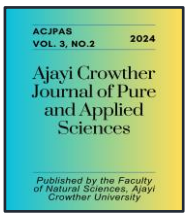
ISSN: 3092-8729 | e-ISSN: 3092-8737

Ajayi Crowther Journal of Pure and Applied Sciences
https://acjpas.acu.edu.ng

Ajayi Crowther J. Pure Appl. Sci. 2024, 3(2), pp. 22-28.
https://doi.org/10.56534/acjpas.v3i2.114



Article

Development of a Three Factor Authentication System for Online Banking

Olufemi Samuel Ojo

[1] Department of Computer Science, Ajayi Crowther University, Oyo, Oyo State, Nigeria.

* Correspondence: O. S. Ojo (os.ojo@acu.edu.ng)

Article history: *received, Jan. 15, 2024; revised, Apr. 10, 2024; accepted, Apr. 16, 2024; published, June 14, 2024*

Abstract

With the increasing reliance on online banking services, ensuring the security of user accounts has become a critical concern for financial institutions and customers alike. To address this challenge, the implementation of multi-factor authentication (MFA) systems has gained significant attention. This paper presents a comprehensive examination of 3FA (Three-Factor Authentication) systems as a robust approach to fortify online banking security. The 3FA system combines the traditional username and password credentials with additional authentication factors, such as biometrics and one-time passwords (OTPs). Through an extensive literature review, this study explores the advantages and limitations of the 3FA system compared to conventional two-factor authentication (2FA) methods. Additionally, it examines the implementation and performance evaluation of the 3FA system. Ultimately, this paper aims to empower financial institutions to make informed decisions regarding the implementation of robust authentication systems, bolstering the trust and confidence of customers in online banking transactions.

Keywords: Online banking, authentication, three-factor authentication, knowledge factor, possession factor, inherence factor, security.

1. Introduction

The rapid growth of online banking has revolutionized the way individuals manage their finances, offering convenience and accessibility like never before. However, this digital transformation has also brought forth numerous security challenges, as cybercriminals continually devise sophisticated techniques to exploit vulnerabilities in online banking systems [1]. Protecting user accounts from unauthorized access and financial fraud has become a paramount concern for financial institutions and customers alike. To combat these threats, the implementation of robust authentication mechanisms is crucial [2].

Traditional username and password authentication were once considered sufficient. Password protection was the very first authentication factor. A password is a secret word or phrase that gives users access to computer resources such as programs, files, messages, printers, internet, etc. [3]. However, individuals prefer to make their passwords short and straightforward as they are easier to remember. This kind of password frequently makes it simple to guess passwords and encourages malicious behavior. According to [4], 20% of all Personal Identification Numbers (PINs) can be cracked by hackers if they are armed with only four possibilities. They can access the accounts of more than 25% of cardholders if you provide them no more than fifteen digits. Single-factor authentication methods are now deemed inadequate in the face of evolving cyber threats. As a result, the concept of multi-factor authentication (MFA) has gained prominence [5]. By requiring users to submit several factors for identity verification—typically combining something the user knows (like a password),

something they own (like a physical token), and/or something they are—multifactor authentication (MFA) adds an extra layer of security. [6].

Two-factor authentication is utilized to alleviate the security flaws of single factor authentication by utilizing additional authentication attributes and expanding the options for user account details [7]. A cost-effective, versatile, and strong authentication is offered to customers through two-factor authentication solutions. Two-factor authentication is, however, also unreliable and susceptible to established attacks. Theoretically, two-factor authentication systems could be hacked if the fraudster had access to the victim's mobile device [8].

In order to increase the likelihood that an entity, usually a computer user, is the rightful owner of that identity, three ways of credentials are integrated as part of the information security procedure known as three-factor authentication [9]. Users are only verified for system access when they enter the proper credentials, which are often based on knowledge (something they know), possession (something they have), and inherence (something they are). The password difficulty increases with each level. In this manner, bots or hackers would have fewer opportunities to get access since even if they succeeded in breaking through first and second levels, it would be impossible for them to get past the third level [10].

While various MFA systems have been developed and implemented, this paper focuses specifically on 3FA (Three-Factor Authentication) systems for online banking. The use of three distinct factors aims to enhance security and further reduce the risk of unauthorized access and identity theft. By integrating multiple factors, 3FA systems provide an additional barrier against cyber threats, requiring potential attackers to overcome multiple hurdles to gain unauthorized access to user accounts.

1.1 Related Works

In response to the grave state of network security, Huang et al. [11] first suggested the use of biometrics as a factor in a three-factor authentication scheme. They proposed a viable three-factor authentication system consisting of biometrics, smart cards, and passwords. Face recognition was incorporated into the software that was created for this study which was inspired by the idea, of how current technology has advanced, and a thorough examination of the negative effects of lax security measures. The discussion of biometrics' speed and flow in comparison to other authentication factors had a significant impact on how this research developed. The presented scheme could resist various attacks and protect the host's multimedia and web resources, which in response, made it very attractive as a potential starting off point.

A method for using smart phones as a biometric service for web authentication is presented by Michelin et al [12]. The provided authentication system collects biometric information using the built-in facial recognition feature of Android. The suggested system requires a smart phone, a limited web server, and a PC running a web client. A request containing the user's information is sent to the web server by the user whenever they attempt to access it. The server will then determine if this is a valid user. If the user is found to be valid, the server will create a hash using the user's information and a timestamp. The user then receives this hash from the server so that their web browser can display it as a QR code. By using their smartphone to scan the QR code, the users are able to demonstrate their physical location at the computer. The smart phone can be used as a biometric scanner since it is now considered the user's physical property. The server will receive a list of available biometric readers from the smartphone. A fresh biometric reading or a new QR-code sent to the web client to verify that the user is still at the computer could be necessary if the server now has to confirm that the user still has possession of the smartphone.

In a study involving 200 Android users, Kovalan *et al.* [13] suggested a three-factor authentication (3FA) system to be employed in a mobile banking environment. The obtained OTP must be properly entered in the designated field before using biometric authentication to activate the account with fingerprint access. The authors found that two factor authentication makes a cloud environment more robust. To

increase security, a single-server environment has adopted the idea of mutual authentication scheme key agreement.

For online voting, Sathishkumar *et al.* [14] created an authentication model. The authentication mode involves fingerprint, facial, and OTP. The use of this suggested voting framework has the benefit of increasing vote frequency while requiring less staff. The goal is to make voting more equitable so that more individuals can exercise their right to vote.

In contrast to using a pin or pattern for login, research by Mohamed [15] suggested a three-factor authentication system with a password. This is because using a password makes one more secure against shoulder surfing attacks, wireless Bluetooth-based tokens provide security against other types of attacks, and ear biometrics are unique and have advantages over other biometrics. The proposed authentication technique is impractical for mobile banking because it depends on ear biometrics. The use of a Bluetooth-based token is additionally inconvenient because the Bluetooth service must be activated and uses more energy. The convenience and security flaws that could be produced by employing Bluetooth connection for authentication are not addressed by this proposal.

2. Methodology

In developing a three-factor authentication system for an online banking application, the following steps were involved (Figure 1):

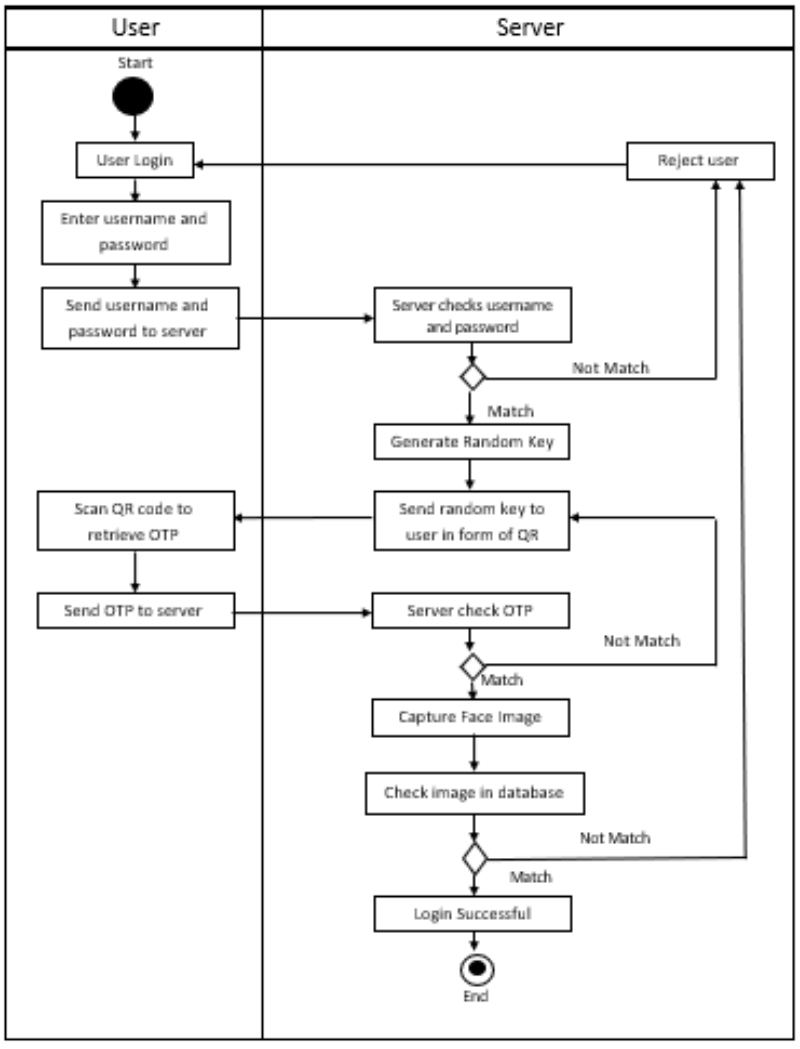


Figure 1: System Flowchart

i. Registering users is the initial step. After registering, the user gives the server their username, password, email address, mobile number, and face ID.
ii. On the system or application login page, the user inputs their username and password.
iii. The server uses the user's phrase as a key to decrypt the password and validate the username and password from the database. This ensures accuracy.
iv. If the username and password match is found in the database, the server will generate a random key. The random key is then sent in QR code format to the user's registered email address; otherwise, access is denied.
v. The user retrieves the 6-digit OTP by scanning a QR code with their smartphone while using a web browser. The user enters the verification code on the login page.
vi. The OTP is sent to the backend server to authenticate. The system will compare the OTP generated and the user input. The user will be granted access to the next level if their input is the same. The system will generate a new 6-digit OTP once it is different, and the user will need to enter it in order to obtain access.
vii. The next stage is the facial recognition process. The computer has a built-in camera to capture biometric. The system retrieves the biometric key to share with the web server.
viii. If all three-authentication factor is valid, the user will be granted to use the service of the system, otherwise the user receives a failed alert message.

3. Results and Discussion

The user registration page is shown in Figure 2. On this page, the user registers with the server by providing the important credentials. After clicking the "Sign up" button, a camera frame pops up to capture the user's face. When registration is a success, the user is redirected to the login page. On the user login page, the user is expected to input both their email address and password. The system will display an error message if the email address or password of the user is incorrect.

Once the email address and password of the user are both correct, the system send an OTP encrypted by the private key to the email address of the user in the form of a QR code. The user decrypts the message using the Google authentication app on their smartphones to scan the QR code sent to their email and gets the 6-digit OTP. The 6-digit passcode factors in the current time of day to ensure that each passcode is unique. The passcodes are changed every 30 seconds for further security. The user inputs the 6-digits OTP generated back to the system. The system will display an error message if the OTP the user inputs is different from the OTP generated by the system.

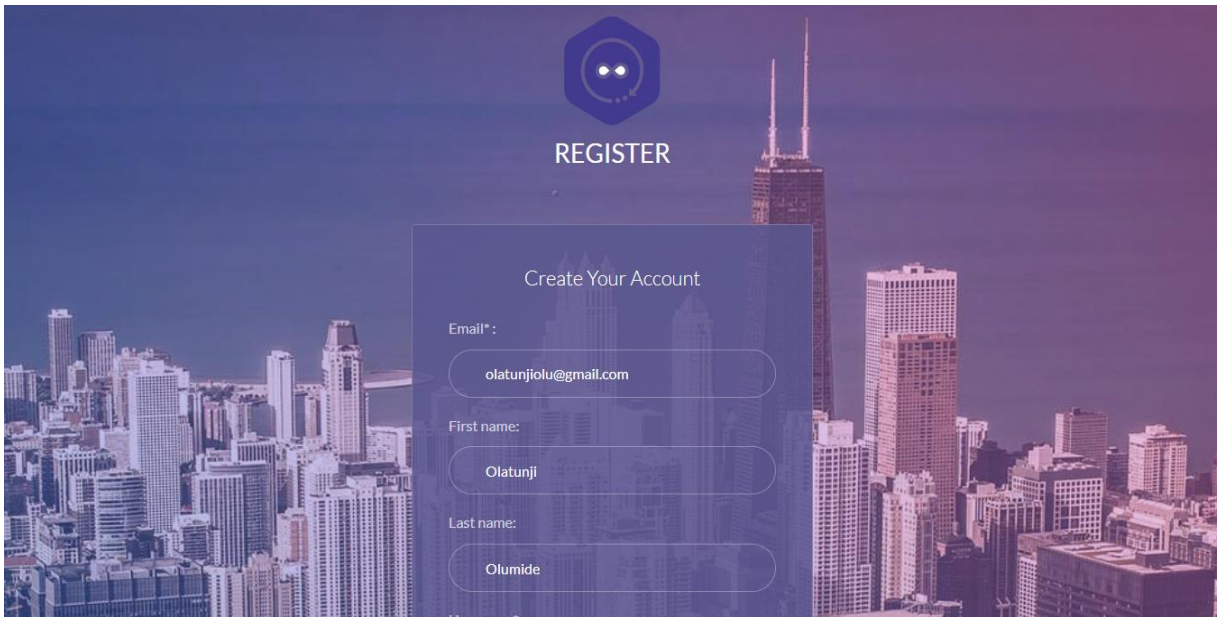


Figure 2: Registration page

The third and final factor necessary for user login is the facial recognition. A camera frame pops up on the screen to detect the user's face. The system then compares the face with the registered faces stored in the database. If the user's face does not match the face stored in the database, the user is redirected back to the login page. Authorized users are given access to their specific dashboard.

3.1 System Performance Evaluation

In order to assess the performance of face recognition systems, a comprehensive evaluation was conducted. This evaluation aimed to measure the accuracy, sensitivity, and specificity of the system using a carefully collected database of facial information. The dataset was split into training and testing sets, with the former utilized to train the system. Performance evaluation criteria were selected to gauge the system's effectiveness in recognizing registered users and differentiating them from non-registered users.

A specialized database comprising facial information was assembled for the purpose of training and testing the face recognition system. This database incorporated diverse sets of facial images, capturing variations in lighting conditions, posture, facial expressions, and elapsed time. The inclusion of these factors ensured a realistic representation of real-world scenarios and enhanced the robustness of the evaluation.

To accurately assess system performance, the collected database was divided into two subsets: a training dataset and a testing dataset. The training set was utilized to train the face recognition system, enabling it to learn and recognize facial features and patterns. Subsequently, the trained system was subjected to evaluation using the independent testing dataset.

The performance evaluation of the face recognition system employed well-established measurement criteria, including accuracy, sensitivity, and specificity. These metrics provide a comprehensive understanding of the system's capabilities in identifying registered users and rejecting non-registered individuals. The evaluation process involved comparing the face image of an individual, either from the training or registered set, with the corresponding test biometric information to be recognized. The system then computed the similarities between the two sets of information, thereby determining the accuracy and efficacy of recognition.

One valuable tool for performance analysis is the confusion matrix. It displays the performance indices, including True Positive (TP), False Positive (FP), False Negative (FN), and True Negative (TN). As shown in the table below, the confusion matrix facilitates a comprehensive understanding of the system's ability to correctly identify registered users (TP) and non-registered users (TN), as well as its propensity for false positive (FP) and false negative (FN) classifications. The confusion matrix result is presented in Table1.

Table 1: Confusion matrix

	PREDICTED YES	**PREDICTED NO**
ACTUAL YES	TP = 43	FN = 7
ACTUAL NO	FP = 2	TN = 18

$$\textbf{Accuracy} = TP + TN/TP + TN + FP + FN * 100\% = 43 + 18/43 + 18 + 7 + 2 * 100\%$$

$$= 61/70 * 100\% = 87.14\%$$

$$\textbf{Sensitivity} = TP/TP+FN * 100\% = 43/43 + 7 * 100\% = 86\%$$

$$\textbf{Specificity} = TN/TN + FP * 100\% = 18/18 + 2 *100\% = 90\%$$

Hence, the result of the system has an accuracy of 87.14%, sensitivity and specificity of 86% and 90% respectively. It is essential to acknowledge that the results obtained from the performance evaluation of facial recognition systems may vary due to several factors. Variations in lighting conditions, postures, facial expressions, and elapsed time can impact the system's performance. Consequently, the evaluation should account for these factors to provide a comprehensive assessment of the system's effectiveness in real-world scenarios.

4. Conclusions

This paper has focused on the design and implementation of a three-factor authentication (3-FA) system that combines the use of a password, QR code, and facial recognition for user verification. The objective was to enhance the security of digital systems and services while providing a convenient and user-friendly authentication process. Through extensive research, development, and evaluation, several key findings and contributions have been made.

Firstly, the integration of three distinct factors—password, QR code, and facial recognition—offers a multi-layered approach to authentication, significantly improving the system's resistance to unauthorized access attempts. The password factor serves as a familiar and widely-used authentication mechanism, while the QR code factor adds an additional layer of verification through a unique visual representation. The facial recognition factor provides a biometric-based authentication method, leveraging the unique facial features of users for enhanced security.

Secondly, the implementation of the 3-FA system demonstrated promising results in terms of security, usability, and compatibility. The combination of the three factors provided a robust defense against various attack vectors, including password guessing, QR code forgery, and facial spoofing. Furthermore, the system achieved a balance between security and usability, ensuring that the authentication process remained convenient and efficient for users.

References

1. Yathiraju, N. and Dash, B. (2023). Gamification Of E-Wallets With The Use Of Defi Technology-A Revisit To Digitization In Fintech. *International Journal of Engineering, Science 3*(1): 1-11.
2. Efijemue, O., Obunadike, C., Taiwo, E., Kizor, S., Olisah, S., Odooh, C. and Ejimofor, I. Cybersecurity Strategies for Safeguarding Customers Data and Preventing Financial Fraud in the United States Financial Sectors. *International Journal of Soft Computing* 14(3): 10-21.
3. Akinwale, A. T., Ibharalu, F. T. (2009). Password authentication scheme with secured log in interface. *Annals Computer Science series* 7: 71-85
4. Wang, D., Gu, Q., Huang, X., and Wang, P. (2017). Understanding human-chosen pins: characteristics, distribution and security. *In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security.* pp. 372-385.
5. Otta, S. P., Panda, S., Gupta, M. and Hota, C. (2023). A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet*, *15*(4): 1-20
6. Mohammed, A. H. Y., Dziyauddin, R. A. Latiff, L. A. (2023). Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges. *International Journal of Advanced Computer Science and Applications 14*(1): 166-178
7. Wang, C., Wang, Y., Chen, Y., Liu, H. and Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks* 170: 107-118.
8. Kabir, M. S., Olanrewaju, O. M. and Mukhtar, A. (2024). RatHole: Authentication Algorithm for Controlling Access to Mobile Phone File Management System. *Journal of Basics and Applied Sciences Research* 2(1): 35-45.
9. Fatima, M. N., Obaidat, M. S., Mahmood, K., Shamshad, S., Saleem, M. A. and Ayub, M. F. (2023). Privacy-Preserving Three-Factor Authentication Protocol for Wireless Sensor Networks Deployed in Agricultural Field. *ACM Transactions on Sensor Networks*. 1-21
10. Chauhan, E. V., Parekh, C. and Joshi, V. (2021). Three Factor Authentication Novel Framework through Improve System Privacy and Data Security. *International Journal of Scientific Research in Science, Engineering and Technology*. 8(3): 183-190
11. Huang, X., Xiang, Y., Chonka, A., Zhou, J. and Deng, R. H. (2010). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems 22*(8): 1390-1397.
12. Michelin, R. A., Zorzo, A. F., Campos, M. B., Neu, C. V. and Orozco, A. M. (2016). Smartphone as a biometric service for web authentication. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).* pp. 405-408.
13. Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A. and Pitchan, M. A. (2021). A systematic literature review of the types of authentication safety practices among internet users. *International Journal of Advanced Computer Science and Applications* 12(7): 829-837.
14. Sathishkumar D., SureshAmnad M, JeganAmaranth J, SangeeriniDevi A and Gurusubramani S. (2019). I-Voting on Cloud Framework, *International Journal of Engineering & Advanced Technology* 9(15): 61-64.
15. Mohamed, T. S. (2014). Security of Multifactor Authentication Model to Improve Authentication Systems. ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) 4(6)

Funding
Not applicable.

Institutional Review Board Statement
Not applicable.

Informed Consent Statement
Not applicable.

Acknowledgements
Not applicable

Conflict of Interest
The author declared no conflict of interest in the manuscript.

Authors' Declaration
The author(s) hereby declare that the work presented in this article is original and that any liability for claims relating to the content of this article will be borne by them.

Author Contributions
Not applicable

Cite article as:
Ojo, O.S. Development of a Three Factor Authentication System for Online Banking. *Ajayi Crowther J. Pure Appl. Sci.* **2024**, 3(2), pp. 22--28. | **doi:** https://doi.org/10.56534/acjpas.v3i2.114