VECTORAL PUBLISHING

Research Article: Quarterly Journal of Emerging Technologies and Innovations Volume: 08

Evaluating the Usability and User Acceptance of Biometric Authentication in Different Applications

Ahmed Mahdi Abdulkareem
Saurashtra University, PhD Research Scholar

Anna Gordon
Research Associate, botfed research society

Abstract

This study investigates the usability and user acceptance of biometric authentication across different applications, including mobile devices and smartphones, access control systems, banking and financial applications, healthcare systems, and travel and border control. The research aims to identify the factors that influence user acceptance and the potential challenges faced in each domain. The findings reveal that biometric authentication in mobile devices and smartphones is widely accepted due to its convenience and speed. However, concerns related to false acceptance or rejection rates, sensor accuracy, and privacy issues can affect user acceptance. Similarly, in access control systems, fast and reliable biometric systems with seamless user experiences are more likely to be accepted. Challenges such as long verification times, high false rejection rates, and complex enrollment processes can impact user acceptance negatively. In banking and financial applications, user acceptance depends on the perceived security and privacy of biometric data. Trust in the system, a user-friendly interface, and clear instructions are crucial factors influencing user acceptance. Healthcare systems face unique challenges, including hygiene concerns, ease of use for elderly or disabled patients, and adherence to privacy and security regulations. User acceptance in healthcare settings is influenced by these factors, along with overall system reliability. In travel and border control, biometric authentication, particularly facial recognition, is gaining popularity for identity verification and immigration processes. User acceptance is influenced by factors such as accuracy, speed, and perceived effectiveness in enhancing security and reducing queues. Privacy concerns and data protection policies also play a role in shaping user acceptance.

Keywords: *Biometric authentication, Usability, User acceptance, Security, Privacy*

Full article:

https://vectoral.org/index.php/QJETI/article/view/5

https://vectoral.org/index.php/QJETI/article/view/5/5

References

[1] D. Bhattacharyya and R. Ranjan, "Biometric authentication: A review," *Journal of u-and e …*, 2009.

[2] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Online risk-based authentication using behavioral biometrics," *Multimed. Tools Appl.*, vol. 71, no. 2, pp. 575–605, Jul. 2014.

[3] K. Daimi, G. Francia III, and L. H. Encinas, *Breakthroughs in digital biometrics and forensics*. Cham, Switzerland: Springer Nature, 2022.

[4] A. M. M. Chowdhury and M. H. Imtiaz, "Contactless fingerprint recognition using deep learning—A systematic review," *J. Cybersecur. Priv.*, vol. 2, no. 3, pp. 714–730, Sep. 2022.

[5] P. Uyyala, "SECURE CRYPTO-BIOMETRIC SYSTEM FOR CLOUD COMPUTING," *Journal of interdisciplinary cycle research*, vol. 14, no. 6, pp. 2344–2352, 2022.

[6] A. N. Kataria, D. M. Adhyaru, A. K. Sharma, and T. H. Zaveri, "A survey of automated biometric authentication techniques," in *2013 Nirma University International Conference on Engineering (NUiCONE)*, 2013, pp. 1–6.

[7] Q. Xiao, "Security issues in biometric authentication," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, pp. 8–13.

[8] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[9] P. Uyyala, "COLLUSION DEFENDER PRESERVING SUBSCRIBERS PRIVACY IN PUBLISH AND SUBSCRIBE SYSTEMS," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 4, pp. 2639–2645, 2021.

[10] S. S. Ali, V. S. Baghel, I. I. Ganapathi, and S. Prakash, "Robust biometric authentication system with a secure user template," *Image Vis. Comput.*, vol. 104, p. 104004, Dec. 2020.

[11] P. Uyyala and D. D. C. Yadav, "The advanced proprietary AI/ML solution as Anti-fraudTensorlink4cheque (AFTL4C) for Cheque fraud detection," *The International journal of analytical and experimental modal analysis*, vol. 15, no. 4, pp. 1914–1921, 2023.

[12] P. Uyyala, "Privacy-aware Personal Data Storage (P-PDS): Learning how toProtect User Privacy from External Applications," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 6, pp. 3257–3273, 2021.

[13] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proceedings of the 7th workshop on Multimedia and security*, New York, NY, USA, 2005, pp. 111–116.

[14] P. Uyyala, "MULTILEVEL AUTHENTICATION SYSTEM USING HIERARCHICAL INTRUSION DETECTION ARCHITECTURE FOR ONLINE BANKING," *The International journal of analytical and experimental modal analysis*, vol. 15, no. 5, pp. 644–650, 2023.

[15] R. R. Dixit, "Investigating Healthcare Centers' Willingness to Adopt Electronic Health Records: A Machine Learning Perspective," *ERST*, vol. 1, no. 1, pp. 1–15, Jan. 2017.

[16] P. Ambalakat, "Security of biometric authentication systems," *21st Computer Science Seminar*, 2005.

[17] A. K. Singh, A. Anand, Z. Lv, H. Ko, and A. Mohan, “A Survey on Healthcare Data: A Security Perspective,” *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 17, no. 2s, pp. 1–26, May 2021.
[18] P. Uyyala, “Delegated Authorization Framework for EHR Services using Attribute Based Encryption,” *The International journal of analytical and experimental modal analysis*, vol. 13, no. 3, pp. 2447–2451, 2021.
[19] P. Dhake, R. Dixit, and D. Manson, “Calculating a Severity Score of an Adverse Drug Event Using Machine Learning on the FAERS Database,” *IIMA/ICITED UWS*, 2017.
[20] M. A. Veronin, R. P. Schumaker, R. R. Dixit, and H. Elath, “Opioids and frequency counts in the US Food and Drug Administration Adverse Event Reporting System (FAERS) database: a quantitative view of the epidemic,” *Drug Healthc. Patient Saf.*, vol. 11, pp. 65–70, Aug. 2019.
[21] M. A. Veronin, R. Dixit, and R. P. Schumaker, “A Decision Tree Analysis of Opioid and Prescription Drug Interactions Leading to Death Using the FAERS Database,” in *IIMA/ICITED Joint Conference 2018*, 2018, pp. 67–67.
[22] S. S. Thenuwara, C. Premachandra, and H. Kawanaka, “A multi-agent based enhancement for multimodal biometric system at border control,” *Array*, vol. 14, p. 100171, Jul. 2022.
[23] J. J. Robertson, R. M. Guest, S. J. Elliott, and K. O’Connor, “A Framework for Biometric and Interaction Performance Assessment of Automated Border Control Processes,” *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 6, pp. 983–993, Dec. 2017.
[24] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, “Biometric Recognition in Automated Border Control: A Survey,” *ACM Comput. Surv.*, vol. 49, no. 2, pp. 1–39, Jun. 2016.
[25] V. Matyáš and Z. Říha, “Biometric authentication — security and usability,” in *Advanced Communications and Multimedia Security*, Boston, MA: Springer US, 2002, pp. 227–239.
[26] A. Kumar and D. Zhang, “Improving Biometric Authentication Performance From the User Quality,” *IEEE Trans. Instrum. Meas.*, vol. 59, no. 3, pp. 730–735, Mar. 2010.
[27] P. Uyyala, “Secure Channel Free Certificate-Based Searchable Encryption Withstanding Outside and Inside Keyword Guessing Attacks,” *The International journal of analytical and experimental modal analysis*, vol. 13, no. 2, pp. 2467–2474, 2021.
[28] P. Uyyala, “Efficient and Deployable Click Fraud Detection for Mobile Applications,” *The International journal of analytical and experimental modal analysis*, vol. 13, no. 1, pp. 2360–2372, 2021.
[29] P. Møhl, “Biometric Technologies, Data and the Sensory Work of Border Control,” *Ethnos*, vol. 87, no. 2, pp. 241–256, Mar. 2022.
[30] A. K. Jain and A. Kumar, “Biometric Recognition: An Overview,” in *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras, Eds. Dordrecht: Springer Netherlands, 2012, pp. 49–79.