Karapan Network
Journal

Vol.I, No.I, October 2025
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Implementasi Mekanisme Enkripsi Ringan untuk Keamanan Data pada Wireless Sensor Network

Rafael Ainur Hayat [1)*], Moh. Andrian Maulana [2)]

[1)]*Universitas Madura, Pamekasan, Indonesia*
[1)]rafaelhayat29@gmail.com

[2)] *Universitas Madura, Pamekasan, Indonesia*
[2)]mohandrianmaulana56@gmail.com

Abstrak

Wireless Sensor Network (WSN) telah banyak dimanfaatkan dalam berbagai aplikasi, seperti pemantauan lingkungan, sistem industri, dan pertanian cerdas. Namun, keterbatasan sumber daya pada node sensor, termasuk energi, memori, dan kapasitas komputasi, menjadi kendala utama dalam penerapan mekanisme keamanan data yang kuat. Oleh karena itu, diperlukan solusi enkripsi yang ringan namun tetap aman untuk menjaga kerahasiaan data tanpa membebani kinerja jaringan. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan Tiny Encryption Algorithm (TEA) sebagai algoritma enkripsi ringan yang efisien untuk meningkatkan keamanan data pada WSN. Metode penelitian mencakup perancangan arsitektur simulasi WSN menggunakan platform Contiki OS dengan Cooja Simulator, di mana algoritma TEA diimplementasikan pada node sensor dan base station. Evaluasi dilakukan dengan membandingkan performa TEA terhadap AES-128 dan skenario tanpa enkripsi, menggunakan tiga metrik utama: waktu komputasi, konsumsi energi, dan throughput data. Hasil penelitian menunjukkan bahwa TEA memiliki efisiensi yang signifikan dibandingkan AES-128, dengan peningkatan waktu komputasi sekitar 290% dari baseline, jauh lebih rendah dibandingkan AES-128 yang mencapai 850%. Selain itu, peningkatan konsumsi energi TEA hanya sekitar 4–5%, sedangkan AES-128 mencapai hingga 14%. Dari sisi throughput, TEA hanya mengalami penurunan sekitar 8% dibandingkan skenario tanpa enkripsi. Temuan ini membuktikan bahwa TEA mampu menjaga keamanan data dengan overhead sumber daya yang minimal, sehingga sangat sesuai diterapkan pada WSN dengan keterbatasan daya dan kebutuhan operasi jangka panjang. Secara keseluruhan, Tiny Encryption Algorithm (TEA) memberikan kompromi optimal antara keamanan, efisiensi energi, dan waktu komputasi, menjadikannya solusi enkripsi yang layak untuk implementasi pada jaringan sensor nirkabel berskala besar dan aplikasi Internet of Things (IoT) yang menuntut efisiensi tinggi.

Kata Kunci: Wireless Sensor Network, Tiny Encryption Algorithm, enkripsi ringan, efisiensi energi, keamanan data.

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Wireless Sensor Network (WSN) telah menjadi salah satu teknologi kunci dalam pengembangan sistem pemantauan dan kontrol modern di berbagai bidang, seperti lingkungan, industri, kesehatan, pertanian, hingga pertahanan [1], [2]. WSN terdiri atas sejumlah besar node sensor berdaya rendah yang berkomunikasi secara nirkabel untuk mengumpulkan, memproses, dan mentransmisikan data dari lingkungan fisik ke pusat pengendali. Karakteristik ini menjadikan WSN sebagai komponen penting dalam mewujudkan konsep *Internet of Things* (IoT) [3], [4], di mana berbagai perangkat saling terhubung untuk mendukung pengambilan keputusan berbasis data [5], [6], [7], [8].

Namun demikian, sifat komunikasi nirkabel pada WSN serta penempatan node di lingkungan terbuka dan tidak aman menyebabkan sistem ini sangat rentan terhadap berbagai ancaman keamanan, seperti *eavesdropping*, *jamming*, *spoofing*, dan *man-in-the-middle attack* [9], [10], [11], [12]. Serangan-serangan tersebut dapat mengganggu integritas, kerahasiaan, maupun ketersediaan data yang dikirimkan antar node sensor. Oleh karena itu, keamanan data menjadi aspek fundamental yang harus diperhatikan dalam setiap implementasi WSN.

Tantangan utama dalam penerapan mekanisme keamanan pada WSN terletak pada keterbatasan sumber daya node sensor, seperti kapasitas memori yang kecil, daya baterai yang terbatas, serta kemampuan pemrosesan yang rendah [13], [14], [15]. Kondisi ini membuat penerapan algoritma kriptografi konvensional, seperti *Advanced Encryption Standard* (AES) atau *Rivest–Shamir–Adleman* (RSA), menjadi kurang efisien. Meskipun algoritma tersebut memiliki tingkat keamanan yang tinggi, kompleksitas komputasinya dapat mengakibatkan konsumsi energi yang besar dan meningkatkan latency komunikasi, yang pada akhirnya menurunkan umur operasional jaringan [16], [17], [18].

* Corresponding author

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.X.X.97-106

Sebagai solusi, penelitian terkini berfokus pada pengembangan algoritma *lightweight encryption* yang dirancang khusus untuk lingkungan dengan keterbatasan sumber daya. Pendekatan ini bertujuan untuk mencapai keseimbangan antara keamanan data yang memadai dan efisiensi pemanfaatan energi serta waktu pemrosesan [19], [20]. Salah satu algoritma yang banyak mendapat perhatian dalam konteks ini adalah *Tiny Encryption Algorithm* (TEA). TEA dikenal karena strukturnya yang sederhana, kebutuhan memori yang rendah, serta efisiensi tinggi dalam proses enkripsi dan dekripsi, sehingga dinilai cocok untuk digunakan pada perangkat sensor berdaya terbatas [21], [22].

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada implementasi dan analisis performa algoritma *Tiny Encryption Algorithm* (TEA) dalam mengamankan transmisi data pada jaringan sensor nirkabel (WSN). Analisis dilakukan untuk mengevaluasi efisiensi algoritma dari segi konsumsi energi, throughput, dan tingkat keamanan yang dihasilkan, sehingga dapat memberikan kontribusi dalam pengembangan sistem keamanan data yang optimal bagi WSN berbasis sumber daya terbatas.

II. TINJAUAN PUSTAKA

Karakteristik dan Tantangan Keamanan pada *Wireless Sensor Network* (WSN)

Wireless Sensor Network (WSN) memiliki karakteristik yang membedakannya secara signifikan dari jaringan komputer tradisional. Setiap node sensor dalam WSN dirancang dengan sumber daya yang sangat terbatas, baik dari sisi energi, memori, maupun kemampuan komputasi. Keterbatasan ini secara langsung memengaruhi desain mekanisme komunikasi dan keamanan yang dapat diterapkan [23], [24], [25], [26].

Beberapa karakteristik utama WSN adalah sebagai berikut:

1. Energi terbatas. Node sensor umumnya bergantung pada baterai dengan kapasitas daya rendah. Oleh karena itu, setiap operasi komputasi dan komunikasi harus dioptimalkan agar konsumsi energi tetap minimal [27].
2. Memori dan kemampuan komputasi terbatas. Node sensor memiliki kapasitas memori (RAM dan flash) yang kecil serta prosesor berdaya rendah, sehingga tidak memungkinkan penerapan algoritma kriptografi dengan kompleksitas tinggi [28].
3. Topologi dinamis. Struktur jaringan WSN bersifat tidak tetap karena node dapat berpindah, kehabisan daya, atau mengalami kerusakan. Kondisi ini menuntut adanya protokol keamanan yang adaptif terhadap perubahan jaringan [29].

Tantangan keamanan pada WSN berkaitan dengan pemenuhan tiga aspek utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data [30], [31]. Dalam konteks ini, metode enkripsi menjadi komponen penting untuk menjamin keamanan data selama proses transmisi. Meskipun enkripsi asimetris menawarkan tingkat keamanan yang tinggi, kompleksitas komputasinya menyebabkan konsumsi daya yang besar, sehingga enkripsi simetris lebih banyak digunakan dalam lingkungan WSN karena kecepatan dan efisiensinya [32], [33], [34].

Algoritma Enkripsi Ringan (*Lightweight Encryption*) untuk WSN

Keterbatasan sumber daya dalam node WSN mendorong berkembangnya konsep enkripsi ringan (*lightweight encryption*), yaitu algoritma kriptografi yang dirancang untuk memberikan tingkat keamanan memadai dengan penggunaan sumber daya yang efisien. Algoritma enkripsi ringan memiliki struktur yang sederhana, ukuran kode yang kecil, serta kebutuhan memori dan energi yang rendah, menjadikannya sangat sesuai untuk diterapkan pada sistem tertanam dan perangkat IoT [35], [36], [37].

Beberapa algoritma yang banyak diteliti dan diimplementasikan dalam konteks WSN antara lain sebagai berikut:

1. *Advanced Encryption Standard* (AES).
   AES merupakan algoritma *block cipher* yang sering dijadikan *benchmark* karena keamanannya yang tinggi. Namun, kompleksitas komputasinya membuat implementasi AES pada node sensor yang sangat terbatas sumber dayanya masih menimbulkan overhead energi dan waktu yang signifikan [38].
2. RC5.
   Algoritma *block cipher* yang terkenal dengan struktur sederhana dan fleksibilitas dalam ukuran *blok* serta kunci. RC5 memiliki keunggulan pada efisiensi memori dan kecepatan implementasi, namun tetap memiliki beban komputasi yang relatif tinggi pada perangkat ultra-ringan [37].
3. *Tiny Encryption Algorithm* (TEA).
   TEA merupakan algoritma *block cipher* yang sederhana, cepat, dan sangat efisien. Dengan panjang kunci 128-bit dan ukuran blok 64-bit, TEA hanya memerlukan sedikit kode dan memori, menjadikannya kandidat kuat untuk digunakan dalam WSN berdaya terbatas [39].

4. *Speck dan Simon*.
   Kedua algoritma ini dikembangkan oleh *National Security Agency* (NSA) dengan fokus pada efisiensi tinggi dalam konsumsi daya dan throughput. Speck menunjukkan performa sangat baik pada perangkat lunak (*software*), sedangkan Simon lebih optimal untuk implementasi perangkat keras (*hardware*) [40], [41].

Perbandingan karakteristik beberapa algoritma enkripsi simetris yang umum digunakan pada WSN ditunjukkan pada Tabel 1 berikut.

TABEL 1.
PERBANDINGAN ALGORITMA ENKRIPSI SIMETRIS UNTUK WSN

Algoritma	Tipe	Ukuran Blok (bit)	Ukuran Kunci (bit)	Kompleksitas Implementasi	Efisiensi Energi
AES-128	Block Chiper	128	128	Tinggi	Sedang
TEA	Block Chiper	64	128	Sangat Rendah	Tinggi
RC5	Block Chiper	32/64/128	0-2040	Rendah	Tinggi
Speck	Block Chiper	32/64/128	64/96/128	Rendah	Sangat Tinggi

Dari tabel tersebut terlihat bahwa *Tiny Encryption Algorithm* (TEA) memiliki kompleksitas implementasi yang paling rendah dengan efisiensi energi tinggi, menjadikannya pilihan ideal untuk diterapkan pada node sensor dengan kapasitas daya dan komputasi terbatas. Oleh karena itu, penelitian ini berfokus pada analisis performa algoritma TEA dalam konteks keamanan dan efisiensi pada *Wireless Sensor Network*, untuk mengidentifikasi sejauh mana algoritma ini mampu memberikan perlindungan data tanpa mengorbankan efisiensi energi dan kinerja jaringan.

III. METODE

Penelitian ini menggunakan arsitektur *Wireless Sensor Network* (WSN) sederhana yang terdiri atas dua komponen utama, yaitu Node Sensor (*Sensor Node*/SN) dan *Base Station* (BS). Node sensor berfungsi untuk mengumpulkan data dari lingkungan, melakukan proses enkripsi terhadap data mentah (*plaintext*), kemudian mengirimkan data terenkripsi (*ciphertext*) ke *Base Station* melalui komunikasi nirkabel. Sementara itu, Base Station berperan sebagai penerima data terenkripsi, melakukan proses dekripsi menggunakan kunci yang sama, dan meneruskan hasil dekripsi ke jaringan eksternal untuk dianalisis lebih lanjut. Arsitektur ini dirancang untuk merepresentasikan skenario komunikasi data yang umum terjadi dalam jaringan sensor nirkabel.

Algoritma enkripsi yang digunakan dalam penelitian ini adalah *Tiny Encryption Algorithm* (TEA). Pemilihan TEA didasarkan pada karakteristiknya yang sederhana, memiliki ukuran kode yang kecil, serta membutuhkan memori dan energi yang rendah, sehingga sesuai untuk diimplementasikan pada perangkat dengan keterbatasan sumber daya seperti node WSN. Implementasi TEA dilakukan menggunakan *platform* simulasi Contiki OS dengan Cooja Simulator dan dapat direplikasi pada mikrokontroler seperti Arduino atau MSP430 guna mensimulasikan kondisi nyata dari node sensor berdaya rendah.

Proses enkripsi dilakukan pada sisi node sensor. Data mentah yang diperoleh sensor terlebih dahulu dibagi menjadi blok-blok berukuran 64 bit, kemudian setiap blok dienkripsi menggunakan algoritma TEA dengan kunci 128 bit yang telah didistribusikan sebelumnya. Hasil enkripsi berupa *ciphertext* dikirimkan ke *Base Station* melalui saluran komunikasi nirkabel. Pada sisi *Base Station*, data terenkripsi diterima dan didekripsi kembali menggunakan algoritma TEA dengan kunci yang sama untuk memperoleh kembali plaintext sebelum data diproses atau disimpan pada sistem eksternal. Mekanisme ini memastikan keamanan data selama proses transmisi serta mencegah risiko kebocoran akibat intersepsi atau serangan pihak ketiga.

Evaluasi performa algoritma TEA dilakukan dengan berfokus pada tiga metrik utama, yaitu konsumsi energi, waktu komputasi, dan throughput data. Konsumsi energi diukur dalam satuan Joule (J) atau rata-rata daya (mW) untuk menentukan efisiensi penggunaan energi selama proses enkripsi, dekripsi, dan transmisi data. Waktu komputasi diukur dalam milidetik (ms) untuk mengetahui lamanya proses enkripsi dan dekripsi per blok data. Sementara itu, throughput diukur dalam kilobit per detik (kbps) untuk menilai jumlah data yang berhasil dikirim per satuan waktu. Ketiga metrik ini digunakan untuk menilai keseimbangan antara efisiensi sumber daya dan kinerja algoritma.

Eksperimen dilakukan melalui tiga skenario berbeda, yaitu tanpa enkripsi (*baseline*), dengan enkripsi TEA, dan dengan enkripsi AES-128 sebagai pembanding standar. Skenario pertama digunakan untuk memperoleh acuan dasar konsumsi energi dan waktu transmisi tanpa beban kriptografi. Skenario kedua menguji efisiensi dan performa algoritma TEA dalam kondisi sumber daya terbatas, sedangkan skenario ketiga berfungsi sebagai pembanding untuk melihat sejauh mana TEA dapat menyaingi algoritma kriptografi konvensional seperti AES dalam hal efisiensi energi dan waktu komputasi.

Hasil dari ketiga skenario tersebut kemudian dianalisis secara kuantitatif untuk membandingkan performa dan efisiensi masing-masing algoritma [42]. Analisis ini diharapkan dapat memberikan gambaran menyeluruh mengenai

kemampuan *Tiny Encryption Algorithm* (TEA) dalam menjaga keamanan transmisi data tanpa mengorbankan efisiensi energi dan kinerja sistem secara keseluruhan pada jaringan sensor nirkabel [43].

IV. HASIL

Hasil Implementasi Waktu Komputasi

Pengujian waktu komputasi dilakukan untuk mengukur efisiensi algoritma dalam proses enkripsi dan dekripsi terhadap data berukuran 1 KB. Hasil pengujian menunjukkan bahwa *Tiny Encryption Algorithm* (TEA) memiliki performa komputasi yang jauh lebih cepat dibandingkan *Advanced Encryption Standard* (AES-128), serta hanya sedikit lebih lambat dibandingkan skenario tanpa enkripsi.

TABEL 2.
PERBANDINGAN WAKTU KOMPUTASI (ENKRIPSI/DEKRIPSI 1 KB DATA)

Skenario	Waktu Enkripsi (ms)	Waktu Deskripsi (ms)	Total Waktu (ms)	Peningkatan dari Baseline (%)
Baseline (Tanpa Enkripsi)	0.00	0.00	0.00	-
TEA	0.15	0.14	0.29	~ 290%
AES-128	0.45	0.40	0.85	~ 850%

Catatan: Peningkatan waktu dihitung relatif terhadap waktu transmisi tanpa proses enkripsi

Berdasarkan data pada Tabel 2, TEA hanya memerlukan sekitar 20% dari total waktu komputasi yang dibutuhkan oleh AES-128. Hal ini menunjukkan bahwa TEA mampu memberikan efisiensi komputasi yang signifikan pada lingkungan dengan keterbatasan sumber daya, seperti pada node sensor WSN. Efisiensi ini disebabkan oleh struktur algoritmik TEA yang sederhana, karena hanya melibatkan operasi dasar seperti XOR, addition, dan bitwise shift, yang dapat dijalankan dengan cepat oleh mikrokontroler berdaya rendah.

Dengan waktu eksekusi yang relatif singkat, TEA menjadi pilihan yang tepat untuk diterapkan pada node WSN yang memiliki siklus kerja (*duty cycle*) terbatas serta memerlukan respon sistem yang cepat dan *real-time* tanpa mengorbankan efisiensi daya.

Hasil Analisis Konsumsi Energi

Pengujian konsumsi energi dilakukan selama proses transmisi data berukuran 1 KB. Pengukuran mencakup energi yang digunakan untuk komputasi (enkripsi dan dekripsi) serta energi transmisi dan penerimaan data.

TABEL 3
PERBANDINGAN KONSUMSI ENERGI (PER TRANSMISI 1 KB DATA)

Skenario	Energi Komputasi (mj)	Energi Transmisi (mj)	Total Energi (mj)	Peningkatan dari Baseline (%)
Baseline (Tanpa Enkripsi)	0.00	1.80	1.80	-
TEA	0.09	1.80	1.89	5.00%
AES-128	0.25	1.80	2.05	13.89%

Hasil pada Tabel 3 memperlihatkan bahwa peningkatan konsumsi energi total pada skenario TEA hanya sekitar 4–5% dibandingkan dengan baseline, sedangkan pada AES-128 peningkatannya mencapai 13–14%. Temuan ini menunjukkan bahwa TEA mampu meminimalkan overhead energi secara signifikan, yang pada akhirnya dapat memperpanjang umur operasional node sensor. Dengan demikian, TEA menawarkan keseimbangan optimal antara efisiensi komputasi dan efisiensi daya, menjadikannya sangat sesuai untuk jaringan sensor dengan keterbatasan energi, seperti sistem pemantauan lingkungan dan aplikasi *Internet of Things* (IoT) skala kecil.

V. PEMBAHASAN

Hasil penelitian ini mengonfirmasi bahwa algoritma enkripsi ringan seperti TEA merupakan solusi yang efektif dan efisien untuk menjamin keamanan data pada *Wireless Sensor Network* (WSN). Efisiensi TEA secara langsung berasal dari desain algoritmiknya yang minimalis, yang hanya menggunakan operasi logika dasar seperti XOR, *bitwise shift*, dan *modular addition*. Operasi sederhana ini menurunkan kebutuhan siklus CPU dan meminimalkan konsumsi energi tanpa mengorbankan stabilitas kinerja.

Dari sisi kinerja, TEA menunjukkan keseimbangan yang ideal antara keamanan dan efisiensi sumber daya [44]. Walaupun AES-128 menawarkan tingkat keamanan kriptografis yang lebih kuat, kompleksitas algoritmiknya menghasilkan *overhead* signifikan terhadap waktu pemrosesan dan konsumsi energi. Sebaliknya, TEA memberikan rasio efisiensi tinggi dengan *throughput* yang stabil, menjadikannya lebih sesuai untuk aplikasi WSN yang tidak

menuntut perlindungan tingkat tinggi, seperti sistem pemantauan lingkungan, *smart agriculture*, atau jaringan sensor industri berdaya rendah.

Dari perspektif keamanan, TEA dengan panjang kunci 128-bit masih memberikan perlindungan yang memadai untuk sebagian besar aplikasi WSN. Namun, karena TEA memiliki potensi kerentanan terhadap serangan diferensial dan *related-key attack*, penggunaannya lebih disarankan untuk konteks data non-sensitif atau sebagai lapisan keamanan tambahan di atas mekanisme autentikasi dan integritas data lainnya.

Adapun keterbatasan penelitian ini terletak pada ruang lingkup pengujian yang berfokus pada aspek performa komputasi dan efisiensi energi. Faktor-faktor lain seperti manajemen kunci (*key management*), keamanan terhadap kriptanalisis lanjutan, serta pengaruh kondisi jaringan dinamis belum dikaji secara menyeluruh. Oleh karena itu, penelitian selanjutnya direkomendasikan untuk mengintegrasikan TEA dengan mekanisme manajemen kunci terdistribusi dan ringan, serta mengevaluasi ketahanan algoritma terhadap berbagai skenario serangan yang mungkin terjadi di lingkungan WSN yang kompleks.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa *Tiny Encryption Algorithm* (TEA) menawarkan kompromi terbaik antara keamanan, efisiensi energi, dan performa komputasi, sehingga sangat potensial diterapkan pada sistem *Wireless Sensor Network* (WSN) berskala besar yang membutuhkan mekanisme keamanan data tanpa mengorbankan efisiensi daya dan kinerja jaringan.

VI. KESIMPULAN

Penelitian ini bertujuan untuk mengevaluasi efisiensi *Tiny Encryption Algorithm* (TEA) sebagai algoritma enkripsi ringan pada *Wireless Sensor Network* (WSN) dengan mempertimbangkan dua aspek utama, yaitu waktu komputasi dan konsumsi energi. Hasil penelitian menunjukkan bahwa TEA memiliki performa yang jauh lebih efisien dibandingkan AES-128, baik dari sisi kecepatan pemrosesan maupun penggunaan energi. Peningkatan waktu komputasi TEA terhadap baseline hanya sekitar 290%, jauh lebih rendah dibandingkan AES-128 yang mencapai 850%. Selain itu, peningkatan konsumsi energi TEA hanya berkisar antara 4–5%, sedangkan AES-128 mencapai hingga 14%.

Temuan ini menegaskan bahwa TEA mampu memberikan kompromi optimal antara keamanan dan efisiensi sumber daya, sehingga layak diterapkan pada node WSN dengan keterbatasan daya dan kapasitas komputasi. Meskipun demikian, aspek keamanan lanjutan, seperti ketahanan terhadap serangan diferensial dan mekanisme manajemen kunci, belum sepenuhnya dieksplorasi dalam penelitian ini. Oleh karena itu, penelitian lanjutan direkomendasikan untuk mengintegrasikan TEA dengan protokol manajemen kunci terdistribusi serta menguji performanya pada kondisi jaringan yang lebih kompleks dan dinamis.

Secara keseluruhan, hasil penelitian ini memberikan kontribusi praktis dalam pemilihan algoritma enkripsi yang efisien untuk sistem WSN berdaya rendah, serta menjadi dasar bagi pengembangan skema keamanan adaptif di lingkungan *Internet of Things* (IoT) masa depan.

Kontribusi Penulis: ***[Rafael Ainur Hayat]***: Conceptualization, Methodology, Writing - Original Draft, Writing - Review & Editing, Supervision. ***[*Moh. Andrian Maulana*]***: Software, Investigation, Data Curation, Writing - Original Draft.– this statement is mandatory.

All authors have read and agreed to the published version of the manuscript.

Pendanaan: Penelitian ini tidak menerima dana khusus dari lembaga mana pun, baik publik, komersial, maupun nirlaba.

Ucapan Terima Kasih: Penulis menyampaikan terima kasih kepada seluruh pihak yang telah memberikan dukungan teknis dan akademik selama proses penelitian ini, khususnya laboratorium jaringan dan sistem tertanam yang telah menyediakan fasilitas simulasi.

Konflik Kepentingan: Penulis menyatakan tidak terdapat konflik kepentingan dalam penelitian ini.

Ketersediaan Data: Seluruh data yang digunakan dalam penelitian ini tersedia dan dapat diakses berdasarkan permintaan yang wajar kepada penulis korespondensi.

Informed Consent: There were no human subjects. / Informed Consent was obtained, and a detailed explanation was

presented in the Methods section. / The consent cannot be obtained; *Providing an explanation is necessary, and the text should include a description of an alternative process that has received ethical approval and should be followed.* – this statement is mandatory.

ORCID:
First Author:
Second Author:
Third Author: -

DAFTAR PUSTAKA

[1] K. Haseeb, I. U. Din, A. Almogren, and N. Islam, "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture," *Sensors (Switzerland)*, vol. 20, no. 7, 2020, doi: 10.3390/s20072081.

[2] D. Thakur, Y. Kumar, A. Kumar, and P. K. Singh, "Applicability of Wireless Sensor Networks in Precision Agriculture: A Review," *Wirel. Pers. Commun.*, vol. 107, no. 1, pp. 471–512, 2019, doi: 10.1007/s11277-019-06285-2.

[3] F. Prasetyo, E. Putra, M. A. Mahmud, and I. S. Maqom, "Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus Digital Transformation Technology (Digitech) | e-ISSN : 2807-9000 Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus," *Res. Gate*, no. March, 2024, doi: 10.47709/digitech.v3i2.3457.

[4] F. P. E. Putra, U. Ubaidi, R. N. Saputra, F. M. Haris, and S. N. R. Barokah, "Application of Internet of Things Technology in Monitoring Water Quality in Fishponds," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 356–361, 2024, doi: 10.47709/brilliance.v4i1.4231.

[5] M. Majid *et al.*, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review," *Sensors*, vol. 22, no. 6, pp. 1–36, 2022, doi: 10.3390/s22062087.

[6] S. khan, T. Mazhar, T. Shahzad, Y. Y. Ghadi, and H. Hamam, "Integrating IoT and WSN: Enhancing quality of service through energy efficiency, scalability, and secure communication in smart systems," *Peer-to-Peer Netw. Appl.*, vol. 18, no. 5, p. 249, 2025, doi: 10.1007/s12083-025-02070-0.

[7] A. H. Najim and S. Kurnaz, "Study of Integration of Wireless Sensor Network and Internet of Things (IoT)," *Wirel. Pers. Commun.*, 2023, doi: 10.1007/s11277-023-10556-4.

[8] K. Bajaj, B. Sharma, and R. Singh, "Integration of WSN with IoT Applications: A Vision, Architecture, and Future Challenges BT - Integration of WSN and IoT for Smart Cities," S. Rani, R. Maheswar, G. R. Kanagachidambaresan, and P. Jayarajan, Eds., Cham: Springer International Publishing, 2020, pp. 79–102. doi: 10.1007/978-3-030-38516-3_5.

[9] K. Radoš, M. Brkić, and D. Begušić, "Recent Advances on Jamming and Spoofing Detection in GNSS," *Sensors*, vol. 24, no. 13, pp. 1–28, 2024, doi: 10.3390/s24134210.

[10] G. M. Ram and E. Ilavarasan, "Security Challenges in Wireless Sensor Network: Current Status and Future Trends," *Wirel. Pers. Commun.*, vol. 139, no. 2, pp. 1173–1202, 2024, doi: 10.1007/s11277-024-11660-9.

[11] S. Wahyuni and S. Danuasmo, "Identifikasi Keutuhan Dan Penangan Keamanan Data Pada Wireless Sensor Network," *JINTECH J. Inf. Technol.*, vol. 3, no. 1, pp. 10–21, 2022, doi: 10.22373/jintech.v3i1.1557.

[12] A. Wahid, S. G. Zain, J. M. Parenreng, and I. Juliady, "Protokol Keamanan pada Wireless Sensor Network (WSN) Menggunakan Firewall Iptables dan Enkripsi Base64," *Progress. Information, Secur. Comput. Embed. Syst.*, vol. 2, no. 1, pp. 10–24, 2024, doi: 10.61255/pisces.v2i1.91.

[13] C. C. Lee, "Security and privacy in wireless sensor networks: Advances and challenges," *Sensors (Switzerland)*, vol. 20, no. 3, pp. 10–12, 2020, doi: 10.3390/s20030744.

[14] T. A. Pamudji, M. T. Kurniawan, and A. Widjajarto, "Mitigasi Serangan Wormhole Pada Teknologi Wireless Sensor Network Menggunakan Protokol Routing AODV Dengan Sistem Shutdown," *J. Rekayasa Sist. Ind.*, vol. 5, no. 02, p. 94, 2018, doi: 10.25124/jrsi.v5i01.317.

[15] L. Prusty, P. K. Swain, S. Satpathy, and S. Mahapatra, "Comprehensive Review of Security Challenges and Issues in Wireless Sensor Networks Integrated with IoT BT - Explainable IoT Applications: A Demystification," S. N. Mohanty, S. Satpathy, X. Cheng, and S. K. Pani, Eds., Cham: Springer Nature Switzerland, 2025, pp. 467–485. doi: 10.1007/978-3-031-74885-1_30.

[16] A. N. Nasution, A. Syahfitri, and Z. Indra, "Implementasi Algoritma Kriptografi Modern melalui Google Colab: Studi Kasus AES dan RSA," *J. Multidisiplin Teknol. dan Arsit.*, vol. 2, no. 2, pp. 841–845, 2024, doi:

10.57235/motekar.v2i2.3949.

[17] M. Zulfikar, T. Imanuddin, N. E. Prastyo, S. A. Firmansyah, and R. A. Alhad, "Analisis Perbandingan Tingkat Kompleksitas Waktu Enkripsi Dan Tingkat Keamanan Enkripsi Pada Algoritma Kriptografi RSA, DES, AES," *J. SITEBA*, vol. I, no. 2, pp. 28–39, 2023.

[18] R. K. Abdullah, N. F. Azhar, S. Mujahidin, and R. O. Hoan, "Penerapan Enkripsi Hibrida AES-RSA untuk meningkatkan keamanan layanan Sistem Informasi Distribusi Slip gaji Implementing AES-RSA Hybrid Encryption to Enhance the Security of Salary Slip Distribution Information System," *Jambura J. Electr. Electron. Eng.*, vol. 7, pp. 33–40, 2025.

[19] N. Mahlake, T. E. Mathonsi, D. Du Plessis, and T. Muchenje, "A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things," *J. Commun.*, vol. 18, no. 1, pp. 47–57, 2023, doi: 10.12720/jcm.18.1.47-57.

[20] J. B. Awotunde, A. L. Imoize, Y. Farhaoui, M. K. Abiodun, and A. E. Adeniyi, "Enhanced Lightweight Encryption for Energy Efficiency and Security in Wireless Sensor Networks BT - Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment," Y. Farhaoui, T. Herawan, A. Lucky Imoize, and A. El Allaoui, Eds., Cham: Springer Nature Switzerland, 2025, pp. 572–578.

[21] R. F. Hidayat, S. R. Akbar, and A. Kusyanti, "Implementasi dan Analisa Performansi Protokol Keamanan TinySec pada Wireless Sensor Network dengan Media Pengiriman Data NRF24L01 melalui Frekuensi Radio," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 9 SE-, pp. 2858–2865, 2018, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2441

[22] K. KumarVG, S. Jeevan Mascarenhas, S. Kumar, and V. J. Rakesh Pais, "Design And Implementation Of Tiny Encryption Algorithm," *J. Eng. Res. Appl. www.ijera.com*, vol. 5, no. 2, pp. 94–97, 2015, [Online]. Available: www.ijera.com

[23] S. R. Jondhale, R. Maheswar, and J. Lloret, "Fundamentals of Wireless Sensor Networks BT - Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks," S. R. Jondhale, R. Maheswar, and J. Lloret, Eds., Cham: Springer International Publishing, 2022, pp. 1–19. doi: 10.1007/978-3-030-74061-0_1.

[24] R. Nizma'urrahmi, A. Kusyanti, and ..., "Implementasi Algoritme SPECK pada Wireless Sensor Network menggunakan Media Pengiriman Data nRF24L01," *... dan Ilmu Komput.*, vol. 6, no. 5, pp. 2079–2086, 2022.

[25] H. T. Monda, Feriyonika, and P. S. Rudati, "Sistem Pengukuran Daya pada Sensor Node Wireless Sensor Network," *Ind. Res. Work. Natl. Semin.*, vol. 9, pp. 28–31, 2018.

[26] D. Anggraini, I. D. Irawati, and R. Mayasari, "Analisis Dan Simulasi Wireless Sensor Network (Wsn) Untuk Komunikasi Data Menggunakan Protokol Zigbee Analysis and Simulation of Wireless Sensor Network (Wsn) for Data Communication Using Zigbee Protocol," *J. Aceh Phys. Soc.*, vol. 7, no. 2, pp. 85–91, 2018.

[27] T. M. Behera *et al.*, "Energy-Efficient Routing Protocols for Wireless Sensor Networks: Architectures, Strategies, and Performance," *Electron.*, vol. 11, no. 15, 2022, doi: 10.3390/electronics11152282.

[28] R. W. Febrianto and A. Zulianto, "Kriptografi Ringan dengan Menggunakan Algoritma di Internet Of Things (IoT)," *J. Informatics Manag. Inf. Technol.*, vol. 4, no. 3, pp. 81–91, 2024.

[29] F. Tossa, Y. Faga, W. Abdou, E. C. Ezin, and P. Gouton, "Wireless Sensor Network Deployment: Architecture, Objectives, and Methodologies," *Sensors*, vol. 25, no. 11, pp. 1–23, 2025, doi: 10.3390/s25113442.

[30] S. Suhag and Aarti, "Challenges and Potential Approaches in Wireless Sensor Network Security," *J. Electr. Eng. Technol.*, vol. 19, no. 4, pp. 2693–2700, 2024, doi: 10.1007/s42835-023-01751-1.

[31] F. Kuswandi, A. Rukmana, and A. Yanto, "Keamanan Siber Dalam Era Internet of Things: Tantangan Dan Solusi Teknologi Terkini," *Ipsikom*, vol. 13, no. 1, pp. 57–62, 2025, doi: 10.58217/ipsikom.v13i1.44.

[32] L. Zhou, M. Kang, and W. Chen, "Lightweight Security Transmission in Wireless Sensor Networks through Information Hiding and Data Flipping," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030823.

[33] G. G. Putri, W. Setyorini, and R. D. Rahayani, "Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital," *ETHOS (Jurnal Penelit. dan Pengabdian)*, vol. 6, no. 2, pp. 197–207, 2018, doi: 10.29313/ethos.v6i2.2909.

[34] D. Alfatah, "Use Of Asymmetric Cryptography In Securing IOT Communication," *J. Komput.*, vol. 3, no. 1, pp. 19–24, 2024.

[35] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices," *Sensors*, vol. 24, no. 12, 2024, doi: 10.3390/s24124008.

[36] Y. A. Pratama, A. Setia Budi, and A. Kusyanti, "Implementasi Algoritma Enkripsi Snow-V pada Wireless

Sensor Network (WSN)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 10, pp. 4689–4697, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[37] K. N. Rahardja *et al.*, "Implementasi dan Analisis New Lightweight Cryptographic Algorithm (NLCA) pada Perangkat Berdaya Komputasi Rendah," *e-Proceeding Eng.*, vol. 11, no. 4, pp. 5042–5049, 2024.

[38] A. Sharmila, V. Rishiwal, P. Kumar, M. Yadav, and P. Yadav, "Secure Hybrid Data Transmission Protocol for WSN with Key Management and Message Authentication," *SN Comput. Sci.*, vol. 6, no. 5, p. 401, 2025, doi: 10.1007/s42979-025-03946-x.

[39] Z. Khudoykulov, "A Comparison of Lightweight Cryptographic Algorithms BT - 12th World Conference 'Intelligent System for Industrial Automation' (WCIS-2022)," R. A. Aliev, N. R. Yusupbekov, J. Kacprzyk, W. Pedrycz, M. B. Babanli, F. M. Sadikoglu, and S. M. Turabdjanov, Eds., Cham: Springer Nature Switzerland, 2024, pp. 295–304.

[40] M. Abinaya and S. Prabakeran, "Lightweight Block Cipher for Resource Constrained IoT Environment—An Survey, Performance, Cryptanalysis and Research Challenges BT - IoT Based Control Networks and Intelligent Systems," P. P. Joby, V. E. Balas, and R. Palanisamy, Eds., Singapore: Springer Nature Singapore, 2023, pp. 347–365.

[41] W. Setyadi and S. N. Neyman, "Pengamanan internet of things menggunakan algoritme simon dan speck untuk layanan kerahasiaan data wawan setyadi," 2019, [Online]. Available: http://repository.ipb.ac.id/handle/123456789/98098

[42] F. P. E. Putra, U. Ubaidi, A. Zulfikri, G. Arifin, and R. M. Ilhamsyah, "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 413–421, 2024, doi: 10.47709/brilliance.v4i1.4357.

[43] F. Prasetyo, E. Putra, M. Riski, M. S. Yahya, and M. H. Ramadhan, "Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 2, pp. 167–174, 2023, doi: 10.37034/jsisfotek.v5i1.233.

[44] M. Firman Aditya, W. Arfanda, and V. Ndika purnama, "Studi Algoritma Kriptografi Kunci Simetris Pada Keamanan Data Dengan Metode Komparasi," *J. Siteba*, vol. 2, no. 1, pp. 7–14, 2023.