International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 250-254 www.ijaem.net ISSN: 2395-5252

Keyless Kingdom: A Journey into the Realm of Password less Authentication.

Anis Fatini binti Mohd Zawayi[1*], Mohd Fadli bin Zolkipli[2]
[12]*School of Computing, Univeristi Utara Malaysia, Kedah.*

Date of Submission: 05-07-2024 Date of Acceptance: 15-07-2024

ABSTRACT: The traditional method of authentication using passwords has been widely adopted across various applications and services. However, it is plagued with several drawbacks such as vulnerability to security breaches, user forgetfulness, and user inconvenience. To address these limitations, the concept of passwordless authentication has emerged as a promising alternative. This research paper aims to explore the topic of passwordless authentication, comparing it with traditional authentication methods and examining the challenges faced in its adoption.

KEYWORDS: Passwordless, Authentication.

I. INTRODUCTION

The digital landscape has witnessed a significant shift in the way users interact with online systems, with the increasing adoption of passwordless authentication methods. The persistence of password- based cyber-attacks and the damage they cause are driving forces behind the growing demand for hardened ways to verify the identity information of customers and employeesinteracting with systems. Current password-based approaches are too vulnerable, and the need for more secure methods has become pressing.

This paper, titled "Keyless Kingdom: A Journey into the Realm of Passwordless Authentication," explores the factors facilitating the journey to passwordless login and the role of digital identity proofing in this transition.

The study draws upon research by the World Economic Forum, which highlights the importance of authentication in digital transformation efforts and the need for adaptive, secure, and privacy-minded building blocks to foster user trust and drive better adoption of services [2].

By examining the evolution of authentication practices and the benefits of passwordless technologies, this paper aims to provide a comprehensive overview of the keyless kingdom and its implications for the future of digital identity proofing.

II. LITERATURE REVIEW

The literature review for "Keyless Kingdom: A Journey into the Realm of Passwordless Authentication" should delve into the significance of passwordless authentication in the contemporary digital environment. Traditional authentication methods centered around passwords have inherent limitations and are prone to security vulnerabilities, underscoring the necessity to explore passwordless authentication solutions in today's digital landscape [10].

Passwordless authentication represents a paradigm shift in digital security, offering a more robust and user-friendly approach to verifying identities without the reliance on manually entered passwords. This transition is crucial as passwords have long been the cornerstone of authentication in digital systems but are plagued by issues such as weak or stolen passwords, leading to a high prevalence of data breaches [3].

By eliminating the need for passwords, passwordless authentication not only enhances security but also streamlines user experience, reduces costs associated with password management, and mitigates the risks of data breaches. The adoption of passwordless technology presents a strategic opportunity for organizations to enhance productivity, improve customer satisfaction, and bolster cybersecurity defenses in an increasingly interconnected digital landscape.

Furthermore, the growing adoption of passwordless authentication methods across various sectors, including financial services and healthcare, underscores the transformative potential of this innovative approach to authentication. As organizations grapple with the challenges posed by traditional password-based systems, the shifttowardspasswordless authentication emerges as a pivotal step towards fortifying digital trust, enhancing cybersecurity, and ushering in a new era of secure and seamless authentication mechanisms

III. DISCUSSION

1. Traditional versus passwordless authentication method

The debate between traditional password-based authentication and passwordless authentication methods has been ongoing, with each approach having its own set of advantages and disadvantages. Traditional password-based authentication methods, such as those used in the era of ubiquitous access to myriad applications and services, have been criticized for their vulnerabilities to theft and phishing, as well as their lack of user-friendliness [22][12].

In contrast, passwordless authentication methods aim to provide enhanced security and a moreseamless user experience. For instance, a survey conducted by IDG found that nearly nine in ten respondents believed passwordless authentication is "critical" or "very important" for a zero-trust strategy, citing benefits such as reduced security risk, improved user experience, and reduced burden on IT resources [12].

One of the primary concerns with traditional password-based authentication is the risk of brute- force attacks and the lack of robust security measures. In 2020, Verizon reported that 81% of data breaches involved weak or stolen passwords, highlighting the need for more secure authentication methods [22].

Passwordless authentication methods, such as those based on biometrics or zero-knowledge proofs, can offer an even greater level of convenience and speed for users while significantly reducing the risk of security breaches [13].

However, the adoption of passwordless authentication methods is not without its challenges. Integration issues due to technological complexity, data privacy concerns, and cost concerns are some of the major hurdles that need to be addressed [12]. Despite these challenges, the trend toward, passwordless authentication is gaining momentum, with many organizations recognizing the need for more robust and user-friendly authentication methods.

In conclusion, the choice between traditional password-based authentication and passwordless authentication methods depends on the specific needs and requirements of an organization. While traditional methods have been the norm for a long time, the benefits of passwordlessauthentication, including enhanced security and improved user experience, make it an attractive alternative for many organizations.

2. Adoption of passwordless authentication

The adoption of passwordless authentication is gaining significant traction in the cybersecurity landscape. This shift is driven by the need for enhanced security, improved user experience, and reduced operational costs. In 2020, a survey conducted by IDG found that nearly nine in ten respondents believed passwordless authentication is "critical" or "very important" for a zero-trust strategy, citing benefits such as reduced security risk, improved user experience, and reduced burden on IT resources.

One of the primary advantages of passwordless authentication is its ability to simplify the login process, thereby increasing productivity. A study by Forrester Research highlighted that the adoption of passwordless authentication can save nearly 15 hours of user productivity per year, translating to significant costsavings for organizations with large user bases. Additionally, passwordless authentication can reduce the time and resources spent on password recovery and remediation efforts, further enhancing its overall value proposition.

Another significant benefit of passwordless authentication is its ability to provide robust security. By leveraging advanced technologies such as biometric verification and public/private key cryptography, passwordless authentication methods can effectively eliminate the potential for credential theft and phishing attacks. This is particularly important in today's digital landscape where weak passwords remain a primary vulnerability exploited by cyber attackers.

The market for password less authentication is also growing rapidly. A recent study found that 92% of organizations have a strategy to transition to passwordless technology, with 95% already implementing a password- free experience. This trend is driven by the need for stronger authentication measures in e- commerce and the increasing regulatory requirements for digital security.

However, the adoption of passwordless authentication is not without its challenges. Integration issues due to technological complexity, data privacy concerns, and cost concerns are some of the major hurdles that need to be addressed. Nevertheless, the benefits of passwordless authentication make it an attractive alternative for many organizations seeking to enhance their cybersecurity posture.

In conclusion, the adoption of passwordless authentication is a critical step towards achieving robust security and improving user experience. As the cybersecurity landscape continues to evolve, the needforpasswordless authentication will only grow more pressing.

3. Overcoming the challenges of adoption

The adoption of passwordless authentication is gaining significant traction in the cybersecurity landscape. This shift is driven by the need for enhanced security, improved user experience, and reduced operational costs. In 2020, a survey conducted by IDG found that nearly nine in ten respondents believedpasswordlessauthentication is "critical" or "very important" for a zero-trust strategy, citing benefits such as reduced security risk, improved user experience, and reduced burden on IT resources.

3.1. Enhancing Productivity through Passwordless Authentication

One of the primary advantages of passwordless authentication is its ability to simplify the login process, thereby increasing productivity. A study by Forrester Research highlighted that the adoption of passwordless authentication can save nearly 15 hours of user productivity per year by refining the login process. When extrapolated to an organization with 1,000 users, the productivity improvements could translate to savings between $500,000 to $1,000,000 annually.

3.2. Overcoming Challenges

Despite the benefits, there are several challenges to overcome in the adoption of passwordless authentication. Integration issues due to technological complexity are a major concern, with 41% of respondents citing this as a significant obstacle. Additionally, data privacy concerns, particularly related to the use of biometrics, are a significant hurdle, with nearly half of respondents in the APAC region expressing concern. Other challenges include managing employee expectations, accommodating legacy applications, and managing the overall cost of implementation.

3.3. Market Potential

The adoption of passwordless authentication is gaining momentum, with many corporations recognizing its cybersecurity-boosting potential. Tech giants like Google and Apple are ditching passwords from their products. Moreover, a recent study showed that 92% of organizations have a strategy to transition to passwordless technology, with 95% already implementing a password- free experience. The continuous rise of e-commerce—coupled with national and international digital regulatory directives—compels large enterprises to implement strong authentication measures for customer verification.

IV. CONCLUSION

The journey into the realm of passwordless authentication, as explored in this paper titled "Keyless Kingdom: A Journey into the Realm of Passwordless Authentication," unveils a landscape ripe with transformative potential. Traditional methods reliant on passwords have long grappled with vulnerabilities, leading to security breaches, user inconvenience, and escalating costs. However, the emergence of passwordless authentication heralds a paradigm shift, offering a robust and user- friendly alternative.

Through an extensive examination of literature and discussions, this paper underscores the critical importance of transitioning towards passwordless authentication methods in contemporary digital environments. Passwordless authentication not only enhances security but also streamlines user experience, reduces operational costs, and mitigates the risks associated with data breaches.

The debate between traditional password-based authentication and passwordless methods highlights the clearcadvantages of the latter, including heightened security, improved user experience, and reduced burden on IT resources. While challenges such as technological integration complexities and data privacy concerns persist, the momentum towards passwordless authentication is undeniable.

The market potential for passwordless authentication is vast, with organizations recognizing its strategic significance in bolstering cybersecurity defenses and meeting regulatory requirements. Tech giants' endorsement and the widespread adoption across various sectors underscore the inevitability of this transition.

In conclusion, the adoption of passwordless authentication represents a critical step towards fortifying digital trust, enhancing cybersecurity resilience, and ushering in a new era of secure and seamless authentication mechanisms. The journey into the keyless kingdom promises not only enhanced security butalsoa more efficient and user-centric digital landscape.

V. ACKNOWLEDGMENT

The authors would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the System and Network Security Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. Alqubaisi, F., Wazan, A.S., Ahmad, L., & Chadwick, D.W. (2020). Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication? 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC), 1-6.

[2]. Andriotis, P., Kirby, M. & Takasu, A. Bu-Dash: a universal and dynamic graphical password scheme (extended version). Int. J. Inf. Secur. 22, 381–401 (2023). https://doi.org/10.1007/s10207-022-00642-2

[3]. Bicakci, K., &Uzunay, Y. (2022). Is FIDO2 Passwordless Authentication a Hype or for Real?: A Position Paper. 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY), 68-73.

[4]. Burgess, M. (2022, September 7). Apple kills passwords in IOS 16 and MacOS Ventura. WIRED. https://www.wired.com/story/apple-passkeys-password-iphone-mac-ios16-ventura/

[5]. Campbell M. Putting the Passe Into Passwords: How Passwordless Technologies Are Reshaping Digital Identity. Computer. 2020;53(8):89–93.doi: 10.1109/MC.2020.2997278

[6]. Chetty, G., Tran, D., Sharma, D., & Balachandran, B. (2007). Password Less Security System Using MultiFactor Biometric Fusion. In B. J. Wysocki, & T. A. Wysocki (Eds.), International Conference on Signal Processing and Telecommunication Systems, ICSPCS 2007 (pp. 1-9). DSP for Communication Systems. http://www.dspcs-witsp.com/icspcs_2007/Proceedings_ICSPCS2007.pdf

[7]. Conners, J., Devenport, C., Derbidge, S., Farnsworth, N.C., Gates, K., Lambert, S., McClain, C., Nichols, P., & Zappala, D. (2022). Let's Authenticate: Automated Certificates for User Authentication. Proceedings 2022 Network and Distributed System Security Symposium.

[8]. Felipe, H. L. A. (2020). FIDO2 web passwordless authentication for SSO systems. RepositorioInstitucional Séneca. https://repositorio.uniandes.edu.co/entities/publication/1fc6d028-3bd3-436f-9c26-423bd6798d04

[9]. Huang, Y., Fu, B., Peng, N., Ba, Y., Liu, X., & Zhang, S. (2022). RFID Authentication System Based on User Biometric Information. Applied Sciences, 12(24). doi:10.3390/app122412865

[10]. Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Al-Banna, A.-K. (2024). Online Banking User Authentication Methods: A Systematic Literature Review. IEEE Access, 12, 741–757. doi:10.1109/ACCESS.2023.3346045

[11]. Lassak, L., Pan, E., Ur, B., & Golla, M. (2024). Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. Extended Version.

[12]. Luckett, J. (2023). Phishing Resistant Systems: A Literature Review. Journal of Computing Sciences in Colleges, 39(3), 347-347.

[13]. Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., &Bugiel, S. (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. 2020 IEEE Symposium on Security and Privacy (SP), 268–285. Retrieved from https://api.semanticscholar.org/CorpusID:216389672

[14]. Mitra, A., Ghosh, A., & Sethuraman, S.C. (2023). TUSH-Key: Transferable User Secrets on Hardware Key. ArXiv, abs/2307.07484.

[15]. Mohammed, R. S., & Ahmed, A. A. (2022). Iris Recognition Technology: Principles, mechanism, and Market Forecasting (2022-2030). ResearchGate. https://www.researchgate.net/publication/358445862_Iris_Recognition_Technology_Principles_Mechanism_and_Market_Forecasting_2022-2030

[16]. Oduguwa, T., &Arabo, A. (2023, December 5). A review of password-less user authentication schemes. arXiv.org. https://arxiv.org/abs/2312.02845

[17]. Oduguwa, T.; Arabo, A. Passwordless Authentication Using a Combination of Cryptography, Steganography, and Biometrics. Preprints 2024, 2024011466. https://doi.org/10.20944/preprints202401.1466.v1

[18]. Owens, K., Anise, O., Krauss, A., & Ur, B. (2021, August). User Perceptions of the Usability and Security of Smartphones as

FIDO2 Roaming Authenticators. Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021), 57–76. Retrieved from https://www.usenix.org/conference/soups2021/presentation/owens

[19]. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019, August). A Usability Study of Five Two-Factor Authentication Methods. Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), 357–370. Retrieved from https://www.usenix.org/conference/soups2019/presentation/reese

[20]. Ryu, J., Son, S., Lee, J., Park, Y., & Park, Y. (2022). Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. IEEE Access, 10, 98944-98958.

[21]. Sethuraman, S. C., Mitra, A., Ghosh, A., Galada, G., & Subramanian, A. (2023, January 4). MetaSecure: a passwordless authentication for the metaverse. arXiv.org. https://arxiv.org/abs/2301.01770

[22]. Ukwandu, Elochukwu and Bennett, Alexis, Exploring the Views of End-Users on Passwordless Authentication Methods. Available at SSRN: https://ssrn.com/abstract=4616393 or http://dx.doi.org/10.2139/ssrn.4616393