International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 267-275 www.ijaem.net ISSN: 2395-5252

Web-based Biometric Authentication System for Health tracking Application

Lateef Q.O, Akinyokun O.K
[1]Student, the Federal University of Technology, Akure, Nigeria
[2]Lecturer, the Federal University of Technology, Akure, Nigeria.

Date of Submission: 05-01-2025 Date of Acceptance: 15-01-2025

ABSTRACT: As technology advances, passwordless authentication is becoming increasingly important for web applications, especially for secure and user-friendly login systems. Biometrics-based authentication offers a promising alternative to traditional password systems, providing greater security and convenience. However, its usability and effectiveness in real-world web applications, particularly in sectors requiring high security like health monitoring, require further investigation. While much of the current research has primarily focused on the security benefits of biometric systems, particularly on mobile devices, there is a gap in understanding their impact on user experience and practical implementation in web applications. Limited research has evaluated how well biometric authentication performs in terms of user satisfaction, ease of use, and technical reliability in such environments. This project develops a health tracker web application incorporating biometrics-based authentication using Passage and NextAuth.js. The study evaluates the system's usability through both quantitative metrics—such as an 85% success rate of biometric logins and authentication times averaging 2.5 seconds—along with qualitative user feedback on the overall experience. User interactions were recorded, and surveys gathered insights into perceived ease of use and satisfaction. The results demonstrate that biometric authentication significantly improves user convenience while maintaining a high level of security. Success rates for biometric logins were high, and authentication times were faster compared to traditional methods. Users reported a positive experience, indicating that biometrics reduced login friction and increased overall satisfaction with the application. These findings suggest that biometric authentication is not only secure but also highly usable in web applications. These insights can guide developers in designing more user-friendly authentication systems, especially for health-related web platforms, where security and ease of use are both critical.

KEYWORDS: biometrics, fingerprint, webauthn, fido, web, application, webapp, health, tracking.

I. INTRODUCTION

Humans reliance on web applications for personal, financial, and professional activities has greatly increased in recent times. This reliance has led to the need for organizations, institutions, and individuals alike to ensure the security of online data and ensuring good user experience. Traditional password authentication have been, even till today, the standard for decades; however, they present several challenges which includes the vulnerability to phishing attacks, and susceptibility to brute-force attempts. Users are often required to use strong passwords and avoid password reuse which then leads to inconvenience and security vulnerability.

Biometrics, or simply put human measurements, are metrics related to unique person characteristics that distinguish one individual from another. Biometric systems involves measuring and processing of individuals' biological and behavioural traits. Since these traits are difficult to replicate, they thereforr provide enhanced security. Biometric authentication is an authentication approach that relies on individuals unique biometric trait to confirm that they are who they claim to be. It offers an easier-to-use approach as users do not need to remember passwords or use multi-step verification methods like one-time passwords (OTPs).

This research explores the application of biometric authentication in web applications, specifically focusing on evaluating its usability and overall user experience. The study involves implementing biometric authentication in a web-based health tracker application, integrating

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 267-275 www.ijaem.net ISSN: 2395-5252

modern technologies such as Passage and NextAuth.js to create a seamless password-less experience.

Although biometric authentication is widely used on mobile platforms, its adoption in web applications remains relatively low. Web applications, despite growing in complexity and scale, still rely predominantly on password-based systems. The usability and user experience of biometric-based systems in web applications have not been adequately explored. This research aims to fill this gap by evaluating the performance of biometric authentication systems in terms of user satisfaction, speed, and reliability when implemented in a real-world web application.

II. RELATED WORKS

The evolution of authentication methods from traditional password-based systems to more advanced, password-less techniques has garnered significant attention in recent years. This transition is largely driven by the need for more secure, user-friendly, and convenient systems, particularly in high-stakes environments like healthcare, banking, and other sectors requiring robust security.

A key area of focus is the integration of biometric authentication systems, which have been studied extensively for their potential to improve security and enhance user experience. Oogami et al. (2020) conducted a study on the adoption of passkeys and FIDO2 security keys, examining user perceptions and challenges associated with these password-less methods. Their findings indicate that while there is clear enthusiasm for adopting passkeys, barriers to adoption, such as usability concerns, still persist. However, the study was limited by its small sample size, which could affect the generalizability of the results.

Similarly, George (2024) evaluated passkey technology, specifically the implementation of WebAuthn standards, as a more secure and user-friendly alternative to traditional password systems. Their research revealed that passkeys could significantly reduce vulnerabilities like phishing attacks, while also improving user privacy. Despite these advantages, George pointed out the ongoing challenges related to user acceptance and device mobility, which are crucial considerations for the widespread adoption of passkeys.

Biometric authentication systems, particularly those implemented on mobile devices, have been the subject of various studies. Silasai and Khowfa (2020) explored the evolution of biometric systems for mobile devices, highlighting the advancements in fingerprint and facial recognition technologies. They emphasized that while these systems offer promising security benefits, their practical implementation, especially on the web, remains an area requiring further research. The study called attention to the need for robust biometric solutions that integrate seamlessly with web applications, which aligns with the goals of this project.

Matiushin and Korkhov (2021) examined "magic link" authentication, which is another form of password-less method, using Keycloak as the implementation framework. Their findings suggested that magic link technology offers improved security against password-based attacks while providing a user-friendly experience. However, the reliance on email systems for authentication introduces vulnerabilities, such as phishing risks, which need to be addressed for the method to be considered secure in all contexts.

The adoption of FIDO2 passkeys has also been scrutinized in industry-specific studies. Lassak et al. (2024) identified several barriers that companies face when deploying passkeys, despite their security advantages. These barriers include issues related to account recovery, user friction, and regulatory compliance. The study suggests that overcoming these challenges requires careful planning and strategic implementation, particularly in enterprise settings, to ensure the system's scalability and effectiveness.

Furthermore, Parmar et al. (2022) conducted experiments and surveys to assess the security, user acceptance, and effectiveness of passwordless authentication systems. Their study demonstrated that passwordless methods could enhance both security and user convenience, although it was limited by a narrow focus on certain technologies and environments. This highlights the need for broader research that encompasses diverse user experiences and varying security contexts, which is critical for understanding the full potential of passwordless systems.

Finally, Wang and Sun (2020) provided a comprehensive review of web authentication methods, covering both traditional and modern techniques, including biometrics, digital certificates, and session tokens. Their study emphasized the growing importance of robust authentication strategies in safeguarding web applications against unauthorized access. However, they noted that the rapidly evolving nature of web security technologies requires constant adaptation of authentication strategies to maintain their effectiveness.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 267-275 www.ijaem.net ISSN: 2395-5252

III. METHODOLOGY

3.1 Introduction

This chapter outlines the research methods employed to assess the efficacy of biometrics-based authentication systems, with a specific focus on their implementation in a web-based health tracker application. The study employs a mixed-method approach that combines both quantitative and qualitative data collection techniques to provide a holistic evaluation of the system's performance and user satisfaction. This approach is crucial for understanding the usability and security implications of biometric authentication, enabling a balanced view of both technical efficiency and user experience. The System Usability Scale (SUS) is used to gauge user satisfaction, while key usability metrics such as Task Completion Rate (TCR), Average Authentication Time (AAT), and Error Rate (ER) are employed to assess the system's functionality and user interaction.

3.2 Participant Recruitment

Participants were recruited through a targeted outreach strategy, including WhatsApp broadcasts and personal invitations via professional and social groups. Eligibility criteria required participants to:

- Own a biometric-capable device (e.g., smartphones or laptops with fingerprint or facial recognition).
- Be familiar with web applications and basic authentication methods (passwords, OTPs).
- Agree to provide feedback on their experience.

A total of **21 participants** were recruited, representing a mix of demographics, including students, professionals, and tech-savvy users. The diversity of the participant pool aimed to ensure varied perspectives on the usability and acceptance of biometric authentication.

Figure 3.1: Recruitment Advert for Participant Enrollment

3.3 Research Design

The design of the study aims to capture comprehensive insights into the performance of biometric authentication in the health tracker web app. The research incorporates both quantitative measures of system performance and qualitative assessments of user experiences to achieve a well-rounded evaluation.

3.3.1 Quantitative Approach

The quantitative approach centers on evaluating specific usability metrics that offer

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 267-275 www.ijaem.net ISSN: 2395-5252

concrete insights into the system's functionality. Key performance indicators (KPIs) include:

- **Task Completion Rate (TCR):** This metric calculates the percentage of successful biometric authentications, reflecting the system's efficiency and reliability. A higher TCR signifies fewer errors and a smoother user experience.

$$\text{TCR} = \left(\frac{\text{Number of successful authentications}}{\text{Total Number of authentications}}\right) \text{x } 100$$

- **Average Authentication Time (AAT):** AAT measures the time users require to complete the authentication process, providing an indication of how efficient and fast the biometric authentication system is.

$$\text{AAT} = \frac{\sum(\text{Time Taken for Each Successful Authentication})}{\text{Number of Successful Authentications}}$$

- **User Satisfaction Score (USS):** This score is derived from participant feedback and evaluates the perceived ease of use, security, and satisfaction with the biometric authentication process.

$$\text{USS} = \frac{\sum(\text{User Satisfaction Ratings})}{\text{Number of Participants}}$$

- **Drop-off Rate (DR):** The Drop-off Rate measures the number of users who begin the authentication process but fail to complete it. A high drop-off rate can indicate user frustrations or issues with the authentication process.

$$\text{DR} = \left(\frac{\text{Number of Users Who Abandoned the Process}}{\text{Total Number of Users Who Started the Process}}\right) \text{x } 100$$

- **Passkey Readiness (PR):** This metric assesses the compatibility of users' devices with biometric authentication, providing valuable insights into the potential for widespread adoption based on device capabilities.

$$\text{PR} = \left(\frac{\text{NumberofDeviceswithBiometricCapabilities}}{\text{TotalNumberofDevicesAccessingtheWebsite}}\right) \text{x } 100$$

These metrics are quantitatively analyzed to determine the system's usability, performance, and overall acceptance among users.

3.3.2 Qualitative Approach

To supplement the quantitative data, the study includes qualitative feedback from participants gathered through surveys and interviews. This approach enables a deeper understanding of user experiences and attitudes toward biometric authentication. Participants provide insights into:

- Ease of use
- Perceived security
- Convenience
- Any challenges encountered during the authentication process
- Suggestions for improvement

These qualitative insights are analyzed thematically to identify common patterns and potential areas for improvement.

3.3.3 Justification for the Research Design

The mixed-methods research design was chosen to ensure a comprehensive evaluation of the biometric authentication system. While the quantitative data provides objective measurements of the system's performance, the qualitative data allows for a deeper exploration of user attitudes, perceptions, and behaviors. This combined approach is essential for understanding both the technical and human-centered aspects of biometric authentication.

3.4 System Architecture

The system architecture of the health tracker application is designed to facilitate secure

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 267-275 www.ijaem.net ISSN: 2395-5252

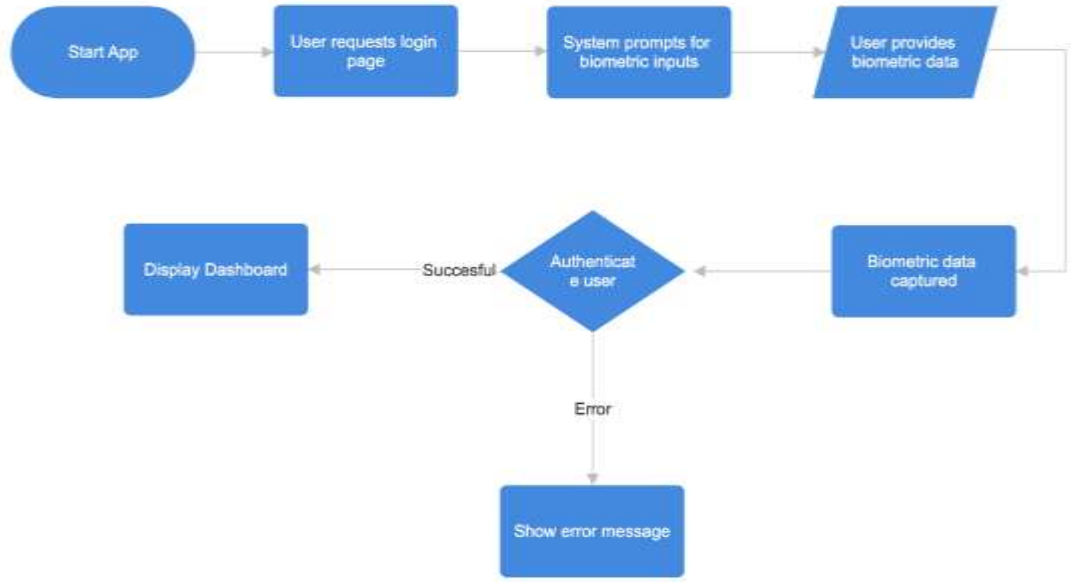
and efficient biometric authentication. The architecture incorporates various components, such as the client-side interface, backend server, authentication provider, and biometric devices, ensuring a seamless user experience.
Passage, a biometric authentication provider, is integrated into the system to handle biometric data securely, while Supabase is used for storing health tracking data.

3.4.1 Overview of the System Architecture

The key components of the system are as follows:

- **Client-Side Interface:** Built using NextJS, this component allows users to interact with the health tracker app and utilize biometric authentication for logging in..
- **Backend Server:** Developed in NextJS, the backend processes user requests, handles data storage, and communicates with the Passage authentication provider.
- **Authentication Provider (Passage):** Passage handles the secure authentication of users via biometric data. It encrypts and stores passkeys, and verifies them against biometric templates to provide token-based authentication.
- **Biometric Devices and Sensors:** Biometric sensors (e.g., fingerprint scanners) on users' devices are used to capture and process biometric data.
- **Encryption and Secure Communication:** All communication within the system is encrypted using TLS, ensuring data confidentiality and integrity. Biometric data is also encrypted both in transit and at rest.

Figure 3.1: Flowchart of the web application



3.4.2 Data Flow for Biometrics-Based Authentication

The data flow for biometric authentication in the health tracker app follows these sequential steps:

1. **User Initiates Login:** The user selects biometric authentication on the login page of the health tracker app.
2. **Biometric Data Capture:** The app prompts the user to scan their fingerprint or other biometric data using the device's sensors.
3. **Secure Storage of Passkey:** The biometric data is converted into a passkey, which is encrypted and stored securely on the user's device.
4. **Verification and Authentication:** The authentication provider (Passage) verifies the passkey by matching it with the stored biometric template.
5. **Token-Based Authentication:** If the authentication is successful, Passage generates an authentication token, which is sent to the client-side interface.
6. **Access Granted:** The backend server validates the authentication token and grants the user access to the health tracker application.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 267-275 www.ijaem.net ISSN: 2395-5252

This data flow ensures that the biometric authentication process is secure, efficient, and user-friendly.

IV. RESULTS

The study evaluated the effectiveness and usability of biometric authentication in a web-based health tracker application. Data was collected from 129 authentication events across 21 participants, with a focus on task completion rates, authentication times, and user satisfaction.
This section presents the findings, structured around quantitative metrics and qualitative feedback.

Quantitative Results

1. Task Completion Rate (TCR):

The overall Task Completion Rate was **73.64%**, indicating that most participants successfully completed the authentication tasks. Login events achieved a higher completion rate of **78.26%**, while registration events had a lower rate of **62.16%**. Biometric authentication outperformed OTP, with a completion rate of **80.72%** compared to OTP's **60.87%**.

2. Average Authentication Time (AAT):

Biometric authentication demonstrated significantly faster performance, with an average time of **9.60 seconds**. OTP authentication, by comparison, averaged **42.30 seconds**, reflecting the additional steps required for OTP-based login.

3. Error Rate and Drop-Off Rate:

Biometric authentication exhibited a lower drop-off rate of **19.28%**, whereas OTP authentication had a higher rate of **39.13%**, attributed to technical issues and user frustrations.

4. System Usability Scale (SUS) Scores:

The biometric system achieved an average SUS score of **85 out of 100**, indicating "excellent" usability. Most participants found the system intuitive and efficient, although a minority reported challenges with device compatibility and sensor responsiveness.

Qualitative Results

1. **Positive User Experiences**
   - Many participants praised the system's **convenience** and **speed**, noting that it eliminated the need to remember complex passwords.
   - Participants with prior experience using biometric systems reported smoother interactions and faster task completions.
2. **Challenges and Feedback**
   - A few users experienced issues with biometric sensor responsiveness, particularly under poor conditions (e.g., wet fingers).
   - Some participants relying on OTP due to device limitations expressed frustration with the additional steps and longer authentication times.
   - Repeated login attempts highlighted minor system inconsistencies in processing passkey-based authentications.
3. **Comparison with Traditional Methods** Participants overwhelmingly favored biometric authentication over passwords and PINs. The majority cited improved usability, reduced cognitive load, and enhanced security as key benefits.

Observations from Device Usage

- **Device Compatibility:**

Out of 21 participants, **78%** used Android devices, and **22%** used iPhones. Android devices exhibited higher biometric sensor reliability, while iPhone users noted some restrictions due to system integrations.

- **Biometric Readiness:**

Approximately **61%** of participants had prior experience with biometric systems, which positively influenced their interactions and overall satisfaction.

V. CONCLUSIONS AND DISCUSSIONS

This research explored the implementation and evaluation of biometric authentication in a web-based health tracker application, addressing the limitations of traditional password-based systems. By leveraging biometric passkeys integrated through Passage, the study aimed to enhance user convenience, security, and overall usability.

Key Findings

The results demonstrate that biometric authentication offers several advantages over traditional methods:

1. **Improved Usability:** Biometric authentication achieved a high System Usability Scale (SUS) score of 85, reflecting its intuitiveness and user satisfaction. Task Completion Rates were higher for biometric methods than for OTP authentication, emphasizing the effectiveness and reliability of the system.
2. **Enhanced Efficiency:** Biometric authentication significantly reduced Average Authentication Times, completing tasks

approximately 77% faster than OTP-based methods.

3. **Lower Drop-Off Rates:** Participants were less likely to abandon the biometric login process, indicating a smoother user experience and reduced friction compared to traditional methods.
4. **User Acceptance:** Qualitative feedback highlighted users' preference for biometrics due to its convenience, perceived security, and ease of use. However, minor concerns such as device compatibility and sensor responsiveness were noted.

Contributions to Knowledge

This study contributes to the growing body of research on passwordless authentication by highlighting the practical benefits and challenges of implementing biometric systems in web applications. It bridges the gap between theoretical discussions of biometrics and their real-world application, particularly in health-related platforms where security and user experience are critical.

Limitations

While the findings are promising, the study has several limitations:

1. **Sample Size:** The study was conducted with a relatively small sample of participants, which may limit the generalizability of the results.
2. **Device Dependence:** Variations in device capabilities impacted user experiences, particularly for those without access to reliable biometric sensors.
3. **Context-Specific Insights:** The findings are specific to the health tracker application and may not fully translate to other types of web applications.

Recommendations for Future Work

1. Expanding the sample size and demographic diversity to gain broader insights into user acceptance and performance across different populations.
2. Exploring additional biometric modalities (e.g., facial recognition, voice authentication) to improve compatibility and inclusivity.
3. Investigating the long-term scalability and security implications of biometric authentication systems in diverse web application contexts.

Conclusion

Biometric authentication holds significant potential as a secure and user-friendly alternative to traditional password-based systems. The findings from this research underscore its effectiveness in improving login efficiency, reducing user frustrations, and enhancing overall satisfaction. By addressing the identified challenges and scaling the solution, developers can leverage biometrics to create more robust and accessible web authentication systems for the future.

REFERENCES

[1]. A review of multi-factor authentication in the Internet of Healthcare Things. (n.d.). https://doi.org/10.1177/20552076231177144

[2]. Authentication—OWASP Cheat Sheet Series. (n.d.). Retrieved September 17, 2024, from https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[3]. Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C. Neal, C. (n.d.). 2011 Data Breach Investigations Report.

[4]. Biel, B., Grill, T., & Gruhn, V., (2010). Exploring the benefits of the combination of a software architecture analysis and a usability evaluation of a mobile application. Journal of Systems and Software, 83(11), 2031–2044. https://doi.org/10.1016/j.jss.2010.03.079

[5]. Brooke, J., (1995). SUS: A quick and dirty usability scale. Usability Eval. Ind., 189.

[6]. Chowhan, R., & Tanwar, R., (2019). Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites. https://doi.org/10.4018/978-1-5225-8100-0.ch008

[7]. Committee, N. R. C. (US) W. B., Pato, J. N., & Millett, L. I., (2010). Introduction and Fundamental Concepts. In Biometric Recognition: Challenges and Opportunities. National Academies Press (US). Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK219892/

[8]. Derisma, D., (2020). The Usability Analysis Online Learning Site for Supporting Computer programming Course Using System Usability Scale (SUS) in a University. (pp. 182–195). International Association of Online Engineering. Retrieved from https://www.learntechlib.org/p/217827/

[9]. Desk, O., (2024, January 16). The Benefits Of Passwordless Authentication For User Experience And Security. Retrieved June 23, 2024, from OLOID website:

https://www.oloid.ai/blog/the-benefits-of-passwordless-authentication/

[10]. Fatima, K., Nawaz, S., & Mehrban, S., (2019). Biometric Authentication in Health Care Sector: A Survey. 2019 International Conference on Innovative Computing (ICIC), 1–10. https://doi.org/10.1109/ICIC48496.2019.8966699

[11]. FIDO (Fast Identity Online). (n.d.). Retrieved September 14, 2024, from https://www.pingidentity.com/en/resources/identity-fundamentals/authentication/passwordless-authentication/fido.html

[12]. Forecast number of mobile users worldwide 2020-2025. (n.d.). Retrieved June 19, 2024, from Statista website: https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

[13]. George, D. A. S. (2024). The Dawn of Passkeys: Evaluating a Passwordless Future. Partners Universal Innovative Research Publication, 2(1), 202–220. https://doi.org/10.5281/zenodo.10697886

[14]. Justinha., (2024, August 6). Microsoft Entra passwordless sign-in—Microsoft Entra ID. Retrieved September 17, 2024, from https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

[15]. Laborde, S., (2023, November 29). 90+ Key Password Breach Statistics in 2023. Retrieved September 19, 2024, from The Tech Report website: https://techreport.com/statistics/cybersecurity/password-breach-statistics/

[16]. Lassak, L., Pan, E., Ur, B., & Golla, M., (2024). Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In USENIX Security Symposium. USENIX. https://www.usenix.org/system/files/sec24summer-prepub-618-lassak.pdf

[17]. Lewis, J., (2018). The System Usability Scale: Past, Present, and Future. International Journal of Human-Computer Interaction, 1–14. https://doi.org/10.1080/10447318.2018.1455307

[18]. Matiushin, I., & Korkhov, V., (2021). Passwordless Authentication Using Magic Link Technology. 9th International Conference "Distributed Computing and Grid Technologies in Science and Education," 434–438. Crossref. https://doi.org/10.54546/MLIT.2021.89.13.001

[19]. Olanrewaju, R. F., Khan, B. U. I., Morshidi, M. A., Anwar, F., & Kiah, M. L. B. M. (2021). A Frictionless and Secure User Authentication in Web-Based Premium Applications. IEEE Access, 9, 129240–129255. https://doi.org/10.1109/ACCESS.2021.3110310

[20]. Oogami, W., Gomi H., Yamaguchi S., Yamanaka S., & Higurashi, T. (n.d.). Observation Study on Usability Challenges for Fingerprint Authentication Using WebAuthn-enabled Android Smartphones.

[21]. Onsiri, S., & Wachana, K., (2020). The Study on Using Biometric Authentication on Mobile Device. NU. International Journal of Science 2020; 17(1) : 90-110.

[22]. Passwordless login with passkeys | Authentication. (n.d.). Retrieved June 23, 2024, from Google for Developers website: https://developers.google.com/identity/passkeys

[23]. Rzemyk, T. J., (2017). Chapter 10—Biometrics in the Criminal Justice System and Society Today. In L. J. Fennelly (Ed.), Effective Physical Security (Fifth Edition) (pp. 249–254). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-804462-9.00010-5

[24]. Sandhu, R., (2019). Password Less Authentication. Indian Journal of Science and Technology, 12(43), 1–6. https://doi.org/10.17485/ijst/2019/v12i43/145555

[25]. Selamat, S.R., (2020, July 27). Enhanced Authentication for Web-Based Security Using Keystroke Dynamics. [SSRN Scholarly Paper]. Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=3926925

[26]. Taylor, D., (n.d.). What's the Password? Account Sharing in the Context of Passwordless Authentication.

[27]. Usability. (2024, March 13). Retrieved September 7, 2024, from Digital.gov website: https://digital.gov/topics/usability/

[28]. View of The Dawn of Passkeys: Evaluating a Passwordless Future. (n.d.). Retrieved September 7, 2024, from https://puirp.com/index.php/research/article/view/44/38

[29]. Viral P., Harshal S., Riki P., & Abhijit P., (n.d.). A Comprehensive Study on Passwordless Authentication. Retrieved June

19, 2024, from https://www.researchgate.net/publication/360229809_A_Comprehensive_Study_on_Passwordless_Authentication

[30]. Wang C., Wang Y., Chen Y., Liu H., & Liu J., (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, 107118. https://doi.org/10.1016/j.comnet.2020.107118

[31]. Wang Z., & Sun W., (2020). Review of Web Authentication. Journal of Physics: Conference Series, 1646(1), 012009. https://doi.org/10.1088/1742-6596/1646/1/012009

[32]. Yi P.X., Kasmin I.F., Amin S., & Zainal N.K., (2022). Implementation of One-Time Password in Online Banking System Among Malaysian Bank Users to Reduce Cyber Fraud. International Journal of Data Science and Advanced Analytics, 4, 20–26. https://doi.org/10.69511/ijdsaa.v4i0.138