

DAFTAR PUSTAKA

- [1] “Smart Lighting Market Driving Energy Efficiency and Innovation for the Future,” Precedence Research. Accessed: Sep. 20, 2025. [Online]. Available: <https://www.precedenceresearch.com/smart-lighting-market>
- [2] “Zigbee Security Market Research Report 2033,” DATAINTELO. Accessed: Oct. 10, 2025. [Online]. Available: <https://dataintel.com/report/zigbee-security-market>
- [3] “Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About,” CM Alliance. Accessed: Aug. 28, 2025. [Online]. Available: <https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about>
- [4] “IoT Security Risks: Stats and Trends to Know in 2025,” JumpCloud. Accessed: Aug. 28, 2025. [Online]. Available: <https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025>
- [5] E. Ronen, C. O’Flynn, A. Shamir, and A. O. Weingarten, “IoT Goes Nuclear: Creating a ZigBee Chain Reaction,” *Proc IEEE Symp Secur Priv*, pp. 195–212, 2017, doi: 10.1109/SP.2017.14.
- [6] N. Hussein and A. Nhlabatsi, “Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control,” *Internet of Things*, vol. 3, no. 4, pp. 450–472, 2022, doi: 10.3390/iot3040024.
- [7] “CVE-2020-6007 Detail,” NIST. Accessed: Oct. 15, 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2020-6007>
- [8] P. Sharma and L. K. Awasthi, “Unveiling the hidden dangers: Security risks and forensic analysis of smart bulbs,” *Forensic Science International: Digital Investigation*, vol. 50, p. 301794, 2024, doi: <https://doi.org/10.1016/j.fsidi.2024.301794>.
- [9] M. El-hajj, H. Mousawi, and A. Fadlallah, “Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform †,” *Future Internet*, vol. 15, no. 2, pp. 1–29, 2023, doi: 10.3390/fi15020054.

- [10] S. Kumar, D. Kumar, R. Dangi, G. Choudhary, N. Dragoni, and I. You, "A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices," 2024, *Tech Science Press*. doi: 10.32604/cmc.2023.047084.
- [11] K. Lora, "Implementasi Algoritme PRESENT untuk Proses Enkripsi pada Modul," ... *Teknologi Informasi dan Ilmu Komputer e ...*, vol. 5, no. 5, pp. 2050–2057, 2021.
- [12] T. A. Khoa *et al.*, "Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study," *Wirel Commun Mob Comput*, vol. 2020, 2020, doi: 10.1155/2020/8896637.
- [13] T. Aji Shamasta and S. Dhiya Ayuni, "Automatic Control of Lights in a Room Using IoT-Based PIR Sensor [Rancang Bangun Kontrol Otomatis Lampu Pada Ruangan Menggunakan Sensor PIR Berbasis IoT]," pp. 1–7, 2023.
- [14] D. A. Jatmiko and S. U. Prini, "Implementasi dan Uji Kinerja Algoritma Background Subtraction pada ESP32," *Komputika : Jurnal Sistem Komputer*, vol. 8, no. 2, pp. 59–65, 2019, doi: 10.34010/komputika.v8i2.2194.
- [15] J. Damodharan, E. R. Susai Michael, and N. Shaikh-Husin, "High Throughput PRESENT Cipher Hardware Architecture for the Medical IoT Applications," *Cryptography*, vol. 7, no. 1, Mar. 2023, doi: 10.3390/cryptography7010006.
- [16] H. Y. Naser, A. K. Mattar, M. A. Saare, M. A. Almaiah, and R. Shehab, "A Comparison of Lightweight Cryptographic Protocols for Energy-Efficient and Sustainable IoMT Authentication," *Engineering, Technology and Applied Science Research*, vol. 15, no. 4, pp. 25746–25756, Aug. 2025, doi: 10.48084/etasr.12204.
- [17] M. Al-Shatari, F. A. Hussin, A. A. Aziz, T. A. E. Eisa, X. T. Tran, and M. E. E. Dalam, "IoT Edge Device Security: An Efficient Lightweight Authenticated Encryption Scheme Based on LED and PHOTON," *Applied Sciences (Switzerland)*, vol. 13, no. 18, 2023, doi: 10.3390/app131810345.
- [18] F. S. Putranta, R. Munadi, and Y. G. Bisono, "Perancangan Dan Analisis Sistem Smart Lighting Berbasis Wireless Sensor Network Untuk

- Meningkatkan Kenyamanan Aktivitas Di Dalam Rumah,” *TEKTRIKA - Jurnal Penelitian dan Pengembangan Telekomunikasi, Kendali, Komputer, Elektrik, dan Elektronika*, vol. 2, no. 1, 2018, doi: 10.25124/tektrika.v2i1.1659.
- [19] Pandu Mardya Wijaya, Abdi Pandu Kusuma, and Rizki Dwi Romadhona, “Prototype of a Warehouse Shoe Lamp Automation System Using Motion Sensors Based on the Internet of Things (IoT),” *JOSAR (Journal of Students Academic Research)*, vol. 9, no. 2, pp. 63–73, Sep. 2024, doi: 10.35457/josar.v9i2.3888.
- [20] A. Nugroho, R. Syaifudin, and A. I. Fauziawan, “Analisis Dampak Keamanan IoT dan Integrasi Sistem Informasi terhadap Perlindungan Data dan Kinerja Operasional di Perusahaan Telekomunikasi Yogyakarta,” 2024.
- [21] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, “Review of Smart-Home Security Using the Internet of Things,” Aug. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics13163343.
- [22] A. S. Kumari Mahalinga V Mandi, “Implementation of Present Cipher on FPGA for IoT Applications.” [Online]. Available: www.ijert.org
- [23] G. Arányi and V. Szücs, “IoT related security issues and black-box testing experiences in a smart lighting system.”
- [24] D. Indrajati and W. M. Ashari, “Evaluation of the Effectiveness of Lightweight Encryption Algorithms on Data Performance and Security on IoT Devices,” 2025. [Online]. Available: <http://jurnal.polibatam.ac.id/index.php/JAIC>
- [25] E. A. Al-Yousfi and M. Alkhawani, “Comprehensive Survey of Lightweight Ciphers for Resource-Constrained IoT Devices,” *Science and Technology Journal for Engineering and Technology*, vol. 3, no. 1, 2025, doi: 10.59222/ustjet.3.1.4.
- [26] R. Hidayati, I. Nirmala, and P. Studi Rekayasa Sistem Komputer Fakultas MIPA Universitas Tanjungpura Jl DrHHadari Nawawi, “Suhardi et al, Smart Lamp: Kendali dan Monitor lampu Berbasis Internet Of Things... 507.”

- [27] R. W. Febrianto and A. Zulianto, "Kriptografi Ringan dengan Menggunakan Algoritma di Internet Of Things (IoT)," *Journal of Informatics Management and Information Technology*, vol. 4, no. 3, pp. 81–91, 2024, doi: 10.47065/jimat.v4i3.403.
- [28] A. F. D. Suryawan, F. G. D. Putra, V. A. Lovely, and A. Setiawan, "Keamanan IoT dan Sistem Terdistribusi," *Journal of Internet and Software Engineering*, vol. 1, no. 3, p. 10, Jun. 2024, doi: 10.47134/pjise.v1i3.2619.
- [29] W. Fei, H. Ohno, and S. Sampalli, "A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions," *ACM Comput. Surv.*, vol. 56, no. 5, Nov. 2023, doi: 10.1145/3625094.
- [30] A. Sadeghi-Niaraki, "Internet of Thing (IoT) review of review: Bibliometric overview since its foundation," *Future Generation Computer Systems*, vol. 143, pp. 361–377, 2023, doi: <https://doi.org/10.1016/j.future.2023.01.016>.
- [31] A. Alammari, S. A. Moiz, and A. Negi, "Internet of Things Sensors and Actuators Layered Fog Service Delivery Model SALFSD," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer, 2019, pp. 15–25. doi: 10.1007/978-3-030-33709-4_2.
- [32] Jameswilson, "ESP32 Pinout, Datasheet, Features & Applications," THE ENGINEERING PROJECTS. Accessed: Sep. 15, 2025. [Online]. Available: <https://www.theengineeringprojects.com/2020/12/esp32-pinout-datasheet-features-applications.html>
- [33] J. Fraden, *Handbook of Modern Sensors*.
- [34] M. 'Toby S. Pratika, I. N. Piarsa, and A. A. K. A. C. Wiranatha, "Rancang Bangun Wireless Relay dengan Monitoring Daya Listrik Berbasis Internet of Things," *JITTER : Jurnal Ilmiah Teknologi dan Komputer*, vol. 2, no. 3, p. 515, 2021, doi: 10.24843/jtrti.2021.v02.i03.p10.
- [35] "What is a man-in-the-middle (MITM) attack?," Rapid7. [Online]. Available: <https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/>
- [36] H. Fereidouni, O. Fadeitseva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," *Security and Privacy*, vol. 8, no. 2, 2025, doi: 10.1002/spy2.70016.

- [37] S. Evanczuk, "IoT Security Fundamentals—Part 1: Using Cryptography," DigiKey. [Online]. Available: <https://www.digikey.com/en/articles/iot-security-fundamentals-part-1-using-cryptography?>
- [38] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, and A. Poschmann, "PRESENT : An Ultra-Lightweight Block Cipher".
- [39] Z. Haider, K. Javeed, M. Song, and X. Wang, "A Low-Cost Self-Test Architecture Integrated with PRESENT Cipher Core," *IEEE Access*, vol. 7, no. March, pp. 46045–46058, 2019, doi: 10.1109/ACCESS.2019.2907717.
- [40] A. I. , & S. A. Purnamasari, "Pengembangan Passive Infrared Sensor (PIR) HC-SR501 dengan Microcontrollers ESP32-CAM Berbasikan Internet of Things (IoT) dan Smart Home sebagai Deteksi Gerak untuk Keamanan Perumahan.," *In Prosiding Seminar Nasional SISFOTEK (Sistem Informasi Dan Teknologi Informasi)*, vol. (Vol. 3, No. 1)., 2019, [Online]. Available: https://scholar.google.com/scholar?hl=id&as_sdt=0%2C5&q=Pengembangan+Passive+Infrared+Sensor+%28PIR%29+HC-SR501+dengan+Microcontrollers+ESP32-CAM+Berbasikan+Internet+of+Things+%28IoT%29+dan+Smart+Home+sebagai+Deteksi+Gerak+untuk+Keamanan+Perumahan&btnG=
- [41] O. Penerangan *et al.*, "MIND-80," *MIND Journal | ISSN*, vol. ISSN, no. 2, pp. 80–95, 2019, doi: 10.26760/mindjournal.
- [42] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.
- [43] E. Engström, M. A. Storey, P. Runeson, M. Höst, and M. T. Baldassarre, "How software engineering research aligns with design science: a review," *Empir Softw Eng*, vol. 25, no. 4, pp. 2630–2660, Jul. 2020, doi: 10.1007/s10664-020-09818-7.
- [44] D. Escudero-Mancebo, N. Fernández-Villalobos, Ó. Martín-Llorente, and A. Martínez-Monés, "Research methods in engineering design: a synthesis of

- recent studies using a systematic literature review,” *Res Eng Des*, vol. 34, no. 2, pp. 221–256, Apr. 2023, doi: 10.1007/s00163-022-00406-y.
- [45] A. G. Putrada, M. Abdurohman, D. Perdana, and H. H. Nuha, “CIMA: A Novel Classification-Integrated Moving Average Model for Smart Lighting Intelligent Control Based on Human Presence,” *Complexity*, vol. 2022, 2022, doi: 10.1155/2022/4989344.
- [46] R. J. R. P. S. W. M. I. N. A. D Annisa, “RANCARAN PENERAPAN IOT UNTUK SISTEM ALARM ANTI MALING MENGGUNAKAN SENSOR PIR SMOOTH APPLICATION OF IOT FOR ANTI-THEFT ALARM SYSTEM USING PEAR SENSOR Creative Commons License Artikel ini berlisensi Creative Common Attribution-ShareAlike 4.0 International,” 2024.
- [47] P. Panahi, C. Bayılmış, U. Çavuşoğlu, and S. Kaçar, “Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications,” *Arab J Sci Eng*, vol. 46, no. 4, pp. 4015–4037, 2021, doi: 10.1007/s13369-021-05358-4.
- [48] Y. Anugrah, M. Hannats, H. Ichsan, and A. Kusyanti, “Implementasi Algoritme SHA-256 Menggunakan Protokol MQTT pada Budidaya Ikan Hias,” 2019. [Online]. Available: <http://j-ptiik.ub.ac.id>
- [49] R. Bharathi and N. Parvatham, “Light-Weight Present Block Cipher Model for IoT Security on FPGA,” *Intelligent Automation and Soft Computing*, vol. 33, no. 1, pp. 35–49, 2022, doi: 10.32604/iasc.2022.020681.
- [50] D. Indrajati and W. M. Ashari, “Evaluation of the Effectiveness of Lightweight Encryption Algorithms on Data Performance and Security on IoT Devices,” 2025. [Online]. Available: <http://jurnal.polibatam.ac.id/index.php/JAIC>
- [51] V. N. Ngo, A. N. Le, and D.-H. Kim, “Security Challenges and Lightweight Cryptography in IoT: Comparative Study and Testing Method for PRESENT-32bit Cipher,” in *Parallel and Distributed Computing, Applications and Technologies*, J. S. Park, H. Takizawa, H. Shen, and J. J. Park, Eds., Singapore: Springer Nature Singapore, 2024, pp. 295–305.

- [52] Z. Kasiran, S. Abdullah, and N. M. Nor, "An advance encryption standard cryptosystem in iot transaction," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1548–1554, 2020, doi: 10.11591/ijeecs.v17.i3.pp1548-1554.
- [53] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Present Scenarios of IoT Projects with Security Aspects Focused," in *Digital Twin Technologies and Smart Cities*, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, and H. Jahankhani, Eds., Cham: Springer International Publishing, 2020, pp. 95–122. doi: 10.1007/978-3-030-18732-3_7.
- [54] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," NIST Special Publication 800-38A, National Institute of Standards and Technology, Dec. 2001. [Online].

