E-AUTHENTICATION SYSTEM USING QR CODE

Pranav Gupta, Akul sharma, Vineet Mehan
Department of Computer Science and Engineering,
Apex Institute of Technology,
Chandigarh University, Mohali, Punjab, India
pentest.pranav@gmail.com, akul.hep@gmail.com., vineet.e13038@cumail.in

Abstract— In the field of online learning and e-assessment, e-authentication is one of the most crucial topics. This method establishes trust in user identities provided electronically to an information system. The terms "digital authentication" or "e-authentication" may be used interchangeably when referring to the authentication process that confirms or verifies a person's identity to an information system. The terms "digital authentication" or "e-authentication" may be used interchangeably when referring to the authentication process that confirms or verifies a person's identity. As a result, many authentication methods are used to achieve e-authentication, including facial recognition, which verifies who the user is; passwords and security questions, which verify who they are; and OTPs, which verify what they own. Therefore, the main goal of this article is to describe all of the investigations that have been carried out to develop and improve e-authentication.

Keywords— Digital Authentication, E- Authentication, One-Time password, Multi-factor Authentication, Privacy

I. INTRODUCTION

E-authentication is now a key component of online security due to the development of digital technology. For the purpose of safeguarding sensitive data and guaranteeing secure access to online services, authentication is the process of confirming a user's identity. But conventional authentication techniques like passwords, PINs, and security questions are susceptible to online dangers like phishing, hacking, and identity theft. E-authentication systems have developed to include more advanced and secure techniques to overcome these issues.

Use of Quick Response (QR) codes, which are two-dimensional barcodes that can be quickly scanned with a mobile device, is one such technique. As a practical and user-friendly way to store and share information, QR codes have grown in popularity.
In numerous applications, including online banking, tickets, and document authentication, they have also been utilized for authentication reasons.

In this research study, we suggest a QR code-based e-authentication system that offers a safe and convenient method for online authentication. The suggested approach is intended to improve the security of online services by overcoming the drawbacks of conventional authentication techniques. Asymmetric cryptography and QR code technology are combined by the system to guarantee safe and trustworthy user authentication.

A two-dimensional barcode known as a QR code, or quick response code, is made up of black and white squares organized in a specified pattern. It was developed in 1994 as a technique to track automobiles during manufacture by a Japanese company called Denso Wave, but it has since found widespread use for a number of purposes.

Numerous pieces of data, including website addresses, phone numbers, descriptions of products, and more, can be included in QR codes. They are frequently used in payments, event and transportation ticketing, and marketing to make it simple for consumers to access product information or special offers.

The suggested e-authentication system's design and implementation, evaluation of its security and usability, and comparison of its performance with existing authentication techniques are the main goals of this study.
The methodology employed in this study comprises the creation of the QR code-based e-authentication system, several trials to assess its usability and security, and a performance comparison with existing authentication techniques.

The primary contribution of this work is the creation of an easy-to-use and secure QR code-based e-authentication system that can be quickly implemented into a variety of online services. The findings of this research will be helpful in understanding the efficacy of QR code-based authentication techniques and how they might improve the security of online services.

II. RELATED WORK

The use of QR codes for authentication has drawn more and more attention in recent years. Numerous studies have looked into the viability and security of authentication systems based on QR codes, and a number of commercial products have been created and put into use.

[1] Isobe et al. worked on personal authentication system and in this they proposed a method of public key encryption technology and created a smart card which would include the user's unique identity in the form of digital certificates. Also, when biometric personal authentication is applied to wide range of users, one problem will be those individuals for whom the fingerprint is objectionable as a means of personal authentication. So, this system is not limited to fingerprint method only it comprises of other types of biometrics data that is best suited to the user.

[2] Uotinen et al. carried out a study to investigate user experiences of students while using e-authentication system which include face recognition, voice recognition, key dynamics, etc. Also, some barriers were taken into consideration and that were, if the system doesn't work or its too difficult to use and hence creating a technical barrier and second one was, psychological barrier may exist if using the system is unpleasant or arouses suspicion. Derived that e-Authentication in e-assessment and online education is a current issue for higher education institutions.

[3] Chen et al. proposed a Curve Digital signature algorithm which basically includes, key generation and signature verification using the concept of Conic curves over a finite field. So, a distributed e-business authentication scheme was taken into consideration which included unique license generation, distribution of license and at last registration and verification and concluded that as existing internet electronic registration has a security problem so that's why their proposed system overcomes that problem by verification and new generation of license used in the authentication process.

[4] Zhang et al. proposed a solution of e-authentication services using Public Key Infrastructure where they design EAS as to provide authentic identities and identify verification services for participants involved in e-business activities. Also, X.509 v3 format public key digital certificate is adopted by them in this solution. Even, various models were proposed by them in this work for cross-domain trust, trust source management. Also, were able to provide a better solution of e-authentication system which was based on PKI using various models for identity verification and cross-domain trust.

[5] Ranjan et al. worked on a Quick Response code mechanism rather than using the existing mobile OTPs system. The code is generated using the client's transfer data and at last the client has to enter the code in order to complete the transaction. In this the communication takes place via an SSL/TLS tunnel in which the certification authority can share the sequence number of the customer's smart-phone through a secure mechanism. Also, the OTP value is changed if an altered PIN is entered. So, if a valid code is entered the transaction is successfully executed. So, this work eliminated the security risk of transaction by making use of Quick response code.

[6] Patil et al. proposed a system which includes, face detection and along with OTP verification as an alternate approach. Face detection is recognizing a person's face and face recognition based on the person's features that uniquely describe that person. During face detection person's face is extracted, then according to requirement it is cropped, resized, and converted into grayscale. During face recognition, the detected face is compared with the face stored in the database by applying a face recognition algorithm. Algorithms used in this system were HAAR Cascade algorithm, LBPH algorithm to get an accurate output and hence, successfully made the e-authentication using Face recognition.

[7] Kim et al. proposed a system in order to achieve various goals like stopping vicarious attendance, preventing attendee's departure at intermission, etc. So, the researches made use of method which consists of an attendance management server and client system. The server system consists of web server, attendance management system and database & client system consists of attendance modules for faculty and students. The Attendance management module for the professor allows the attendance management server to set a timer and send the wireless AP list, so when the management server allows attendance certification it provides data which can determine whether the class's students are in the same location as the professor and concluded that, the suggested system uses smartphones, recognizing that almost all students have their own smartphone, and wireless AP.

III. PROPOSED METHODOLOGY

Asymmetric encryption and QR code technology are the foundations of the proposed e-authentication system employing QR codes. The user registration module is in charge of creating a public-private key pair for each user as well as registering new users in the system. The private key is encrypted and safely saved on the user's device, while the public key is kept on the server.
The server generates and displays a QR code containing encrypted credentials, which are used by the authentication module. The user uses a smartphone to scan the QR code, and the smartphone uses the user's private key to decrypt the user credentials. The user is given access if the credentials are valid after being decrypted and transmitted to the server for validation.

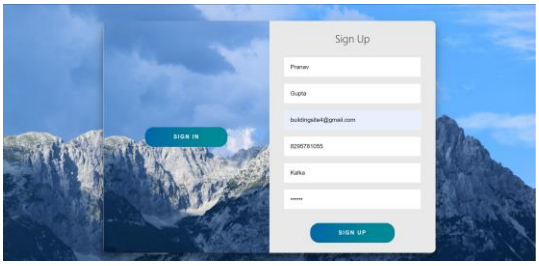
In order to create QR codes and confirm user credentials, the server module is in charge. It keeps access control rules, encrypted user credentials, and user public keys. In order to protect the confidentiality and integrity of user data, the server additionally employs a secure communication protocol while interacting with the user's device.

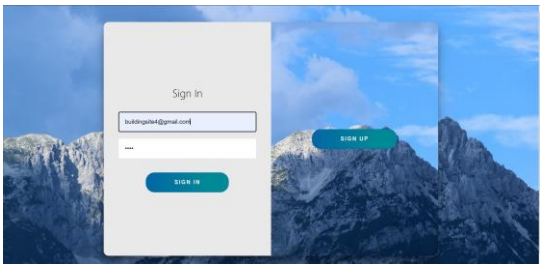
The security and usability of the system will be tested using the proposed approach through a series of experiments. The system will be tested in the experiments against prevalent cyberthreats such as phishing attacks, hacking, and identity theft. Surveys and user comments will also be used to gauge

user experience and satisfaction. The overall goal of the suggested methodology is to offer an easy-to-integrate QR code e-authentication system that is secure and user-friendly.

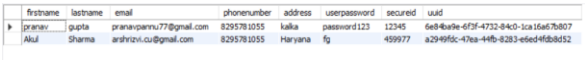
The proposed system methodology is as follows:

1. Sign up and Login Using a Web Portal:
   The proposed system will have a web portal that users can access using a regular web browser. Users can sign up and register on the site by entering their contact details, including name, email, phone number, and secure password. With their email address and password, users who have previously registered can log in. All user information will be kept in a MySQL database, and the login and registration processes will be secured using SSL encryption.





2. Fetched data is saved in a MySQL database: After a user register on a web portal, their information is kept in a MySQL database. User information including name, email, phone number, password, and any other pertinent information required for the system to operate will be stored in this database.

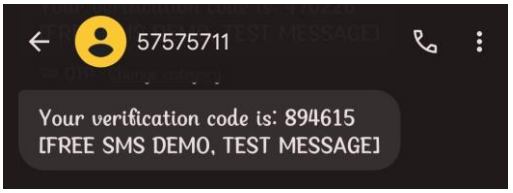


firstname	lastname	email	phonenumber	address	userpassword	secureid	uuid
pranav	gupta	pranavpannu77@gmail.com	8295781055	kalka	password123	12345	6e84ba9e-6f3f-4732-84c0-1ca16a67b807
Akul	Sharma	arshrizvi.cu@gmail.com	8295781055	Haryana	fg	459977	a2949fdc-47ea-44fb-8283-e6ed4fdb8d52

3. OTP and a Unique Number are Generated Using the Python Library UUID:
   The system will produce a one-time password (OTP) and a special number when the user has successfully signed in using the Python package known as UUID. The user will be identified throughout the system by this special number.

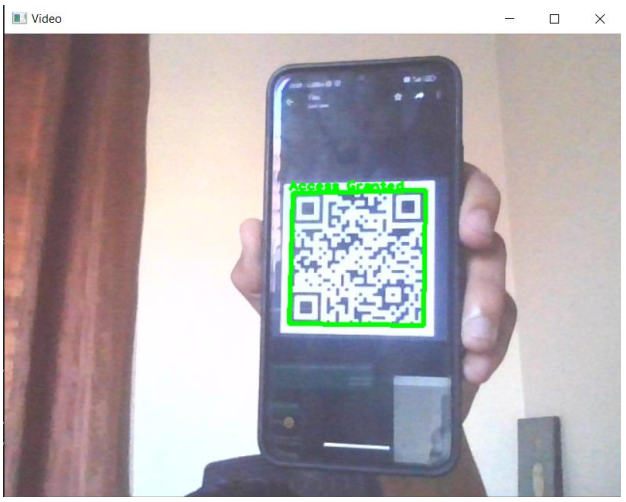
```
Generated unique code: f5792682-4a54-4322-9e61-cc6c5fecb952
Message sent successfully.
```

4. OTP is then sent: Depending on the user's selection, the system will send the OTP to the registered mobile number or email address of the user after creating it. The user will then be able to log in and confirm their identity.

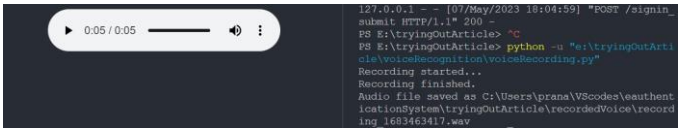


5. A special code is generated and sent to a registered email along with a QR code:
   A QR code with the special number obtained in step 3 will be emailed to the user's registered email address. Later, this QR code will be checked for accuracy. The SMTP server will be used to attach the QR code to an email when it has been created using a QR code creation API.

6. QR and OTP Verification is Complete:
   The user must scan the QR code with their mobile device and enter the OTP they received on their registered cellphone number or email address after receiving the QR code and OTP. By doing this, the user's identity will be confirmed, ensuring that they are the same person who initially registered with the system. To match the OTP and QR code with the user's registered information, the system will employ sophisticated algorithms.



7. Using one of its characteristics called its shape, audio is recorded and verified:
   The system will prompt the user to record their voice using the audio recording capability after the user has been authenticated. The system will ask the user to recite a list of predetermined words or phrases, and it will then examine the shape of the recorded audio. The user can be recognized by the shape of the audio, which is dictated by the particular qualities of their vocal cords. The system will examine the audio structure using cutting-edge signal processing techniques and compare it to the user's stored information.



8. Advanced Security Features: The suggested system approach will make use of a number of advanced security features to improve the security of the system. These include SSL encryption to protect the user data and the online portal, two-factor authentication with

OTP and QR codes, audio verification with *distinctive audio forms, and real-time monitoring of user behavior to catch any suspect conduct.*

IV. CONCLUSION

In summary, the proposed system methodology uses a web portal for user registration and login, stores user data in a MySQL database, generates an OTP and a unique number using the Python library called UUID, sends the OTP to the user's registered mobile number or email address, attaches the unique number to a QR code, and sends the unique number to the user's registered email address. The user's identity is then verified using the QR code and OTP. A number of cutting-edge security elements are also included in the suggested system technique to guarantee the security of the system and user data.

In conclusion, employing QR codes for e-authentication is a practical and efficient solution to providing secure access to online tools and services. To verify users and transfer authentication data in a trustworthy and secure fashion, QR codes offer a quick and easy solution. Due to the extensive use of smartphones and other mobile devices, QR codes are now a commonplace feature of modern life and are becoming more and more popular as a means of e-authentication.

Numerous e-authentication applications, including secure login, access control, digital signatures, and payment authentication, can use QR codes. In comparison to more established authentication techniques, QR codes are simpler to use, more scalable, and less expensive. However, as with any type of authentication, it is crucial to make sure that the necessary security precautions are taken.

In terms of digital security research and development, e-authentication utilizing QR codes is a promising subject. The authentication and authorization of digital transactions and services are going to depend more and more on QR codes as technology advances.

V. REFERENCES

[1] Yoshiaki Isobe, Yoichi Seto, and Masanori Kataoka "Development of Personal: Authentication System Using Fingerprint with Digital Signature Technologies", Sensors, Issue 20, 25 December 2001.

[2] Sanna Uotinen, Tarja Ladonlahti, Merja Laamanen "DEVELOPING E-AUTHENTICATION: FOR E-ASSESSMENT – DIVERSITY OF STUDENTS TESTING THE SYSTEM IN HIGHER EDUCATION" , Sensors, Volume 23, Issue 13, 15 July 2020

[3] Xinxia Song, Zhigang Chen "A Distributed Electronic Authentication Scheme in E-Business: System", Sensors, Volume 13, Issue 09, 11 August, 2008

[4] Xiaoqi Zhang, Meina Song, Junde Song "A Solution of Electronic Authentication Services: Based on PKI for Enabling e-Business", Sensors, Issue 29, 30 May 2009

[5] Sagar, Raju Ranjan "E-Authentication System with QR Code", Sensors, Volume 8 Issue 12,May 2022

[6] Preeti Patil, Mayuri Lonkar, Mrunali Sonkar, Megha Sinha, Aditi Kannadkar "E Authentication System Using Face Recognition", Sensors, Volume 9, Issue 2, April 2022

[7] Jin Kim, Seung-Kook Cheong "Research on an Authentication Algorithm for an Electronic Attendance System in the Constructing of a Smart Campus", Sensors, Volume 7, Issue 6, 19 June, 2018

[8] Sahu, R. K., & Singh, N. K. (2018). An Overview of QR Code-based Authentication Techniques. International Journal of Computer Applications, 179(41), 11-15.

[9] Kim, Y. J., & Kim, Y. S. (2019). A Review of Authentication Technologies for Mobile Payment Systems. Journal of Information Processing Systems, 15(5), 1183-1199.

[10] Tiwari, S., Chakraborty, S., & Kar, S. (2019). Secure Authentication in Mobile Banking using QR Code. International Journal of Computer Science and Mobile Computing, 8(2), 24-33.

[11] Li, C., Huang, C., & Zhang, K. (2020). A Secure and Efficient QR Code-based Authentication Scheme for Internet of Things. Journal of Network and Computer Applications, 154, 102472.

[12] Bhattacharya, S., & Paul, S. (2021). Secure Mobile-based Authentication using QR Code. International Journal of Recent Technology and Engineering, 9(2), 1794-1799.

[13] Kyei, E. K., & Kyeremeh, P. K. (2021). QR Code Authentication for Mobile Applications: A Systematic Literature Review. Journal of Information Security and Cybercrimes, 4(1), 14-24.

[14] Singh, S., & Vyas, O. P. (2021). QR Code-based Authentication for Enhanced Security and Privacy in Cloud Computing. Computers and Security, 104, 102232.

[15] Niazi, M., Hussain, S., & Ullah, A. (2021). A Novel QR Code-based Secure E-Authentication Scheme for Smart Grid Networks. Journal of Ambient Intelligence and Humanized Computing, 12(1), 563-576.

[16] Xu, J., Luo, X., Liu, Y., & Luo, Y. (2019). A Secure Authentication Scheme for Internet of Things based on QR Code. IEEE Access, 7, 156636-156646.

[17] Maiti, A. K., Sharma, A., & Kumari, R. (2020). QR Code-based Authentication for Internet of Things: A Review. Journal of Ambient Intelligence and Humanized Computing, 11(6), 2367-2383.

[18] Jain, A., Saxena, A., & Singh, G. (2020). QR Code-based Two Factor Authentication using Elliptic Curve Cryptography. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1235-1245.

[19] Singh, A., Singh, A., & Chhabra, M. (2021). Design and Implementation of Secure QR Code-based Authentication System for Smart Grid. International Journal of Electrical Power and Energy Systems, 129, 106817.