

## DAFTAR PUSTAKA

- Agarwal, L., Khan, H., Hengartner, U., 2016. Ask Me Again But Don ' t Annoy Me : Evaluating Re-authentication Strategies for Smartphones This paper is included in the Proceedings of the re-authentication strategies for smartphones. Symp. Usable Priv. Secur. 221–236.
- Alam, M.S., Vuong, S.T., 2013. Random forest classification for detecting android malware. Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCOM 2013 663–669. <https://doi.org/10.1109/GreenCom-iThings-CPSCOM.2013.122>
- Ayaz, M., Pasha, M.F., Alahmadi, T.J., Abdullah, N.N.B., Alkahtani, H.K., 2023. Transforming Healthcare Analytics with FHIR: A Framework for Standardizing and Analyzing Clinical Data. Healthc. 11. <https://doi.org/10.3390/healthcare11121729>
- Ayaz, M., Pasha, M.F., Alzahrani, M.Y., Budiarto, R., Stiawan, D., 2021. The Fast Health Interoperability Resources (FIHR) Standard: Systematic literature review of implementations, pplications, challenges and opportunities. JMIR Med. Informatics 9, 1–21. <https://doi.org/10.2196/21929>
- Braunstein, M.L., 2022. Mark L. Braunstein. Health Informatics.
- Cabarcos, P.A., Krupitzer, C., Becker, C., 2019. A survey on adaptive authentication. ACM Comput. Surv. 52. <https://doi.org/10.1145/3336117>
- Doerfler, P., Marincenko, M., Ranieri, J., Jiang, Y., Moscicki, A., McCoy, D., Thomas, K., 2019. Evaluating login challenges as a defense against account takeover. Web Conf. 2019 - Proc. World Wide Web Conf. WWW 2019 372–382. <https://doi.org/10.1145/3308558.3313481>
- Dutson, J., Allen, D., Eggett, D., Seamons, K., 2019. Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. Proc. - 4th IEEE Eur. Symp. Secur. Priv. Work. EUROS PW 2019 119–128. <https://doi.org/10.1109/EuroSPW.2019.00020>
- James, G., DanielaWitten, Hastie, T., Tibshirani, R., 2021. An Introduction to Statistical Learning wth application in R second edition. Springer Texts in Statistics Gareth.
- Kumari, S., 2023. Identity and access management: "Elevating security and efficiency: Unveiling the crucial aspects of identity and access management". Int. J. Eng. Technol. 12, 11–14.
- Misbahuddin, M., Bindhumadhava, B.S., Dheeptha, B., 2017. Design of a Risk Based Authentication System uisng Machine Learning Techniques. IEEE 53, 130.
- Mohamed, A.K.Y.S., Auer, D., Hofer, D., Küng, J., 2022. A systematic literature review for authorization and access control: definitions, strategies and models. Int. J. Web Inf. Syst. 18, 156–180. <https://doi.org/10.1108/IJWIS-04-2022-0077>
- Prasad, K.K., Aithal, P.S., 2016. A Study on Enhancing Mobile Banking Services using Location based Authentication. Int. J. Manag. Technol. Soc. Sci. 1, 48–58. <https://doi.org/10.47992/ijmts.2581.6012.0006>
- Rahat, T. Al, Feng, Y., Tian, Y., 2022. Cerberus: Query-driven Scalable Vulnerability Detection in OAuth Service Provider Implementations. Proc. ACM Conf. Comput. Commun. Secur. 2459–2473. <https://doi.org/10.1145/3548606.3559381>
- Roy, A., Dasgupta, D., 2018. A fuzzy decision support system for multifactor authentication. Soft Comput. 22, 3959–3981. <https://doi.org/10.1007/s00500-017-2607-6>
- Sarker, I.H., 2021. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Comput. Sci. 2, 1–21. <https://doi.org/10.1007/s42979-021-00592-x>
- Solapurkar, P., 2016. Building secure healthcare services using OAuth 2.0 and JSON web

- token in IOT cloud scenario. Proc. 2016 2nd Int. Conf. Contemp. Comput. Informatics, IC3I 2016 99–104. <https://doi.org/10.1109/IC3I.2016.7917942>
- Speiser, J.L., Miller, M.E., Tooze, J., Ip, E., 2019. A comparison of random forest variable selection methods for classification prediction modeling. *Expert Syst. Appl.* 134, 93–101. <https://doi.org/10.1016/j.eswa.2019.05.028>
- Sujudi, H.M., Heryawan, L., 2022. An Automatic Data Mapping for Interoperability of OpenEMR Medical Practice Management Software Using the Fast Healthcare Interoperability Resources. *Adv. Biomed. Eng.* 11, 186–193. <https://doi.org/10.14326/abe.11.186>
- Taneja, M., 2013. An analytics framework to detect compromised IoT devices using mobility behavior. *Int. Conf. ICT Conver.* 38–43. <https://doi.org/10.1109/ICTC.2013.6675302>
- Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., Bursztein, E., 2017. Data Breaches, phishing, or malware? understanding the risks of stolen credentials. *Proc. ACM Conf. Comput. Commun. Secur.* 1421–1434. <https://doi.org/10.1145/3133956.3134067>
- Wiefling, S., Dürmuth, M., Lo Iacono, L., 2021. What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based Authentication Characteristics. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* 12675 LNCS, 361–381. [https://doi.org/10.1007/978-3-662-64331-0\\_19](https://doi.org/10.1007/978-3-662-64331-0_19)
- Wiefling, S., Jørgensen, P.R., Thunem, S., Iacono, L. Lo, 2022. Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. *ACM Trans. Priv. Secur.* 26, 1–35. <https://doi.org/10.1145/3546069>
- Zhang, F., Kondoro, A., Muftic, S., 2012. Location-based authentication and authorization using smart phones. *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012* 1285–1292. <https://doi.org/10.1109/TrustCom.2012.198>