DAFTAR PUSTAKA

Amael, J. T., Istiyanto, J. E., Hakim, Z., Sari, R. H., Frisky, A. Z. K., & Natan, O. (2024). Securing Ventilators: Integrating Hardware Security Modules with SoftHSM and Cryptographic Algorithms. *2024 IEEE 33rd International Symposium on Industrial Electronics (ISIE)*, 1–6. https://doi.org/10.1109/ISIE54533.2024.10595781

Brandao, A., & Georgieva, P. (2020). Log Files Analysis For Network Intrusion Detection. *2020 IEEE 10th International Conference on Intelligent Systems (IS)*, 328–333. https://doi.org/10.1109/IS48319.2020.9199976

Dalenogare, L. S., Benitez, G. B., Ayala, N. F., & Frank, A. G. (2018). The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of Production Economics*, *204*, 383–394. https://doi.org/10.1016/j.ijpe.2018.08.019

Dinlersoz, E., & Wolf, Z. (2023). Automation, labor share, and productivity: Plant-level evidence from U.S. manufacturing. *Economics of Innovation and New Technology*, 1–23. https://doi.org/10.1080/10438599.2023.2233081

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics*, *210*, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

Hupp, W., Hasandka, A., De Carvalho, R. S., & Saleem, D. (2020). Module-OT: A Hardware Security Module for Operational Technology. *2020 IEEE Texas*

Power and Energy Conference (TPEC), 1–6. https://doi.org/10.1109/TPEC48276.2020.9042540

Jafarzadeh, H., & Jahanian, A. (2020). Real Vulnerabilities in Partial Reconfigurable Design Cycles; Case Study for Implementation of Hardware Security Modules. *2020 20th International Symposium on Computer Architecture and Digital Systems (CADS)*, 1–4. https://doi.org/10.1109/CADS50570.2020.9211860

Jaiswal, M., & Lata, K. (2018). Hardware Implementation of Text Encryption using Elliptic Curve Cryptography over 192 bit Prime Field. *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 343–349. https://doi.org/10.1109/ICACCI.2018.8554410

Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021). Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 791–796. https://doi.org/10.1109/ESCI50559.2021.9397005

Kuzminykh, I., Yevdokymenko, M., & Ageyev, D. (2020). Analysis of Encryption Key Management Systems: Strengths, Weaknesses, Opportunities, Threats. *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 515–520. https://doi.org/10.1109/PICST51311.2020.9467909

Luo, S., Hua, Z., & Xia, Y. (2018). TZ-KMS: A Secure Key Management Service for Joint Cloud Computing with ARM TrustZone. *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 180–185. https://doi.org/10.1109/SOSE.2018.00030

Mallik, A., Ahsan, A., Shahadat, M. Md. Z., & Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Muhammad, N., Zain, J. M., & Mohd Saman, M. Y. (2013). Loop-based RSA key generation algorithm using string identity. *2013 13th International Conference on Control, Automation and Systems (ICCAS 2013)*, 255–258. https://doi.org/10.1109/ICCAS.2013.6703904

Mulder, V., Mermoud, A., Lenders, V., & Tellenbach, B. (Eds.). (2023). *Trends in Data Protection and Encryption Technologies*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33386-6

Naik, N., & Jenkins, P. (2018). A Fuzzy Approach for Detecting and Defending Against Spoofing Attacks on Low Interaction Honeypots. *2018 21st International Conference on Information Fusion (FUSION)*, 904–910. https://doi.org/10.23919/ICIF.2018.8455555

Pott, C., Jungklass, P., Csejka, D. J., Eisenbarth, T., & Siebert, M. (2021). Firmware Security Module: A Framework for Trusted Computing in Automotive Multiprocessors. *Journal of Hardware and Systems Security*, *5*(2), 103–113. https://doi.org/10.1007/s41635-021-00114-4

Prawira P, M. M., Kurniandi, R., & Amiruddin, A. (2020). Secure SMS Using Pseudo-Random Bit Generator Based on Chaotic Map, and AES on Arduino UNO Board and SIM 900 Module. *2020 International Workshop on Big Data and Information Security (IWBIS)*, 91–96. https://doi.org/10.1109/IWBIS50925.2020.9255625

Qadir, A. M., & Varol, N. (2019). A Review Paper on Cryptography. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757514

Rady, H., Hossam, H., Saied, M. S., & Mostafa, H. (2019). Memristor-Based AES Key Generation for Low Power IoT Hardware Security Modules. *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, 231–234. https://doi.org/10.1109/MWSCAS.2019.8885031

Rasori, M., Manna, M. L., Perazzo, P., & Dini, G. (2022). A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things. *IEEE Internet of Things Journal*, *9*(11), 8269–8290. https://doi.org/10.1109/JIOT.2022.3154039

Schuh, G., Anderl, R., Dumitrescu, R., & Krüger, A. (n.d.). *Industrie 4.0 Maturity Index*.

Wang, S., & Liu, G. (2011). File Encryption and Decryption System Based on RSA Algorithm. *2011 International Conference on Computational and Information Sciences*, 797–800. https://doi.org/10.1109/ICCIS.2011.150

Yilmaz, B., & OzdemIr, S. (2018). Performance comparison of cryptographic algorithms in internet of things. *2018 26th Signal Processing and Communications Applications Conference (SIU)*, 1–4. https://doi.org/10.1109/SIU.2018.8404524