JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5970

USABILITY EVALUATION OF MOBILE MULTI-FACTOR AUTHENTICATION BASED ON FACE AUTHENTICATION, GEOLOCATION AND QR CODE

I Kadek Dendy Senapartha[1*]; Matahari Bhakti Nendya[2]

Department of Informatics [1,2]
Duta Wacana Christian University, Yogyakarta, Indonesia[1,2]
www.ukdw.ac.id[1,2]
dendy.prtha@staff.ukdw.ac.id[1*], didanendya@staff.ukdw.ac.id [2]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract*—The swift progress of information technology has led to the adoption of mobile-based multi-factor authentication (MFA) systems for attendance management, addressing inefficiencies, security issues, and errors inherent in traditional methods. By utilizing multiple layers of authentication—such as face recognition, geolocation, and QR code scanning—these systems significantly enhance security and reliability. This study evaluates the usability of a mobile MFA system, focusing on user-friendliness and learnability. Two iterations of the system were tested using cognitive walkthrough approaches, chosen for their effectiveness in simulating the experience of new users and identifying usability issues in system learnability. The initial version of the system utilized MobileFaceNet_v2, which had an input size of 112x112. This resulted in a false acceptance rate (FAR) of 0.26, a false rejection rate (FRR) of 0.2, and a half total error rate (HTER) of 0.23. Failures in face verifications and inadequate instructions led to significant user dissatisfaction. In the second iteration, improvements were made by providing better instructions during location and QR scan steps, adding a face capture confirmation screen, and increasing the input size of the face anti-spoof detection model to 224x224. This reduced the FAR to 0.11 but increased the FRR to 0.4, resulting in HTER to 0.25. While these updates improved security, usability issues such as ambiguous user feedback and inadequate instructions persisted. These results emphasize the need for an integrated approach that combines both technological improvements in authentication models and enhancements in UI design to create a more user-friendly experience.*

Keywords*: face authentication, geolocation, mobile MFA, usability evaluation, QR code.*

Intisari—*Kemajuan pesat teknologi informasi telah mendorong adopsi sistem otentikasi multi-faktor mobile (MFA) untuk manajemen kehadiran, mengatasi ketidakefisienan, masalah keamanan, dan kesalahan yang melekat pada metode tradisional. Dengan memanfaatkan beberapa lapisan autentikasi—seperti pengenalan wajah, geolokasi, dan pemindaian kode QR—sistem ini secara signifikan meningkatkan keamanan dan keandalan. Studi ini mengevaluasi usability sistem MFA mobile, dengan fokus pada kemudahan penggunaan dan kemampuan belajar. Dua iterasi sistem diuji menggunakan pendekatan cognitive walkthrough, yang dipilih karena efektivitasnya dalam mensimulasikan pengalaman pengguna baru dan mengidentifikasi masalah learnability sistem. Versi awal dari sistem ini menggunakan MobileFaceNet_v2, yang memiliki ukuran input 112x112. Ini menghasilkan false acceptance rate (FAR) sebesar 0,26, false rejection rate (FRR) sebesar 0,2, dan half total error rate (HTER) sebesar 0,23. Kegagalan dalam verifikasi wajah dan instruksi yang tidak memadai menyebabkan ketidakpuasan pengguna yang signifikan. Pada iterasi kedua, perbaikan dilakukan dengan memberikan instruksi yang lebih detail pada saat pengecekan lokasi dan pemindaian kode QR, menambahkan tampilan konfirmasi tangkapan wajah, dan meningkatkan ukuran input model deteksi anti-spoof wajah menjadi 224x224. Ini mengurangi FAR menjadi 0,11 tetapi meningkatkan FRR menjadi 0,4, menghasilkan HTER sebesar 0,25. Meskipun pembaruan ini meningkatkan keamanan, masalah usability seperti feedback yang ambigu dan instruksi yang kurang memadai tetap ada. Hasil penelitian ini menekankan*

perlunya pendekatan terpadu yang menggabungkan peningkatan teknologi dalam model autentikasi dan desain UI untuk menciptakan pengalaman yang lebih ramah pengguna.

***Kata Kunci**: autentikasi wajah, geolokasi, MFA seluler, evaluasi kegunaan, kode QR.*

INTRODUCTION

The swift progress of information technology has greatly altered several facets of organizational administration, such as the monitoring and verification of attendance. Traditional attendance management techniques, such as manual sign-ins and RFID card-based systems, suffer from several shortcomings, including security vulnerabilities, inefficiencies, and susceptibility to human error [1], [2]. These limitations compromise the reliability and integrity of attendance data, particularly in contexts where secure and accurate verification is crucial. Mobile device-based solutions, using multi-factor authentication (MFA), are increasingly replacing traditional methods due to their ability to provide enhanced security and convenience[3], [4].

Despite the advantages of MFA systems, significant gaps persist in both existing research and industry practices regarding their usability, particularly in attendance management. Many MFA systems prioritize security over user experience, resulting in cumbersome authentication procedures that frustrate users and hinder efficiency[2], [3]. For example, overly complex interfaces, inadequate instructions, and unresponsive system behaviours have been identified as common barriers to effective user interaction, impacting user adoption and satisfaction [4], [5].

Furthermore, there is a lack of comprehensive usability evaluations for MFA systems in attendance contexts. Most existing studies focus primarily on technical metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR), with limited attention given to usability issues such as user-friendliness and learnability [6]. This lack of emphasis on usability poses significant challenges to the widespread adoption of MFA technologies in organizational environments, where ease of use and user satisfaction are critical for operational success. MFA employs several security measures, including facial recognition, geolocation, and QR codes, to authenticate users' identities and confirm their physical presence at a specified place for a particular task. This technique is especially crucial in contexts where the utmost importance is placed on security and accuracy in attendance control [7]. Usability refers to the degree to which users can engage with a system efficiently, effectively, and successfully [8]. It plays a crucial role in the acceptance and continued use of technology in organizational environments. An intricate, sluggish, or excessively complicated system might compromise its intended security benefits by causing frustration among users and decreasing operating efficiency.

This study seeks to assess the usability of a mobile MFA system that is particularly created for managing attendance, considering the difficulties that arise in this context. The Cognitive Walkthrough approach is employed to identify issues related to system learnability and simulate new user experiences [9]. By focusing on these usability aspects, the study aims to provide practical insights and design recommendations that enhance the balance between security and usability, contributing to the development of more user-friendly and efficient mobile MFA-based attendance systems. The specific research questions guiding this study are:

1. How effective is the mobile MFA system in terms of user-friendliness and satisfaction when used for attendance management?
2. What usability challenges do users face during the authentication process, and how do these challenges affect overall user experience?
3. How can improvements be made to enhance the usability of mobile MFA systems without compromising security?

By addressing these research questions, this study intends to highlight critical usability challenges, propose design improvements, and ultimately support the development of MFA systems that strike an optimal balance between security and user experience.

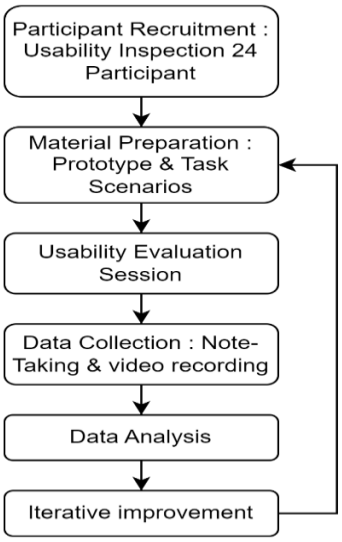
MATERIALS AND METHODS

The study design focuses on creating and assessing the MFA system prototype using the Cognitive Walkthrough method to evaluate the prototype's learnability by simulating a new user's experience and assessing how intuitive and accessible the system is for first-time users [10]. The Cognitive Walkthrough method was chosen for its effectiveness in evaluating system learnability, particularly for complex systems like MFA. Compared to other usability evaluation methods, such as heuristic evaluation or usability testing, the Cognitive Walkthrough is particularly suitable for identifying issues that first-time users might face

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5970

during their initial interactions. MFA systems often require users to navigate multiple steps and authentication factors, which can be challenging for those unfamiliar with the technology. The Cognitive Walkthrough method simulates a step-by-step user journey, focusing on whether a new user would be able to understand and successfully complete each task without external assistance.

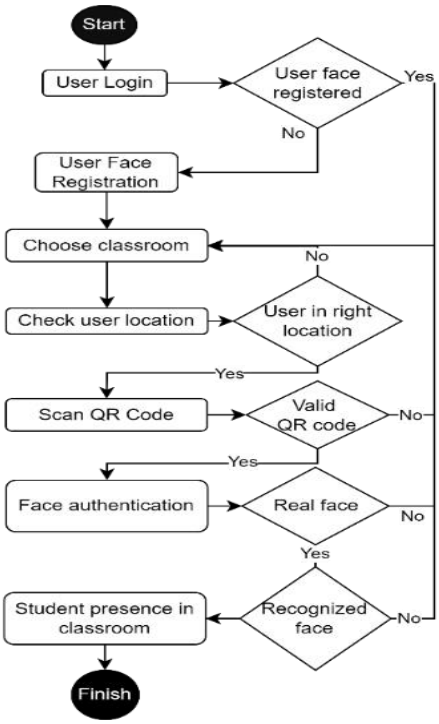


Source: (Research Results, 2024)

Figure 1. Steps taken during the usability evaluation process, from participant recruitment to iterative improvements based on the findings.

Source: (Research Results, 2024)

Figure 1Figure 1 representing the method used in this study. A total of 24 participants were involved, divided into two groups of 12 for two iterations of the usability inspection. The participants consisted of students aged 20 to 25 years, representing a diverse range of educational backgrounds. Sixteen of the participants came from disciplines unrelated to computer science, such as business, humanities, and social sciences, while the remaining eight were from technical fields, specifically computer science and related disciplines. This diversity was important to capture usability issues across different types of users, including those with no technical expertise as well as those with a higher understanding of technology [11]. By including both novice and experienced users, the study aimed to generate insights that would be applicable to a broader user base, making the results more generalizable.



Source: (Result of the Research, 2024)

Figure 2. Mobile MFA system flow that incorporates crucial components such as geolocation verification, QR code scanning and face authentication.

Before beginning the walkthrough sessions, a functioning prototype of the mobile MFA system is prepared, as shown in **Error! Reference source not found.** consists of a working prototype and Figure 2 showing mobile MFA flow that incorporates crucial components such as face identification, geolocation verification, and QR code scanning. These applications and system flows serve as the basis for evaluating the system's usability. A standardized set of tasks was developed as shown at Table 1, outlining specific scenarios that participants had to complete, such as face registration, geolocation verification, and QR code scanning. Each participant followed these tasks in a predetermined order to ensure a consistent experience across the study.

Table 1. Test scenarios and activities for usability evaluation

No	Scenario	Steps
1	Testing user face registration	1. Log in using the proper email address. 2. Click on the "Face Registration" button. 3. Take a photo of their face, ensuring that the photo-taking gadget is positioned parallel to the eye line and that the lighting

No	Scenario	Steps
		conditions range between 80 and 120 lux.
2	Testing with precise location, QR scan, genuine face, and recognized face	1. Sign in with registered email. 2. choose the attendance class. 3. choose timetable. 4. Refer to room location. 5. QR code scan in 5 minutes. 6. face-photography utilizing actual face. 7. return to schedule page
3	Testing using incorrect geolocation coordinates, correct QR scan, actual face, recognized identity.	1. Sign in with registered email. 2. choose the attendance class. 3. choose timetable. 4. View location in other rooms and beyond 10 M. 5. Return to schedule page
4	Testing with accurate geolocation coordinates, faulty QR scan, actual face, & recognized face	1. Sign in with registered email. 2. choose the attendance class. 3. choose timetable. 4. Refer to room location. 5. Scan wrong QR code. 6. The system pops up saying the QR code doesn't match. 7. Return to the scan QR page
5	Testing with accurate geolocation, QR scan, fake face, and recognized face	1. Sign in with registered email. 2. choose the attendance class. 3. choose timetable. 4. Verify user location. 5. QR code scan in 5 minutes. 6. Using the user's facial picture to face authentication. 7. Show info "Fake face detected!" 8. Return to schedule page.
6	Testing using precise geolocation, A correct QR scan, Real face, Unknown face	1. Sign in with registered email. 2. choose the attendance class. 3. choose timetable. 4. Verify user location. 5. QR code scan in 5 minutes. 6. When authenticate face using other faces, "Unknown face" pop up appears. 7. Return to schedule page.

Source: (Research Results, 2024)

Participants were selected through purposive sampling, which aimed to ensure a balanced representation of both technical and non-technical users. The sample size of 24 was considered adequate to identify significant usability issues while keeping the process manageable, ensuring that detailed Cognitive Walkthroughs could be conducted with each participant [12]. This sample size allowed for the in-depth exploration of user interactions with the system, particularly focusing on areas of difficulty that could influence the system's learnability and usability.

A mixed-methods approach was used to evaluate the usability of the MFA system. The study included both qualitative and quantitative measures to provide a comprehensive understanding of system performance and user experience [13]. Quantitative evaluation employed metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Half Total Error Rate (HTER) to assess authentication performance across iterations [6], [14]. The qualitative evaluation focused on usability aspects, using oral input, observational notes, and video recordings of user interactions. Evaluators followed a set of scenarios to ensure consistency in observations, noting participants' task completion rates, errors, and user feedback. Data analysis employed qualitative content analysis to identify common themes and usability challenges. Combining qualitative and quantitative findings ensured a comprehensive evaluation, focusing on making the system secure, user-friendly, and accessible. This systematic approach allowed the identification of key usability issues and provided actionable insights into improving the MFA system's learnability and overall user experience.

RESULTS AND DISCUSSION

The usability assessment of the mobile MFA system developed for attendance management unveiled some significant obstacles encountered by users during their contact with the system. The obstacles were found using cognitive walkthrough methodologies, which allowed for a thorough understanding of user difficulties and their effects on user happiness and operational efficiency. The data obtained from both strategies were compared to comprehend the areas of overlap and distinctive elements emphasized by each methodology.

User Feedback Analysis on Security Concerns (First Iteration)

This initial iteration of the mobile MFA system was developed using MobileFaceNet_v2, employing a 112x112 input size to identify and defend against face spoofing. The system achieved the following performance metrics: True Negative (TN) 5376, False Positive (FP) rate 1936, False Negative (FN) rate 63, and True Positive (TP) rate 260. Based on these measurements, FAR was 0.26, FRR was 0.2, and the HTER was 0.23. The high FAR of 0.26 represented a significant security concern, as unauthorized users were incorrectly accepted. This issue may directly influenced user trust in the system, as it implied that the system's security measures were insufficient.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5970

User Feedback Analysis on Usability Concerns (First Iteration)

A usability evaluation on the first iteration as shown in Table 2 reveal problem faced by user. Positive feedback is given by six individuals indicated that they found the whole application process to be readily understandable and user-friendly. Furthermore, one participant conveyed gratitude for the facial recognition system and the GPS feature, which enables the determination of whether a student is inside the specified radius of the room.

Table 2. The first Cognitive Walkthrough usability assessment with 12 respondents included positive and negative comments.

Positive	Negative
1. The application flow is easy to understand and use. (6 subject) 2. GPS detects if pupils are inside the class radius, which is helpful. (1 subject) 3. The facial authentication flow is easy to use. (1 Subject)	1. Failed to verify the original face, making users feel disappointed. (4 subject) 2. Need information to determine face-camera distance. (3 subject). 3. First-time QR scan checking was difficult. (2 subject). 4. The lack of a loading screen made facial authentication confusing. (1 subject) 5. There were concerns about registration and face authentication delays. (2 subject). 6. struggled to re-scan the QR after it failed. (1 subject) 7. had trouble registering her face because there were no face image positioning guidelines. (1 subject)

Source: (Research Results, 2024)

However, notable limitations in terms of usability were recorded, resulting from the flaws in facial recognition systems. Four participants expressed dissatisfaction when the system was unable to authenticate their first face, highlighting the direct influence of the system's FAR and FRR. In addition, users have indicated a need for enhanced details on the distance between the face and the camera, together with precise guidelines for optimal positioning of the face. This information has the potential to reduce the frequency of incorrect rejections. Further obstacles included difficulties with the first QR scan, confusion resulting from the lack of a loading screen during facial verification, and delays experienced during the registration and face authentication processes.

User Feedback Analysis on Security Concerns (Second Iteration)

In the second iteration, several improvements were made to enhance the system's usability and security. The input size of face anti-spoof model is increase to 224x224. This model has flowing performance: TN rate 6479, TP rate 195, FP rate 791, and FN rate 128. Through these improvements, the FAR was brought down to 0.11, which is a significant drop. However, the FRR increased to 0.4. This reduction of the FAR to 0.11 represented a significant security improvement, reducing the likelihood of unauthorized access.

However, the increase in the FRR to 0.4 suggested that the system had become overly stringent, resulting in more frequent rejections of legitimate users. This indicated that the system still faced challenges in balancing strict security measures with usability. The high FRR affected user satisfaction, as legitimate users struggled to gain access, which could deter them from using the system in the long term. Furthermore, the HTER increase to 0.25, which is an indication that additional improvements are required to strike a balance between the characteristics of usability and security.

User Feedback Analysis on Usability Concerns (Second Iteration)

The second iteration addressed several usability issues identified in the first iteration. Improvement is made by give more information during user location check and QR scan steps. New implementation also made by adding face capture confirmation screen to inform user on captured face during face registration and face authentication. This helped to reduce confusion and improve user confidence. This improvement, as shown in Table 3 resulting positive feedback where three participants indicated that they did not encounter any notable challenges, while two emphasized the simplicity of comprehending the application process. Furthermore, the face registration procedure received acclaim for its straightforwardness, and the warnings presented during inaccurate QR scans were deemed to be unambiguous and beneficial.

Table 3. The Second Usability examination using Cognitive Walkthrough with 12 respondents offers positive and negative comments.

Positive	Negative
1. No significant difficulties (3 respondents) 2. Application flow is easy to understand. (2 respondents)	1. Difficulties during face authentication, perhaps due to inappropriate lighting. (3 respondents)

Positive	Negative
3. Face registration process is easy to use. 4. The process and indicators when scanning the wrong QR are quite clear.	2. Can be given a notification if the lighting is not good. (1 respondent) 3. There is confusion when scanning the QR code, because there are no instructions. (3 respondents) 4. Information about attendance needs to be improved. (2 respondents) 5. Feel less confident when registering faces, because the image capture is not optimal. (1 respondent) 6. QR codes for attendance expire too quickly. (1 respondent) 7. Need to load indicators when checking the geolocation position. (1 respondent) 8. There needs to be a tutorial for onboarding new users. (1 respondent)

Source: (Research Results, 2024)

However, several usability issues continued to exist. A total of three participants experienced challenges when undergoing face authentication, especially in situations with inadequate lighting. This highlights the necessity for enhanced illumination instructions throughout the authentication process. One subject proposed including alerts to notify users when the illumination is inadequate. Furthermore, the absence of clear instructions during QR code scanning continued to cause confusion, and certain users expressed reduced confidence during face registration as the picture-capturing procedure appeared to be suboptimal. Additional criticisms encompassed the rapid expiration of QR codes used for attendance tracking, the lack of load indications during geolocation verification, and the necessity for a training to aid new users throughout the onboarding process.

Discussion

Table 4. Comparison of face anti-spoof model used by each iteration. First iteration using 112x112 input size and second iteration using 224x224 input size.

112x112 input size	224x224 input size
True Negative = 5376	True Negative = 6479
False Positive = 1936	False Positive = 791
False Negative = 63	False Negative = 128
True Positive = 260	True Positive = 195
FAR = 0.26	FAR = 0.11
FRR = 0.2	FRR = 0.4
HTER = 0.23	HTER = 0.25

Source: (Research Results, 2024)

This usability assessment of the mobile MFA system revealed that enhancements in the face anti-spoofing capabilities as shown at Table 4 had a significant impact on the overall usability. Despite the enhancement in face anti-spoof model performance in second iteration, several users still had difficulties during face authentication, especially in circumstances with inadequate lighting, and proposed the necessity for warnings related to appropriate illumination. Research indicates that lighting intensity significantly affects critical variables, including the area and colour of captured images [15]. It is important to note that proper lighting is essential for maintaining the precision of image processing systems. Therefore, addressing lighting conditions is essential for enhancing the accuracy and overall user satisfaction in facial authentication systems, like adaptive lighting controls [16] and notifications to inform users of unsuitable lighting conditions, may become a solution to solve this issue.

However, the authentication model's underlying performance was not the only factor affecting usability. The user interface (UI) design played a significant role in shaping the user experience and satisfaction [17]. Based on user feedback analysis from each iteration, participants consistently reported difficulties such as inadequate instructions on face positioning, the lack of indicators during facial verification and geolocation checks, and the rapid expiration of QR codes without clear notifications. These issues created confusion and frustration for users, especially during crucial interactions like face authentication in low-light conditions. The second iteration saw improvements, such as adding a face capture confirmation screen and more detailed instructions, but these enhancements only partially mitigated the usability challenges.

The future experiment should be placed on optimizing the UI to further improve usability. Incorporating more intuitive visual cues, real-time feedback mechanisms, and adaptive instructions could significantly enhance user satisfaction. Addressing lighting conditions with adaptive prompts and providing a more informative onboarding process would also help reduce user errors and misunderstandings. Achieving a seamless user experience requires not only enhancing the model's accuracy but also designing a UI that effectively guides users throughout the authentication process, balancing security with ease of use to create a reliable and user-friendly MFA system.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 2 NOVEMBER 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i2.5970

CONCLUSION

This study evaluated the usability of a mobile multi-factor authentication (MFA) system for attendance management, focusing on the balance between security and user experience across two iterations. The first iteration showed a FAR of 0.26 and an FRR of 0.2, indicating that the system struggled to reject unauthorized users and, at the same time, occasionally prevented legitimate users from gaining access. Improvements in the second iteration reduced the FAR to 0.11, enhancing the system's security; however, the FRR increased to 0.4, highlighting usability challenges, particularly under adverse conditions such as poor lighting. These metrics underscore the difficulties in achieving an optimal balance between high security and seamless usability, which is a critical challenge for MFA systems. Although several users experienced enhancements like the addition of a face capture confirmation screen and more detailed user prompts, others noted ongoing difficulties attributed to the absence of adequate instructions, lack of visual feedback, and confusing interactions, such as rapid QR code expiration, which contributed to a less-than-optimal user experience. This finding revealed that system usability is not only impacted by the underlying model's performance but is also heavily influenced by the user interface (UI) design.

The implications of these findings provide valuable insights for the design of future mobile MFA systems, suggesting that a balance between security and usability is crucial for broader applications, such as access control, secure transactions, and identity verification. By focusing on reducing the FAR without excessively increasing the FRR and enhancing UI elements to better guide users through the authentication process, future MFA systems can achieve improved performance and greater user satisfaction. Finally, investigating alternative biometric techniques or multi-modal authentication might offer useful insights into minimizing false positive rates while preserving security, hence assuring a balance between usability and protection in future mobile MFA systems.

REFERENCE

[1] S. Mujeye, "A Survey on Multi-Factor Authentication Methods for Mobile Devices," in *ACM Other conferences*, New York, NY, USA: Association for Computing Machinery, 2021, pp. 199–205. doi: 10.1145/3451471.3451503.

[2] S. Baseer and K. Charumathi, "Multi-Factor Authentication: A User Experience Study," *Available at SSRN 4840295*, 2024, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4840295

[3] A. Kruzikova, M. Muzik, L. Knapova, L. Dedkova, and ..., "Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction," *Computers & …*, Vol 138, 2024, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823005771

[4] J. Oluwafemi and J. Feng, "How users perceive authentication of choice on mobile devices," *13 th International Conference on Advances …*, pp. 345-351, 2020, [Online]. Available: https://www.researchgate.net/profile/Akintunde-Oluwafemi/publication/351365246_How_Users_Perceive_Authentication_of_Choice_on_Mobile_Devices/links/60942110458515d315ffd3d8/How-Users-Perceive-Authentication-of-Choice-on-Mobile-Devices.pdf

[5] H. Mpirirwe, D. Mirembe, J. Lubega, J. Agaba, and ..., "A Multifactor Authentication Framework for Usability in Education Sectors in Uganda," *… Conference on Data …*, pp. 205-216, 2024, doi: 10.1007/978-981-97-3242-5_15.

[6] G. I. W. Tamtama and I. K. D. Senapartha, "Fake Face Detection System Using MobileNets Architecture," *Com, Engine, Sys, Sci*, vol. 8, no. 2, p. 329, Jul. 2023, doi: 10.24114/cess.v8i2.43762.

[7] Y. Kornelius, I. K. D. Senapartha, and G. I. W. Tamtama, "Sistem Presensi Multi Factor Dengan Menggunakan Deteksi Lokasi, Scan Qrcode, Pengecekan Antispoof Dan Pengenalan Wajah," in *Prosiding Seminar Nasional Hasil Penelitian dan Pengabdian Masyarakat*, Universitas Islam Indonesia: Universitas Islam Indonesia, 2023, pp. 198–207. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/45812

[8] F. Paz *et al.*, "Qualitative and Quantitative Approaches to Conduct Heuristic Evaluations: A Comparison Study," in *SpringerLink*, Cham, Switzerland: Springer, 2024, pp. 310–323. doi: 10.1007/978-3-031-61351-7_22.

[9] R. da C. Lopes *et al.*, "Breaking the Wall of E-Waste Recycling Education by Means of a Digital Game," in *SpringerLink*, Cham,

Switzerland: Springer, 2024, pp. 103–117. doi: 10.1007/978-3-031-51452-4_8.

[10] J. R. Lewis and J. Sauro, "Usability And User Experience: Design And Evaluation," in *Wiley Online Library*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2021, pp. 972–1015. doi: 10.1002/9781119636113.ch38.

[11] S. Rutter, E. Zamani, J. McKenna-Aspell, and Y. Wang, "Embedding equality, diversity and inclusion in usability testing: Recommendations and a research agenda," *Int. J. Hum. Comput. Stud.*, vol. 188, p. 103278, Aug. 2024, doi: 10.1016/j.ijhcs.2024.103278.

[12] M. Hertzum, "Concurrent or Retrospective Thinking Aloud in Usability Tests: A Meta-Analytic Review," *ACM Trans. Comput.-Hum. Interact.*, vol. 31, no. 3, pp. 1–29, Aug. 2024, doi: 10.1145/3665327.

[13] J. W. Creswell, *A Concise Introduction to Mixed Methods Research*. Thousand Oaks, CA, USA: SAGE Publications Ltd, 2024. [Online]. Available: https://uk.sagepub.com/en-gb/asi/a-concise-introduction-to-mixed-methods-research/book266037

[14] Z. Ming, M. Visani, M. M. Luqman, and J.-C. Burie, "A Survey On Anti-Spoofing Methods For Face Recognition with RGB Cameras of Generic Consumer Devices," Oct. 08, 2020, *arXiv*: arXiv:2010.04145. Accessed: Jul. 20, 2022. [Online]. Available: http://arxiv.org/abs/2010.04145

[15] Z. Zhu, X. Fang, and C. Zhao, "Influence of light intensity and magnification on the precision of nanoscale positioning in micro-vision-based dark-field imaging," *Opt. Lasers Eng.*, vol. 169, p. 107753, Oct. 2023, doi: 10.1016/j.optlaseng.2023.107753.

[16] S. Boovaraghavan *et al.*, "Mites: Design and Deployment of a General-Purpose Sensing Infrastructure for Buildings," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 7, no. 1, pp. 1–32, Mar. 2023, doi: 10.1145/3580865.

[17] D. A. Norman, *Design for a Better World: Meaningful, Sustainable, Humanity Centered*. Cambridge, MA, USA: The MIT Press, 2024. [Online]. Available: https://www.amazon.com/Design-Better-World-Meaningful-Sustainable/dp/0262548305