International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Digital Security: A QR Code and OTP-Based E-Authentication System

Mohammed Awad Mohammed Ataelfadiel*

Submitted: 07/05/2023 **Revised:** 16/07/2023 **Accepted:** 07/08/2023

Abstract*:* In an era where digital security is paramount, the Quick response "QR" Code and One time password "OTP"-Based E-Authentication System" proposes an innovative approach to enhance user authentication. With the rapid proliferation of wireless communication technology, the importance of user authentication is growing to ensure the security of the system. An essential role in the authentication process is played by passwords. In the authentication procedure, the user's password is transmitted along with the traffic to the authentication server, enabling the server to grant access to the legitimate user. Adversaries may exploit this opportunity to attempt to intercept other individuals' passwords to engage in illicit activities under false identities, thereby evading detection. Various strategies have been proposed to enhance the security of wireless communication technologies in response to these challenges. The suggested approach will be employed to enhance the security of the system in this investigation. One-time passwords, hashing, and two-factor authentication have been selected as the resolution. Additionally, a novel solution utilizing QR codes will be introduced to store more information securely. The objective of the system's outcome is to enhance the current login authentication mechanism. It offers methodologies to heighten the complexity of password cracking and encourage individuals to opt for and utilize intricate passwords.

Keywords: *E-Authentication, Two-Factor Authentication (2FA), QR Code Security, One-Time Password (OTP), Digital Security Systems*

1. Introduction

Security is of paramount importance when accessing services in a web-based context, particularly for both consumers and suppliers. It is crucial that the handling of accessed data is done in a manner that does not compromise its security. The confidentiality of passwords is upheld when users keep them undisclosed. The risks associated with leaked passwords and other security breaches are not universally recognized. Recent trends indicate a rise in client-side attacks on online banking and e-commerce due to a lack of security awareness among end users. Consequently, end users may be unaware of potential vulnerabilities in their computer systems or platforms that could be exploited in client-side attacks. Presently, passwords stand as the most widely utilized form of authentication. To engage in any financial transactions online, users are mandated to input their passwords into the online system. The ongoing advancements in technology impacting payment methods necessitate enhanced security measures for transaction verification in the online sphere. This research endeavor proposes a resolution to these security challenges by integrating multiple authentication methods and techniques to facilitate a secure online transaction environment between clients and servers. Moreover, it introduces an anti-form snatching approach that thwarts attackers from intercepting and modifying sensitive data during transmission from the client to the server, thereby safeguarding online content. The system also mitigates the risk of online attacks by incorporating One Time Passwords (OTPs) that validate a single login session within a specified timeframe, along with the utilization of email as a secondary verification channel.

a Applied college, King Faisal university
Al-Ahsa, KSA, melfadiel@kfu.edu.sa
ORCID No: 0009-0000-1497-4381

2. Literature Review

Cybercriminals are increasingly utilizing intricate methods to target online consumers, making certain attacks challenging to detect as they seem to originate from the legitimate user's web browser. Consequently, the user's account information is covertly altered to the attacker's details, raising significant concerns, especially regarding financial fraud, which has led to substantial monetary losses. The financial services sector has emerged as a primary focus of cyber-attacks globally, with losses reaching $54 billion in 2009, a notable increase from $48 billion in 2008[1].

The frequency of cyber assaults on financial institutions, notably in European consumer and corporate banking fields, surged dramatically in 2010. Hackers are keen on acquiring sensitive data, like account information, to exploit for personal benefit. To address these security challenges, enhanced security protocols must be implemented to ensure the reliability of data transmitted to institutional servers.

Verizon Communications Inc.'s Data Breach Investigation Report for New York highlighted 63,000 security incidents reported in 2014 across 95 countries, emphasizing that authentication attacks pose a severe threat to businesses. Conventional single-factor authentication systems, such as username and password combinations, prove inadequate in safeguarding against such attacks. Existing literature lacks definitive or universally applicable solutions for establishing a dependable and secure authentication framework, despite exploring various methodologies, albeit with drawbacks like reduced precision and prolonged processing times. Leveraging biometric traits and two-dimensional barcodes offers diverse authentication variables.

Authentication based on ownership commonly relies on smart cards, with the prevalence of mobile devices prompting the need for a mobile phone and Quick Response code-centric

authentication mechanism [3].

In order to achieve authentication, the integration of the biometric template into the Quick Response code is considered. The integration of authentication systems with smart devices is crucial for enabling faster and more effective authentication processes. A notable challenge of biometric systems is the time-consuming nature of registering and identifying individuals, particularly when dealing with a group of users. The extraction of biometric characteristics poses significant time and inconvenience issues. Automated authentication systems operate discreetly, enhancing their efficiency[2].

The rise in cyber threats during online financial transactions underscores the demand for secure and efficient authentication mechanisms. Encrypted QR codes can be leveraged for this purpose. Various multimodal biometric systems are discussed in existing literature. However, the vulnerability of these systems to spoofing attacks highlights the feasibility of spoofing irrespective of fusion type. Given the higher resistance of vein-based modalities, effective fusion mechanisms are essential.

Contemporary authentication research predominantly centers on diverse methods for acquiring biometric attributes from users. The growing number of internet users corresponds with an increase in authentication attack varieties. Consequently, enhancing the security of authentication systems emerges as a pivotal issue, prompting an exploration of different authentication system models. The evolving landscape of computationally intensive applications necessitates enhanced authentication solutions.

Despite its prevalence, the current e-authentication framework exhibits security vulnerabilities due to its reliance on a traditional password-centric model lacking mutual authentication between users and financial institution servers. Consequently, users are exposed to risks such as spam, phishing, communication interception, and database breaches. An alternative authentication approach could enhance transaction security while maintaining user simplicity. By enabling https communication between users and servers, the proposed method ensures authenticated certificates for user validation and digital signatures. Users can display a QR code on their screens, which can be decoded by their mobile phones to generate a one-time password (OTP) using transfer details, preferred transfer time, and mobile phone serial numbers instead of security cards. Both user-generated and server-generated OTPs are verified prior to transaction completion. To prevent data breaches, securing the user database is imperative.

Any form of authentication, regardless of its effectiveness, becomes futile if users are unwilling to adopt it[5]. Hence, it is imperative to explore the acceptability of electronic authentication technologies. Acceptability denotes the positive perception a user holds towards a tool prior to its utilization[6]. Insights from diverse students offer valuable insights to both developers of e-authentication tools and Higher Education Institutions (HEIs) that either employ or plan to implement them. A student might reject an e-authentication system that proves to be ineffective, inefficient, poses numerous risks, or is simply inconvenient to use. Digital Learning Environments (DLEs) must possess robust and reliable security measures to ensure their trustworthiness, as outlined in the latest European regulations[7].

Trust stands out as a crucial element in the success of any emerging technology, especially within the educational realm[8], and the trust in e-authentication seems multifaceted. For instance, biometric authentication could enhance user experience by reducing the need for creating and remembering passwords, yet it introduces fresh concerns like privacy issues[7][9].

According to scholarly sources[8], various layers of trust are linked to the institution, e-authentication tools, tool deployment, data usage, and the outcomes of the process. Moreover, acceptance plays a pivotal role in biometric systems[10], shedding light on individuals' willingness to integrate biometric identifiers into their daily routines.

E-authentication is presently a distinctive process[11]. The existing body of literature addressing the impact of e-authentication systems on diverse end users remains limited. Okada, Whitelock, Holmes, and Edwards[11] delved into the viewpoints and encounters of 328 higher education students at the Open University (UK) who interacted with an e-authentication system developed under the TeSLA project[12]. They observed that remote education students generally held a positive view of e-authentication technology, although critical feedback was also received. For instance, students with disabilities were more inclined to reject e-authentication due to concerns related to their specific educational requirements. Female students exhibited lower enthusiasm in sharing personal information compared to males, while younger students hesitated to embrace e-authentication due to apprehensions regarding data privacy and security. The needs of students should be a key consideration in the realm of e-authentication. Hence, understanding the varied responses of different students towards electronic identification is crucial[11]. For instance, researchers are still exploring the perspectives of SEND (Special Educational Needs and Disabilities) students regarding the utilization of e-authentication.

3. Background

3.1. QUICK RESPONSE (QR) code

Denso Wave, a Japanese organization, introduced the QR code, a two-dimensional barcode known as a Matrix code. This code encodes information both vertically and horizontally, enabling it to store significantly more data than traditional barcodes. By capturing an image of the code with a camera, such as one integrated into a mobile phone, and then utilizing a QR scanner, the data can be retrieved[3].

This technology has been in existence for close to a decade and has transformed into a tool for advertisers to target tech-savvy mobile phone users. Although QR Codes, also referred to as Quick Response Codes, are not a recent innovation, they have been utilized in Japan and Europe for advertising and inventory management purposes for the past decade. It is worth noting that one-dimensional (1D) barcodes offer a lower level of security compared to two-dimensional (2D) barcodes[4].

The simplicity of reading 1D barcodes results from the absence of lines and spaces. 2D barcodes pose a challenge for human eyes due to their intricate visual design. One-dimensional barcodes are designed to only be scanned in one direction to be effective. Failure to align the scan line properly would result in inaccurate data interpretation. Conversely, 2D barcodes provide a wider range of scanning possibilities. The key differentiating factor between the two lies in the amount of data they can store and transmit. QR codes, a type of two-dimensional grid barcode, can encode numerical, alphabetic, and kanji characters as information. On the other hand, scanner tags are one-dimensional codes with a maximum capacity of 20 digits[3].

The enhanced data capacity and convenience make QR codes particularly suitable for small businesses. Scanning a QR code with an iPhone, Android, or other camera-equipped phone allows for seamless access to rich online content, as well as the initiation of various phone functions such as email, instant messaging, and SMS, while also linking the phone to web applications[4].

The utilization of QR codes as a security measure has been demonstrated to be significant in various aspects[4]:

i. The linkage between your online and offline media is facilitated by QR codes. Traditional print media, such as flyers, brochures, billboards, and business cards, typically do not have a direct connection to online platforms like websites. However, the inclusion of QR codes enables this connection, as seen in the growing trend among B2B businesses. By scanning a QR code, potential customers can effortlessly access the organization's website without the need for additional information like website addresses or phone numbers.

ii. Efficiency and accuracy are key advantages of utilizing QR codes. In the absence of QR codes, a URL is the primary method of directing individuals to online content. Nevertheless, entering a URL on a smartphone can be time-consuming and error-prone. Conversely, scanning a QR code is a much faster and error-free process for customers.

iii. QR codes offer the opportunity for enhanced audience engagement through the dissemination of rich content in print marketing. For instance, Chef's Basket incorporated a QR code on the packaging of one of their pasta products. Upon scanning the QR code, customers are directed to a video showcasing the recipe for the pasta dish.

iv. By leveraging QR codes, marketers can create interactive promotional campaigns and gather feedback from their target audience. Whether it is organizing contests, registering individuals for events or products, obtaining feedback, or enabling direct purchases from printed materials like newspaper ads or flyers, QR codes enhance the interactivity of marketing initiatives.

v. The traceability of QR codes is a valuable asset for marketers seeking to analyze the performance of their campaigns.

Unlike digital media, traditional print media lacks inherent tracking capabilities. QR codes address this limitation by enabling the monitoring of scanning activities associated with print media marketing efforts. Marketers can track metrics such as the number of scans, timing of scans, and locations of scans, providing valuable insights into campaign effectiveness.

Moreover, QR codes offer event tracking functionality, which details how users interact with the content linked to the QR code post-scanning.

3.2. One Time Password

One-time password (OTP) is a security measure that enables individuals to access a network or service only once during a session, thereby mitigating the risk of identity theft by protecting user credentials and ensuring that authentication cannot be reused. Typically, a user's login remains consistent across sessions, whereas the OTP changes, necessitating verification with a new OTP each time to enhance security. Moreover, OTPs serve to counteract replay attacks, phishing schemes, and various other threats targeting conventional passwords[13].

Furthermore, they offer supplementary advantages such as anonymity, portability, extensibility, and the capacity to prevent data breaches. Various methods for transmitting OTPs include text messages through gateways, unique symbols, web-based techniques, Secure Code devices, and Grid files. The latest iteration of Grid files employs a hash file type to validate user authentication requests, though this introduces susceptibility to tampering. Despite their differences, all these methods adhere to universally recognized text-centric strategies. In essence, OTPs constitute a robust form of authentication that can fortify corporate networks, online financial platforms, and other systems handling confidential data.

OTPs address numerous issues associated with traditional passwords, notably mitigating vulnerabilities such as susceptibility to replay attacks and phishing scams. Unlike standard passwords, an expired OTP cannot be exploited by an adversary who intercepts it post-use, thereby enhancing security. Nevertheless, a drawback of OTPs is their inherent complexity, posing a challenge for users to memorize them[13].

4. Applied study

This system integrates QR codes and One-Time Passwords (OTP) to fortify the security mechanisms of online platforms. The process begins with users logging in through traditional credentials, followed by the generation of a QR code by the system. This QR code, when scanned by the user's mobile device using an application like Google Authenticator, produces a time-based OTP. The user then enters this OTP into the system, providing a second layer of verification. By combining QR code technology and time-sensitive OTPs, this system addresses vulnerabilities associated with single-factor authentication and ensures a robust defense against unauthorized access. This research elaborates on the design, implementation, and efficacy of the proposed system, highlighting its potential to significantly improve security in digital transactions and user authentication processes.

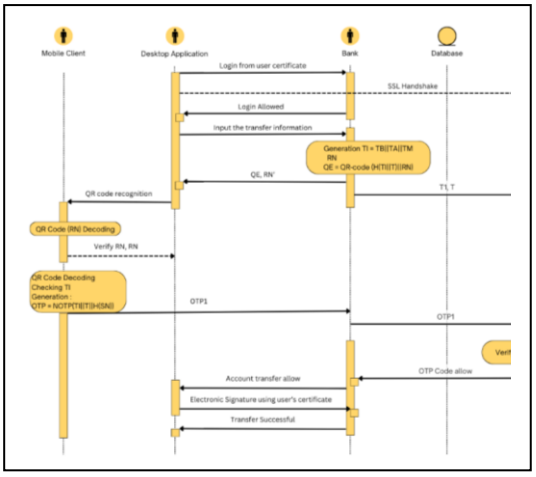

Fig1. E-authentication system working scenario

Fig1 illustrates the proposed system involving a Mobile Client, Desktop Application, Bank, Database, and Certificate Authority (CA). The user logs in to the Desktop Application using a certificate, initiating an SSL handshake with the Bank. The user inputs transfer details, and the Bank generates transfer information (TI) and a QR code (QE) containing a random number (RN). The Mobile Client scans and decodes the QR code, verifies RN, and generates an OTP. The Desktop Application forwards this OTP to the Bank for verification. Upon successful OTP verification, the transfer is authorized, signed electronically by the user, and completed successfully. This system combines certificate-based login, QR code verification, and OTP validation for secure transactions.

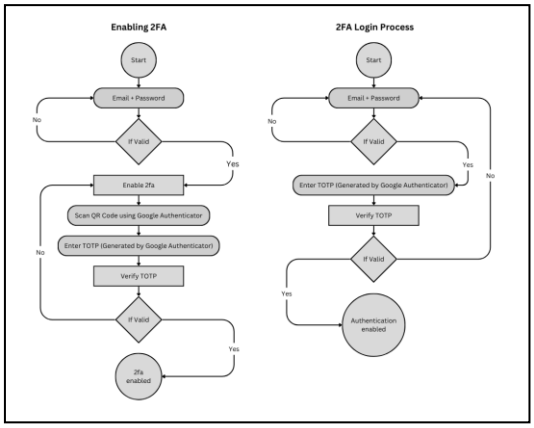

Fig2. E-Authentication Login Process Flow Chart

Fig2. illustrates the process of enabling and using Two-Factor Authentication (2FA) for secure login.

Enabling 2FA:

1. Users log in with email and password.
2. If valid, they enable 2FA.
3. Users scan a QR code with Google Authenticator.
4. They enter the generated TOTP (Time-based One-Time Password).
5. If the TOTP is valid, 2FA is enabled.

2FA Login Process:

1. Users log in with email and password.
2. If valid, they enter the TOTP generated by Google Authenticator.
3. The system verifies the TOTP.
4. If the TOTP is valid, the user is authenticated.

This process adds an extra layer of security by requiring a second form of verification from the Google Authenticator app.

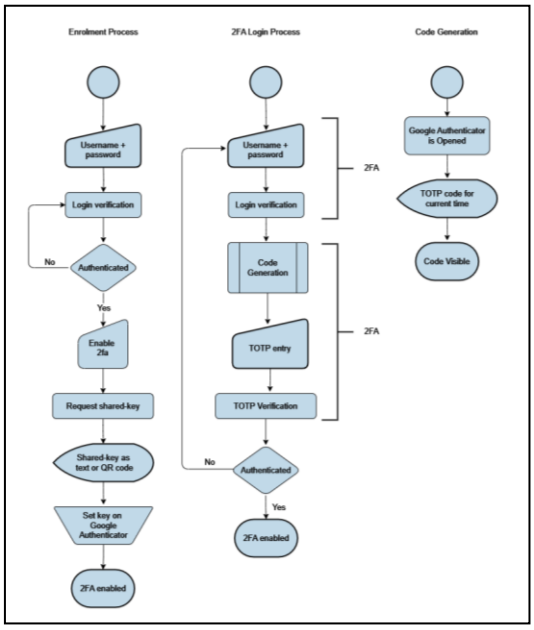

Fig3. Flow Chart of E-Authentication Login and Code Generation Process

Fig3 outlines the enrolment and login processes for Two-Factor Authentication (2FA) using Google Authenticator.

Enrolment Process:

1. Users log in with their username and password.
2. If authenticated, they enable 2FA.
3. The system generates a shared key (text or QR code).
4. Users set this key in Google Authenticator.
5. 2FA is then enabled.

2FA Login Process:

1. Users log in with their username and password.
2. If authenticated, they are prompted to enter a TOTP from Google Authenticator.
3. The system verifies the TOTP.
4. If valid, the user is authenticated and logged in.

Code Generation:

- Google Authenticator generates a TOTP based on the shared key and current time, which the user then enters during the 2FA login process.

This process adds an additional security layer by requiring both a password and a TOTP for user authentication.

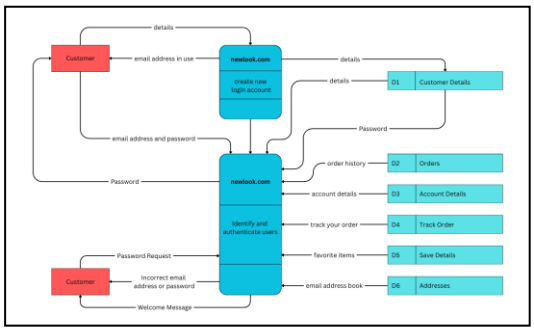

Fig4. E-Authentication DFD

Figure 4 outlines customer interactions with the "newlook.com" website, focusing on account creation and user authentication. Customers provide their details to create a new account, which is verified and stored in the Customer Details (D1) data store. For login, customers enter their email and password, which are authenticated by the site. Successful logins lead to access to various services: order history (D2), account details (D3), order tracking (D4), favorite items (D5), and address book (D6). Incorrect credentials prompt error messages, while successful authentication results in a welcome message. The flow ensures efficient account management and service access for customers.

The QR Code and OTP-Based E-Authentication System offers a compelling solution to the growing need for enhanced digital security. By integrating QR codes and OTPs, the system introduces a two-factor authentication process that is both user-friendly and highly secure. The enrolment process, involving QR code scanning and TOTP generation, ensures that only authenticated users can enable 2FA. The login process further validates users through an additional layer of OTP verification. This dual-layered approach mitigates risks associated with traditional authentication methods, providing a robust safeguard against cyber threats. The proposed system not only strengthens security but also maintains simplicity and ease of use, making it a viable solution for widespread adoption in various online platforms. Through detailed analysis and implementation, this research demonstrates the system's effectiveness, positioning it as a significant advancement in the field of e-authentication.

5. Conclusion

In conclusion, the system meets the extensive security requirements of online users, shielding them from diverse security risks. Moreover, the system operates without necessitating any technical expertise, rendering it highly accessible to users. Consequently, the E-Authentication system demonstrates its flexibility and utility for both consumers and merchants in improving operational effectiveness. Consequently, most enterprises employ it for the promotion and marketing of their goods.

One-time passwords (OTPs) are transmitted in the form of an image, posing a challenge for unauthorized individuals in detecting the presence of confidential information. The transmission of an email containing the OTP is directed to the relevant party. Clients engaged in online banking can conveniently retrieve the encrypted OTP from their email accounts through the scanning of a QR code. Consequently, solely the software authorized by the financial entity possessing the QR representation can decipher the QR code in a safeguarded transaction. The utilization of the AES technique for encoding OTPs contributes to enhancing the security of the system.

The system currently in operation is notably more advanced compared to other systems, and it is apparent that the duration required to decrypt it will exceed the practical lifespan of OTPs. One-time passwords are generated singularly per session and possess a finite duration. Once the OTP has lapsed, it becomes non-operational. The prevalent adoption of QR codes enhances user-friendliness in the process, enabling even a neophyte user with rudimentary computer skills to become acquainted with it.

Acknowledgements

I extend my heartfelt gratitude to King Faisal University for providing the necessary resources and facilities. I would like also to extend my sincere thanks and appreciation to my colleague Ayman Algam for the extensive assistance he provided me in designing the figures in the applied study. Special thanks to my family for their unwavering encouragement and understanding during this journey. Their support was instrumental in the completion of this work.

Author contributions

Mohammed Awad Mohammed Ataelfadiel: did all the research procedures starting from the idea and going through all the details until the final conclusion.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Tiwari, S. (2016, December). An introduction to QR code technology. In 2016 international conference on information technology (ICIT) (pp. 39-44). IEEE.

[2] Sharma, M. K., & Nene, M. J. (2020). Dual factor third-party biometric-based authentication scheme using quantum one-time passwords. Security and Privacy, 3(6), e129.

[3] Saranya, K., Reminaa, R. S., & Subhitsha, S. (2016, March). Modern applications of QR-Code for security. In 2016 IEEE International Conference on Engineering and Technology (ICETECH) (pp. 173-177). IEEE.

[4] Ataelfadiel, M. A. (2022, September). E-Authentication System Using QR Code & OTP. Research Journal of Innovations in Engineering and Technology - IRJIET, pp. 75-81.

[5] Karim, N. A., & Shukur, Z. (2016). Proposed features of an online examination interface design and its optimal values. Computers in Human Behavior, 64, 414–422. https://doi.org/10.1016/j.chb.2016.07.013.

[6] Alexandre, B., Reynaud, E., Osiurak, F., & Navarro, J. (2018). Acceptance and acceptability criteria: A literature review. Cognition, Technology & Work, 20(2), 165–177. https://doi.org/10.1007/s10111-018-0459-1.

[7] Karim, N. A., & Shukur, Z. (2015). Review of user authentication methods in online examination. Asian Journal of Information Technology, 14(5), 166–175.

[8] Edwards, C., Holmes, W., Whitelock, D., & Okada, A. (2018). Student trust in e-authentication. In Proceedings of the Fifth Annual ACM Conference on Learning at Scale, UK, Article No.: 42, 1–4. https://doi.org/10.1145/3231644.3231700.

[9] Moini, A., & Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: A systems perspective. IEEE Systems Journal, 3(4), 469–476. https://doi.org/10.1109/JSYST.2009.2038957.

[10] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349.

[11] Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2019). E-authentication for online assessment: A mixed-method study. British Journal of Educational Technology, 50(2), 861–875. https://doi.org/10.1111/bjet.12608.

[12] TeSLA. (2016). The TeSLA project home page. https://tesla-project.eu/. Accessed 18 Feb 2018.

[13] Srivastava, S., & Sivasankar, M. (2016, August). On the generation of alphanumeric one time passwords. In 2016 International Conference on Inventive Computation Technologies (ICICT) (Vol. 1, pp. 1-3). IEEE.