DAFTAR PUSTAKA

[1] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[2] A. A. Cook, G. Misirli, and Z. Fan, "Anomaly Detection for IoT Time-Series Data: A Survey," *IEEE Internet Things J*, vol. 7, no. 7, pp. 6481–6494, Jul. 2020, doi: 10.1109/JIOT.2019.2958185.

[3] K. DeMedeiros, A. Hendawi, and M. Alvarez, "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks," *Sensors*, vol. 23, no. 3, p. 1352, Jan. 2023, doi: 10.3390/s23031352.

[4] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses," *Sensors*, vol. 21, no. 19, p. 6432, Sep. 2021, doi: 10.3390/s21196432.

[5] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[6] B. Yapakçı, Z. Akdağcık, B. Ayvaz, and A. F. Ergenç, "Application of Process Mining to Production Lines Using Industrial Internet of Things," in *2023 IEEE 5th Eurasia Conference on IOT, Communication and Engineering (ECICE)*, IEEE, Oct. 2023, pp. 347–352. doi: 10.1109/ECICE59523.2023.10383119.

[7] M. Hasan, Md. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[8] K. Gupta, N. Jiwani, M. H. Uddin Sharif, M. A. Mohammed, and N. Afreen, "Smart Door Locking System Using IoT," in *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, IEEE, Nov. 2022, pp. 1–4. doi: 10.1109/ICACCM56405.2022.10009534.

[9] L. Aversano, M. L. Bernardi, M. Cimitile, R. Pecori, and L. Veltri, "Effective Anomaly Detection Using Deep Learning in IoT Systems," *Wirel Commun Mob Comput*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/9054336.

[10] S. K. Sahu and K. Mazumdar, "Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance," *Front Artif Intell*, vol. 7, May 2024, doi: 10.3389/frai.2024.1397480.

[11] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.

[12] M. Macak, I. Vanat, M. Merjavy, T. Jevocin, and B. Buhnova, "Towards Process Mining Utilization in Insider Threat Detection from Audit Logs," in *2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS)*, IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/SNAMS52053.2020.9336573.

[13] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *J Big Data*, vol. 6, no. 1, p. 111, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[14] C. Bell, "What Is the Internet of Things?," in *MicroPython for the Internet of Things*, Berkeley, CA: Apress, 2024, pp. 1–27. doi: 10.1007/978-1-4842-9861-9_1.

[15] "EXAMINING THE SECURITY ESSENCES OF INTERNET OF THINGS (IOT) DEVICES IN SMART HOMES: CHALLENGES, VULNERABILITIES, AND COUNTERMEASURES," *Issues In Information Systems*, 2024, doi: 10.48009/1_iis_2024_123.

[16] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer (Long Beach Calif)*, vol. 44, no. 9, pp. 51–58, Sep. 2011, doi: 10.1109/MC.2011.291.

[17] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A Systemic Approach for IoT Security," in *2013 IEEE International Conference on Distributed Computing in Sensor Systems*, IEEE, May 2013, pp. 351–355. doi: 10.1109/DCOSS.2013.78.

[18] F. Zijie, M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Wireless sensor networks in the internet of things: review, techniques, challenges, and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, p. 1190, Aug. 2023, doi: 10.11591/ijeecs.v31.i2.pp1190-1200.

[19] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," *Sensors*, vol. 23, no. 16, p. 7194, Aug. 2023, doi: 10.3390/s23167194.

[20] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[21] A. A. Zaidan *et al.*, "A survey on communication components for IoT-based technologies in smart homes," *Telecommun Syst*, vol. 69, no. 1, pp. 1–25, Sep. 2018, doi: 10.1007/s11235-018-0430-8.

[22] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: A Review," *Informatics*, vol. 11, no. 4, p. 71, Sep. 2024, doi: 10.3390/informatics11040071.

[23] Y. Wu, "Cloud-Edge Orchestration for the Internet of Things: Architecture and AI-Powered Data Processing," *IEEE Internet Things J*, vol. 8, no. 16, pp. 12792–12805, Aug. 2021, doi: 10.1109/JIOT.2020.3014845.

[24] M. Brambilla, E. Umuhoza, and R. Acerbis, "Model-driven development of user interfaces for IoT systems via domain-specific components and patterns," *Journal*

of Internet Services and Applications, vol. 8, no. 1, p. 14, Dec. 2017, doi: 10.1186/s13174-017-0064-1.

[25] O. Alruwaili, F. Mohammed Alotaibi, M. Tanveer, S. Chaoui, and A. Armghan, "PSAF-IoT: Physically Secure Authentication Framework for the Internet of Things," *IEEE Access*, vol. 12, pp. 78549–78561, 2024, doi: 10.1109/ACCESS.2024.3407353.

[26] H.-W. Lee, "Design of Multi-Functional Access Control System," *IEEE Access*, vol. 9, pp. 85255–85264, 2021, doi: 10.1109/ACCESS.2021.3087917.

[27] F. Skopik, M. Landauer, and M. Wurzenberger, "Online Log Data Analysis With Efficient Machine Learning: A Review," *IEEE Secur Priv*, vol. 20, no. 3, pp. 80–90, May 2022, doi: 10.1109/MSEC.2021.3113275.

[28] B.F. van Dongen, "Process Mining: A Two-Step Approach to Balance Between Underfitting and Overfitting," *BPM Center Report Series*, 2005.

[29] W. van der Aalst, *Process Mining*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016. doi: 10.1007/978-3-662-49851-4.

[30] W. van der Aalst, T. Weijters, and L. Maruster, "Workflow mining: discovering process models from event logs," *IEEE Trans Knowl Data Eng*, vol. 16, no. 9, pp. 1128–1142, Sep. 2004, doi: 10.1109/TKDE.2004.47.

[31] W. M. P. van der Aalst, V. Rubin, H. M. W. Verbeek, B. F. van Dongen, E. Kindler, and C. W. Günther, "Process mining: a two-step approach to balance between underfitting and overfitting," *Softw Syst Model*, vol. 9, no. 1, pp. 87–111, Jan. 2010, doi: 10.1007/s10270-008-0106-z.

[32] A. Rozinat, I. S. M. de Jong, C. W. Gunther, and W. M. P. van der Aalst, "Process Mining Applied to the Test Process of Wafer Scanners in ASML," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 39, no. 4, pp. 474–479, Jul. 2009, doi: 10.1109/TSMCC.2009.2014169.

[33] J. Carmona, B. van Dongen, A. Solti, and M. Weidlich, *Conformance Checking*. Cham: Springer International Publishing, 2018. doi: 10.1007/978-3-319-99414-7.

[34] W. M. P. van der Aalst, *Process Mining*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. doi: 10.1007/978-3-642-19345-3.

[35] P. Nafasa, I. Waspada, N. Bahtiar, and A. Wibowo, "Implementation of Alpha Miner Algorithm in Process Mining Application Development for Online Learning Activities Based on MOODLE Event Log Data," in *2019 3rd International Conference on Informatics and Computational Sciences (ICICoS)*, IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/ICICoS48119.2019.8982384.

[36] Y. A. Effendi and R. Sarno, "PARALLEL PROCESS DISCOVERY USING A NEW TIME-BASED ALPHA++ MINER," *IIUM Engineering Journal*, vol. 21, no. 1, pp. 126–141, Jan. 2020, doi: 10.31436/iiumej.v21i1.1173.

[37]   A. J. M. M. Weijters and W. M. P. van der Aalst, "Rediscovering workflow models from event-based data using little thumb," *Integr Comput Aided Eng*, vol. 10, no. 2, pp. 151–162, May 2003, doi: 10.3233/ICA-2003-10205.

[38]   Wenbing Zhao, "Handbook of Access Control Systems: Security, Identity Management and Trust Models," *Springer* , 2019.

[39]   W. van der Aalst, *Process Mining*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016. doi: 10.1007/978-3-662-49851-4.

[40]   A. Rozinat and C. W. Günther, "Disco: Discover Your Processes," Fluxicon Process Mining Academy. Accessed: Nov. 14, 2024. [Online]. Available: https://fluxicon.com/disco/

[41]   M. Dumas, M. La Rosa, J. Mendling, and H. A. Reijers, *Fundamentals of Business Process Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. doi: 10.1007/978-3-642-33143-5.