and security.

g) **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.

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.

REFERENCES

- "Design and Implementation of Two-factor Authentication Using OTP and QR Code" by R. Suganya and R. Deepa, International Journal of Engineering and Technology, 2018.
- "A New Two-Factor Authentication Scheme Using QR-Code and One-Time Password for Secure Internet Services" by J.-S. Yoon, K.-B. Kim, and Y.-H. Kim, Journal of Information Processing Systems, 2018.
- "A Two-Factor Authentication System Using QR Code and One-Time Password" by H. Kim and M. Yoon, International Journal of Engineering and Technology, 2017.