Multi-Factor Authentication: A User Experience Study

Shagufta Baseer[1], **K. S. Charumathi**[2]

[1] Computer Department, Pillai College of Engineering, New Panvel, Mumbai, Maharashtra - 410206, India
[2] Professor, Computer Department, Pillai College of Engineering, New Panvel, Mumbai, Maharashtra - 410206, India

ABSTRACT

Usability issues prevent multi-factor authentication (MFA) systems from being widely used, despite the fact that they are essential for improving security measures. This study explores the problems with MFA systems' usability and suggests possible fixes to enhance the user experience. The study emphasizes the value of good design while highlighting the efficacy of graphical password systems as a user-friendly substitute for conventional MFA techniques. The report also makes recommendations for future research directions, such as assessing resilience against complex assaults, improving support for mobile applications, and weighing the benefits and drawbacks of image-based authentication systems. Comprehensive user research and assessments can yield important insights to improve the effectiveness and usability of different MFA approaches. Additionally, a two-way image-based mobile device authentication system devices is introduced in the article, demonstrating improved login success rates and security threat resistance. In order to further enhance the authentication process, future development will focus on scalability, user input surveys, and bolstering system security.

Keywords: Multi-Factor Authentication (MFA), User Experience (UX), Security, Usability, Graphical Passwords, Biometric Authentication, Mobile Devices, Image- Based Authentication, Psychological Aspects, Resilience,Scalability, Advanced Security Features

1. Introduction

The world is currently experiencing a new computing revolution. Quantum computing is the vehicle for this transformation[2]. This transformation will revolutionize people's lifestyles, but it also presents significant information security challenges[2].

With multi-factor authentication, an application or website can only be accessed by a computer user once they have successfully provided two or more factors, or pieces of proof[3]. It is the first line of defense opposing hackers as the traditional login procedures—password and username—are not totally secure against them since tools make it simple for hackers to guess them[3]. Additional security measures used by current systems include the usage of token devices, biometric verification (fingerprint, face recognition and the iris or retina of the eye), and two-factor verification using a one-time password through email or mobile device[3.

Traditional authentication techniques, such as passwords that are just text-based, have demonstrated vulnerabilities to various security threats[1]. In fact, whether credentials are obtained by brute force hacking or social engineering, they are involved in 61% of all breaches[1]. For systems to be secure, a strong user authentication technique is essential. Using a multi-factor authentication system and combining text and graphical passwords can work well. Biometrics and other advanced authentication technologies are safe, but their effective use requires extra infrastructure[1].

People can retrieve pictures more quickly and easily than words, according to psychological research and contemporary practices[3]. When you read about anything, like a car or a book, your mind instinctively creates an image of it; but, when terms like "amount," "level," or "ease" are mentioned, your mind might not create any images at all and it might just recall the phrases[3].

The uptake of multi-factor authentication (MFA) solutions by users is still inconsistent despite these advancements. Many consumers object to the widespread use of MFA because they find it difficult to use or confusing. The purpose of this study is to investigate the user experience (UX) of different MFA techniques in order to pinpoint adoption hurdles and recommend enhancements that can make these systems more approachable. Through comprehension of the pragmatic and psychological facets of user engagement with MFA, we may devise tactics to augment security while maintaining usability. In the end, this will assist in bridging the gap between the requirement for a flawless user experience and the necessity for strong security measures.

2. Literature Review

Diego Carrillo-Torres, Jesús Arturo Pérez-Díaz et al.(2023) author said that, In order to set up this paper on a brand-new multi-factor authentication system built using user-established associations, users must upload images and create relationships between them. These relationships are then saved specifically for the purpose of authentication. Users are required to select particular photographs and construct relations between them for verification as part of the authentication process, which is distinguished by its choice of images and relationships created by users algorithm. The algorithm's usability and efficacy were evaluated through a series of user tests including a heterogeneous set of individuals. These tests demonstrated the algorithm's novel approach to authentication, which eliminates the need for extra hardware or biometric data.
The following steps are involved in the authentication process[1]: Step 1: The user starts
the process of authentication.
Step 2: The user is prompted by the algorithm to choose particular photographs according to per-established standards.
Step 3: The user creates connections between the pictures they have chosen.

Step 4: To authenticate the user, the algorithm confirms the chosen photos and relationships[1].

Meghesh Solanki, Leena Ghatiya et al. (2022) author said that the methodology's main goal is to enhance planning and administration by breaking software development up into phases. Agile development is the selected methodology; it is an iterative process that prioritizes quick response and ongoing enhancement. To keep the process going, agile teams gather in person every day to collaborate.

Sanjida Akter Sharna, and Sheikh Ashraf Ali (2022) author state that there are registration and login steps in the proposed two-factor image-based authentication system's technique. Users are required to register with a unique username and 4-digit key number, which are both securely kept and encrypted using AES-128[5]. Upon entering their username during the login process, users are shown a 10x10 image grid if their usernames match. They have to choose pictures and input a key pattern that was made at registration. For authentication to be successful, both this pattern and the quantity of clicks must be duplicated. The system employs randomized picture grids to stop shoulder surfing, graphical passwords for further security, and AES encryption for data security. You may find more information and technical specifications in the original document.

Bandar Omar ALSaleem, and Abdullah I. Alshoshan(2021) state that in this document's methodology is centered on the suggested graphical password-based multi-factor authentication solution. This is a thorough breakdown of the methodology:
The suggested system.

The registration process involves the user creating a password, entering personal data, and creating a username.
During the registration procedure, the user chooses three photos in a certain order from various categories.
The user inputs their password and username to log in.

Each image receives a passcode from the system, which also shows a graphical screen with nine randomly chosen images—three of which are correct—displayed[3].
Based on the registration sequence, the user must choose the appropriate photos in the appropriate order.
Additionally, codes related to the displayed photos must be entered by the user. For authentication, the system compares the entered codes to the user's saved data.

During registration, user-selected images and passwords are hashed and stored. During login, the system presents a set of images, including the correct ones. The user enters codes associated with the correct images in the correct order. The system verifies these codes against the stored hashed data for authentication. The document doesn't provide specific equations but uses hashing algorithms like SHA256 for secure storage and verification.

Dr. K. Suresh Kumar, Poreddy Govardhan Reddy et al. (2021) state that the paper proposes a two-way image-based mobile device authentication system. During registration, users select three images and create unique patterns on a grid for each image, with the number of clicks and patterns stored in a database. In the unlocking phase, users must draw the pattern and match the click count for a given image. Over three weeks, legitimate user login success increased from 85% to 92%. The paper also examines the system's resilience to random guessing and shoulder surfing attacks. Limitations are noted, and future work includes implementing the system in online web applications for added security.

MASOUD ALAJMI, IBRAHIM ELASHRY et al. (2020) said that the paper on the "An Authentication System Based on Passwords and the CAPTCHA AI Issue[6]" uses a comprehensive approach to validate the system's security and efficiency. It includes tests like Histogram analysis, entropy, and ocular inspection calculations to ensure images are indistinguishable. Probabilistic property tests, like correlation coefficient calculations, verify immunity to attacks. Security proofs, including lemmas on XOR operations and game setups, demonstrate resistance to adaptive chosen-challenge text attacks. These components ensure the system's robustness and effectiveness in secure user authentication and information protection.

3. Observation

1) The study emphasizes the need for alternatives by highlighting the drawbacks of conventional authentication techniques as well as the difficulties associated with biometric technologies. While the accuracy, security, and usability of the suggested algorithm appear promising, more investigation is required to uncover any potential flaws before implementing it in a practical setting. Additionally, the research does not specify the precise techniques employed for relation establishment and image identification, implying that more investigation and optimization are required.

According to the paper, the suggested multi-factor authentication could provide a more convenient and economical option than techniques like one-time passwords or biometric authentication. Subsequent investigations might concentrate on strengthening the algorithm's resistance to security breaches and investigating its scalability for greater user populations or a wider range of devices. Expanding user feedback studies may also offer insightful information about preferences and potential areas for streamlining the login procedure.

2) Graphical passwords may have limited complexity compared to traditional text- based passwords, which could make them more vulnerable to attacks.

To make graphical password approaches more secure and efficient, more research is needed. With consideration for elements like image selection, length, and memorability, user studies can investigate preferences and behaviors. Additional research can reveal vulnerabilities and create solutions. Studies that compare graphical passwords to conventional and biometric techniques can assess them favorably. Subsequent investigations ought to augment usability and user experience, emphasizing interface design, accessibility, and password management.

3) The research gap reveals limitations in the current image-based password system: reliance on textual usernames, weak randomization using only the date, lack of password recovery, and static AES key usage. These flaws compromise security and usability, demanding immediate attention for improvement.

The future work and scope of this paper entail several key enhancements to bolster system security. Firstly, the integration of steganography will enable concealing the username within images, offering an additional layer of security during login processes. Secondly, employing randomized encryption keys instead of static AES keys will further fortify system security. Additionally, an extra feature will be implemented to prevent brute force attacks, enhancing overall protection against unauthorized access attempts.

4) This multi-factor authentication solution has relatively little security complexity. There is no defense against keyloggers or screen captures. Compared to forms, regular visuals are simpler to recall.

Future research could include extensive user studies to evaluate the system's effectiveness and user experience. Further development might enhance the system to support mobile applications, considering the growing use of mobile platforms. Additionally, integrating advanced security features like biometric authentication could improve overall security and user convenience.

5) The complexity of security of this image based authentication system is very less. We can add more authentication layer to provide more security.

The document in question makes reference to the potential for future system implementation in online web applications for increased security, but it offers no recommendations or specifics. A thorough analysis of current image-based authentication systems should be carried out to determine their advantages and disadvantages in order to improve future research. It would help to suggest changes or create a fresh strategy to deal with these restrictions. Furthermore, investigating usability and user acceptability through research and assessments would offer insightful information for additional improvement and application.

6) System security is emphasized throughout the article, however scalability and performance are not covered in great detail. Future studies could examine the system's capacity to support several users and how well it functions under various loads. It's also critical to take usability and user experience into account. One important research gap might be filled by looking into user perceptions, ease of use, and potential obstacles.

Investigating multi-factor authentication integration could improve security. A potential line of inquiry is how token-based or biometric systems might be enhanced by CAPTCHA AI. Case studies and real-world applications across a range of industries can provide insights about usefulness in practice. Future study should focus on evaluating resilience against sophisticated attacks using adversarial machine learning.

4. Conclusion And Knowledge Gaps

With a focus on user experience and striking a balance between security and usability, this survey study has looked at a variety of multi-factor authentication (MFA) system methodologies, approaches, and technological improvements. Since traditional text- based passwords have demonstrated to have serious weaknesses, multi-factor authentication (MFA) solutions such as biometrics, token devices, and image-based authentication systems have been developed in response to the growing demand for strong security measures.
The literature review brought to light a number of cutting-edge techniques that show promise for improving security without requiring complicated biometric data or additional hardware, such as picture recognition and user-established associations. Even though these methods offer some promising qualities, a number of research gaps and potential topics for further investigation have been noted.

The literature's main conclusions indicate that although MFA systems can greatly increase security, adoption of these systems is hampered by usability issues. MFA is frequently viewed by users as complicated and burdensome, which emphasizes the need for more logical and user-friendly solutions. Given that individuals can recall visuals more quickly than words, graphical password systems may be a good substitute provided they are properly designed, according to psychological study.

Future study should focus on these several interesting avenues. Comprehensive user research to assess the efficiency and usability of various MFA approaches will yield important information about user preferences and their practical usefulness. We made five unexpected yet, in our judgment, very important discoveries:

1) Future study should focus on evaluating resilience against sophisticated attacks using adversarial machine learning.

2) Further development might enhance the system to support mobile applications, considering the growing use of mobile platforms. Additionally, integrating advanced security features like biometric authentication could improve overall security and user convenience.

3) A thorough analysis of current image-based authentication systems should be carried out to determine their advantages and disadvantages in order to improve future research. It would help to suggest changes or create a fresh strategy to deal with these restrictions. Furthermore, investigating usability and user acceptability through research and assessments would offer insightful information for additional improvement and application.

4) Further research is needed to increase the complexity and security of graphical password systems while ensuring they remain user-friendly.

5) To make graphical password approaches more secure and efficient, more research is needed. With consideration for elements like image selection, length, and memorability, user studies can investigate preferences and behaviors. Additional research can reveal vulnerabilities and create solutions. Studies that compare graphical passwords to conventional and biometric techniques can assess them favorably. Subsequent investigations ought to augment usability and user experience, emphasizing interface design, accessibility, and password management.

REFERENCES

1. Carrillo-Torres, D., Pérez-Díaz, J. A., Cantoral-Ceballos, J. A., & Vargas-Rosales,

C. (**2023**). A novel multi-factor authentication algorithm based on image recognition and user established relations. Applied Sciences, 13(3), 1374.

2. Solanki, M., Ghatiya, L., Joshi, B., & Jangid, J. GRAPHICAL PASSWORD AUTHENTICATION SYSTEM. (Volume:04/Issue:11/November-**2022**)

3. Sharna, S. A., & Ali, S. A. (**2022**). Image Based Password Authentication System. arXiv preprint arXiv:2205.12352.

4. ALSaleem, B. O., & Alshoshan, A. I. (**2021**, March). Multi-factor authentication to systems login. In 2021 National Computing Colleges Conference (NCCC) (pp. 1-4). IEEE.

5. Kumar, K. S., Govardhan Reddy, P., & Sivakumar, A. (**2021**, July). A Two Factor Image Based Authentication System. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC).

6. Alajmi, M., Elashry, I., El-Sayed, H. S., & Faragallah, O. S. (**2020**). A password- based authentication system based on the CAPTCHA AI problem. IEEE Access, 8, 153914-153928.

7. Sinha, A.; Shrivastava, G.; Kumar, P. A Pattern-Based Multi-Factor Authentication System. Scalable Comput. Pract. Exp. **2019**, 20, 101–112. [CrossRef]

8. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy,

Y. Multi-Factor Authentication: A Survey. Cryptography **2018**, 2, 1. [CrossRef]

9. Ibrahim, D.; The, J.; Abdullah, R. Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization. Inf. Secur. J. Glob. Perspect. **2019**, 30, 149–159. [CrossRef]

10. ALSaleem, B.O.; Alshoshan, A. Multi-Factor Authentication to Systems Login. In Proceedings of the **2021** National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 27–28 March 2021. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9428806&isnumber=942 8786 (accessed on 17 November 2022).

11. Sharayu S. Ganorkar1, Prof. H. V. Vyawahare 2 “Review Paper on Graphical Password Authentication Techniques “Volume 5, Issue 03, March -**2018**.

12. A. N. O. Hammed M, “PREVENTING SHOULDER SURFING ATTACK IN

graphical passwords authentication SCHEME,” Ann. Comput. Sci. Ser. Tome 18, Fasc. 1, vol. XVIII, **2020**.

13. S. A. K. K Himaja Sri, M Vishnu Vardhan, K Nikitha, K M Kiran, "Graphical Password Authentication - Survey," J. X i 'an Univ. Archit. Technol., vol. XII, no. IV,
p. 3701, **2020**.

14. Gunasinghe and E. Bertino, "PrivBioMTAuth: Privacy Preserving Biometrics- Based and User Centric Protocol for User Authentication From Mobile Phones," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 1042- 1057, April **2018**, doi: 10.1109/TIFS.2017.2777787.

15. V. Nguyen, Z. Huang, S. Bethini, V. S. P. Ippagunta and P. H. Phung, "Secure Captchas via Object Segment Collages," in IEEE Access, vol. 8, pp. 84230-84238, **2020**, doi: 10.1109/ACCESS.2020.2989258.

16. C. Meshram and M. S. Obaidat, ‘‘An efficient provably secure ibs tech nique using integer factorization problem,’’ in Proc. 1st Int. Conf. Comput., Commun., Cyber-Secur., **2020**, pp. 427–439.

17. Y. Huang, Z. Su, F. Zhang, Y. Ding, and R. Cheng, ‘‘Quantum algorithm for solving hyperelliptic curve discrete logarithm problem,’’ Quantum Inf. Process., vol. 19, no. 2, p. 62, Feb. **2020**.

18. F. H. Alqahtani and F. A. Alsulaiman, ‘‘Is image-based CAPTCHA secure

against attacks based on machine learning? An experimental study,’’ Com put. Secur., vol. 88, Jan. **2020**, Art. no. 101635.

19. H.-P. Ren, C.-F. Zhao, and C. Grebogi, ‘‘One-way hash function based on delay- induced hyperchaos,’’ Int. J. Bifurcation Chaos, vol. 30, no. 02, Feb. **2020**, Art. no. 2050020.

20. M. Zhou and C. Wang, ‘‘A novel image encryption scheme based on

con servative hyperchaotic system and closed-loop diffusion between blocks,’’ Signal Process., vol. 171, Jun. **2020**, Art. no. 107484.

21. K. Hövelmanns, E. Kiltz, S. Schäge, and D. Unruh, ‘‘Generic authenticated key exchange in the quantum random oracle model,’’ in Proc. IACR, **2020**, pp. 389–422.

22. Zaenchkovski, A., Lazarev, A., & Masyutin, S. (**2022**, September). Multi-factor authentication in innovative business systems of industrial clusters. In International Russian Automation Conference (pp. 271-281). Cham: Springer International Publishing.

23. Ahmad, M. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (**2023**). BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities. Sensors, 23(5), 2757.

24. Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (**2023**). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences, 13(19), 10871.

25. Obaidat, M., Brown, J., Obeidat, S., & Rawashdeh, M. (**2020**). A hybrid dynamic encryption scheme for multi-factor verification: a novel paradigm for remote authentication. Sensors, 20(15), 4212.

26. Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M.

D. (2021). A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. Sensors, 21(18), 6018.

27. Maranco, M., Logeshwari, R., Sivakumar, M., & Manikandan, V. (2024). Improvised Multi-Factor Authentication for End-User Security in Cyber Physical System. International Journal of Intelligent Systems and Applications in Engineering, 12(15s), 416-424.

28. Shaikh, M. I., & Lokhande, P. S. (2024). Tackling Threats: A Study of Vulnerability Testing and Mitigation in Web Applications. Available at SSRN 4823623.

29. Zhu, D., Zhou, H., Li, N., Song, L., & Zheng, J. (**2024**). Multi-factor authentication scheme based on custom attributes. Cluster Computing, 1-16.

30. Rizqullah, N. Z., Alekhine, J., Purnomo, R. M. R., & Yuhana, U. L. (**2024**, February). Enhancing School Data Security with Multi Factor Authentication. In 2024 IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS) (pp. 1-6). IEEE.

31. Kim, S., Mun, H. J., & Hong, S. (**2022**). Multi-factor authentication with randomly selected authentication methods with DID on a random terminal. Applied Sciences, 12(5), 2301.

32. Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (**2021**). A new hybrid online and offline multi-factor cross-domain authentication method for iot applications in the automotive industry. Energies, 14(21), 7437.