**Implementasi dan Analisis Performa Algoritma Enkripsi ChaCha20 Berbasis Protokol Komunikasi ESP-NOW Pada Wireless Sensor Network**

**Naufal Farras Trikusuma1, Agung Setia Budi2**

Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Brawijaya

Email: 1naufalfarr@student.ub.ac.id, 2penulis.dua@ub.ac.id

**Abstrak**

*Wireless Sensor Network* (WSN) telah berkembang pesat dalam mendukung proses otomasi, seperti pengumpulan data sensor, pengendalian sistem nirkabel, dan *monitoring*. Namun, keamanan data menjadi tantangan utama karena data yang ditransmisikan sering kali bersifat sensitif dan rentan terhadap ancaman seperti data breach dan akses tidak sah. Keterbatasan sumber daya perangkat WSN, seperti daya komputasi, memori, dan energi, juga menjadi hambatan dalam penerapan algoritma kriptografi konvensional yang membutuhkan sumber daya besar. Oleh karena itu, diperlukan lightweight cryptography (LWC) yang efisien namun tetap aman. Penelitian ini menganalisis performa algoritma enkripsi ChaCha20 pada protokol komunikasi ESP-NOW menggunakan perangkat berbasis ESP8266, yang tidak dilengkapi *cryptographic hardware accelerators*. Pengujian dilakukan secara komparatif terhadap algoritma AES-CBC, Clefia, dan Snow-V, dengan mengevaluasi kecepatan enkripsi-dekripsi, konsumsi daya, serta aspek keamanan terkait konfidensialitas data. Implementasi sistem menggunakan ESP8266 serta sensor INA219 untuk mengukur konsumsi daya pada sistem pengukur. Hasil pengujian menunjukkan ChaCha20 memiliki performa terbaik dalam hal waktu komputasi dan efisiensi energi, baik untuk ukuran data 5 KB maupun 10 KB. Tanpa bergantung pada akselerator perangkat keras, ChaCha20 menjadi solusi ideal bagi perangkat WSN dengan keterbatasan sumber daya. Temuan ini mendukung ChaCha20 sebagai algoritma enkripsi yang efisien untuk meningkatkan keamanan data tanpa mengorbankan efisiensi.

**Kata kunci**: *Wireless Sensor Network, ChaCha20, Lightweight Cryptography, ESP-NOW, Keamanan Data, Efisiensi Sumber Daya, Algoritma Enkripsi.*

**Abstract**

*Wireless Sensor Networks (WSNs) have significantly advanced in supporting automation processes, such as sensor data collection, wireless system control, and monitoring. However, data security remains a critical challenge since transmitted data is often sensitive and vulnerable to threats such as data breaches and unauthorized access. The limited resources of WSN devices, including computational power, memory, and energy, further hinder the implementation of conventional cryptographic algorithms, which require substantial resources. Therefore, lightweight cryptography (LWC) is needed to provide efficient yet secure solutions. This study analyzes the performance of the ChaCha20 encryption algorithm on the ESP-NOW communication protocol using ESP8266-based devices, which lack cryptographic hardware accelerators. The evaluation is conducted in comparison with AES-CBC, Clefia, and Snow-V algorithms, focusing on encryption-decryption speed, energy consumption, and data confidentiality. The system implementation employs a DHT22 temperature and humidity sensor as the data source and an INA219 sensor to measure energy consumption. The results demonstrate that ChaCha20 achieves the best performance in terms of computational speed and energy efficiency for data sizes of 5 KB and 10 KB. Without relying on hardware accelerators, ChaCha20 emerges as an ideal solution for WSN devices with limited resources. These findings support ChaCha20 as an efficient encryption algorithm to enhance data security while maintaining computational and energy efficiency.*

**Keywords**: *Wireless Sensor Network, ChaCha20, Lightweight Cryptography, ESP-NOW, Data Security, Energy Efficiency, Cryptographic Hardware Accelerators.*

# PENDAHULUAN

Perkembangan teknologi dalam bidang Wireless Sensor Network (WSN) semakin pesat dalam beberapa tahun terakhir. WSN, yang terdiri dari jaringan node sensor yang saling terhubung secara nirkabel, memungkinkan pengumpulan data, pengendalian sistem, serta pengawasan secara otomatis (Astuti & Wibisono, 2017). Meskipun demikian, tantangan utama dalam implementasi WSN adalah keterbatasan sumber daya perangkat keras, seperti daya komputasi, penyimpanan, dan konsumsi energi. Di sisi lain, aspek keamanan data menjadi hal krusial, terutama pada aplikasi yang melibatkan data sensitif yang rawan terhadap ancaman seperti *data breach* atau akses tidak sah (Sarker et al., 2020). Oleh karena itu, diperlukan metode kriptografi yang mampu memberikan perlindungan pada data tanpa mengorbankan efisiensi perangkat.

Salah satu pendekatan yang sedang berkembang adalah *lightweight cryptography* (LWC), yang dirancang untuk memenuhi kebutuhan keamanan pada perangkat dengan sumber daya terbatas (Gunathilake et al., 2019). Algoritma ChaCha20, sebuah *stream cipher* berkecepatan tinggi yang dikembangkan oleh Bernstein tahun 2008, menawarkan solusi dengan kebutuhan sumber daya yang rendah sekaligus memberikan tingkat keamanan yang setara dengan algoritma modern lainnya. Dalam konteks WSN, di mana perangkat seperti ESP8266 yang tidak memiliki akselerator perangkat keras kriptografi sering digunakan, ChaCha20 menjadi kandidat yang menarik karena tidak bergantung pada dukungan perangkat keras khusus. Menurut Jin (2022) pada penelitian sebelumnya menunjukkan bahwa algoritma seperti AES yang memanfaatkan akselerator perangkat keras dapat meningkatkan performa secara signifikan, tetapi jika fitur ini tidak tersedia, efisiensi dapat menurun drastis hingga 257,8%.

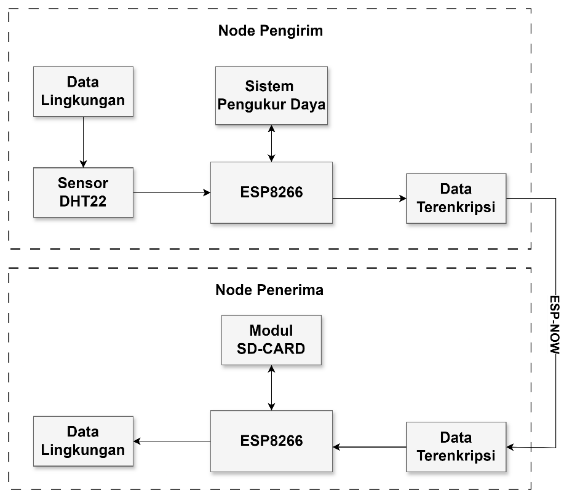
Dalam penelitian ini, dilakukan analisis performa ChaCha20 pada protokol komunikasi ESP-NOW berbasis mikrokontroler ESP8266. Penelitian ini bertujuan untuk mengevaluasi waktu komputasi algoritma, pengaruhnya terhadap penggunaan sumber daya komputasi, serta efektivitasnya dalam meningkatkan aspek kerahasiaan data. Dengan membandingkan performa ChaCha20 dengan algoritma lain seperti AES, Clefia, dan Snow-V, penelitian ini diharapkan dapat memberikan gambaran menyeluruh terkait efisiensi dan keamanan algoritma enkripsi dalam skenario sistem tertanam yang memiliki keterbatasan sumber daya.

Metodologi yang digunakan meliputi desain prototipe menggunakan tiga perangkat ESP8266 yang dilengkapi sensor DHT22 yang berfungsi dalam pengambilan data uji, yang mencakup kecepatan enkripsi-dekripsi, konsumsi daya, dan aspek keamanan khususnya *confidentiality* (kerahasiaan) pada data. Pengujian algoritma dilakukan secara komparatif, dengan mempertimbangkan efisiensi komputasi dan aspek keamanan data melalui validasi vektor uji dan pengukuran konsumsi energi menggunakan modul INA219.

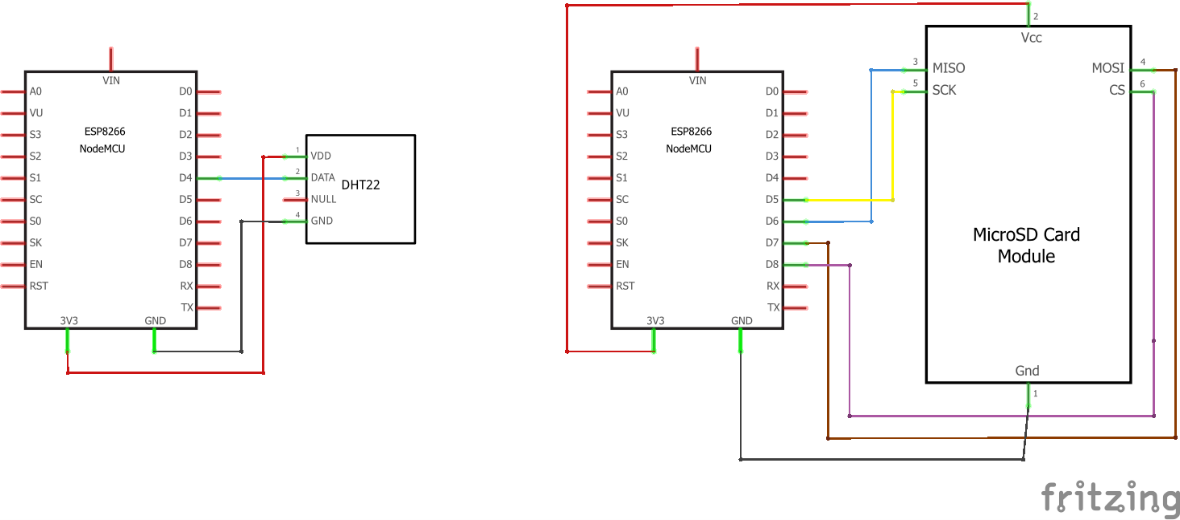
Hasil dari penelitian ini diharapkan dapat memberikan kontribusi signifikan pada pengembangan WSN, terutama dalam memilih algoritma enkripsi yang efisien, cepat, dan sesuai untuk perangkat dengan sumber daya terbatas. Selain itu, penelitian ini juga diharapkan dapat memberikan referensi bagi pengembang atau peneliti untuk mengintegrasikan metode keamanan yang lebih hemat sumber daya pada sistem WSN di masa depan.

# 2. PERANCANGAN DAN IMPLEMENTASI

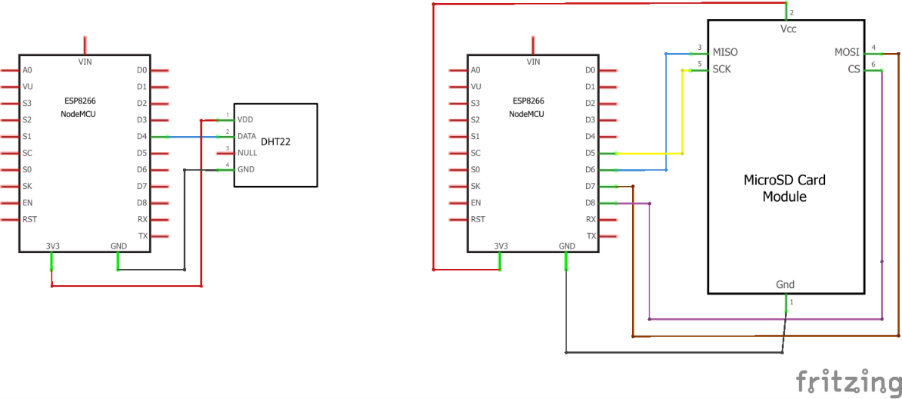
# 2.1 Perancangan Sistem



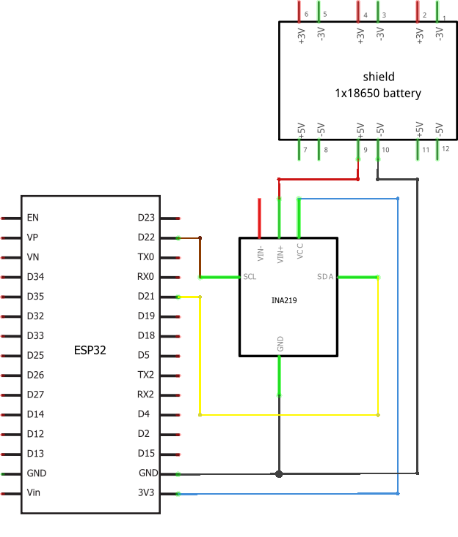
Gambar 1. Diagram Blok Perancangan Sistem



Gambar 2. Skematik Perancangan Sistem Node Pengirim

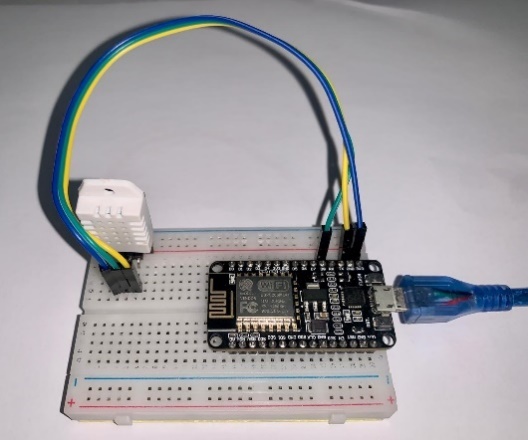


Gambar 3. Skematik Perancangan Sistem Node Penerima

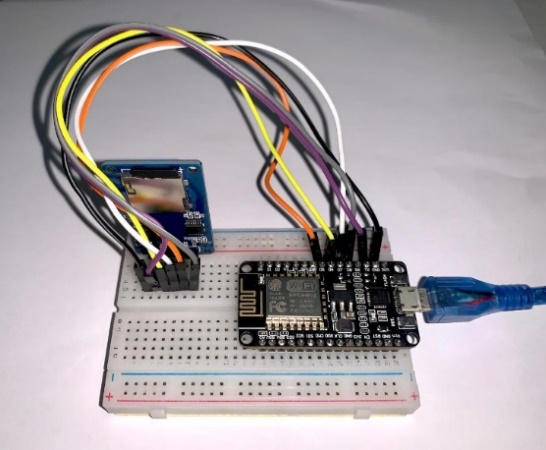


Gambar 4. Skematik Perancangan Sistem Pengukur

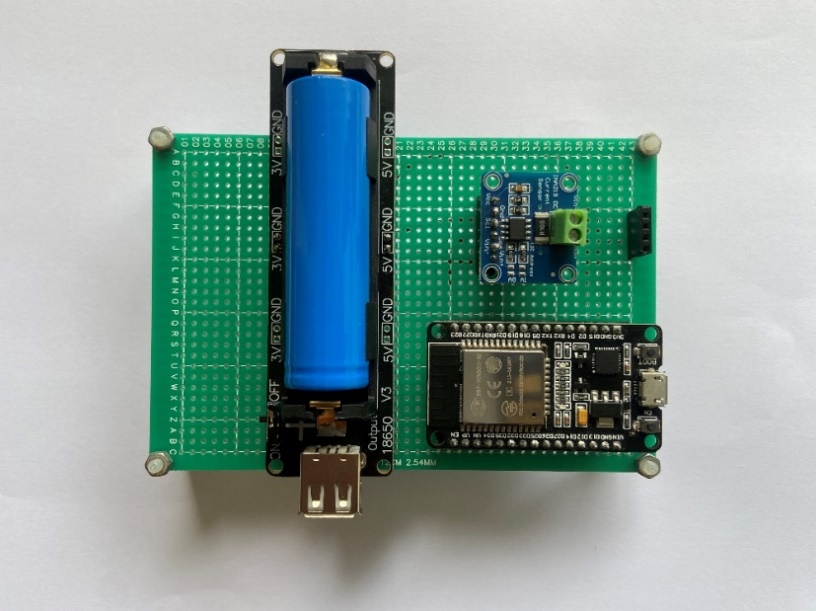
# 2.2 Implementasi Sistem



Gambar 5. Implementasi Sistem Pengirim



Gambar 6. Implementasi Sistem Penerima



Gambar 7. Implementasi Sistem Pengukur Daya

# 3. PENGUJIAN DAN ANALISIS

# 3.1 Pengujian

# 3.2 Analisis

# 4. KESIMPULAN DAN SARAN

# 4.1 Kesimpulan

# 4.2 Saran

# 4. DAFTAR PUSTAKKA

# TABEL DAN GAMBAR

Tabel dan gambar harus diberi nomor dan judul lengkap serta harus diacu dalam tulisan. Contoh: Tabel 1, Tabel 2(a), Gambar 1, Gambar 2(a). Berikut ini diberikan contoh penulisan tabel dan gambar.

## 3.1. Penulisan Tabel

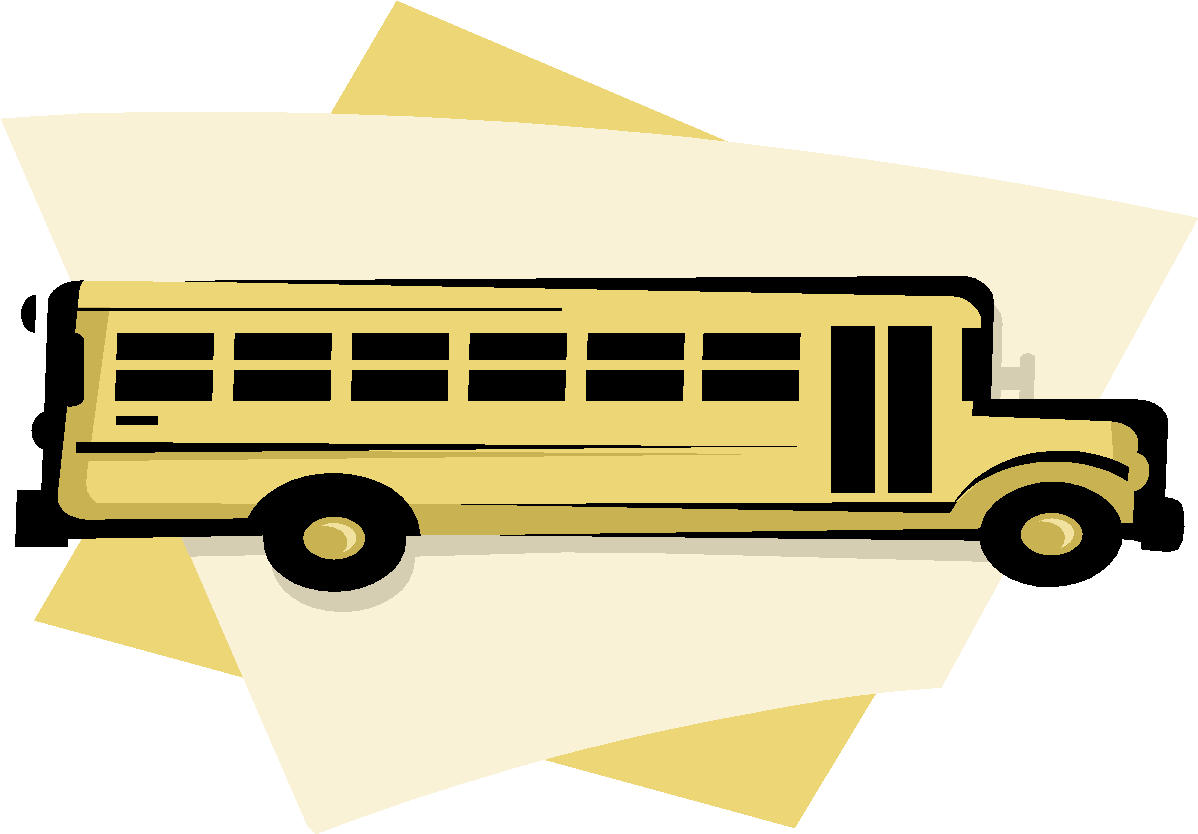
Perhatikan contoh penulisan Tabel 1. Keterangan tabel dituliskan pada bagian atas tabel. Sebisa mungkin hindari penggunaan garis vertikal.

Tabel 1. Rancangan Analisis Komputasi

|  |  |  |
| --- | --- | --- |
| **mesin** | **operasi** | **waktu(menit)** |
| 1 | 5 | 10 |
|  | 4 | 12 |
|  | 4 | 16 |
| 2 | 3 | 18 |
|  | 4 | 20 |

## 3.2. Penggunaan Gambar

Perhatikan contoh penggunaan Gambar 1. Keterangan gambar dituliskan pada bagian bawah gambar.



Gambar 1. Contoh penggunaan gambar

# SUMBER PUSTAKA/RUJUKAN

Sumber pustaka/rujukan sedapat mungkin merupakan pustaka-pustaka terbitan 10 tahun terakhir. Pustaka yang diutamakan adalah sumber-sumber primer berupa laporan penelitian (termasuk Skripsi/Tugas Akhir, Tesis, Disertasi) atau naskah-naskah penelitian dalam jurnal dan/atau majalah ilmiah.

Cara penulisan di daftar pustaka bisa dilihat pada contoh Daftar Pustaka. Sumber pustaka dituliskan terurut alfabetis dan kronologis.

Sumber pustaka yang digunakan bisa berupa:

* makalah jurnal;
* makalah konferensi ilmiah (*proceeding*);
* buku teks;
* laporan penelitian;
* skripsi atau thesis;
* makalah dalam buku kumpulan makalah ilmiah (*book section*).

# ATURAN LAIN

Semua naskah ditelaah secara blind-review oleh mitra bestari (reviewers) yang ditunjuk oleh redaksi menurut bidang kepakarannya. Penulis naskah diberi kesempatan untuk melakukan perbaikan (revisi) naskah atas dasar rekomendasi/saran dari mitra bestari dan redaksi pelaksana. Kepastian pemuatan atau penolakan naskah akan diberitahukan secara tertulis melalui email.

Pemeriksaan dan penyuntingan cetak-coba dikerjakan oleh redaksi dan/atau dengan melibatkan penulis. Naskah yang sudah dalam bentuk cetak-coba dapat dibatalkan pemuatannya oleh redaksi jika diketahui bermasalah.

Segala sesuatu yang menyangkut perijinan pengutipan atau penggunaan software komputer untuk pembuatan naskah atau hal lain yang terkait dengan HAKI yang dilakukan oleh penulis naskah, berikut konsekuensi hukum yang mungkin timbul karenanya, menjadi tanggung jawab penuh penulis naskah tersebut.

# CONTOH DAFTAR PUSTAKA

Dao, S. D. & Marian, R. 2011. Optimisation of precedence-constrained production sequencing and scheduling using genetic algorithms. *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, 16-18 March, Hong Kong.

Gen, M. & Cheng, R. 2000. *Genetic Algorithms and Engineering Optimization.* John Wiley & Sons, Inc., New York.

Liliana, D. Y. & Mahmudy, W. F. 2006. Penerapan Algoritma Genetika pada Otomatisasi Penjadwalan Kuliah. *Laporan Penelitian DPP/SPP.* FMIPA Universitas Brawijaya, Malang.

Marian, R. M., Luong, L. & Dao, S. D. 2012. Hybrid genetic algorithm optimisation of distribution networks—a comparative study. *Dalam:* AO, S. I., CASTILLO, O. & HUANG, X. (editor.) *Intelligent Control and Innovative Computing.* Springer, US.

Phanden, R. K., Jain, A. & Verma, R. 2013. An approach for integration of process planning and scheduling. *International Journal of Computer Integrated Manufacturing*, 26(4), 284-302.

Ridok, A. 2014. Peringkasan dokumen Bahasa Indonesia berbasis non-negative matrix factorization. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 1(1), 39-44.

Tala, F. Z. 2003. A Study of Stemming Effects on Information Retrieval in Bahasa Indonesia. *Ph.D. Thesis*. Universiteit van Amsterdam.

Wang, L. 2007. *Process planning and scheduling for distributed manufacturing.* Springer, London.

Wibawa, A. P., Nafalski, A. & Mahmudy, W. F. 2013. Javanese `speech levels machine translation: improved parallel text alignment based on impossible pair limitation. *IEEE International Conference on Computational Intelligence and Cybernetics*, 3-4 December, Yogyakarta, Indonesia. 16-20.