E-Authentication System Using QR And OTP

Jay Bardhan Singh Dhakrey
BE. CSE- Cloud Computing
Chandigarh University
Mohali,Punjab
jay.b.singh09@gmail.com

Kumari Swati Singh
BE. CSE- Cloud Computing
Chandigarh University
Mohali,Punjab
swatisingh1432003@gmail.com

Pankaj Chauhan
BE. CSE- Cloud Computing
Chandigarh University
Mohali,Punjab
Pankajchauhan.0175@gmail.com

Dipesh Goyal
BE.CSE- Cloud Computing
Chandigarh University
Mohail,Punjab
dipeshgoyal30@gmail.com

Jagjit Singh
Chandigarh University
Mohali,Punjab
jagjit.e15190@cumail.in

***Abstract*— For the protection of sensitive data and the provision of seamless user experiences in the digital era, effective and secure authentication mechanisms are essential. This abstract proposes a E-Authentication System that harnesses the strength of One-Time Passwords (OTP) and QR codes to create reliable user identification and authorization procedures. The E-Authentication System uses OTPs and QR codes together as part of a verification process. By scanning a QR code located on the authentication screen, users start the authentication process. When this is done, the system generates a time-sensitive OTP and sends it over a secure channel to the user's registered device. To finish the authentication process, the user enters this OTP. The dual-layer mechanism's requirement for both the user's device and knowledge of the OTP increases security. The system is applicable in many different fields. It guarantees safe account access and transaction authorization for online banking. This system's ease of use and simplicity rank among its main benefits. Users no longer have to manually enter complicated credentials, which lowers the chance of error and increases customer happiness. OTPs give an extra degree of security by preventing replay attacks and illegal access attempts with their limited validity and one-time use.**

Keywords—OTP, QR CODE, E-AUTHENTICATION, USER IDENTIFICATION, SECURE ACCESS, DIGITAL SECURITY, IDENTITIY VERIFICATION

I. Introduction

The necessity for safe and dependable access to internet services, apps, and sensitive data has become crucial in today's quickly expanding digital landscape. However, conventional methods of authentication that only require usernames and passwords have shown to be weak against a number of online risks, such as hacking, phishing, and illegal access. This has increased the need for sophisticated E-Authentication Systems that can successfully handle these security issues. The main issue is that traditional authentication systems don't offer sufficient protection against contemporary cyber dangers. Static passwords and even one factor authentication is ineffective since they can be easily stolen, cracked, or corrupted. Due of this, people and companies are susceptible to identity theft, data breaches, and other financial losses.

With the use of One-Time Password (OTP) and Quick Response (QR) code technologies, the project intends to create an innovative E-Authentication System. With this approach, you should be able to access online services and apps safely and easily.
Following are the two major objectives:
1. *OTP Generation and Verification*: Implement a time-limited, one-time password generating and verification system that offers safe OTPs to increase security during login attempts.
2. *QR Code Registration:* Create a method for users to register their devices using QR codes in order to guarantee a safe and simple on boarding procedure.

The E-Authentication System using OTP and QR codes is expected to deliver a secure, user-friendly, and adaptable solution for organizations and services seeking to enhance their authentication processes. By combining these two technologies, the system will offer improved protection against cyber threats, avoid the hacking of accounts through shoulder surfing and misuse of login credentials while maintaining ease of use, encouraging safer online interactions across various industries.

II. LITERATURE REVIEW

Alshehri et al. [2018] proposed a two-factor authentication scheme that combines QR codes and OTPs. The system is designed to enhance security in online transactions. QR codes are generated and scanned as one factor, while OTPs serve as the second factor. The paper provides insights into the architecture, implementation, and security considerations of this approach, making it a foundational work in the field.

Adithya et al. [2015] present a QR-based two-factor authentication system, shedding light on the practical implementation of such systems. The paper discusses the use of QR codes for user authentication and emphasizes the simplicity and user-friendliness of the approach. While the focus is on implementation, the authors also touch on security aspects.

Sahadevan et al. [2018] evaluates the security of QR code authentication schemes combined with OTPs, particularly in the context of the Internet of Things (IoT). It identifies potential vulnerabilities and threats in such systems. The research highlights the importance of robust security measures in IoT applications, where sensitive data is often involved.

Rahman et al. [2017] explore the integration of elliptic curve cryptography (ECC) into QR code-based authentication systems. ECC is known for its strong security properties and efficiency, making it a valuable addition to the authentication process. The paper provides insights into the cryptographic aspects of QR code-based authentication.

Kabir et al. [2019] present a detailed account of designing and implementing an OTP-enhanced QR code-based authentication system. The research focuses on practical considerations, performance metrics, and security measures. It offers valuable guidance for developers looking to implement similar systems

Azad et al. [2020] assesses the real-world security of two-factor authentication systems using QR codes and OTPs. It offers insights into the strengths and weaknesses of these systems when used by actual users. The research can inform system designers about user behavior and potential security gaps.

Kumaravel et al. [2019] conducted a comprehensive survey of QR code-based authentication protocols, including those incorporating OTPs. The survey provides an overview of various approaches, their features, and security considerations. It serves as a valuable resource for researchers seeking an understanding of the landscape.

Rahman et al. [2016] proposes an enhanced security mechanism for two-factor authentication by combining QR codes, OTPs, and data encryption techniques. The authors discuss the benefits of adding data encryption to the authentication process, further safeguarding sensitive information.

Mallick et al. [2018] provide a survey of QR code authentication methods and their applications in e-commerce. The paper discusses how QR codes, often combined with OTPs, are used to enhance security in online shopping and financial transactions. It sheds light on practical applications of these technologies.

Hossain et al. [2015] review the use of QR code authentication in mobile devices, a popular application area for this technology. The paper highlights the convenience and usability of QR code-based authentication on mobile platforms and examines the role of OTPs in enhancing security.

III. PROBLEM STATEMENT

This project focuses on building an e-Authentication system using a combination of QR code and OTP for enhanced security. The e-Authentication system is designed to avoid the hacking of accounts through shoulder surfing and misuse of login.

IV. METHODOLGY

For incorporating a QR and OTP together in this E-authentication project, Python is used. A framework of python called kivy is used for developing a cross-platform application. For the management of database MYSQL is used. Components of the application are

- Login Screen: - Firstly, a Login screen is made for the user to enter their username and password and login into their account.
- Registration Screen: - A registration Screen is made where a non-registered user can create an account by entering the required details and creating a new username and password. The username should be unique else a warning will be displayed. There is a button to go back to login screen
- QR generation Screen: - This screen contains a button that creates a QR. After the button is clicked a QR is generated and displayed.
- The QR is encoded with a random text of length 15 which is unique every time a QR code is generated. It also encodes user data that was entered at the time of registration that is fetched from the database which is linked with username.
- The QR is time bound and expires after 30 seconds. After the QR is expired a Go Back to Login page button appears which when clicked takes the user back to login page.
- The data is stored and handled with the help of MYSQL database where all the user data is stored and fetched from.

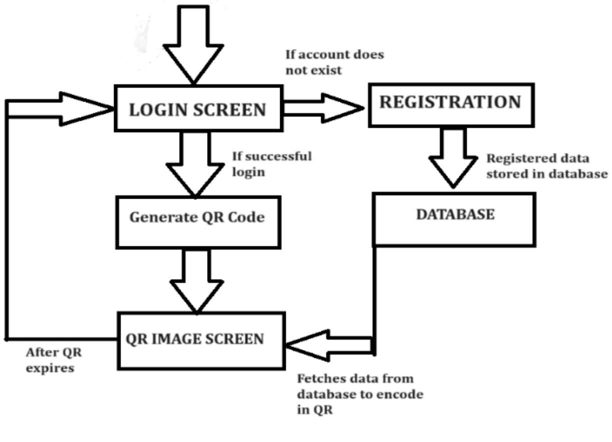
If account does not exist
LOGIN SCREEN
REGISTRATION
If successful login
Registered data stored in database
Generate QR Code
DATABASE
QR IMAGE SCREEN
After QR expires
Fetches data from database to encode in QR

Fig 1

According to Fig 1 the User opens the Application and lands on the login page first. If the his/her account does not exist they are directed to a Registration Screen where they enter their details and create a new username and password. The Username created must be unique else a warning will be displayed the user will be asked to enter the username again.

After successful creation of account, the data is stored into the database. User then navigates back to login screen and enters the credentials, if the credentials entered are correct the user moves on to next screen which displays a generate QR code button. After the button is pressed Data is fetched from data base and encoded to a QR along with a 15 length OTP. The QR code is active for 30 seconds and after it expires user is redirected back to the login page.

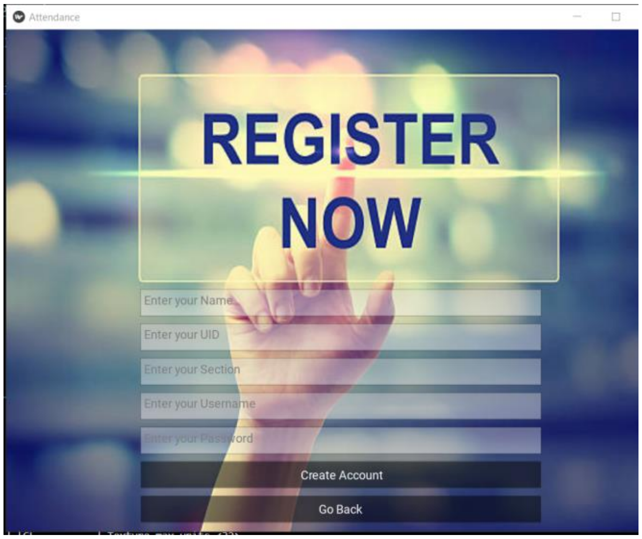

Fig 2

V. CONCLUSION

This application provides user-friendly, easy and effective way of authentication with the help of password during login phase and via QR code and OTP for an enhanced layer of authentication. An additional degree of security is provided by combining OTPs and QR codes. The OTP acts as a one-time, time-sensitive validation code, while the QR code often links to a distinctive user identity.

Due to this, it is much more difficult for unauthorized people to access. It increases the flexibility of users by implementing such systems on a variety of platforms and devices.

Users can use their PCs, tablets, or smartphones to authenticate themselves.

There may be upfront expenses for development, integration, and user training when establishing and maintaining an e-authentication system with QR and OTP. Reduced help for password resets and heightened security, however, frequently balance these expenses.

Numerous widespread vulnerabilities connected to conventional password-based systems like Shoulder Surfing and hacking are mitigated by this method.

REFRENCES

[1] N. Kumar, A. Berg, P. Belhumeur, and S. Nayar, “Describable visual attributes for face verification and image search,” IEEE Trans. Pattern Anal. and Mach. Intell., vol. 33, no. 10, pp. 1962–1977, 2011.

[2] P. Samangouei, V. M. Patel, and R. Chellappa, “Attribute-based continuous user authentication on mobile devices,” in Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst., 2015, pp. 1–8.

[3] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. M. Makela, and H. Ailisto, “Identifying users of portable devices from gait pattern with accelerometers,” in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, March 2005, vol. 2, pp. ii/973–ii/976.

[4] M. Derawi, C. Nickel, P. Bours, and C. Busch, “Unobtrusive user-authentication on mobile phones using biometric gait recognition,” in Proc. Int. Conf. Intelligent Inform. Hiding and Multimedia Signal Processing, Oct. 2010, pp. 306–311.

[5] F. Juefei-Xu, C. Bhagavatula, A. Jaech, U. Prasad, and M. Savvides, “Gait-ID on the move: Pace independent human identification using cell phone accelerometer dynamics,” in Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst., Sept. 2012, pp. 8–15.

[6] C. Nickel, C. Busch, S. Rangarajan, and M. Mobius, “Using Hidden Markov Models for accelerometer-based biometric gait recognition,” in Proc. IEEE Int. Colloq. Signal Processing and Its Applicat., March 2011, pp. 58–63.

[7] H. M. Thang, V. Q. Viet, N. D. Thuc, and D. Choi, “Gait identification using accelerometer on mobile phone,” in Proc. Int. Conf. Control, Automation and Inform. Sci., Nov. 2012, pp. 344–348.

[8] M. Muaaz and R. Mayrhofer, “An analysis of different approaches to gait recognition using cell phone based accelerometers,” in Proc. Int. Conf. Advances in Mobile Computing and Multimedia, 2013, pp. 293:293–293:300.

[9] Y. Zhong, Y. Deng, and G. Meltzner, “Pace independent mobile gait biometrics,” in Proc. IEEE Int. Conf. Biometrics Theory, Applicat. and Syst., Sept. 2015,pp. 1–8.

[10] Y. Zhong and Y. Deng, “Sensor orientation invariant mobile gait biometrics,” in Proc. IEEE Int. Joint Conf. Biometrics, Sept. 2014, pp. 1–8.

[11]Yogita Borse and Irfan Siddavatam. “A Novel Secure Remote User Authentication Protocol using Three Factors”, International Journal of Computer Applications, vol. 87, no. 17, pp. 1-6, February 2014.

[12] Dwiti Pandya, Ram Narayan, Sneha Thakkar, Tanvi Madhekar and Bhushan Thakare “An Overview of Various Authentication Methods and Protocols”, International Journal of Computer Applications, vol. 131, no. 9, pp. 25-27, 2015.

[13] Khaled Baqer, Johann Bezuidenhoudt, Ross Anderson and Markus Kuhn, “SMAPs: Short Message Authentication Protocols”, pp. 119- 132, 2017.

[14] JC Mitchell, A Roy, P Rowe and A Scedrov “Analysis of EAP-GPSK authentication protocol”, International Conference on Applied Cryptography and Network Security, pp. 309-327, 2008.

[15] Li Ping Du and Jian WeiGuo Ying Li, "Research on Micro-Certificate Based Security System for Internet of Things", Applied Mechanics and Materials, vol. 263, pp. 3125-3129, 2013.

[16] Sonal Fatangare and Archana Lomte, “SWAP: Secure Web Authentication Protocol on Windows Mobile App”, International Journal of Computer Science and Mobile Computing, vol. 3, no. 6, pp. 674–680, 2014.

[17] P. Pacyna and R. Chrabąszcz, "Evaluation of EAP re-authentication protocol”, 17th International Telecommunications Network Strategy and Planning Symposium (Networks), Montreal, pp. 45-49, 2016.

[18] K. Bhatele, A. Sinhal and M. Pathak, "A novel approach to the design of a new hybrid security protocol architecture," IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, pp. 429-433, 2012.

[19] Xiumei Liu, Junjiang Liu and Guiran Chang, “nPAKE: An Improved Group PAKE Protocol”, IEEE Ninth Web Information Systems and Applications Conference, 2012.

[20] Bahareh Shojaie, Iman Saberi, Mazleena Salleh, MahanNiknafskermani and Seyyed Morteza Alavi, “Improving EAP TLS Performance Using Cryptographic Methods”, International conference on computer & Information Science 2012.

[21] N. Asokan, Vaitteri Niemi and Kaisa Nyberg “Man-in-the Middle in Tunneled Authentication Protocols” Nokia Research Centre, Finland, 2002.

[22] Umesh Kumar, Praveen Kumar and Sapna Gambhir, “Analysis and Literature Review of IEEE 802.1x(Authentication) Protocols”, International Journal of Engineering and Advanced Technology, vo. 3, no. 5, pp. 163-168, 2014.

[23]J. Steinhardt, P. W. Koh, and P. Liang, ”Certified defenses for data poisoning attacks,” in Advances in Neural Information Processing Systems 30 (NIPS 2017), Long Beach, CA, USA, pp. 3517-3529.

[24] C. Ledig etal., ”Photo-Realistic single image super-resolution using a generative adversarial network,” in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, pp. 4681-4690.

[25] Feng, Q., He, D., Zeadally, S., Liang, K., June 2020. BPAS: blockchain-assisted privacypreserving authentication system for vehicular ad hoc networks. In: IEEE Transactions on Industrial Informatics, vol. 16, pp. 4146–4155.

[26] Guo, S., Hu, X., Guo, S., Qiu, X., Qi, F., March 2020. Blockchain meets edge computing: a distributed and trusted authentication system. In: IEEE Transactions on Industrial Informatics, vol. 16, pp. 1972–1983