

DAFTAR PUSTAKA

- [1] M. Raihan, “Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia),” *J. Inov. Penelit.*, vol. 3, no. 10, pp. 7849–7850, 2023.
- [2] F. I. Adristi and E. Ramadhani, “Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya,” *Sel. Manaj. J. Mhs. Bisnis Manaj.*, vol. 2, no. 6, pp. 196–212, 2024, [Online]. Available: <https://journal.uui.ac.id/selma/article/view/35529>
- [3] B. O. ALSaleem and A. I. Alshoshan, “Multi-Factor Authentication to Systems Login,” *Natl. Comput. Coll. Conf.*, 2021, [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9428806&isnumber=9428786>
- [4] D. D. and D. K. A. Biryukov, “Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications,” *IEEE Eur. Symp. Secur. Priv.*, pp. 292–302, 2016, doi: 10.1109/EuroSP.2016.31.
- [5] J. Informatika, F. Teknik, U. P. Semarang, G. P. Lantai, K. Jl, and S. Timur, “IMPLEMENTASI MULTI-FACTOR AUTHENTICATION (MFA) DENGAN METODE HASHING (SHA-256) UNTUK MENINGKATKAN KEAMANAN PENGGUNA E-COMMERCE Tahap terakhir adalah Implementasi , di mana sistem MFA dikembangkan menggunakan dengan implementasi algoritma SHA-256 , sem,” vol. 9, no. Sens 9, pp. 624–630, 2024.
- [6] Suendri, “Hashing Argon2 Untuk Keamanan Password Pada Sistem Berbasis Web,” *J. Islam. Sci. Technol.*, vol. 4, no. 1, pp. 46–56, 2019.
- [7] Lucas Lee, *Hash Power: Cryptographic Hash Functions and Their Applications*. Norwegia: Publifye AS, 2025.
- [8] R. Renaldy and J. Informatika, “PENERAPAN MULTI-FACTOR AUTHENTICATION MENGGUNAKAN,” vol. 9, no. Sens 9, pp. 638–650, 2024.
- [9] S. Eum, H. Kim, M. Song, and H. Seo, “Optimized Implementation of Argon2 Utilizing the Graphics Processing Unit,” *Appl. Sci.*, vol. 13, no. 16, 2023, doi: 10.3390/app13169295.
- [10] P. A. Johnston, “Login System,” Manchester, 2005.
- [11] D. Marisa Khairina, “Analisis Keamanan Sistem Login,” *J. Inform. Mulawarman*, vol. Vol. 6 No., no. 2, pp. 64–67, 2011.
- [12] R. Sofana, Iwan & Primarthe, *Network Security Dan Cyber Security*. Bandung: Informatika, 2019.
- [13] A. W. Samsico, “Desain Algoritma Randomisasi pada persoalan Hashing:

Studi Kasus SPOJ 40643 AHASHREV - The Revenge Of Anti Hash,” 2024.

- [14] I. Malviya and T. Chetty, “International Journal on Recent and Innovation Trends in Computing and Communication: Performance and Limitation Review of Secure Hash Function Algorithm,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 7, no. 6, pp. 48–51, 2019, [Online]. Available: <http://www.ijritcc.org>
- [15] K. Phan, “Implementing Resiliency of Adaptive Multi-Factor Authentication Systems,” vol. 65, pp. 1–96, 2018, [Online]. Available: https://repository.stcloudstate.edu/msia_etdshttps://repository.stcloudstate.edu/msia_etds/65
- [16] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A review of multi-factor authentication in the Internet of Healthcare Things,” *Digit. Heal.*, vol. 9, 2023, doi: 10.1177/20552076231177144.
- [17] M. Fanti, *Implementing Multifactor Authentication: Protect Your Applications from Cyberattacks with the Help of MFA*. Packt Publishing, 2023. [Online]. Available: https://www.google.co.id/books/edition/Implementing_Multifactor_Authentication/r-zDEAAQBAJ?hl=id&gbpv=1
- [18] I. Yurita, M. Kevin Ramadhan, M. Candra, and U. Muhammadiyah Kotabumi, “Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime,” *J. Huk. Leg.*, pp. 144–155, 2023, [Online]. Available: <https://jurnal.umko.ac.id/index.php/legalita/article/view/995>
- [19] K. Mubarak and M. A. Romli, “Implementation of Rule Based Method in Detecting Brute Force Attacks on Owncloud Implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada Owncloud,” vol. 5, no. January, pp. 159–167, 2025.
- [20] M. C. Sinaga, *Kriptografi Python*. Tarutung, 2017. [Online]. Available: https://books.google.co.id/books?id=HCroDwAAQBAJ&printsec=frontcover&hl=id&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- [21] Y. Mulyanto and A. Algi Fari, “ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA),” *J. Inform. Teknol. dan Sains*, vol. 4, no. 3, pp. 145–155, 2022, doi: 10.51401/jinteks.v4i3.1897.
- [22] A. R. Naufal, D. A. Nawangnugraeni, and A. T. Suseno, “Rancang Bangun Sistem Informasi Point of Sale Multi Outlet Dengan Menggunakan Framework Laravel Di Koperasi Itsnu Pekalongan,” *J. Tek. Inf. dan Komput.*, vol. 5, no. 2, p. 280, 2022, doi: 10.37600/tekinkom.v5i2.591.
- [23] R. Permana, A. Abdilah, Fuad Nur Hasan, and Mahmud Syarif, “Estimation Effort Pengembangan Software Inventory PT. Infinity Global Mandiri Menggunakan Metode Use Case Point,” *J. RESTIKOM Ris. Tek. Inform. dan Komput.*, vol. 5, no. 2, pp. 73–84, 2023, doi:

10.52005/restikom.v5i2.144.

- [24] M. Shalahuddin and R. A. Sukamto, “Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek Edisi Revisi,” pp. 25–41, 2018.
- [25] “Mengenal Android Studio,” Developers.Android. [Online]. Available: <https://developer.android.com/studio/intro?hl=id>
- [26] Fauzan M, Rinandi A, and Maulid H, “Jago Menabung Aplikasi Untuk Mengelola Uang Saku Bebas Mobile,” *e-Proceeding Appl. Sci.*, vol. 10, no. 1, pp. 419–425, 2024, [Online]. Available: <https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/22496/21647>
- [27] R. Risqi and A. Herlambang, “Penggunaan Firebase Analytics pada Pengembangan Aplikasi Mobile I ’ m UII dengan Framework Flutter,” *Automata*, vol. 4, 2023, [Online]. Available: <https://jurnal.uii.ac.id/AUTOMATA/article/view/28841>
- [28] N. Telaumbanua, M. Yusuf, and A. Saifudin, “Implementasi Aplikasi Stock Opname Dengan Metode Waterfal,” *Jubitek J. BIG DATA DAN Teknol. Inf.*, vol. 1, pp. 61–83, 2023.
- [29] Y. F. and C. Taurusta, *Buku ajar rekayasa perangkat lunak terstruktur dan berorientasi objek*. Umsida Press, 2021. doi: <https://doi.org/10.21070/2018/978-602-5914-09-6>.
- [30] W. Setyaningsih, *KONSEP SISTEM PENDUKUNG KEPUTUSAN*, vol. 1. 2015.
- [31] V. Fedorchenko, O. Yeroshenko, O. Shmatko, O. Kolomiitsev, and M. Omarov, “Password Hashing Methods and Algorithms on the .Net Platform,” *Adv. Inf. Syst.*, vol. 8, no. 4, pp. 82–92, 2024, doi: 10.20998/2522-9052.2024.4.11.
- [32] H. Lubis and D. B. Srisulistiowati, “Implementasi Sistem Data Mining Untuk Menentukan Stock Accuracy Pada Warehouse PT Coca-Cola Amatil Indonesia Cibitung–Plant,” *J. Media Inform. Budidarma*, vol. 4, no. 1, p. 72, 2020, doi: 10.30865/mib.v4i1.1795.
- [33] A. Fitriyani, R. Sari, and S. Faiz, “Sistem Informasi Pengelolaan Zakat Dan Infaq Menggunakan Metode RAD,” *J. Inf. Inf. Secur.*, vol. 2, no. 2, pp. 197–210, 2021, [Online]. Available: <http://ejurnal.ubharajaya.ac.id/index.php/jiforty>
- [34] A. Fitriani, Sfenrianto, G. Wang, and A. Susanto, “Examining the security issues of automated teller machine based on revised technical acceptance model,” *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 14, no. 4, pp. 1521–1526, 2016, doi: 10.12928/TELKOMNIKA.v14i4.2920.
- [35] O. Jafari, P. Maurya, P. Nagarkar, K. M. Islam, and C. Crushev, “A Survey on Locality Sensitive Hashing Algorithms and their Applications,” *ACM Comput. Surv.*, 2021, [Online]. Available: <http://arxiv.org/abs/2102.08942>

- [36] A. Sadeghi-nasab and V. Rafe, "A Comprehensive Review on Broken Hashing Algorithms," *J. Comput. Virol. Hacking Tech.*, vol. 19, no. 2, 2023.
- [37] R. M. Saqib *et al.*, "Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security," *Intell. Autom. Soft Comput.*, vol. 32, no. 3, pp. 1633–1647, 2022, doi: 10.32604/IASC.2022.021786.
- [38] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, and J. Chang, "Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22501–22515, 2022, doi: 10.1109/JIOT.2022.3176192.
- [39] T. L. Mello *et al.*, "A New Perspective on Key Expansion for QKD BB84 : The RanA Model".
- [40] K. Tyagi, S. K. Yadav, and M. Singh, "Novel cryptographic approach to enhance cloud data security," *J. Phys. Conf. Ser.*, vol. 1998, no. 1, 2021, doi: 10.1088/1742-6596/1998/1/012022.
- [41] A. K. P. Desi Komalawati¹, Maria Dewi M. R.², Raiseta D. K.³, "The Shock Of Tens Billion Tokopedia InThe Middle Of Data Leaking Cases," *Medio*, vol. 2, pp. 114–122, 2020, [Online]. Available: <https://www.scribd.com/document/765762983/Admin-Medio-the-Shock-of-Tens-Billion-Tokopedia-in-the-Middle-of-Data-Leaking-Cases>
- [42] D. J. Mathew, "Argon2: The Secure Password Hashing Function," *Natl. Conf. Emerg. Comput. Appl.*, vol. 3, no. 1, 2021, [Online]. Available: https://nceca.in/2021/19Argon2_The_Secure_Password_Hashing_Function.pdf
- [43] A. Biryukov, D. Dinu, D. Khovratovich, and S. Josefsson, "RFC 9106: Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications," *Internet Res. Task Force*, pp. 1–21, 2021, [Online]. Available: <https://www.rfc-editor.org/info/rfc9106>