Implementasi *Block Cipher Dongle* Berbasis Gerbang Logika untuk Keamanan Transmisi Data Paralel-Sistem Informasi

Jukardi Kurniawan[1]
Prodi S2 Teknik Informatika, Universitas Pamulang, Banten
email : r.djukardi.k@gmail.com
HP : 081958884838

ABSTRAK: *Keamanan transmisi data merupakan aspek krusial dalam sistem informasi industri, terutama pada lapisan fisik yang menentukan keandalan pertukaran data antarperangkat dan sensor. Penelitian ini bertujuan untuk merancang, mengimplementasikan, dan menguji prototipe block cipher dongle berbasis gerbang logika yang mampu mengacak data menggunakan kunci tertentu serta berfungsi sebagai lapisan keamanan tambahan pada sistem transmisi data paralel. Pendekatan ini difokuskan pada peningkatan keamanan data melalui mekanisme berbasis perangkat keras (hardware-based encryption) tanpa mengandalkan algoritma kriptografi kompleks berbasis perangkat lunak. Metode penelitian meliputi perancangan rangkaian kombinasi gerbang logika dasar (AND dan NOT) sebagai dasar proses pengacakan data, simulasi menggunakan digital circuit simulator, serta pengujian prototipe block cipher dongle pada sistem transmisi paralel. Hasil pengujian menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan tingkat akurasi 100%, di mana data asli dapat dipulihkan sepenuhnya selama kunci logika yang digunakan identik. Selain itu, sistem ini tidak menurunkan kecepatan transmisi data secara signifikan dan memberikan perlindungan fisik yang lebih kuat terhadap akses tidak sah. Kesimpulan penelitian menegaskan bahwa block cipher dongle berbasis gerbang logika layak diterapkan sebagai solusi keamanan tambahan pada sistem informasi industri, terutama pada infrastruktur Industri 4.0 yang memerlukan kecepatan tinggi dan ketahanan terhadap gangguan keamanan siber. Untuk penelitian selanjutnya, disarankan pengembangan sistem dengan kunci logika dinamis berbasis FPGA atau mikrokontroler yang dilengkapi pseudo-random key generator guna meningkatkan fleksibilitas dan tingkat keamanan perangkat keras.*

Kata kunci*: block cipher dongle, gerbang logika, transmisi data paralel, keamanan perangkat keras, sistem informasi*

ABSTRACT: *Data transmission security is a crucial aspect in industrial information systems, especially at the physical layer, which determines the reliability of data exchange between devices and sensors. This research aims to design, implement, and test a logic gate-based block cipher dongle prototype capable of scrambling data using a specific key and serving as an additional security layer in parallel data transmission systems. This approach focuses on enhancing data security through hardware-based encryption mechanisms without relying on complex software-based cryptographic algorithms. The research method includes designing a combination of basic logic gates (AND and NOT) as the basis for the data scrambling process, simulation using a digital circuit simulator, and testing a prototype block cipher dongle on a parallel transmission system. The test results show that the system is capable of performing encryption and decryption processes with a 100% accuracy rate, where the original data can be fully recovered as long as the logic key used is identical. In addition, this system does not significantly*

reduce data transmission speed and provides stronger physical protection against unauthorized access. The research conclusion confirms that the logic gate-based block cipher dongle is feasible as an additional security solution for industrial information systems, especially in Industry 4.0 infrastructure that requires high speed and resilience to cybersecurity threats. For further research, it is recommended to develop a system with a dynamic logic key based on an FPGA or microcontroller equipped with a pseudo-random key generator to increase flexibility and hardware security.

Keywords: block cipher dongle, logic gates, parallel data transmission, hardware security, information systems

PENDAHULUAN

Perkembangan sistem informasi industri *Internet of Things (IoT)* memberikan peluang besar dalam peningkatan efisiensi dan otomatisasi proses industri namun sekaligus menjadi tantangan signifikan terhadap aspek keamanan jaringan khususnya keamanan lapisan fisik (Physical Layer Security) (Liu et al., 2024; Sanenga et al., 2020). Dalam lingkungan industri modern, data dikirimkan melalui berbagai jalur komunikasi, baik secara serial maupun paralel, untuk mendukung sistem kendali otomatis, pemantauan produksi, serta pengolahan informasi secara *real-time*. Peningkatan konektivitas dan kompleksitas sistem tersebut berdampak pada meningkatnya risiko penyadapan, manipulasi, dan kebocoran data. Oleh karena itu, dibutuhkan mekanisme pengamanan yang tidak hanya bergantung pada perangkat lunak, tetapi juga mampu memberikan perlindungan fisik di tingkat perangkat keras. Beberapa skema keamanan berbasis kriptografi kunci public memiliki keterbatasan dalam mencapai *throughput* tinggi tanpa dukungan modul perangkat keras (Rodríguez-Flores et al., 2018). Pendekatan *hardware-based ecryption* menjadi solusi alternatif karena mampu memberikan proteksi tambahan terhadap serangan dari sisi perangkat lunak.

Salah satu pendekatan tersebut adalah penggunaan *block cipher dongle* berbasis gerbang logika, yaitu perangkat keras sederhana yang berfungsi melakukan pengacakan data menggunakan kunci tertentu *(Thumb Wheel)* melalui operasi logika dasar (gerbang *AND* dan *NOT*). *Block cipher* sendiri merupakan metode enkripsi di mana blok teks asli diproses secara keseluruhan untuk menghasilkan blok *cipher text* dengan panjang yang sama.(Stallings, 2005). Dengan prinsip tersebut, sistem transmisi data paralel dapat diamankan melalui lapisan fisik tanpa memerlukan algoritma kriptografi kompleks.

Sebagai ilustrasi, dalam sistem keamanan berbasis PIN empat digit terdapat 10^4 = 10.000 kemungkinan kombinasi, sehingga probabilitas untuk menebak satu kombinasi tertentu dalam satu percobaan acak adalah 1/10.000. Konsep probabilitas keamanan ini digunakan untuk menggambarkan tingkat ketahanan sistem terhadap serangan *brute-force* dan menjadi dasar dalam menilai kekuatan logika kunci yang digunakan pada sistem enkripsi perangkat keras.

Berdasarkan latar belakang tersebut, permasalahan yang diangkat dalam penelitian ini adalah bagaimana merancang *block cipher dongle* berbasis gerbang logika yang mampu melakukan proses enkripsi dan dekripsi data secara akurat, serta memberikan perlindungan tambahan terhadap transmisi tanpa menurunkan kecepatan pengiriman data secara signifikan. Selain itu, penelitian ini juga mengkaji throughput dan efektivitas penggunaan rangkaian kombinasi gerbang logika dasar dalam menghasilkan sistem keamanan berbasis perangkat keras yang efisien dan mudah diimplementasikan.

Tujuan penelitian ini adalah untuk merancang, mengimplementasikan, dan menguji *prototipe block cipher dongle* berbasis gerbang logika yang berfungsi sebagai lapisan keamanan tambahan pada sistem informasi industri. Penelitian ini juga bertujuan untuk membuktikan bahwa peningkatan keamanan data dicapai melalui pendekatan berbasis perangkat keras tanpa ketergantungan pada algoritma kriptografi kompleks berbasis perangkat lunak.

Secara teoretis, penelitian ini mengacu pada konsep dasar gerbang logika kombinasi dan prinsip transmisi data paralel, di mana pengacakan data dilakukan dengan operasi logika menggunakan kunci tertentu. Kajian teori juga didukung oleh penelitian-penelitian terdahulu yang menunjukkan bahwa pendekatan *hardware-based encryption* mampu mengurangi risiko serangan dari sisi perangkat lunak.

Beberapa penelitian terkait sistem keamanan berbasis FPGA *(Field Programmable Gate Array)* (İnce et al., 2024; Rodríguez-Flores et al., 2018) dan mikrokontroler juga menunjukkan potensi besar penggunaan logika digital sederhana untuk meningkatkan integritas data pada sistem kontrol industri.

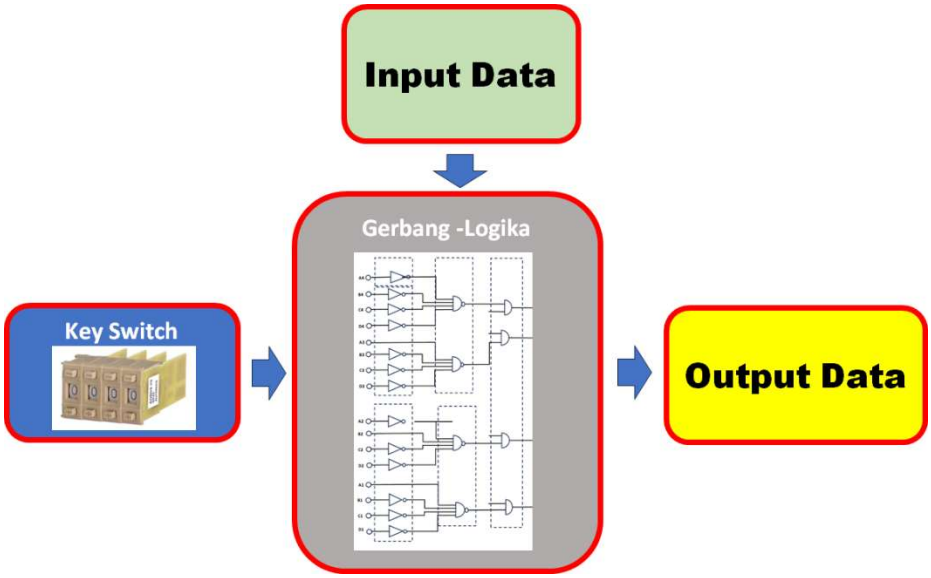
Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem keamanan data berbasis perangkat keras yang efisien, serta menjadi alternatif solusi dalam pendayagunaan teknologi digital untuk mendukung sistem informasi industri yang lebih andal, cepat, dan aman.

METODA

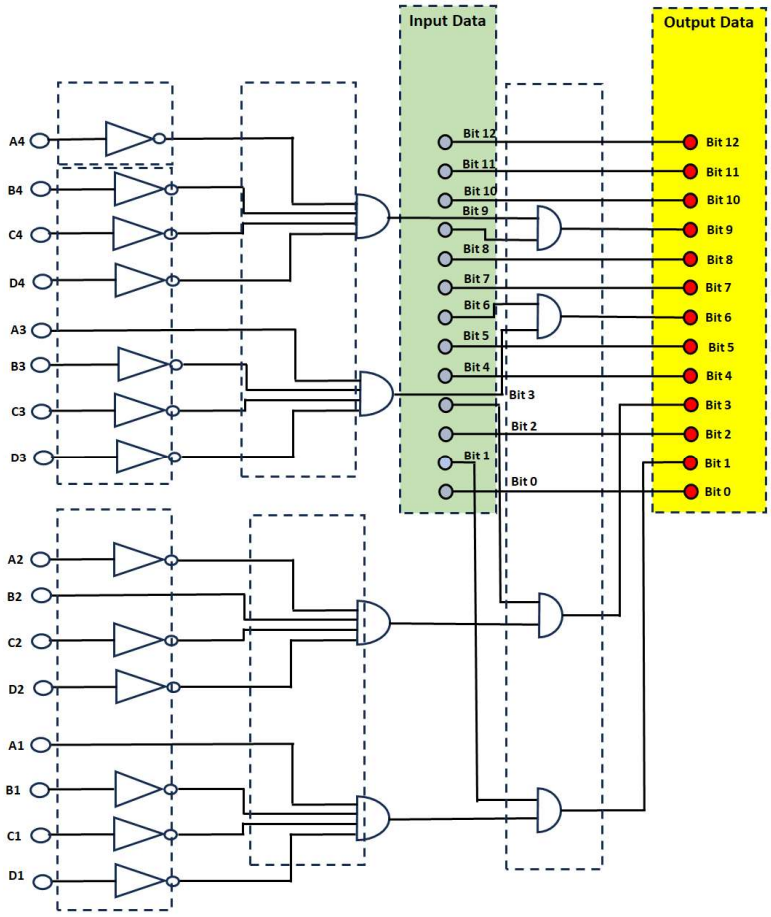
Penelitian ini menggunakan pendekatan rancang bangun yang berfokus pada pembuatan prototipe perangkat keras berupa *block cipher dongle* berbasis gerbang logika untuk meningkatkan keamanan transmisi data paralel pada sistem informasi industri.

Proses perancangan dimulai dari tahap analisis kebutuhan sistem, perancangan logika pengacakan data, implementasi rangkaian, hingga pengujian performa alat. Rangkaian dirancang menggunakan kombinasi gerbang logika dasar (*AND* dan *NOT*) yang disusun untuk menghasilkan fungsi enkripsi sederhana dengan kunci tertentu.

Selanjutnya, rangkaian diimplementasikan pada *breadboard* atau papan percobaan digital, kemudian diintegrasikan dengan sistem transmisi data paralel untuk diuji secara langsung. Data penelitian dikumpulkan melalui observasi terhadap hasil simulasi dan pengujian prototipe, serta pencatatan data keluaran (*output*) dari proses enkripsi dan dekripsi. Selain itu, dilakukan pengujian berulang dengan berbagai kombinasi kunci logika untuk menilai tingkat keakuratan sistem dan kestabilan transmisi.



Gambar 1 Blok Diagram Dongle



. Gambar 2 Rangkaian Gerbang-Logika Dongle

Penelitian dilaksanakan di ruang *intrapreneurship* pada salah satu pabrik ban di Jatiuwung, Tangerang, Banten, selama periode Agustus hingga Oktober 2025. Proses pengolahan data dilakukan dengan membandingkan hasil keluaran *block cipher dongle* dengan data asli untuk mengukur tingkat kesesuaian (akurasi) antara hasil enkripsi dan dekripsi. Analisis dilakukan secara kuantitatif sederhana melalui perbandingan nilai logika biner dan tingkat keberhasilan pengembalian data.

HASIL DAN PEMBAHASAN

1. *Hasil Perancangan Dongle Berbasis Gerbang Logika*

Hasil perancangan menunjukkan bahwa sistem *block cipher dongle* berbasis gerbang logika berhasil dibuat menggunakan kombinasi gerbang *AND* dan *NOT* yang berfungsi sebagai bit mask yang hanya melewati bit-bit tertentu sesuai pola kunci. Pola rangkaian dibentuk untuk menghasilkan proses pengacakan data menggunakan kunci logika yang ditentukan secara manual (pada penelitian ini kunci atau bit mask nya adalah 1210). Rangkaian mampu mengubah data biner masukan dalam satu blok teks menjadi keluaran dalam satu blok teks dengan panjang yang sama (teknik *block cipher*) yang acak sesuai dengan nilai kunci yang digunakan.

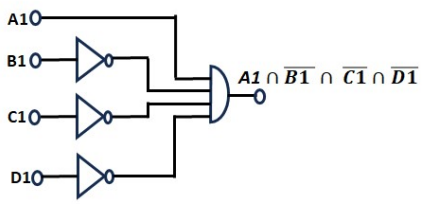
Tabel 1 Tabel kebenaran untuk kunci nilai desimal 1, 2, 3, dan 4

Kunci Nilai Desimal 1					
Truth Table					
Desimal	D1	C1	B1	A1	$A1 \cap \overline{B1} \cap \overline{C1} \cap \overline{D1}$
0	0	0	0	0	0
1	0	0	0	1	1
2	0	0	1	0	0
3	0	0	1	1	0
4	0	1	0	0	0
5	0	1	0	1	0
6	0	1	1	0	0
7	0	1	1	1	0
8	1	0	0	0	0
9	1	0	0	1	0

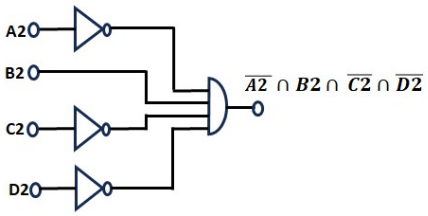
Kunci Nilai Desimal 2					
Truth Table					
Desimal	D2	C2	B2	A2	$\overline{A2} \cap B2 \cap \overline{C2} \cap \overline{D2}$
0	0	0	0	0	0
1	0	0	0	1	0
2	0	0	1	0	1
3	0	0	1	1	0
4	0	1	0	0	0
5	0	1	0	1	0
6	0	1	1	0	0
7	0	1	1	1	0
8	1	0	0	0	0
9	1	0	0	1	0

Kunci Nilai Desimal 3					
Truth Table					
Desimal	D3	C3	B1	A3	$A3 \cap \overline{B3} \cap \overline{C3} \cap \overline{D3}$
0	0	0	0	0	0
1	0	0	0	1	1
2	0	0	1	0	0
3	0	0	1	1	0
4	0	1	0	0	0
5	0	1	0	1	0
6	0	1	1	0	0
7	0	1	1	1	0
8	1	0	0	0	0
9	1	0	0	1	0

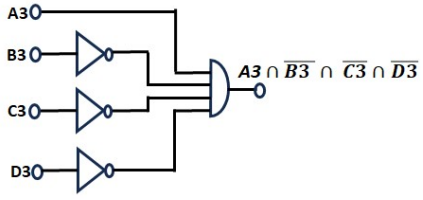
Kunci Nilai Desimal 4					
Truth Table					
Desimal	D4	C4	B4	A4	$\overline{A4} \cap \overline{B4} \cap \overline{C4} \cap \overline{D4}$
0	0	0	0	0	1
1	0	0	0	1	0
2	0	0	1	0	0
3	0	0	1	1	0
4	0	1	0	0	0
5	0	1	0	1	0
6	0	1	1	0	0
7	0	1	1	1	0
8	1	0	0	0	0
9	1	0	0	1	0



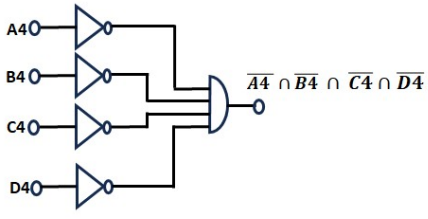
Rangkaian gerbang logika kunci desimal 1



Rangkaian gerbang logika kunci desimal 2



Rangkaian gerbang logika kunci desimal 3

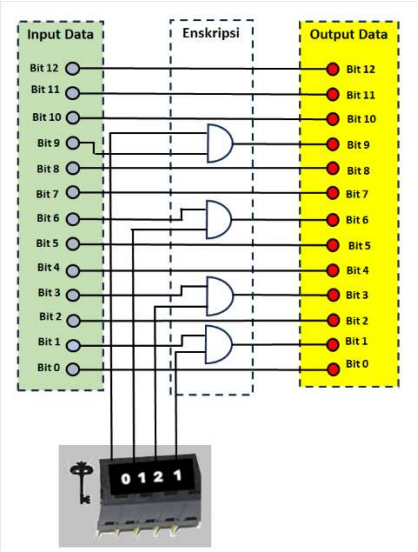


Rangkaian gerbang logika kunci desimal 4

Gambar 3 Rangkaian Gerbang-Logika Dongle untuk kunci desimal 1, 2, 3, dan 4

Fungsi utama dalam pengacakan data terletak pada gerbang *AND* dan *NOT* karena sifatnya yang reversible, yaitu data yang telah dienkripsi dapat dikembalikan ke bentuk semula hanya jika kunci yang

digunakan identik.



Gambar 4 Rangkaian Gerbang-Logika AND berfungsi sebagai bit mask

2. ***Hasil Pengujian Prototipe***

Pengujian prototipe dilakukan dengan menghubungkan *block cipher dongle* ke sistem transmisi data paralel sederhana yang terdiri dari modul pengirim dan penerima. Data uji berupa 13 bit dikirim melalui jalur paralel, dengan kunci logika ditetapkan secara manual pada sakelar input. Berikut hasil pengujian untuk beberapa kombinasi data asli.

Tabel 2 Hasil Uji Enkripsi dan Dekripsi Data Paralel

	Bit													Desimal
	0	1	2	3	4	5	6	7	8	9	10	11	12	
Data Asli (Input)	1	1	1	1	1	1	1	1	1	1	1	1	1	**8191**
Kunci (Key)	1	0	1	0	1	1	0	1	1	0	1	1	1	
Data Terenkripsi	1	0	1	0	1	1	0	1	1	0	1	1	1	**7605**
Data Terdekripsi	1	1	1	1	1	1	1	1	1	1	1	1	1	**8191**
Akurasi (%)	100%													

	Bit													Desimal
	0	1	2	3	4	5	6	7	8	9	10	11	12	
Data Asli (Input)	0	1	0	1	1	0	1	1	0	1	1	1	1	**7898**
Kunci (Key)	1	0	1	0	1	1	0	1	1	0	1	1	1	
Data Terenkripsi	0	0	0	0	1	0	0	1	0	0	1	1	1	**7312**
Data Terdekripsi	0	1	0	1	1	0	1	1	0	1	1	1	1	**7898**
Akurasi (%)	100%													

	Bit													Desimal
	0	1	2	3	4	5	6	7	8	9	10	11	12	
Data Asli (Input)	1	0	1	1	0	1	1	1	1	1	1	0	1	**6125**
Kunci (Key)	1	0	1	0	1	1	0	1	1	0	1	1	1	
Data Terenkripsi	1	0	1	0	0	1	0	1	1	0	1	0	1	**5541**
Data Terdekripsi	1	0	1	1	0	1	1	1	1	1	1	0	1	**6125**
Akurasi (%)	100%													

	Bit													Desimal
	0	1	2	3	4	5	6	7	8	9	10	11	12	
Data Asli (Input)	1	1	0	1	0	0	1	1	0	1	0	0	0	**715**
Kunci (Key)	1	0	1	0	1	1	0	1	1	0	1	1	1	
Data Terenkripsi	1	0	0	0	0	0	0	1	0	0	0	0	0	**129**
Data Terdekripsi	1	1	0	1	0	0	1	1	0	1	0	0	0	**715**
Akurasi (%)	100%													

Sumber: Data hasil pengujian prototipe 2025

Berdasarkan Tabel 2, seluruh proses enkripsi dan dekripsi menunjukkan hasil akurasi 100%, yang berarti sistem mampu mengembalikan data asli tanpa kesalahan bit selama kunci logika sesuai. Ketika kunci yang digunakan tidak identik, hasil keluaran menjadi acak dan tidak dapat dikenali, menandakan fungsi keamanan berjalan efektif.

3. ***Analisis Kinerja Sistem***

Hasil pengujian menunjukkan bahwa penggunaan *block cipher dongle* tidak menurunkan kecepatan transmisi data secara signifikan karena menggunakan transmisi paralel dengan *bit mask* dalam *block cipher* dimana tanpa proses perhitungan matematika dengan software yang memerlukan waktu tambahan eksekusi.

Dari sisi keamanan, sistem berbasis logika digital memiliki keunggulan dibandingkan sistem enkripsi perangkat lunak karena bekerja langsung di level perangkat keras (hardware layer), sehingga sulit diakses oleh perangkat lunak eksternal. Dengan tidak adanya proses komputasi berat di sisi prosesor, konsumsi daya sistem juga menjadi lebih rendah dan stabil.

Selain itu, pendekatan hardware-based encryption seperti ini memiliki ketahanan lebih tinggi terhadap serangan software injection atau modifikasi kode yang sering terjadi pada sistem informasi industri berbasis jaringan. Dengan demikian, rancangan dongle ini relevan diterapkan sebagai lapisan keamanan tambahan pada sistem informasi industri yang membutuhkan transmisi data berkecepatan tinggi dengan tingkat perlindungan fisik yang kuat.

4. ***Pembahasan Relevansi dan Pengembangan Sistem***

Penelitian ini membuktikan bahwa gerbang logika dasar dapat digunakan untuk membangun sistem keamanan data sederhana yang efisien. Pendekatan ini dapat dikembangkan lebih lanjut menggunakan FPGA (*Field Programmable Gate Array*) atau mikrokontroler, sehingga kunci logika dapat

dihasilkan secara dinamis melalui algoritma pseudo-random. Pengembangan ini akan meningkatkan tingkat keamanan sekaligus memberikan fleksibilitas bagi pengguna. Namun, kelemahan FPGA dibandingkan dengan rancang bangun pada penelitian ini dari segi investasi biaya lebih mahal.

Sistem keamanan berbasis perangkat keras dapat mempercepat proses autentikasi tanpa menambah beban komputasi pada sistem utama. Dengan demikian, implementasi *block cipher dongle* berbasis gerbang logika memiliki prospek luas dalam pengembangan industri 4.0, terutama pada sistem informasi industri yang terintegrasi dengan perangkat IoT dan kontrol otomatis.

SIMPULAN DAN SARAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang dilakukan, penelitian ini berhasil mencapai tujuan utamanya, yaitu merancang, mengimplementasikan, dan menguji prototipe *block cipher dongle* berbasis gerbang logika yang berfungsi sebagai lapisan keamanan tambahan pada sistem informasi industri. Hasil penelitian membuktikan bahwa keamanan data dapat ditingkatkan melalui pendekatan berbasis perangkat keras (*hardware-based encryption*) tanpa bergantung pada algoritma kriptografi kompleks berbasis perangkat lunak.

Rancangan sistem yang menggunakan kombinasi gerbang *AND* dan *NOT* terbukti mampu melakukan proses enkripsi dan dekripsi data dengan tingkat akurasi 100%, di mana data asli dapat dikembalikan tanpa kesalahan bit selama kunci logika yang digunakan identik. Proses pengacakan data dilakukan langsung pada level logika digital dengan konsep *block cipher*, sehingga tidak menurunkan kecepatan transmisi secara signifikan dan tidak memerlukan perhitungan matematis yang kompleks. Dari sisi keamanan, *block cipher dongle* ini memiliki keunggulan karena bekerja langsung pada lapisan perangkat keras, menjadikannya lebih tahan terhadap serangan berbasis perangkat lunak (*software attack*) dan lebih efisien dari segi konsumsi daya.

Dengan demikian, hasil penelitian ini menunjukkan bahwa *block cipher dongle* berbasis gerbang logika layak diterapkan sebagai solusi keamanan tambahan bagi sistem informasi industri yang memerlukan transmisi data cepat, stabil, dan terlindungi secara fisik. Pendekatan ini juga relevan untuk mendukung kebutuhan keamanan siber pada era Industri 4.0, terutama pada sistem yang terintegrasi dengan *Internet of Things (IoT)* dan kontrol otomatis.

Sebagai tindak lanjut, penelitian selanjutnya disarankan untuk mengembangkan sistem ini dengan kunci logika dinamis menggunakan *FPGA* atau mikrokontroler yang dilengkapi *pseudo-random key generator* agar keamanan lebih adaptif terhadap ancaman siber modern. Selain itu, perlu dilakukan pengujian kompatibilitas dengan protokol komunikasi industri seperti *Modbus*, *Profibus*, atau *Ethernet/IP* untuk memastikan keandalan sistem di lingkungan industri sebenarnya. Analisis lebih lanjut terhadap efisiensi logika dan konsumsi daya juga diperlukan guna meningkatkan performa ketika diterapkan pada perangkat *IoT* berskala besar.

Akhirnya, pengembangan sistem keamanan secara multi-layer dengan menggabungkan pendekatan logika digital dan enkripsi perangkat lunak diharapkan dapat menghasilkan solusi keamanan data yang lebih kuat, efisien, dan sesuai dengan kebutuhan sistem informasi industri modern.

DAFTAR PUSTAKA

Almalawi, A., Hassan, S., Fahad, A., & Khan, A. I. (2024). A Hybrid Cryptographic Mechanism for Secure Data Transmission in Edge AI Networks. *International Journal of Computational Intelligence Systems*, *17*(1). https://doi.org/10.1007/s44196-024-00417-8

Angueira, P., Val, I., Montalban, J., Seijo, O., Iradier, E., Fontaneda, P. S., Fanari, L., & Arriola, A. (2022). A Survey of Physical Layer Techniques for Secure Wireless Communications in Industry. *IEEE Communications Surveys and Tutorials*, *24*(2), 810–838. https://doi.org/10.1109/COMST.2022.3148857

Chen, X., Zheng, D., & Huang, K. (2024). FCLock: harnessing functional non-combinational cycles in logic locking. *IEICE Electronics Express*, *21*(12). https://doi.org/10.1587/elex.21.20240218

Frank, F., Schmid, M., Klement, F., Palani, P., Weber, A., Kavun, E. B., Xiong, W., Arul, T., & Katzenbeisser, S. (2024). Secure Data-Binding in FPGA-based Hardware Architectures utilizing PUFs. *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 423–435. https://doi.org/10.1145/3634737.3656996

Gaikwad, S. Y. (2024). Secure Data Transmission in the Wireless Sensor Network with Blockchain Cryptography Network. *Journal of Sensors, IoT & Health Sciences*, *2*(2), 41–55. https://doi.org/10.69996/jsihs.2024009

Grossi, M., Alfonsi, F., Prandini, M., & Gabrielli, A. (2024). Increasing the Security of Network Data Transmission with a Configurable Hardware Firewall Based on Field Programmable Gate Arrays. *Future Internet*, *16*(9). https://doi.org/10.3390/fi16090303

İnce, E., Karakaya, B., & Türk, M. (2024). Designing hardware for a robust high-speed cryptographic key generator based on multiple chaotic systems and its FPGA implementation for real-time video encryption. *Multimedia Tools and Applications*, *83*(24), 64499–64532. https://doi.org/10.1007/s11042-023-17972-5

Kumar Yadav, K., & Dharmesh Kirit, D. (n.d.). *Securing Data Transmission from Adversaries in Cybersecurity WSN Using Efficient Key Management Techniques*.

Lim, D. G., & Lee, J. H. (2014). Parallel architecture for high-speed block cipher, HIGHT. *International Journal of Security and Its Applications*, *8*(2), 59–66. https://doi.org/10.14257/ijsia.2014.8.2.06

Liu, X., Xu, F., Ning, L., Zhao, C., & Xia, H. (2024). A Novel Approach for the Enhancement of Security through Defining the Spatial Secrecy Outage Probability in the Industrial Internet of Things. *Electronics (Switzerland)*, *13*(12). https://doi.org/10.3390/electronics13122356

Maqsood, F. (2017). Designing a complex code generator using LFSR for multichannel encryption. *International Journal of Computing and Optimization*, *4*, 1–9. https://doi.org/10.12988/ijco.2017.61023

Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. In *Sensors (Basel, Switzerland)* (Vol. 23, Issue 21). https://doi.org/10.3390/s23218840

Qasim, A., Mohie, N. M., & Azeez, Z. N. (2025). Efficient Multi-Carrier Communication Systems: A Performance Evaluation of Parallel and Sequential Data Processing Models. *Journal of Internet Services and Information Security*, *15*(1), 67–78. https://doi.org/10.58346/JISIS.2025.I1.005

Rodríguez-Flores, L., Morales-Sandoval, M., Cumplido, R., Feregrino-Uribe, C., & Algredo-Badillo, I. (2018). Compact FPGA hardware architecture for public key encryption in embedded devices. *PLoS ONE*, *13*(1). https://doi.org/10.1371/journal.pone.0190939

Sa'adah, N., Gede, I., Astawa, P., & Sudarsono, A. (2018). Trusted Data Transmission Using Data Scrambling Security Method with Asymmetric Key Algorithm for Sychronization. *EMITTER International Journal of Engineering Technology*, *6*(2).

Saeed, A., Ahmadinia, A., & Just, M. (2018). Hardware-assisted secure communication in embedded and multi-core computing systems. *Computers*, *7*(2). https://doi.org/10.3390/computers7020031

Sanenga, A., Mapunda, G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Chuma, J. M. (2020). An overview of key technologies in physical layer security. In *Entropy* (Vol. 22, Issue 11, pp. 1–34). MDPI AG. https://doi.org/10.3390/e22111261

Srinivasan, A., & Kalaichelvi, D. (n.d.). International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Secured Data Transmission in IoT using Homomorphic Encryption. In *Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE* (Vol. 2022, Issue 3). www.ijisae.org

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices, Fourth Edition*.

Sun, W., Yu, S., Xing, Y., & Zhang, D. (2018). A multi-path switching method based on SCTP for heterogeneous wireless networks in smart IoT. *Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018*, 15–22. https://doi.org/10.1109/SmartIoT.2018.00013

Varadharajan, V., Tupakula, U., & Karmakar, K. K. (2024). Techniques for Enhancing Security in Industrial Control Systems. *ACM Transactions on Cyber-Physical Systems*, *8*(1).

https://doi.org/10.1145/3630103
Xu, C., Zhang, J., Zhang, Z., Hou, J., & Wen, X. (2023). Data and Service Security of GNSS Sensors Integrated with Cryptographic Module. *Micromachines*, *14*(2). https://doi.org/10.3390/mi14020454
Yang, H. (2014). Research on Design Method Based on Hardware Encryption and Two-way ID Authentication for Security Mobile Hard Disk. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *12*(4). https://doi.org/10.11591/telkomnika.v12i4.4995
Zhang, Z., Wang, X., Hao, Q., Xu, D., Zhang, J., Liu, J., & Ma, J. (2021). High-efficiency parallel cryptographic accelerator for real-time guaranteeing dynamic data security in embedded systems. *Micromachines*, *12*(5). https://doi.org/10.3390/mi12050560