Next-Gen Touchless Authentication with TOTP and QR Codes

Dr. G. Srilatha[1], B. Akshitha[2], S. Meghana[3], D. Ajay[4], P. Ranjith Kumar[5]

[1]Associate Professor, Department of CSE, Jyothishmathi Institute of Technology and Science, Telangana, India, gksrilatha8@gmail.com

[2]Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, akshithabojja15@gmail.com

[3]Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, samalameghana99@gmail.com

[4]Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, ajaydasari304@gmail.com

[5]Student, Department of CSE(AI&ML), Jyothishmathi Institute of Technology and Science, Telangana, India, paanchalaranjithkumar0@gmail.com

Abstract— **Traditional login systems mainly depend on passwords to verify users, but this approach often creates several security risks. Passwords can be easily guessed, reused across different platforms, or stolen through phishing and brute-force attacks, which may lead to unauthorized access. To address these issues, this paper introduces a Next-Generation Touchless Authentication system that uses QR code technology and Time-Based One-Time Passwords (TOTP) to provide a safer and more convenient login process. In this method, users first confirm their identity through email verification, after which they can access the system without using a traditional password. Instead, authentication is completed using a one-time password generated by an authenticator application. To ensure reliability, the system also provides a backup secret key that allows users to recover their account if they lose access to the authenticator device. This approach improves both security and user convenience by eliminating passwords while maintaining a reliable authentication mechanism.**

Index Terms—**Touchless Authentication, TOTP, QR Codes, Passwordless Login, Web Security.**

1.INTRODUCTION

In today’s digital world, protecting user accounts and personal data has become very important. Most websites and applications still use passwords to verify users, but this method often creates several security problems. Many people use weak passwords or reuse the same password for multiple accounts, which increases the chances of hacking. Attackers can also use techniques such as phishing, password guessing, and brute-force attacks to gain unauthorized access. In

addition to security risks, users often struggle to remember many different passwords for various applications, which makes the login process inconvenient. To solve these problems this passwordless authentication methods are very useful and very popular.

The proposed system removes the need for traditional passwords and introduces a simpler and more secure way for users to log in. In this system, users first register using their email address, and the system verifies the email through a confirmation link to ensure that the account belongs to the

correct user. After the verification process, a unique QR code is generated for the user. This QR code can be scanned using an authenticator application, which then generates time-based one-time passwords (TOTP).

During login, users only need to enter the OTP generated by the authenticator instead of using a password.

In case the user loses access to the authenticator application, a backup secret key is also provided to help recover the account.

By using QR codes and time-based OTPs, the system improves security, reduces the chances of common cyberattacks, and makes the authentication process easier and more convenient for users.

2.BODY OF THE PAPER

2.1 RELATED WORK

In earlier days, most systems depended only on usernames and passwords for authentication. Even though this method is simple and easy to use, it has many security problems. Attackers can easily guess passwords or steal them using phishing and other techniques. Because of this, researchers started focusing on stronger authentication methods.

To improve security, two-factor authentication (2FA) methods were introduced. In this approach, users need to provide an additional verification step along with the password. One popular method is Time-Based One-Time Password (TOTP), where a temporary code is generated that is valid only for a short time. This method reduces the risk of password theft because even if the password is known, the attacker still needs the temporary code.

Many studies have explored the use of mobile-based authentication systems, where OTPs are sent through SMS or generated using authenticator apps. However, SMS-based OTPs are not fully secure because they can be intercepted or delayed. On the other hand, app-based TOTP systems provide better security but still require manual input, which can affect user convenience. Recently, researchers have started focusing on touchless and frictionless authentication methods. These methods aim to improve both security and user experience. QR code-based authentication is one such approach, where users can scan a code instead of typing credentials. This reduces human effort and minimizes errors. Some systems also combine QR codes with TOTP to provide an additional layer of security.

In addition, modern authentication systems are considering user behavior, device information, and environmental factors to make authentication smarter and more adaptive. These systems try to balance security and usability, ensuring that the process is both safe and user-friendly. Despite these advancements, there is still a need for systems that are secure, fast, and easy to use. This has led to the development of next-generation authentication methods that combine TOTP, QR codes and touchless technologies.

Finally, some recent works also highlight the importance of reducing user dependency on remembering credentials and typing inputs. Researchers are trying to design systems where authentication happens in a seamless and natural way without disturbing the user experience. Combining technologies like QR scanning, real-time verification, and time-based codes helps in achieving this goal.

2.2 SYSTEM DESIGN

The proposed system is designed to overcome the limitations of traditional password-based authentication by introducing a secure and touchless login method that does not rely on passwords. Instead of using passwords, the system uses QR codes and Time-Based One-Time Passwords (TOTP) to verify users. system is built using modern web technologies that support a smooth and reliable authentication process. It includes features such as email verification, OTP generation, and secure storage of user data. SQLite is used as the database to store user information securely, and PyOTP is used to generate time-based OTP codes. These technologies help create a system that is simple to implement, secure, and cost-effective for web applications.

- **QR Code Generator:**
For each registered user, the system generates a unique QR code. This QR code is scanned using an authenticator application.

- **Email Service (SMTP):**
An email service is used to send verification messages and recovery links to users.

- **Flask Web Application:**
The Flask framework handles the main functionality of the system. It manages user registration, email verification, login requests, OTP validation.

- **Authenticator Application:**
This application automatically generates a new OTP after a fixed time interval, which is then used for secure login.

- **Database (SQLite):**
The database stores important user details such as email addresses, secret keys used for OTP generation, and verification tokens.

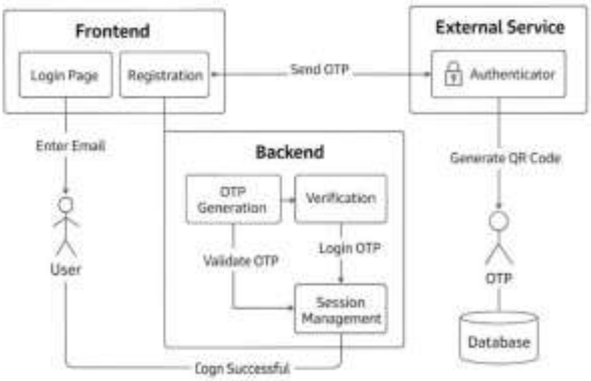


FIG.1. ARCHITECTURE DIAGRAM

Workflow

1. The process begins when a user creates an account on the web application by entering a valid email address.

2. After registration, the system sends a verification link to the provided email address to confirm that the email belongs to the user.

3. Once the email is successfully verified, the system generates a unique QR code along with a secret key for that particular user.

4. The user then scans this QR code using an authenticator application such as Google Authenticator. After scanning, the app begins generating time-based OTP codes that automatically change every 30 seconds.

5. When the user wants to log in, they enter their registered email address along with the OTP generated by the authenticator application.

6. The system checks whether the entered OTP is correct and valid. If the verification is successful, the user is securely logged in and given access to the dashboard.

7. If the user is unable to access the authenticator application, the account can still be recovered using a backup secret key or a recovery link sent to the registered email address.

2.3 IMPLEMENTATION

The implementation of the Next-Gen Touchless Authentication System is based on the integration of QR code technology, Time-Based One-Time Passwords (TOTP), and email verification. These components work together to create a secure passwordless authentication system for web applications.

1.User Registration

- The process starts when a user registers on the web application by providing a valid email address.
- The system checks the database to see whether the email address has already been registered.
- If the email is new, the system generates a secret key along with a verification token.
- A confirmation link containing this token is then sent to the user's email address.
- This step ensures that only users with a valid and accessible email account can complete the registration process.

2. Email Verification

- The user opens the verification email and clicks the confirmation link provided by the system
- The system checks the token in the link with the stored information in the database.
- If the token matches and is still valid, the user account is successfully verified.
- If the token is incorrect or expired, the system displays an error message and asks the user to try again.
- This step confirms that the person registering the account is the actual owner of the email address.

3. QR Code Generation

- After the email is verified, the system creates a unique QR code using the generated secret key
- The QR code follows the standard TOTP format so it can be used with common authenticator applications.
- The QR code and the backup secret key are displayed to the user for secure storage
- The user scans the QR code using an authenticator app such as Google Authenticator.
- This action securely connects the user's device with the authentication system

4. OTP-Based Login

- When logging into the system, the user first enters their registered email address
- The system then asks the user to enter the 6-digit OTP generated by the authenticator application.
- The OTP is validated using the stored secret key and the current time window.
- If the OTP is correct and valid, the user is successfully logged into the system.
- If the OTP is incorrect or expired, access is denied and the user must try again.

5. Account Recovery

- If a user loses access to the authenticator application, the system provides an account recovery option
- The user begins the recovery process by entering their registered email address.
- A recovery link or backup secret verification is used to confirm the user's identity

- Once the verification is successful, the system generates a new QR code and secret key so the user can reconnect their authenticator application

6. Software Components

- The frontend of the system is developed using HTML and CSS to create a simple, clean, and responsive user interface

- The backend is implemented using Python with the Flask framework, which manages routing, authentication logic, and validation processes

- QR codes are generated dynamically using Python libraries to securely connect the user's device with the authentication system

- OTP generation is implemented using the TOTP algorithm, which produces time-based one-time passwords for secure login verification

- The database (SQLite/MySQL) stores important information such as user email addresses, secret keys, verification tokens, and account verification status

7. Testing and Validation

- The system is tested to ensure that email verification links are delivered correctly and function properly

- QR codes are tested with different authenticator applications to confirm compatibility and correct scanning.

- OTP validation is checked across different time intervals to ensure accurate authentication

- Overall testing helps ensure that the system provides a smooth, secure, and reliable touchless authentication experience

2.4 RESULTS AND DISCUSSIONS

The Next-Gen Touchless Authentication System using QR Codes and TOTP was successfully designed, implemented, and tested to provide a secure passwordless login solution. The system integrates several components, including QR code generation, Time-Based One-Time Password (TOTP) authentication, email verification, and database management. Together, these components create a reliable and secure authentication process for web applications without relying on traditional passwords.

During the testing phase, the user registration module performed effectively by checking the validity of email addresses and preventing duplicate registrations. After completing the email verification step, the system generated a unique secret key along with a QR code for the user. This QR code could be scanned using an authenticator application, allowing the user to generate time-based OTPs.

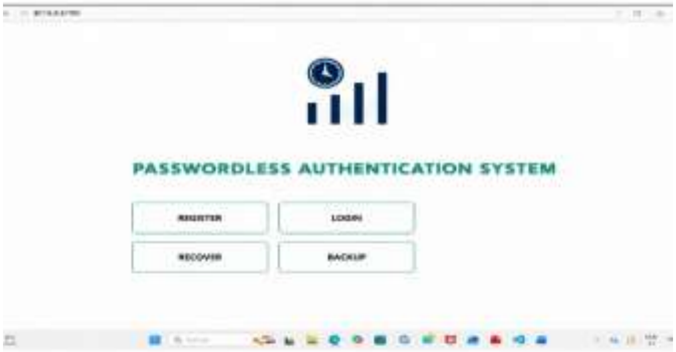


FIG 2: SYSTEM DASHBOARD

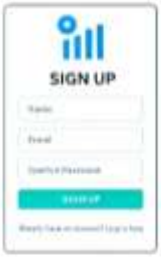


FIG 3: USER REGISTRATION PAGE

It shows the user registration interface, and Figure 7 presents the login page of the system. These pages were designed to provide a clear and user-friendly interface, making it easy for users to complete the authentication steps

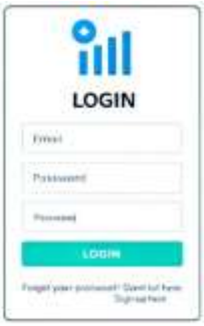
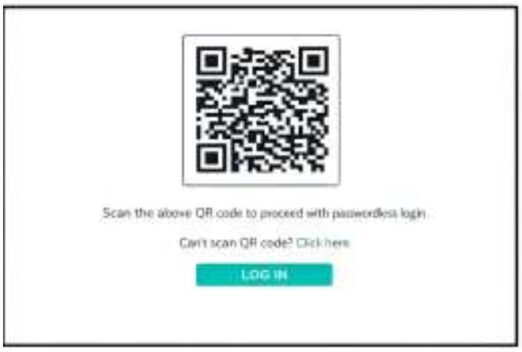


FIG 4: USER LOGIN PAGE

The QR code generation feature worked reliably during testing. Users were able to scan the generated QR codes successfully using authenticator applications. After scanning, the application generated OTPs that were properly synchronized with the backend system, ensuring accurate authentication.



Scan the above QR code to proceed with passwordless login.

Can't scan QR code? Click here

FIG 5: QR CODE GENERATED BY THE SYSTEM

It the QR code generated by the system for linking the authenticator application with the user account.

The login module was able to verify OTPs instantly during the authentication process. When a valid OTP was entered, the user was granted access to the dashboard. If an incorrect or expired OTP was entered, the system denied access, thereby maintaining security. The backup secret key feature also allowed users to recover their accounts when they were unable to access the authenticator application

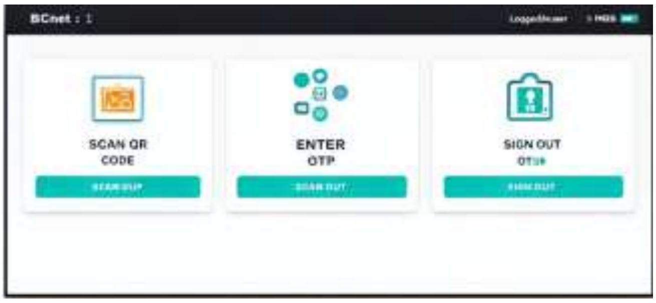


FIG.6: LOGIN INTO A WEBSITE

Overall testing showed that the system improved user convenience, reduced dependence on passwords, and strengthened authentication security. Although the system performed successfully in different scenarios, it is currently in the prototype stage and can be further improved in the future to enhance performance and scalability

3.CONCLUSION AND FUTURE WORK

The proposed passwordless authentication system using QR codes and Time-Based One-Time Passwords (TOTP) provides an effective solution to the security limitations of traditional password-based login methods. In many systems, passwords can be easily guessed, reused, or stolen through attacks such as phishing and brute-force attempts, which puts user accounts at risk. By removing the need for passwords and introducing QR code scanning along with OTP verification, the system offers a safer and more convenient way for users to access web applications. The QR code allows users to quickly connect their authenticator application, while the time-based OTP ensures that only authorized users can log in within a limited time period. This combination improves both security and user experience by reducing reliance on passwords and simplifying the login process. Overall, the proposed system demonstrates a practical and reliable authentication approach that can be applied to modern applications such as banking systems, e-commerce platforms, educational portals, and enterprise services where secure access is essential.

In the future, the proposed authentication system can be enhanced by adding more advanced security features and improving its functionality. Biometric methods such as fingerprint scanning and facial recognition can be integrated to provide an additional layer of user verification. A dedicated mobile application can also be developed so that QR code scanning, OTP generation, and login approvals can be managed directly within the system without depending on external authenticator apps. The system can also be deployed on cloud platforms to support a larger number of users across different locations securely. Instead of manually entering OTPs, push notification–based authentication can be introduced to make the login process faster and more convenient. Additional security measures such as device verification and location-based access control can help detect suspicious login attempts. Artificial intelligence can also be used to analyze user login behavior and identify unusual activity to prevent unauthorized access. Furthermore, the system can be integrated with various platforms such as banking, education, e-commerce, and government services to provide secure and reliable authentication.

REFERENCES

We would like to thank the following authors for their valuable research contributions in the field of authentication, security, QR codes, and one-time password systems. Their work provided essential insights and technical foundations that supported the design and development of this project. Without these studies, understanding modern passwordless and multi-factor authentication mechanisms would have been challenging.

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano,
"The quest to replace passwords: A framework for

comparative evaluation of web authentication schemes,”

Proc. IEEE Symp. Security and Privacy, San Francisco,

CA, USA, 2012, pp. 553–567, doi: 10.1109/SP.2012.44.

[2] E. Grosse and M. Upadhyay, “Authentication at scale,”

IEEE Security & Privacy, vol. 11, no. 1, pp. 15–22, Jan.

2013, doi: 10.1109/MSP.2012.162.

[3] R. F. Olanrewaju, B. U. I. Khan, F. Anwar, and M. Yaacob, “Offline OTP based solution for secure internet banking access,” *Proc. IEEE Conf. e-Learning, eManagement and e-Services*, Nov. 2018, pp. 167–172, doi: 10.1109/IC3e.2018.8632643.

[4] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” *Proc. SPIE*, vol. 7667, Apr. 2010, Art. no. 76670L, doi: 10.1117/12.847886.

[5] J. Thome, L. K. Shar, D. Bianculli, and L. Briand, “An integrated approach for effective injection vulnerability analysis of web applications,” *IEEE Trans. Software Engineering*, vol. 46, no. 2, pp. 163–195, Feb. 2020, doi: 10.1109/TSE.2018.2844343.

[6] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and M. Yaacob, “Scrutinising internet banking security solutions,” *International Journal of Information and Computer Security*, vol. 12, nos. 2–3, pp. 269–302, 2020.

[7] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi:

10.1145/359168.359176.

[8] T. P. Pedersen, “Non-interactive and informationtheoretic secure verifiable secret sharing,” *Proc. Annual International Cryptology Conference*, Santa Barbara, CA, USA, 1991, pp. 129–140, doi: 10.1007/3-540-46766-1_9.

[9] J. Kubovy, C. Huber, M. Jäger, and J. Küng, “A secure token-based communication for authentication and authorization servers,” *Proc. Int. Conf. Future Data Security Engineering*, Can Tho City, Vietnam, 2016, pp. 237–250.

[10] A. Kim, M. Park, and D. H. Lee, “AI-IDS: Application of deep learning to real-time web intrusion detection,” *IEEE Access*, vol. 8, pp. 70245–70261,2020, doi: 10.1109/ACCESS.2020.2986882.

[11] R. Kumar et al., “Evaluating security-durability of web applications using hybrid decision models,” *IEEE Access*, vol. 8, pp. 48870–48885, 2020.

[12] M. Jakobsson and M. Dhiman, *Mobile Authentication*, Springer, New York, NY, USA, 2013, pp. 5–24.

[13] P. Muthukrishnan, V. Sakthivel, B. Ramachandran, and K. Srihari, ‘‘Technical analysis on security realization in web services for e-business management,’’*Inf.Syst.eBus.Manage.*,vol.18,no.3,pp. 427–438,Sep.2020,doi: 10.1007/s10257-019-00423-w.2020

[14] M. S. Mir, M. A. B. Suhaimi, B. U. I. Khan, M. M. U. I. Mattoo, and R. F. Olanrewaju, “Critical security challenges in cloud computing environment: An appraisal,” *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 10, pp. 2234–2248, 2017.

[15] R. F. Olanrewaju, B. U. I. Khan, F. Anwar, and M. Yaacob, “Offline OTP based solution for secure internet banking access,” in *Proc. IEEE Conf. e-Learning, eManagement and e-Services (IC3e)*, Nov. 2018, pp. 167–172, doi: 10.1109/IC3e.2018.8632643.

[16] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in *Proc. IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, 2012, pp. 553–567, doi: 10.1109/SP.2012.44.

[17] T. Van Hamme et al., “Frictionless authentication systems: Emerging trends, research challenges and opportunities,” *arXiv preprint arXiv:1802.07233*, 2018.

[18] E. Grosse and M. Upadhyay, “Authentication at scale,” *IEEE Security & Privacy*, vol. 11, no. 1, pp. 15–22, Jan. 2013, doi: 10.1109/MSP.2012.162.

[19] J. K. Liu et al., “Fine-grained two-factor access control for web-based cloud computing services,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[20] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” *Proc. SPIE*, vol. 7667, Apr. 2010, Art. no. 76670L, doi: 10.1117/12.847886.

[21] G. R. Haron, D. Maniam, L. M. Nen, and N. I. Daud,

"User behaviour and interactions for multimodalauthentication," in *Proc. 14th Annual Conf. Privacy, SecurityTrust (PST)*, Auckland, New Zealand, 2016, pp. 309– 316.

[22] R. Kumar et al., "A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, pp. 48870–48885, 2020.

[23] S. Garg, R. Vig, and S. Gupta, "Multimodal authentication system: An overview," *International Journal of Control Theory and Applications*, vol. 10, no. 13, pp. 111– 119, 2017.

[24] M. Jakobsson and M. Dhiman, *Mobile Authentication*, New York, NY, USA: Springer, 2013, pp. 5–24.

[25] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, R. N. Mir, and M. Yaacob, "Scrutinising internet banking security solutions," *International Journal of Information and Computer Security*, vol. 12, nos. 2–3, pp. 269–30