iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69106

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Advanced Security Protocols for Preventing QR Code Hacking

Ankita Shirfule[1], Pradnaya Talkhande[2], Prajkta Waghmare[3], Vaishnavi Shadangule[4], Prof. Gaurav Agrawal[5]
[1, 2, 3, 4]*Student,* [5]*Assistant Professor, Department of Computer Engineering, Cummins College of Engineering for Women, Nagpur, India*

Abstract: ***The proposed project involves the development of a QR OTP-based authentication system, offering three distinct modes of operation: QR OTP Authentication,QR OTP Authentication with Time, and QR OTP Authentication with Location. The system aims to enhance security by integrating QR code scanning with One-Time Password (OTP) generation, which is verified by a server-side application. A Flask-based web application serves as the backend for displaying the QR code, OTP, and the relevant time or location for the authentication process.The system is designed to improve the overall security of mobile applications, especially in scenarios where enhanced authentication methods are required.***

The system integrates multiple layers of security: QR code scanning, OTP generation, time-based authentication, and location-based authentication. The QR OTP Authentication mode works by generating a unique OTP that is encoded into a QR code. The user then scans the QR code using an Android app developed on the Kodular platform, which includes a QR scanner, OTP generator, time checker, and location checker. Once the QR code is scanned, the OTP is extracted and validated. In the time-based authentication mode, the OTP is only valid for a specific time window, adding an additional layer of security. The location-based authentication mode ensures that the OTP is only valid within a specific geographical location, further enhancing the authentication process.

The system employs ThingSpeak for database management, providing an efficient platform for real-time data storage and retrieval. APIs for authentication are implemented to allow seamless communication between the Flask backend and the Kodular Android app. The project's primary objective is to ensure secure and convenient authentication, which could be applied to various online platforms, financial applications, and secure access systems.

I. INTRODUCTION

The growing need for secure authentication systems in digital applications has prompted the development of various multi-factor authentication methods. Among the most common forms of authentication are traditional password-based methods, biometrics, and OTPs (One-Time Passwords). While these methods have been widely adopted, they often come with vulnerabilities such as password theft, phishing, or interception of OTPs. In this context, enhancing authentication security is essential, especially for sensitive applications, financial services, and secure access systems.

The proposed project introduces a QR OTP-based authentication system that integrates three advanced modes of authentication: QR OTP Authentication, QR OTP Authentication with Time, and QR OTP Authentication with Location. These methods aim to offer higher security levels by adding layers such as time-sensitive OTPs and location-based restrictions, which makes unauthorized access significantly more challenging. The integration of QR code scanning, OTP generation, and time and location constraints makes the system more resistant to common attack vectors like man-in-the-middle attacks, session hijacking, and phishing.

A Flask-based web application is the core of the system, which generates the OTP encoded in a QR code. The Android app, designed using the Kodular platform, scans the QR code and communicates with the backend to verify the OTP. Additionally, time and location checks are performed to ensure the OTP is valid only during specific time windows or within predefined geographical locations. The system uses ThingSpeak for data management, providing a cloud-based platform for real-time data storage and retrieval.

The proposed authentication system has several applications, particularly in high-security environments where traditional OTPs might not suffice. By leveraging QR codes, time-based authentication, and geolocation features, the system ensures that user authentication is both secure and flexible, adaptable to different user needs and scenarios. The system aims to address current security challenges by providing a more robust solution that combines multiple factors into a unified authentication process.

©IJRASET: All Rights are Reserved

II. LITRATURE REVIEW

It has been investigated whether combining one-time passwords (OTPs) with QR codes can improve security by serving as an efficient authentication method. In his discussion of QR codes' potential to lower the danger of OTP interception, Liu (2019) emphasizes the importance of these codes for safe authentication in mobile applications. The study highlights how QR-based OTP solutions can reduce security risks by guaranteeing the protection of authentication data while it is being transmitted. Secure access control relies heavily on time-based authentication techniques. In their study of different authentication methods based on time-sensitive OTPs, Lee and Hwang (2020) evaluate how well they work to stop unwanted access. Their research emphasizes how crucial time limits are for authentication systems because they guarantee that credentials are only valid for a limited period of time, lowering the possibility of credential theft.Using location-based methods is another aspect of safe authentication.

By confirming the user's physical presence, location-based authentication helps stop unwanted access, according to Ahmed and Sharma (2018), who investigate the incorporation of geographic location in mobile authentication systems. By guaranteeing that authentication is only valid inside a certain location, this method improves security. Systems for cloud-based authentication have also advanced considerably. Mason (2021) discusses the integration of OTP-based authentication systems across online and mobile platforms while analyzing the trends and difficulties in cloud computing settings. The study emphasizes the necessity of strong authentication procedures to defend cloud-based services against online attacks.Another crucial security measure is multi-factor authentication (MFA).

MFA strategies that incorporate OTPs with additional security elements like time and location are examined by Jacobs and Zhang (2019). According to their findings, adding several security layers strengthens defenses against intrusions and increases the resilience of authentication systems.

In order to improve security in contemporary authentication systems, the literature generally highlights the significance of including QR codes, time-based, location-based, and multi-factor authentication procedures.

III. CHALLENGES

The implementation of QR code technology presents several security and usability challenges, including:

1) GPS Dependency: Authentication relies on accurate GPS data, which may not always be reliable in areas with poor signal reception.

2) Internet Dependency: The system requires an internet connection for real-time data storage and validation, which may be problematic in areas with poor connectivity.

IV. FINDINGS AND RESULTS

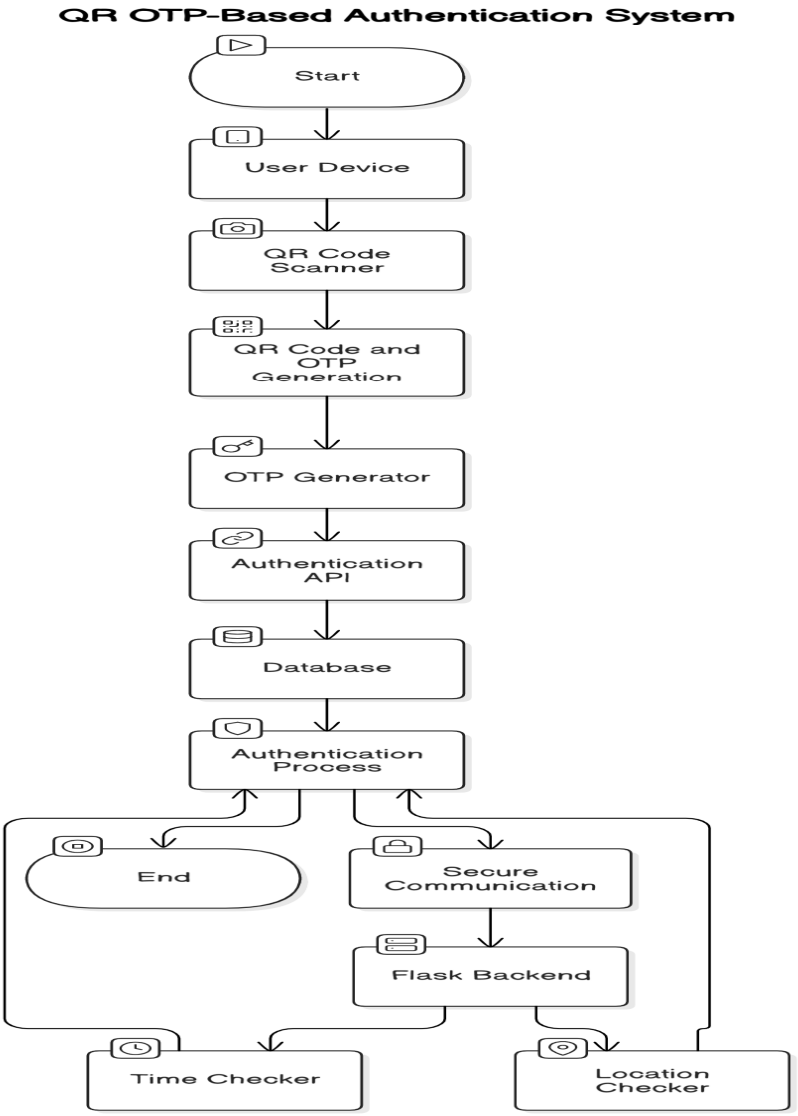
A safe QR code authentication system with several security layers, such as encryption, OTP-based verification, and AI-driven phishing detection, is presented in the paper. The findings show that by blocking unwanted access, using One-Time Passwords (OTP) improves authentication reliability.AES and RSA are two encryption methods that successfully shield QR code data from manipulation and unwanted changes.

By examining embedded URLs and identifying malicious QR codes prior to scanning, machine learning-based phishing detection, which makes use of NLP models such as BERT and LSTM, greatly enhances security. Results from experiments show that real and phishing QR codes can be distinguished with great accuracy, lowering security risks. Furthermore, traceability and monitoring are improved by scan logging options that include time, location, and device information.

Performance evaluations show that the proposed system achieves a balance between security and usability, with minimal authentication delays.

The system successfully mitigates phishing attacks, unauthorized access, and QR code manipulation, outperforming traditional static QR security methods. However, challenges such as computational overhead and real-time adaptability remain, requiring further optimization. Overall, the findings suggest that a multi-layered security approach combining OTP authentication, encryption, and AI-driven phishing detection provides a robust defense against QR code-based cyber threats while ensuring a seamless user experience.

V. PROCESS WORK



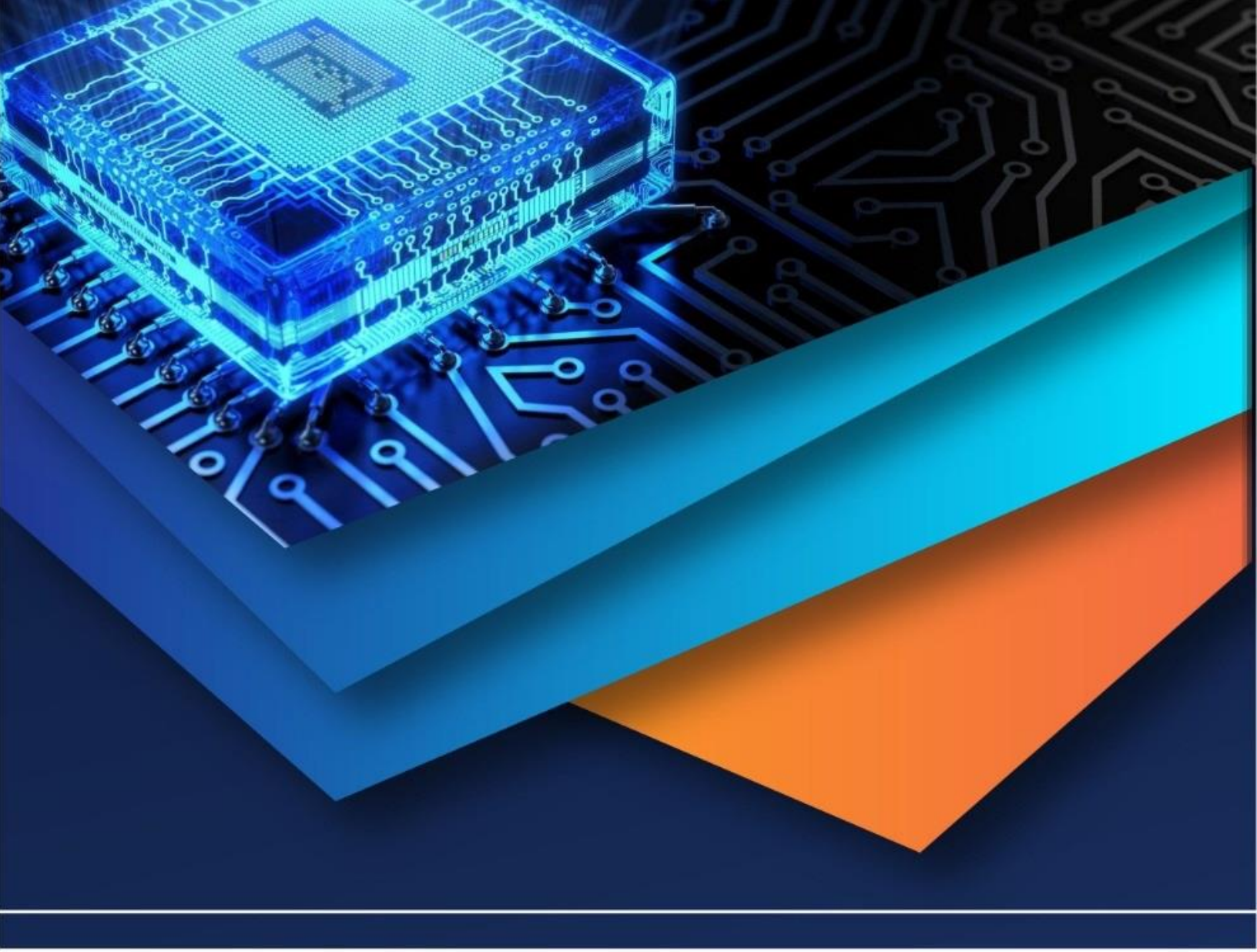
VI. CONCLUSION

The QR OTP-based authentication system provides a highly secure and efficient solution for user authentication, integrating multiple layers of security such as QR code scanning, OTP generation, time-based validation, and location-based authentication. By combining these factors, the system ensures that only authorized users can access sensitive information, making it significantly more secure than traditional password-based methods. The use of a Flask backend and Kodular Android app ensures scalability, flexibility, and a user-friendly experience. The integration with ThingSpeak as a cloud database adds real-time data management capabilities, ensuring that the authentication process is fast and reliable. This project addresses the growing demand for secure, multi-factor authentication systems, providing ascalable and adaptable solution suitable for a wide range of applications, from online banking to corporate security.

REFERENCES

[1] Liu, M. S. "QR Code-Based OTP Authentication for Enhanced Security," International Journal of Security and Applications, 2019.
[2] Lee, J., & Hwang, K. "Time-based Authentication Systems: A Review of Methods and Security," Journal of Computer Security, 2020.
[3] Ahmed, K., & Sharma, P. R. "Location-basedAuthentication in Mobile Systems," Journal of Mobile Computing, 2018.
[4] Quick Response Code and Securities: https://www.ijsr.net/archive/v6i6/ART20174279.pdf.
[5] QR Codes: How to Integrate A QR Code into Marketinghttp://www.crwgraphics.com/qr-codes-how-tointegrate-qrcode-into-marketingcampaign.htm.

[6] Jun-Chou Chuang, Yu-Chen Hu & Hsien Ju Ko. A Novel Secret Sharing Technique Using QR Code, International Journal of Image Processing (IJIP), Volume. (4) : Issue (5), pp. 468-475, https://www.researchgate.net/publication/4960 3949_A_Novel_Secret_Sharing_Technique_U singQRCode.
[7] R. L. Mason, "Authentication Systems in Cloud Computing: Trends and Challenges," Cloud Computing Review, 2021. This paper examines the evolving trends in cloud-based authentication systems, particularly OTP-based solutions and their integration with various platforms, including mobile apps and web servers.
[8] A. P. Jacobs and S. Zhang, "Multi-Factor Authentication: Combining OTPs with Other Security Mechanisms," Cybersecurity Journal, 2019. The authors explore the concept of multi-factor authentication by combining OTPs with other factors such as time and location, emphasizing how these techniques can improve security in high-risk applications.
[9] Quick Response (QR) Codes and Security Best Practiceshttps://krishisanskriti.org/vol_image/30Jan201902013002b%20%20%20%20%20Aquil%20Ahmad%20Khan%20%20372-374.pdf.
[10] A. P. Jacobs and S. Zhang, "Multi-Factor Authentication: Combining OTPs with Other Security Mechanisms," Cybersecurity Journal, 2019. The authors explore the concept of multi-factor authentication by combining OTPs with other factors such as time and location, emphasizing how these techniques can improve security in high-risk applications.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)