E–AUTHENTACTION SYSTEM USING QR CODE AND OTP

V.Srehitha,MD.Zeeshan,G.SaiThanush, K. Rohit ,J.Chaitanya

Department of CSE, Balaji Institute of Technology and Science, Laknepally, Warangal, India

ABSTRACT :This project is all about the authentication of the user if he/she has already registered their data in the database. This project focuses on user authentication by verifyingif their data is already registered in the database. Users with valid credentials can log in to their profiles, while others are denied access. Additionally, it implements a two-factor authentication system, requiring users to enter an OTP and scan a QR code. Frauds are increasing in online payments day by day. You can develop an E-authentication system to safeguard your online transactions and sensitive information. An E-authentication system verifiestheuserthroughmultifactoridentificationandbiometrics.Byenhancingsecurity,you can make your online transactions secure and fraud-free.

1. INTRODUCTION:

With the advent of the electronic era, securing online transactions and user authentication has become a major concern. Methods of authentication based on passwords arewidely used, but also becoming morevulnerableto cybersecurity threats such as phishing, data breaches, and password theft. To counter these challenges, modern authentication schemes, combine factors such as something the user knows (passwords), somethingtheuserhas(smartphonesordevices),andsomethingtheuseris(biometrics).Ifwe discuss a better and efficient method of securing theuser from fraud and improving the user experience,thentheE-AuthenticationSystemusingQRandOTPcomesintothepicture.This system provides a new authentication mechanism that enables users to use two-factor authentication (2FA) which reduces the risk of malicious access.

The process starts with generating a QR code, which isoften shown on a webpage or app. Instead, the user scans the QR code with his or her mobile device or authentication application, which links the user'sdevice to the session in a secure manner. The OTP is the second mode of authorizationand is sent to the registered contact method (email id or phone number) of the user. The user needs to enter the OTP in a matter of few seconds to authenticate himself and gain secure access[1-24].

Doi:10.48047/ijiee.2025.15.5.13

2. LITERATURESURVEY:

BlockchainforDecentralizedAuthentication

Blockchain is increasingly being explored for decentralized authentication, where identity information can be stored securely and privately in a distributed ledger. Zohar et al. (2020)

2025: Blockchain-Enhanced QR + OTP Authentication for Decentralized Systems A recent paper by A. Mishra et al. in 2025 explores the use of blockchain technology combined with QR code and OTP for decentralized authentication. This study introduces a decentralized identity management system that uses QR codes to initiatesecuresessions and OTPs for real-time validation, recorded on the blockchain. The proposed system eliminates single points of failure and ensures trust in peer-to-peer interactions, suitable for a range of applications, including decentralized finance (DeFi) and distributed applications (dApps).

2024: IoT Security with QR Code and OTPAuthentication In 2024, T. Ghosh and R. Desai proposed a solution for securing Internet of Things (IoT) devices using QR code and OTP-based authentication. Their system allowed users to authenticate their IoT devices byscanningaQRcodeandenteringadynamicallygeneratedOTP.Thismethodwasparticularly useful for home automation and smart device management, where strong authentication was needed to prevent unauthorized device control.

2021: QR CodeAuthentication for Secure Mobile Payments In 2021, a study by J. Lee et al. explored the use of QR code authentication for secure mobile payment transactions. Their work demonstrated that QR codes provide an efficient, user-friendly means of authenticating transactions in mobile wallets and payment apps. The study highlighted how QR codes, combined with dynamic OTPs, significantly reduced the risk of phishing attacks and man-in-the-middle attacks by eliminating the need to input sensitive information manually.

2022: Security Vulnerabilities in QR Code Authentication A paper by K. R. Patel and A. Gupta in 2022 focused on the security challenges associated with QR code-based authentication.Although QR codes offer a convenient solution for authentication, the authors emphasized potential threats such as QR code spoofing and malicious redirection. The paper proposed a hybrid authentication method combining QR codes with secure communication protocols and OTP verification to mitigate these threats, enhancing overall system security.

2023:Advanced CryptographicTechniques in QR CodeAuthentication In 2023,A. Kumar et al. presented a study exploring the use of advanced cryptographic techniques in QR code-based authentication systems. They introduced a blockchain-based solution that uses QR codes for initial authentication, followed by OTP verification, to create a decentralized and immutable log of authentication events. The integration of blockchain provided a layer of security against tampering and fraud, ensuring data integrity during the authenticationprocess.

3. EXISTINGSYSTEM:

The current authentication systems demonstrate several crucial issues despite their useful features The modern OTP and QR code systems have better security through MFA implementation but remain vulnerable to potential attacks. Scammers take advantage of QR codesthroughtwomalicioustechniquesthatinvolvespoofsandfakewebsiteredirects.

Doi:10.48047/ijiee.2025.15.5.13

Cellular networks which lack proper encryption protocols or fall under compromised networks pose a threat to the interception of OTPs delivered through SMS or email communication. Security flaws present in these authentication methods have the potential to erode the complete security assurance of the authentication mechanism. The increased security features of QR code and OTP authentication create minor problems with user experiences and convenience issues. The process of using different devices for OTP verification and scanning QR codes creates an inconvenient user experience.

4. PROBLEMSTATEMENT:

In today's digital age, Digital security breaches together with unauthorized access incidents to sensitive data occur frequently within present-day cybersecurity landscape. The current authentication solutions mainly depend on passwords but these show low defence against attackers. Electronic authentication system development became essential due to the increasing number of online transactions combined with digital service usage.

5. PROPOSEDMETHODOLOGY:

The proposed E-Authentication System which implements QR Code and OTP authentication goals to make online authentication more secure and provides better user experiences. The authentication method applies two-factor authentication (2FA) technology through a fusion between simple QR codes and secure One-Time Passwords (OTPs). A specific QR code emerges automatically during each sign-in attempt to surface on the verification page. The system creates a time-sensitive OTP by triggering its production through a mobile device or app once the user scans the provided QR code.Usersreceiveone-timepasswordsthroughtheirregisteredcontactdetailswhichinclude phone number or email address. Under the authentication interface the user enters the received OTP for system verification against both the OTP and QR code for successful authentication. A secure session opens up after the system verifies both the validity of the OTP and QR code. The authentication method stands out for its significantly improved security standard against conventional password approaches that decreases risks related to unauthorized entry and phishing and credential theft.Thesystem demonstrates characteristics of scaling potential and friendly operation with the ability to easily integrate into existing platforms thus making it suitable for applications including online banking, e-commerce and government services. The system resolves major security issues through its encryption techniques and secure session processes alongside One-Time Password timeout preservation thus offering cost-efficient authentication capabilities to users along with service providers

5. UMLDIAGRAMS:

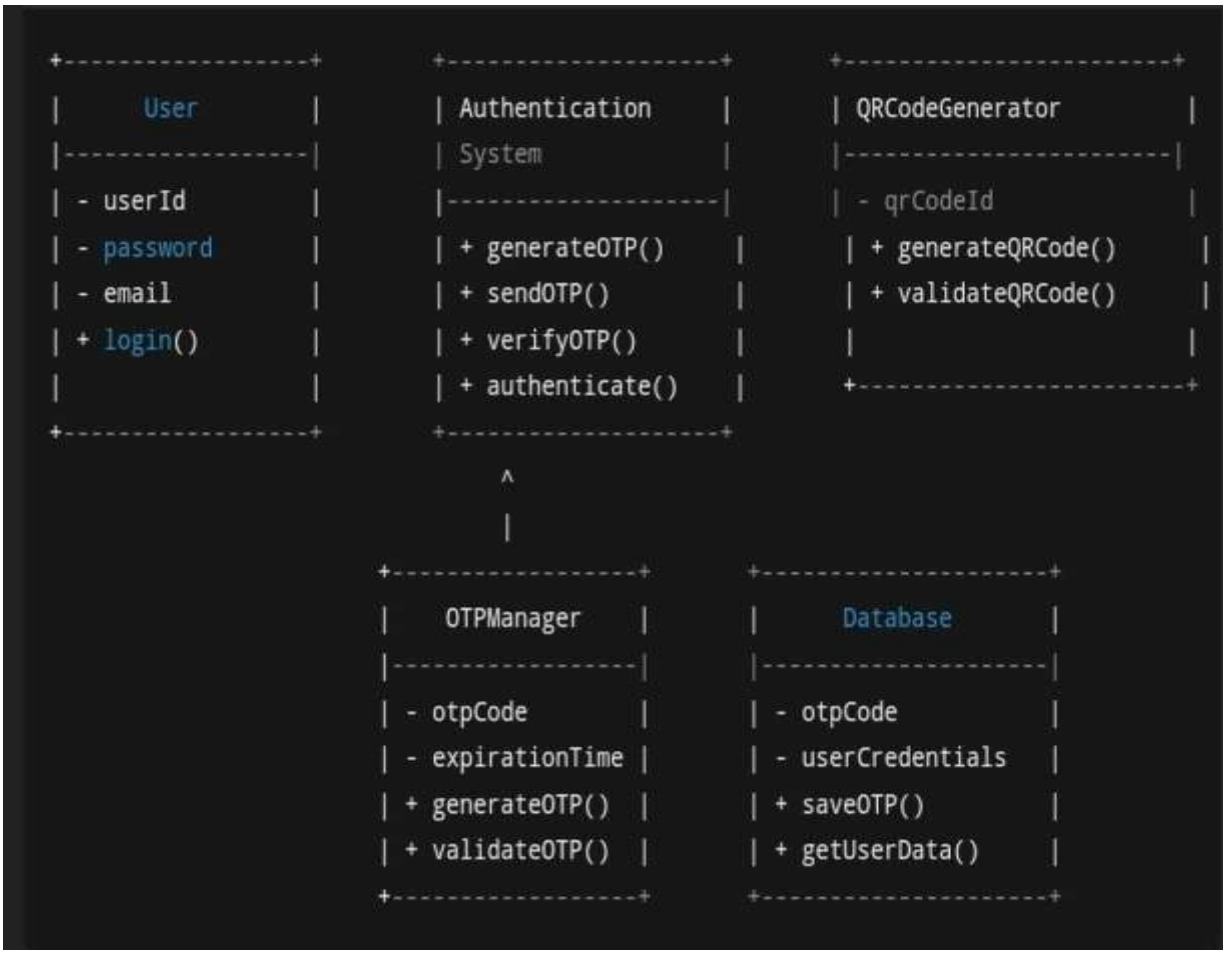
1. UseCase Diagram:

A Use Case Diagram shows the interactions between users and the system. The primary actors are the User and the Authentication System.

Doi:10.48047/ijiee.2025.15.5.13

2. Class Diagram:

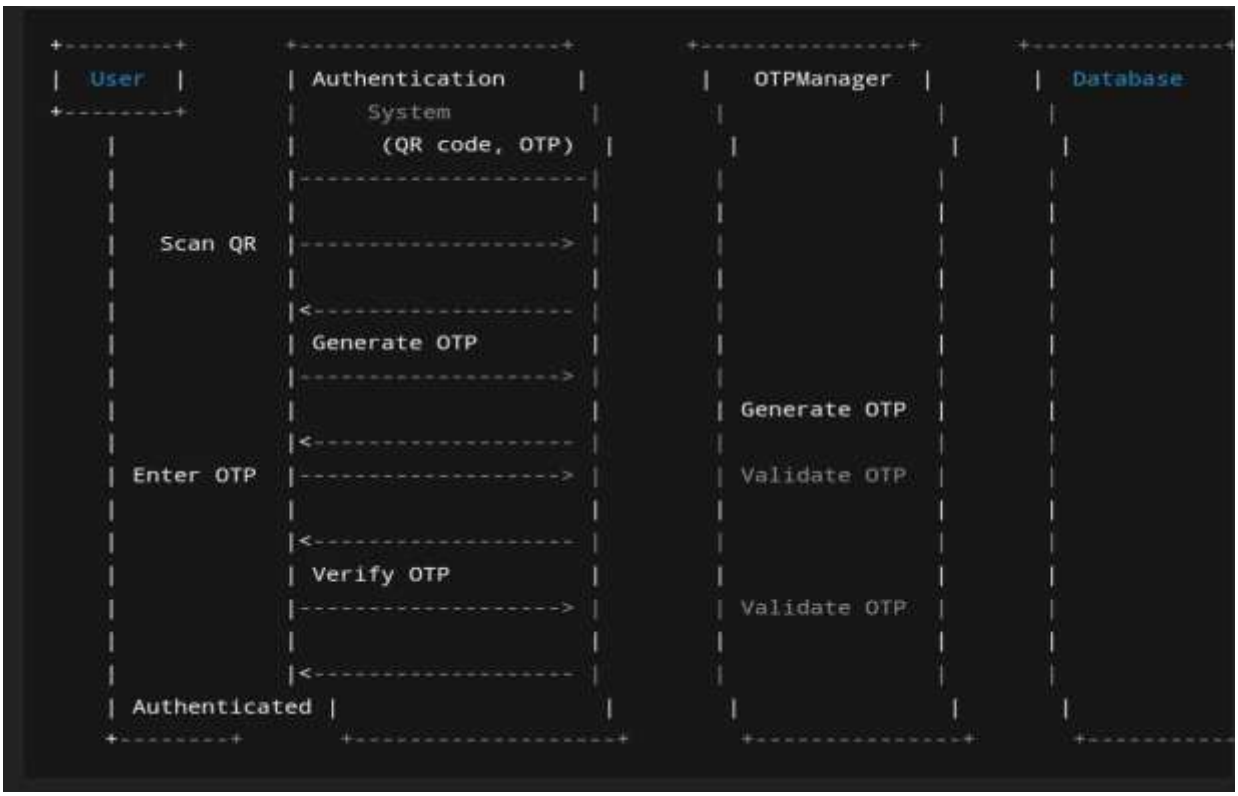
A **Class Diagram** represents the static structure of the system, showing classes, their attributes, methods, and relationships.



Doi:10.48047/ijiee.2025.15.5.13

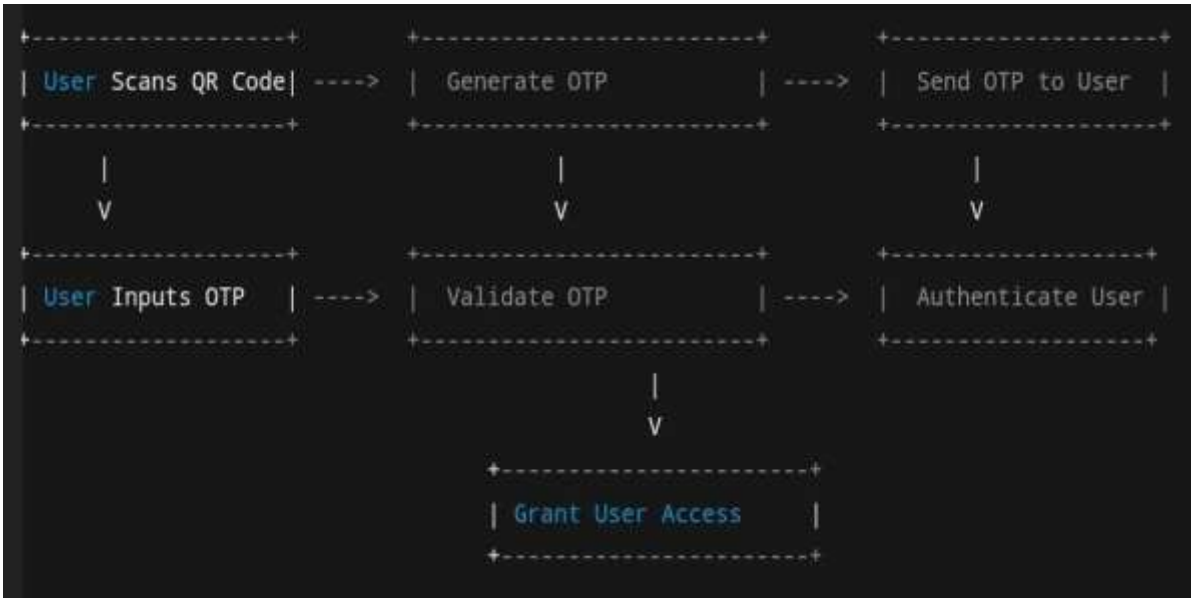
3. SequenceDiagram:

A **SequenceDiagram**illustrateshowobjectsinteractwitheachotherovertime.Here,we have interactions between the **User** and the **AuthenticationSystem**.



4. ActivityDiagram:

An**ActivityDiagram**modelstheflowofcontroloractivitiesinvolvedinthee-authentication process.



Doi:10.48047/ijiee.2025.15.5.13

6. CONCLUSION:

Users gain secure efficient authentication capabilities through an e-authentication system which implements both QR codes andOTPs. Two-factor authentication (2FA) effectively improves security through combined authentication methods to counter unauthorized access. The authentication process using QR codes delivers rapid and secure data transmission through a system which OTPs strengthen through temporary one- time passwords. The system provides a scalable authentication platform with user-friendly features that cut down phishing attack risks. Basic security issues stem from the need to educate users while they depend on communication channels and systems for authentication. The system maintains reliable security for sensitive data transmission across platforms as it is expected to develop further by integrating biometrics and blockchain capabilities.

REFERENCE

1. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960
2. Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.
3. Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
4. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
5. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
6. Bhukya Madhu, M.Venu Gopala Chari, Ramdas Vankdothu,.Arun Kumar Silivery,Veerender Aerranagula " Intrusion detection models for IOT networks via deep learning approaches " Measurement: Sensors Journal,Volume 25, 2022, 100641
7. Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537
8. S. Rakesh [a], NagaratnaP. Hegde [b], M. VenuGopalachari [c], D. Jayaram [c], Bhukya Madhu [d]

Doi:10.48047/ijiee.2025.15.5.13

, MohdAbdul Hameed [a], Ramdas Vankdothu [e], L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" Measurement: Sensors ,Journal,Volume 30, 2023, 100898

9. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.
10. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol. 29, No. 6, (2020), pp. 2875 – 2881
11. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)
12. Ramdas Vankdothu, Dr.Mohd Abdul Hameed "A Security Applicable with Deep Learning Algorithm for Big Data Analysis",Test Engineering & Management Journal,January-February 2020
13. Ramdas Vankdothu, G. Shyama Chandra Prasad " A Study on Privacy Applicable Deep Learning Schemes for Big Data" Complexity International Journal, Volume 23, Issue 2, July-August 2019
14. Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020
15. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)
16. Ramdas Vankdothu, Dr.Mohd Abdul Hameed " Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics", Complexity International Journal , Volume 24, Issue 01, Jan 2020
17. Ramdas Vankdothu, G. Shyama Chandra Prasad" A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools" International Journal For Innovative Engineering and Management Research,Vol 08 Issue08, Aug 2019.
18. Vankdothu, R., Hameed, M.A. "An Effective Congestion and Interference Secure

Doi:10.48047/ijiee.2025.15.5.13

Routing Protocol for Internet of Things Applications in Wireless Sensor Network " Wireless Personal Communication Journal 140, 143–161 (2025)

19. Vankdothu, R., Bhukya, H. & Bhukya, R.R. "Hybrid TDR-MI Based Wireless Sensor Network for Underground Water Pipeline Leakage Detection and Localization Using Pressure Residuals and Classifiers Wireless Personal Communications 139, 803–823 (2024).
20. Vankdothu, R., Cheng, X. "Energy Efficient TDMA and Secure Based MAC Protocol for WSN Using AQL Coding and ASGWI Clustering". Wireless Personal Communications 136, 2125–2143 (2024)
21. Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and Time Efficiency. Wireless Personal Communications (2025).
22. Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and Time Efficiency. Wireless Personal Communications (2025)
23. Ramdas Vankdothu, Mohd Abdul Hameed" Brain MRI Images for Tumor Detection using Storage Optimization Technique",Mobile Radio Communications and 5G Networks,Lecture Notes in Networks and Systems,425-437, Springer .
24. Bandi Krishna , Ramdas Vankdothu , Varun Revuri and B. Prashanth" A brain tumor identification using convolution neural network in the deep learning" MATEC Web of Conferences 392, 01131 (2024) ,https://doi.org/10.1051/matecconf/202439201131 ICMED 2024

Doi:10.48047/ijiee.2025.15.5.13