REFERENCES

[1]R. M. Pramila, M. Misbahuddin, and S. Shukla, "Adaptive authentication is a reliable technique to dynamically select the best mechanisms among multiple modalities to authenticate a user based on the user's risk profile generated using behavior and context-based information," Lecture Notes in Networks and Systems, vol. 462, 2022. https://link.springer.com/chapter/10.1007/978-981-19-2211-4_28

[2]"Continuous Adaptive Authentication: The Future of 2024," LoginRadius, 2024. https://www.loginradius.com/blog/growth/continuous-adaptiveauthentication-future-2024/

[3]D. Preuveneers and W. Joosen, "SmartAuth: dynamic context fingerprinting for continuous user authentication," in Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2015, pp. 2185-2191. https://doi.org/ 10.1145/2695664.2695908

[4]M. Misbahuddin and B. Bindumadhava, "Design of a risk-based authentication system using machine learning techniques," in IEEE SmartWorld, 2017, pp. 149-200. https://doi.org/10.1109/UIC-ATC.2017.8397628

[5]H. Zhang, D. Singh, and X. Li, "Augmenting authentication with context-specific behavioral biometrics," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2019, pp. 7282-7291. https://doi.org/10.24251/hicss.2019.875

[6]P. Arias-Cabarcos, C. Krupitzer, & C. Becker, "A survey on adaptive authentication", Acm Computing Surveys, vol. 52, no. 4, p. 1-30, 2019. https://doi.org/10.1145/3336117

[7]Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). A comprehensive survey of context-aware continuous implicit authentication in online learning environments. Ieee Access, 11, 24561-24573. https://doi.org/10.1109/access.2023.3253484

[8]S. Wiefling, T. Patil, M. Dürmuth, & L. Iacono, "Evaluation of risk-based re-authentication methods",, p. 280-294, 2020. https://doi.org/10.1007/978-3-030-58201-2_19

[9]S. Wiefling, M. Dürmuth, & L. Iacono, "More than just good passwords? a study on usability and security perceptions of risk-based authentication",, 2020. https://doi.org/10.1145/3427228.3427243

[10]R. Agrawal, "A study of touch dynamics biometrics authentication", Interantional Journal of Scientific Research in Engineering and Management, vol. 06, no. 05, 2022. https://doi.org/10.55041/ijsrem15812

[11]A. Buriro, B. Crispo, & M. Conti, "Answerauth: a bimodal behavioral biometric-based user authentication scheme for smartphones", Journal of Information Security and Applications, vol. 44, p. 89-103, 2019. https://doi.org/10.1016/j.jisa.2018.11.008

[12]R. Wang and D. Tao, "Context-aware implicit authentication of smartphone users based on multi-sensor behavior", Ieee Access, vol. 7, p. 119654-119667, 2019. https://doi.org/10.1109/access.2019.2936034

[13]A. Awwad, "An adaptive context-aware authentication system on smartphones using machine learning", International Journal of Safety and Security Engineering, vol. 13, no. 5, p. 903-915, 2023. https://doi.org/10.18280/ijsse.130514

[14]S. Fard, F. Gebali, & M. Mamun, "Using machine learning for dynamic authentication in telehealth: a tutorial", Sensors, vol. 22, no. 19, p. 7655, 2022. https://doi.org/10.3390/s22197655

[15]V. Zimmermann, P. Gerber, & A. Stöver, "That depends -- assessing user perceptions of authentication schemes across contexts of use",, 2022. https://doi.org/10.48550/arxiv.2209.13958

[16]S. Prange, L. Mecke, A. Nguyen, M. Khamis, & F. Alt, "Don't use fingerprint, it's raining!",, p. 1-5, 2020. https://doi.org/10.1145/3399715.3399823

[17]P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on adaptive authentication," ACM Comput. Surv., vol. 52, no. 4, pp. 1–30, 2019. https://dl.acm.org/doi/10.1145/3336117

[18]K. A. Abu Bakar and G. R. Haron, "Adaptive authentication: Issues and challenges," in World Congress on Computer and Information Technology (WCCIT), IEEE, 2013, pp. 1–6. https://dl.acm.org/doi/10.1145/3582696

[19]G. Bendiab, N. Kolokotronis, S. Shiaeles, & S. Boucherkha, "Wip: a novel blockchain-based trust model for cloud identity management",, p. 724-729, 2018. https://doi.org/10.1109/dasc/picom/datacom/cyberscitec.2018.00126

[20]E. Ghazizadeh and B. Cusack, "Evaluation theory for characteristics of cloud identity trust framework",, 2019. https://doi.org/10.5772/intechopen.76338

[21]S. Hamdani, A. Khan, N. Iltaf, J. Bangash, Y. Bangash, & A. Khan, "Dynamic distributed trust management scheme for the internet of things", Turkish Journal

of Electrical Engineering & Computer Sciences, vol. 29, no. 2, p. 796-815, 2021. https://doi.org/10.3906/elk-2003-5

[22]S. Yanushkevich, W. Howells, K. Crockett, J. O'Shea, H. Oliveira, R. Guestet al., "Cognitive identity management: risks, trust and decisions using heterogeneous sources",, p. 33-42, 2019. https://doi.org/10.1109/cogmi48466.2019.00014

[23]S. Shao, "Master-slave multi-chain with risk assessment based access control model for zero trust network",, 2024. https://doi.org/10.21203/rs.3.rs-3869167/v1

[24]G. Bendiab, S. Shiaeles, & S. Boucherkha, "A new dynamic trust model for "on cloud" federated identity management",, p. 1-5, 2018. https://doi.org/10.1109/ntms.2018.8328673

[25]V. Varadharajan and S. Nepal, "Context-aware trust management system for iot applications with multiple domains",, p. 1138-1148, 2019. https://doi.org/10.1109/icdcs.2019.00116

[26]K. Awan, I. Din, A. Almogren, M. Guizani, A. Altameem, & S. Ullah, "Robusttrust – a pro-privacy robust distributed trust management mechanism for internet of things", Ieee Access, vol. 7, p. 62095-62106, 2019. https://doi.org/10.1109/access.2019.2916340

[27]]R. Aluvalu, K. Chennam, M. Jabbar, & S. Ahamed, "Risk aware access control model for trust based collaborative organizations in cloud", International Journal of Engineering & Technology, vol. 7, no. 4.6, p. 49, 2018. https://doi.org/10.14419/ijet.v7i4.6.20235

[28]T. hamme, D. Preuveneers, & W. Joosen, "Managing distributed trust relationships for multi-modal authentication", Journal of Information Security and Applications, vol. 40, p. 258-270, 2018. https://doi.org/10.1016/j.jisa.2018.01.003

[29]Q. Faxin, X. Tong, L. Yu, & Y. Wang, "Personalized project recommendations: using reinforcement learning", Eurasip Journal on Wireless Communications and Networking, vol. 2019, no. 1, 2019. https://doi.org/10.1186/s13638-019-1619-6

[30]S. Erat, H. Kitapçı, & K. Akçin, "Managerial perception and organizational identity: a comparative analysis", Sustainability, vol. 12, no. 6, p. 2278, 2020. https://doi.org/10.3390/su12062278

[31] D. Seng, B. Li, C. Lai, & J. Wang, "Adaptive learning user implicit trust behavior based on graph convolution network", Ieee Access, vol. 9, p. 108363-108372, 2021. https://doi.org/10.1109/access.2021.3100762

[32] K. Hasegawa, N. O'Brien, M. Prendergast, C. Ajah, A. Neves, & S. Ghafur, "Cybersecurity interventions in health care organizations in low- and middle-income countries: scoping review", Journal of Medical Internet Research, vol. 26, p. e47311, 2024. https://doi.org/10.2196/47311

[33] J. Kaur, S. Hasan, S. Orthi, M. Miah, M. Goffer, C. Barikdaret al., "Advanced cyber threats and cybersecurity innovation - strategic approaches and emerging solutions", Journal of Computer Science and Technology Studies, vol. 5, no. 3, p. 112-121, 2024. https://doi.org/10.32996/jcsts.2023.5.3.9

[34] G. Nguyen and M. Ha, "The role of user adaptation and trust in understanding continuance intention towards mobile shopping: an extended expectation-confirmation model", Cogent Business & Management, vol. 8, no. 1, 2021. https://doi.org/10.1080/23311975.2021.1980248

[35] J. Singh, "Zenith armor : advancing security with zero trust measures", Interantional Journal of Scientific Research in Engineering and Management, vol. 08, no. 04, p. 1-5, 2024. https://doi.org/10.55041/ijsrem31326

[36] F. Silva, "Evolving approaches in cybersecurity: metrics and human factors", International Seven Journal of Multidisciplinary, vol. 1, no. 2, 2024. https://doi.org/10.56238/isevmjv1n2-010

[37] W. Meng, K. Choo, S. Furnell, A. Vasilakos, & C. Probst, "Towards bayesian-based trust management for insider attacks in healthcare software-defined networks", Ieee Transactions on Network and Service Management, vol. 15, no. 2, p. 761-773, 2018. https://doi.org/10.1109/tnsm.2018.2815280

[38]J. H. Addae, X. Sun, D. Towey, et al., "Exploring user behavioral data for adaptive cybersecurity," User Modeling and User-Adapted Interaction, vol. 29, pp. 701-750, 2019. https://doi.org/10.1007/s11257-019-09236-5

[39]A. Hassan, B. Nuseibeh and L. Pasquale, "Engineering Adaptive Authentication," 2021 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C), DC, USA, 2021, pp. 275-280, doi: 10.1109/ACSOS-C52956.2021.00068.

[40]Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. 2019. A Survey on Adaptive Authentication. ACM Comput. Surv. 52, 4, Article 80 (July 2020), 30 pages. https://doi.org/10.1145/3336117

[41]"Behavioral Analytics in Cybersecurity," CyberProtex, 2024. https://www.cyberprotex.com/blogs/september-08th-2024

[42]wso2, “GitHub - wso2/product-is: Welcome to the WSO2 Identity Server source code! For info on working with the WSO2 Identity Server repository and contributing code, click the link below.,” GitHub, Mar. 04, 2024. https://github.com/wso2/product-is (accessed Dec. 21, 2024).

[43]H. Fereidouni, Hafid, Abdelhakim Senhaji, D. Makrakis, and Y. Baseri, “F-RBA: A Federated Learning-based Framework for Risk-based Authentication,” arXiv.org, 2024. https://arxiv.org/abs/2412.12324v1 (accessed Apr. 20, 2025).