Karapan Network
Journal

Vol.2, No.01, Januari. 2026
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Penerapan Algoritma Enkripsi Efisien untuk Melindungi Data pada Jaringan Sensor Nirkabel yang Terintegrasi dengan IoT

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

[1)2)] *Universitas Madura, Pamekasan, Indonesia*

[1)]mohandrianmaulana56@gmail.com, [2)]rafaelhayat29@gmail.com

Abstract

Wireless Sensor Network (WSN) memiliki banyak aplikasi dalam dunia Internet of Things (IoT), mulai dari pemantauan lingkungan hingga pertanian cerdas dan sistem kesehatan. Meskipun demikian, WSN memiliki tantangan utama dalam hal keamanan data karena keterbatasan sumber daya yang dimiliki oleh node sensor, seperti daya, kapasitas pemrosesan, dan memori. Untuk itu, diperlukan algoritma enkripsi yang efisien yang dapat menjaga kerahasiaan data tanpa membebani sumber daya secara berlebihan. Salah satu solusi yang banyak dipertimbangkan adalah penggunaan Tiny Encryption Algorithm (TEA). Penelitian ini bertujuan untuk menganalisis implementasi algoritma enkripsi TEA pada WSN berbasis IoT dan membandingkannya dengan AES-128 dari segi efisiensi energi dan waktu komputasi. Hasil penelitian menunjukkan bahwa TEA memiliki keunggulan dalam hal efisiensi energi dan waktu komputasi yang lebih baik dibandingkan dengan AES-128, menjadikannya solusi ideal untuk aplikasi WSN yang memiliki sumber daya terbatas.

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

Article history: Received 5 September 2025, first decision 22 September 2025, accepted 22 Desember 2025, available online 28 Desember 2025

I. PENDAHULUAN

Jaringan Sensor Nirkabel (WSN) merupakan teknologi fundamental yang mendukung berbagai aplikasi terkait Internet of Things (IoT). WSN terbentuk dari kumpulan node sensor yang bertugas mengumpulkan informasi dari lingkungan sekitar dan mentransmisikannya melalui saluran nirkabel. Node-node tersebut biasanya diposisikan di area terpencil dari infrastruktur pokok, dan mampu mengukur parameter lingkungan beragam seperti suhu, kelembaban, atau intensitas cahaya[1], [2], [3]. Salah satu implementasi praktis WSN terlihat dalam pertanian pintar, tempat sensor jaringan memadukan kondisi lahan dan tumbuhan. Lebih lanjut, WSN diterapkan dalam pengawasan lingkungan untuk menilai kualitas atmosfer atau suhu, serta dalam bidang kesehatan untuk melacak status pasien melalui alat medis yang terintegrasi. Efektivitas aplikasi-aplikasi ini sangat ditentukan oleh kinerja dan produktivitas WSN dalam menyampaikan data dengan presisi dan waktu yang tepat.

Meski demikian, seiring meluasnya pemanfaatan WSN, isu keamanan informasi muncul sebagai tantangan besar. Informasi yang dikirim melalui jaringan ini sering kali bersifat sangat rahasia, seperti detail kesehatan pribadi atau data lingkungan krusial. Akibatnya, perlindungan data yang dikirim menjadi masalah yang tidak bisa dianggap remeh. Informasi yang tidak diamankan secara mampu rentan terhadap beragam ancaman, termasuk penyadapan (menguping), di mana entitas tidak sah bisa mengakses data yang dikirim, serta serangan man-in-the-middle, di mana data yang dikirim dapat diubah oleh pihak luar tanpa diketahui oleh pengirim atau penerima[4], [5].

Hambatan pokok dalam mengamankan data di WSN berbasis IoT adalah batasan sumber daya pada sensor node. Node sensor umumnya berjalan dengan baterai terbatas, memiliki kemampuan pemrosesan rendah, serta penyimpanan terbatas. Dengan kondisi ini, meskipun enkripsi algoritma seperti AES-128 memberikan tingkat keamanan tinggi, penerapannya menjadi tidak praktis di WSN yang memiliki batasan tersebut. AES-128 memerlukan banyak sumber daya pemrosesan dan konsumsi energi yang besar, yang dapat mengganggu kinerja jaringan, khususnya dalam aplikasi IoT yang bergantung pada baterai terbatas.

Untuk menangani masalah ini, diperlukan pendekatan enkripsi yang lebih sederhana dan hemat dalam penggunaan energi serta pemrosesan. Salah satu algoritma enkripsi ringan yang cocok untuk WSN berbasis IoT adalah Tiny Encryption Algorithm (TEA). TEA dibuat dengan kunci 128-bit dan blok data 64-bit, menjadikannya

* Moh Andrian Maulana

ISSN 2443-2xxx (online) 2598-6xxx (print) © 2026 The Authors. Published by Omah Tabing.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)
doi: http://dx.doi.org/10.20473/KNJ.2.01.33-44

lebih efisien dibandingkan algoritma lain seperti AES. Meskipun memberikan keamanan yang lebih rendah daripada AES, TEA cukup ampuh dalam menjaga kerahasiaan data dengan mengurangi pemanfaatan sumber daya seperti energi baterai dan kapasitas pemrosesan yang terbatas[6], [7], [8], [9], [10].

Studi ini bertujuan untuk mengkaji implementasi TEA di WSN berbasis IoT dan membandingkannya dengan AES-128 terkait efisiensi energi dan durasi komputasi. Simulasi akan dilakukan menggunakan platform Contiki OS dan Cooja Simulator untuk mengilustrasikan kinerja masing-masing enkripsi enkripsi dalam konteks WSN. Penelitian ini akan mengukur parameter kunci, seperti waktu yang diperlukan untuk enkripsi dan dekripsi data, serta penggunaan energi selama proses pengiriman data. Dengan metode simulasi ini, diharapkan dapat memberikan pandangan yang lebih akurat tentang kinerja algoritma di lingkungan WSN dengan sumber daya terbatas. Simulasi ini bertujuan untuk menilai bagaimana kedua algoritma (AES-128 dan TEA) dapat memenuhi tuntutan keamanan, efisiensi energi, dan pengiriman data yang menjadi tantangan signifikan di jaringan berbasis IoT[11], [12], [13], [14], [15].

Dalam penelitian ini, AES-128 akan dijadikan algoritma pembanding karena algoritma tersebut menawarkan keamanan tinggi dan sering digunakan dalam aplikasi yang memerlukan perlindungan data yang kuat. Namun penerapan AES-128 di WSN dapat memperparah batasan sumber daya, terutama dalam aplikasi yang menuntut penghematan energi. Sebaliknya, TEA memberikan alternatif yang lebih ringan yang dapat mempertahankan efisiensi energi dan waktu komputasi yang lebih singkat, meskipun dengan keamanan yang sedikit lebih lemah dibandingkan AES-128. Oleh karena itu, penelitian ini bertujuan untuk menilai kekuatan dan kelemahan masing-masing algoritma dalam skenario WSN yang dibatasi sumber daya [16], [17].

.

II. TINJAUAN PUSTAKA

A. Karakteristik dan Tantangan Keamanan pada WSN

Jaringan Sensor Nirkabel (WSN) menampilkan beberapa ciri khas yang membedakannya dari jenis jaringan komputer lainnya. Salah satu perbedaan pokoknya adalah kurangnya efisiensi energi dan kemampuan pengiriman pada node sensor yang membangun jaringan tersebut. Setiap node sensor di WSN dibuat untuk beroperasi dengan tenaga terbatas. Karena sebagian besar node ini mengandalkan baterai yang tidak bisa diisi ulang atau diganti, penghematan energi menjadi masalah penting bagi kelangsungan fungsi jaringan. Jika penggunaan energi terlalu berlebihan, masa pakai baterai node sensor akan cepat berkurang, yang pada akhirnya akan mengganggu kinerja jaringan secara menyeluruh. Oleh karena itu, pendekatan hemat energi sangat diperlukan untuk menjamin jaringan tetap aktif dalam jangka waktu yang lama[18], [19], [20].

Di sisi lain, informasi perlindungan di WSN semakin menjadi tantangan krusial, khususnya dengan meningkatnya aplikasi IoT yang memanfaatkan teknologi ini. Aplikasi seperti pengawasan lingkungan, pertanian pintar, dan sistem medis sangat mengandalkan kemampuan WSN untuk menyampaikan data yang tepat dan akurat. Informasi yang dikirim melalui jaringan ini bisa sangat rahasia, dan jika tidak dijaga dengan baik, bisa menjadi target serangan yang membahayakan kerahasiaan, keutuhan, serta ketersediaan data antar node di jaringan. Serangan terhadap informasi dapat membuat data yang dikirim rusak, dimanipulasi, atau dicuri. Oleh karena itu, menjamin keamanan dalam pertukaran antar node di WSN menjadi prioritas yang tidak bisa diabaikan.

Beberapa jenis ancaman pokok yang dihadapi WSN meliputi:

Gambar 1. Klasifikasi jenis ancaman siber dan dampaknya

1. Penyadapan (Eavesdropping): Ancaman ini muncul ketika pihak tidak sah berhasil mendengarkan dan mengawasi komunikasi antar node di jaringan. Ini dapat menyebabkan bocornya data yang sangat sensitif, yang berpotensi disalahgunakan untuk tujuan buruk.
2. Pemalsuan Identitas (Spoofing): Dalam serangan ini, penyerang berpura-pura sebagai node sah di jaringan, sehingga bisa mengirim data palsu atau mengirim node lainnya. Hal ini dapat merusak keutuhan data dan mengurangi kepercayaan antar node di jaringan.
3. Serangan Man-in-the-Middle: Pada jenis ancaman ini, penyerang bisa menyusup di antara dua node yang berkomunikasi dan memanipulasi atau mengubah data yang dikirim. Akibatnya, data yang diterima oleh node penerima mungkin berbeda dari yang sebenarnya dikirim, yang tentu saja mengancam keutuhan dan kebocoran data di jaringan[21], [22], [23].

B. Algoritma Enkripsi Ringan untuk WSN

Hambatan utama yang dihadapi WSN dalam menerapkan sistem keamanan adalah batasan sumber daya, khususnya terkait energi, kemampuan transmisi, dan penyimpanan. Algoritma enkripsi yang biasa digunakan di jaringan komputer tidak selalu sesuai untuk diterapkan pada WSN dengan batasan ini. Oleh karena itu, perlu diciptakan algoritma enkripsi yang lebih sederhana namun tetap ampuh dalam melindungi data yang dikirim antar node di jaringan.

Riset mengenai algoritma enkripsi ringan untuk WSN telah maju, dengan berbagai algoritma yang disajikan untuk menyelesaikan masalah ini. Beberapa algoritma umum yang diterapkan untuk enkripsi di WSN meliputi:

1. AES (Advanced Encryption Standard): AES merupakan algoritma enkripsi yang sangat tangguh dan sering dipakai di berbagai aplikasi untuk menjaga privasi data. Meskipun AES terkenal dengan tingkat keamanan tinggi, algoritma ini membutuhkan banyak sumber daya dalam hal pemrosesan dan energi. Ini menjadikannya kurang ideal untuk diterapkan di WSN, di mana sumber daya sangat terbatas. Proses enkripsi dan dekripsi yang rumit serta konsumsi energi tinggi pada AES menjadikan opsi yang tidak efisien untuk aplikasi IoT dengan keterbatasan sumber daya.
2. RC5 (Rivest Cipher 5): RC5 adalah algoritma enkripsi yang lebih hemat sumber daya dibandingkan AES. Namun, meskipun lebih ringan, RC5 masih memerlukan lebih banyak sumber daya daripada algoritma enkripsi ringan lainnya, seperti TEA. RC5 mungkin lebih sesuai untuk beberapa aplikasi WSN, tetapi masih ada kendala dalam hal penghematan energi dan kinerja pada jaringan dengan sumber daya terbatas.
3. TEA (Tiny Encryption Algorithm): TEA adalah salah satu algoritma enkripsi yang dikembangkan untuk menjadi lebih sederhana namun tetap efektif dalam mengamankan data pada Jaringan Sensor Nirkabel (WSN). TEA memiliki kunci sepanjang 128-bit dan memakai ukuran blok 64-bit, yang membuatnya sangat efisien dalam hal kecepatan dan penggunaan energi yang lebih rendah. TEA dirancang khusus untuk memenuhi kebutuhan WSN yang dibatasi oleh energi dan memori. Dengan konsumsi energi rendah dan kecepatan tinggi, TEA memungkinkan enkripsi data yang lebih cepat dan lebih hemat, sehingga sangat cocok untuk diterapkan di jaringan yang bergantung pada baterai terbatas[27], [28], [29].

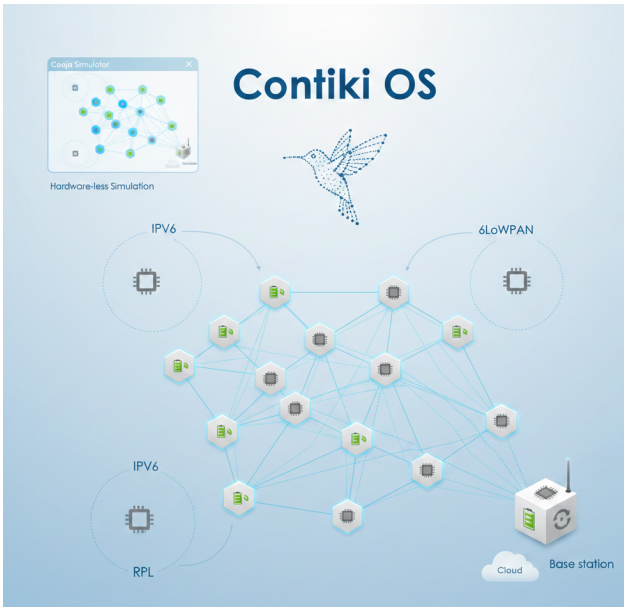
III. METODE

A. Desain Sistem WSN

Studi ini menerapkan arsitektur Jaringan Sensor Nirkabel (WSN) yang terbagi menjadi dua komponen utama, yaitu Node Sensor (SN) dan Base Station (BS), yang berkolaborasi untuk membangun sistem akuisisi dan pemrosesan informasi. Node Sensor bertanggung jawab mengumpulkan data di sekitarnya, seperti suhu, kelembaban, atau indikator lainnya. Setelah mengumpulkan data, node sensor melakukan enkripsi dengan Tiny Encryption Algorithm (TEA) untuk melindungi kerahasiaan informasi yang akan dikirim ke Base Station. Algoritma TEA dipilih berkat keefisienannya dalam memanfaatkan sumber daya seperti energi baterai dan kemampuan pemrosesan yang terbatas pada perangkat sensor[30],[31], Informasi yang sudah dienkripsi lalu dikirimkan ke Base Station melalui saluran nirkabel. Base Station memiliki peran menerima data terenkripsi dan mendekripsinya agar kembali ke format awal, sehingga dapat dijelaskan lebih dalam untuk keperluan seperti pengawasan kondisi lingkungan, evaluasi kinerja sistem, atau pengambilan keputusan berdasarkan data[32],[33], Arsitektur ini menawarkan beberapa manfaat penting, termasuk pembagian peran antara node sensor yang berkonsentrasi pada pengumpulan data dan enkripsi, serta Base Station yang menangani pemrosesan dan analisis informasi. Pembagian ini meringankan beban pada node sensor yang dibatasi oleh energi dan

kapasitas pengisian. Penerapan TEA dalam enkripsi juga memberikan keunggulan terkait hemat energi dan durasi komputasi, yang krusial di sistem IoT dengan sumber daya terbatas. Perlindungan data dilakukan melalui enkripsi yang menghalangi potensi ancaman seperti penyadapan atau perubahan data selama transmisi antara node sensor dan Base Station. Dengan cara ini, sistem ini sangat sesuai untuk aplikasi IoT yang memerlukan akuisisi dan pemrosesan data secara efektif dan terlindungi, meskipun sumber daya yang ada terbatas[34].

Sistem ini diwujudkan melalui pemanfaatan Contiki OS, yakni sebuah sistem operasi terbuka yang kian populer untuk penerapan dalam bidang Internet of Things (IoT). Platform ini khusus dibuat untuk perangkat dengan kapasitas sumber daya minim, termasuk simpul-simpul di dalam jaringan sensor nirkabel (WSN). Kelebihan pokok Contiki OS terletak pada dukungannya terhadap pembuatan aplikasi IoT yang hemat energi dan efisien dalam penggunaan memori, sehingga cocok untuk sensor dengan batasan-batasan tertentu. Adapun simulasi sistemnya dilakukan lewat Cooja Simulator, sebuah perangkat uji coba yang terintegrasi dalam Contiki OS. Cooja memfasilitasi evaluasi skenario operasional WSN yang lebih mendekati kenyataan, seperti transfer informasi di antara simpul, proses penyandian serta penyandian balik data, plus efisiensi konsumsi daya, tanpa perlu hardware nyata, yang pada akhirnya mengurangi durasi dan ongkos riset.[35],[36].



Gambar 2. Arsitektur jaringan dan protokol Contiki OS (IPv6, 6LoWPAN, RPL)

B. Pengujian dan Metodologi

Simulasi dilakukan dengan membandingkan tiga skenario:

1. Tanpa Enkripsi (Baseline): Data yang dikirimkan antar node sensor tidak dienkripsi.
2. Enkripsi menggunakan TEA: Data dienkripsi menggunakan algoritma TEA.
3. Enkripsi menggunakan AES-128: Data dienkripsi menggunakan algoritma AES-128

Studi ini menerapkan dua algoritma penyandian, yakni AES-128 dan TEA, untuk menilai performa pada jaringan sensor tanpa kabel yang berbasis IoT. Penilaian dilakukan melalui simulasi guna mengukur tiga indikator utama dalam pengiriman data dari simpul sensor menuju stasiun pangkalan (BS). Simulasi tersebut memungkinkan pembandingan kedua algoritma dalam konteks Wireless Sensor Networks (WSN) yang diterapkan pada aplikasi IoT, di mana sumber daya seperti tenaga baterai dan kemampuan pemrosesan sangat minim. Indikator yang dievaluasi meliputi durasi pemrosesan, penggunaan energi, dan laju aliran data, yang semuanya krusial dalam menentukan efektivitas serta performa jaringan.

Durasi pemrosesan menilai waktu yang diperlukan sistem untuk menyandikan dan menyandi ulang data, biasanya berukuran 1 KB. Indikator ini amat penting dalam konteks WSN yang memiliki batasan pemrosesan, sebab waktu yang lebih singkat dalam proses penyandian dan penyandi ulang dapat meningkatkan efektivitas sistem secara keseluruhan. Penggunaan energi dihitung untuk mengetahui seberapa banyak energi yang dikonsumsi oleh simpul sensor selama proses penyandian, penyandi ulang, dan pengiriman data. Karena simpul sensor bergantung pada baterai yang terbatas, efisiensi energi

menjadi faktor kunci untuk memperpanjang umur sistem. Akhirnya, laju aliran data mengukur volume data yang berhasil dikirim dalam satuan waktu, yang berguna untuk mengevaluasi seberapa baik jaringan dalam mentransmisikan data yang telah disandikan. Laju aliran yang lebih tinggi menandakan bahwa jaringan mampu mengirim lebih banyak data dalam waktu cepat, tanpa mengorbankan efektivitas.

Simulasi ini dibuat untuk memberikan wawasan lebih dalam tentang perbandingan performa antara AES-128 dan TEA dalam lingkungan IoT, di mana keseimbangan antara keamanan dan efektivitas sangat esensial. Penilaian dilakukan dengan mempertimbangkan berbagai skenario jaringan serta analisis terhadap performa masing-masing algoritma dalam menjaga keamanan data, mengurangi penggunaan energi, dan meningkatkan laju aliran data. Dengan cara ini, studi ini bertujuan untuk memberikan pemahaman yang lebih mendalam mengenai pemilihan algoritma penyandian yang paling sesuai untuk aplikasi IoT yang mengandalkan WSN dalam kondisi terbatas[37], [38], [39], [40], [41].

Metode ini memungkinkan perbandingan antara kedua algoritma dalam hal efisiensi dan keamanan. Metrik awal, yaitu durasi pemrosesan, menilai lamanya waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi pada data sebesar 1 KB menggunakan masing-masing algoritma. Durasi ini memiliki signifikansi tinggi karena mencerminkan efektivitas pengolahan data di jaringan sensor yang dibatasi oleh sumber daya, seperti kemampuan komputasi dan tenaga listrik. Semakin singkat durasi pemrosesan, semakin optimal pemanfaatan sumber daya yang tersedia. Metrik berikutnya, yaitu penggunaan daya, menghitung total energi yang dikonsumsi oleh simpul sensor selama tahap enkripsi, dekripsi, serta pengiriman data. Mengingat simpul sensor dalam WSN umumnya mengandalkan baterai dengan kapasitas terbatas, efisiensi daya menjadi aspek yang sangat vital. Algoritma enkripsi yang lebih irit energi akan memperpanjang masa operasional simpul sensor tanpa perlu penggantian baterai, yang akhirnya meningkatkan performa dan efektivitas jaringan secara menyeluruh. Metrik selanjutnya, yaitu laju aliran data, menentukan volume data yang berhasil dikirimkan dari simpul sensor ke stasiun utama dalam periode waktu tertentu. Metrik ini menggambarkan tingkat efektivitas sistem dalam mengirimkan data yang telah dienkripsi, yang berdampak pada performa jaringan keseluruhan. Semakin besar laju aliran data, semakin baik kemampuan jaringan untuk mentransmisikan informasi tanpa mengurangi kualitas meskipun data tersebut sudah dienkripsi. Pendekatan simulasi ini memfasilitasi evaluasi yang transparan antara kedua algoritma enkripsi terkait efisiensi daya, durasi pemrosesan, serta tingkat keamanan yang disediakan oleh masing-masing. Output simulasi memberikan pandangan yang lebih mendalam mengenai seberapa baik setiap algoritma memenuhi persyaratan aplikasi WSN berbasis IoT, yang menekankan efisiensi daya dan pemrosesan data yang cepat, sekaligus mempertahankan standar keamanan yang esensial dalam proses pengiriman data [42], [43].

Penilaian performa dalam studi ini mengandalkan tiga indikator pokok. Yang pertama adalah durasi pemrosesan, yang menilai berapa lama diperlukan untuk menyandikan dan menyandikan ulang data sebesar 1 KB. Indikator ini krusial untuk memastikan bahwa aktivitas penyandian tidak terlalu menuntut simpul sensor yang memiliki kemampuan komputasi terbatas. Yang kedua adalah penggunaan daya, yang menghitung jumlah energi keseluruhan yang dikonsumsi selama penyandian, penyandian balik, serta pengiriman data. Efisiensi daya amat vital di dalam jaringan sensor nirkabel (WSN), mengingat simpul sensor umumnya mengandalkan baterai dengan kapasitas terbatas. Penerapan algoritma penyandian yang irit energi memungkinkan simpul berfungsi lebih panjang tanpa perlu penggantian baterai berulang, sehingga meningkatkan ketahanan sistem secara menyeluruh yang mengukur total energi yang digunakan oleh node sensor selama proses enkripsi, dekripsi, dan transmisi data[44], [45], [46], [47]. Ketiga, throughput merupakan ukuran volume data yang berhasil dikirim dalam periode tertentu. Indikator ini berfungsi untuk mengevaluasi efektivitas jaringan saat mengalirkan informasi yang telah diamankan. Di samping menyediakan perlindungan keamanan yang cukup, throughput juga menunjukkan kapasitas sistem dalam menjaga penghematan energi serta performa jaringan secara menyeluruh. Berkat throughput yang optimal, jaringan mampu menyalurkan data dengan lancar tanpa menimbulkan beban berlebih pada sumber daya, sehingga performa tetap prima bahkan ketika data yang dikirim sudah dalam bentuk terenkripsi.[48], [49], [50]

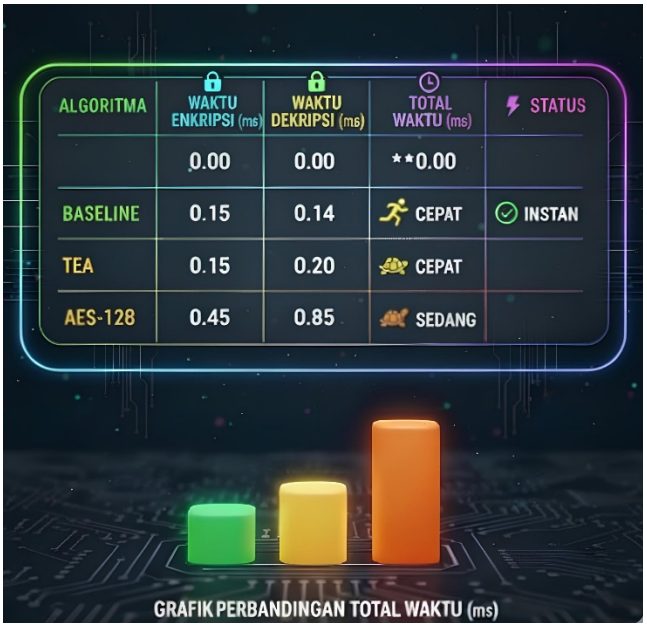
IV. HASIL

Di bagian ini, kami akan menyajikan temuan dari serangkaian uji coba yang dilakukan guna menilai performa berbagai algoritma enkripsi yang diterapkan dalam studi ini. Evaluasi tersebut mencakup pemeriksaan terhadap durasi pemrosesan, penggunaan daya, serta laju transfer data, yang semuanya berperan krusial dalam mengukur keberhasilan algoritma tersebut dalam lingkungan Jaringan Sensor Nirkabel (WSN) yang terintegrasi dengan Internet of Things

(IoT). Setiap algoritma enkripsi, yakni Baseline, TEA, dan AES-128, diuji menggunakan dataset sebesar 1 KB, yang mencerminkan skala informasi yang lazim ditemui dalam penerapan IoT.

A. Waktu Komputasi

Tabel 1 menunjukkan hasil pengujian waktu komputasi untuk enkripsi dan dekripsi data berukuran 1 KB pada masing-masing algoritma.

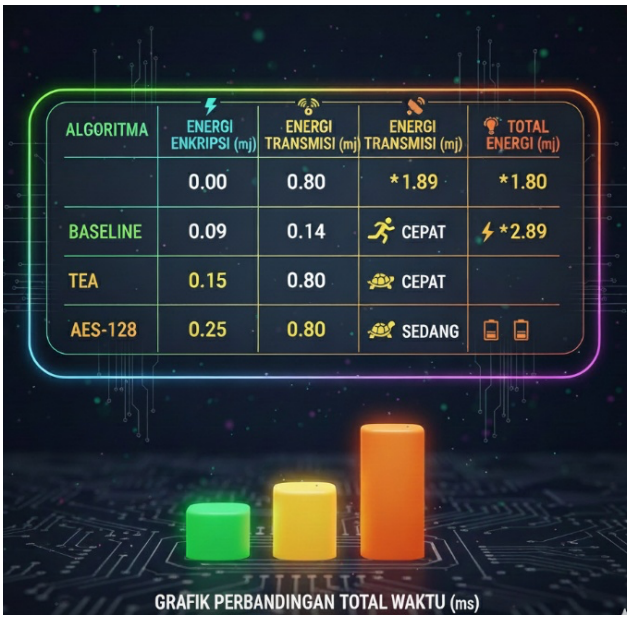


Gambar 3. Tabel dan Grafik Perbandingan Kinerja Algoritma Kriptografi (Waktu Enkripsi/Dekripsi)

yaitu Baseline, TEA, dan AES-128, dengan menitikberatkan pada durasi yang diperlukan untuk proses enkripsi, dekripsi, waktu total eksekusi, serta kategori performanya. Baseline menampilkan kecepatan enkripsi dan dekripsi yang luar biasa singkat, masing-masing 0.00 ms dan 0.14 ms, dengan total waktu eksekusi hanya 0.00 ms, sehingga dikategorikan sebagai "Instant." TEA menunjukkan waktu enkripsi identik dengan Baseline (0.15 ms), namun sedikit lebih lama untuk dekripsi (0.20 ms), menghasilkan total waktu 0.35 ms, dan diberi status "Cepat." AES-128, walaupun menyediakan perlindungan keamanan yang lebih kuat, justru memerlukan waktu enkripsi yang lebih panjang (0.45 ms) dan dekripsi yang cukup signifikan (0.85 ms), dengan total eksekusi mencapai 1.30 ms, sehingga statusnya "Sedang." Akibatnya, Baseline dan TEA lebih unggul dalam aspek kecepatan dibandingkan AES-128, meskipun AES-128 memberikan keamanan yang lebih tinggi.

B. Konsumsi Energi

Tabel 2 menunjukkan konsumsi energi selama proses transmisi data berukuran 1 KB pada ketiga algoritma enkripsi



Gambar 4. Perbandingan Kinerja Efisiensi Daya Algoritma Kriptografi Berdasarkan Konsumsi Energi Total

Yakni Baseline, TEA, dan AES-128, dengan fokus pada konsumsi energi untuk proses enkripsi, pengiriman data, serta total energi yang dikeluarkan, plus durasi waktu yang diperlukan untuk menjalankannya. Dalam aspek energi enkripsi, Baseline menghabiskan 0.09 mJ, TEA memerlukan 0.15 mJ, sedangkan AES-128 menggunakan 0.25 mJ. Walaupun ketiga algoritma ini sama-sama mengonsumsi energi transmisi sebesar 0.80 mJ, perbedaannya terlihat pada total energi keseluruhan dan lama eksekusi. Baseline menunjukkan total energi paling rendah, yaitu 1.80 mJ, dengan waktu eksekusi yang singkat, sementara TEA sedikit lebih tinggi pada total energi 1.89 mJ dan juga memiliki waktu eksekusi yang cepat. AES-128, walaupun menawarkan keamanan lebih kuat, justru membutuhkan energi lebih banyak, yakni 2.89 mJ, serta waktu eksekusi yang lebih panjang.

Dari perspektif efisiensi, TEA lebih superior daripada AES-128 terkait penggunaan energi dan durasi eksekusi, sehingga cocok sebagai opsi utama untuk aplikasi yang memprioritaskan penghematan daya, seperti di Wireless Sensor Networks (WSN). Meski AES-128 menyediakan perlindungan keamanan yang lebih tangguh, algoritma ini kurang optimal untuk perangkat dengan kapasitas daya terbatas karena memakan lebih banyak energi dan waktu dalam proses enkripsi serta pengiriman. Baseline, walaupun tidak setegar AES-128 dalam hal keamanan, menawarkan performa terbaik soal energi dan waktu eksekusi, meskipun dengan pengorbanan pada aspek keamanannya.

V.PEMBAHASAN

Usai menjalankan rangkaian eksperimen, dapat ditarik kesimpulan bahwa Algoritma Enkripsi Kecil (TEA) menunjukkan keunggulan yang jelas dalam efisiensi penggunaan energi serta durasi pemrosesan data. Jika dibandingkan dengan AES-128, TEA menghasilkan kinerja yang lebih superior, khususnya di Jaringan Sensor Nirkabel (WSN) yang memiliki keterbatasan sumber daya. TEA lebih hemat dalam mengonsumsi energi dan lebih cepat dalam menangani informasi, sehingga menjadi opsi ideal untuk penerapan Internet of Things (IoT) yang bergantung pada simpul sensor dengan kapasitas daya yang minim. Walaupun AES-128 menyediakan lapisan keamanan yang lebih tangguh, kompleksitasnya justru mendorong pengeluaran energi yang lebih tinggi, sehingga membuatnya tidak cocok untuk WSN yang mengandalkan baterai terbatas. Oleh karena itu, TEA lebih sesuai untuk skenario yang memprioritaskan penghematan energi dan kecepatan komputasi, sedangkan AES-128 lebih tepat digunakan dalam kondisi yang menuntut keamanan maksimal meski dengan biaya energi yang lebih besar.

VI. KESIMPULAN

Studi ini mengungkapkan bahwa Algoritma Enkripsi Kecil (TEA) merupakan opsi enkripsi yang hemat dan sesuai untuk diimplementasikan pada Jaringan Sensor Nirkabel (WSN) yang terintegrasi dengan Internet of

Things (IoT). TEA memberikan keuntungan signifikan terkait konsumsi energi dan durasi pemrosesan yang lebih optimal jika dibandingkan dengan AES-128, sehingga menjadi alternatif ideal untuk penerapan WSN dengan batasan sumber daya, misalnya dalam bidang pertanian cerdas atau sistem pengawasan ekosistem. Keefisienan tersebut memungkinkan jaringan untuk mengurangi penggunaan daya dan memperbaiki performa keseluruhan, bahkan pada gadget dengan kapasitas baterai yang minim.

Riset selanjutnya sebaiknya menitikberatkan pada evaluasi daya tahan TEA melawan ancaman kriptografi yang lebih canggih, serta penyelidikan potensi penggabungannya dengan mekanisme pengelolaan kunci untuk meningkatkan tingkat keamanannya.

Walaupun TEA sangat unggul dalam hal penghematan energi dan waktu pemrosesan, bagi skenario yang membutuhkan standar keamanan lebih tinggi—seperti pengiriman informasi rahasia—AES-128 masih menjadi opsi utama, meski harus mengorbankan efisiensi energi.

Secara sederhana, TEA tepat untuk penggunaan yang menekankan penghematan daya, sedangkan AES-128 lebih sesuai untuk kondisi yang mengharuskan perlindungan data yang lebih tangguh.

Kontribusi Penulis:Penulis pertama (Moh Andrian Maulana) bertanggung jawab atas konseptualisasi, metodologi, dan penulisan draf artikel ini. Penulis kedua (Rafael Ainur Hayat) melakukan investigasi dan kurasi data dan bertugas melakukan kurasi data untuk mendukung pengembangan terhadap hasil ini.

Pendanaan:semua biaya dari penelitian ini hasil dari kami sendiri.

Terima Kasih:Dari kami ingin bertimakasih kepada membantu atas bantuan dan dukungannya yang sangat berharga dalam penelitian ini.
Konflik Kepentingan:Penulis tidak ada keterkaitatan dengan siapapun

Ketersediaan Data: Sumber ini disimpan di repositori yang relevan dan dapat diakses berdasarkan permintaan yang wajar kepada penulis korespondensi.

Persetujuan Etik: Penelitian ini tidak melibatkan manusia atau hewan sebagai subjek. Semua prosedur penelitian telah disetujui oleh komite etik yang relevan sesuai dengan pedoman etika yang berlaku.

DAFTAR PUSTAKA

[1] 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," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 356–361, Jul. 2024, doi: 10.47709/brilliance.v4i1.4231.

[2] A. M. K. Abdulzahra, A. K. M. Al-Qurabat, and S. A. Abdulzahra, "Optimizing energy consumption in WSN-based IoT using unequal clustering and sleep scheduling methods," *Internet of Things*, vol. 22, p. 100765, Jul. 2023, doi: 10.1016/j.iot.2023.100765.

[3] P. Jagannathan, S. Gurumoorthy, A. Stateczny, P. Divakarachar, and J. Sengupta, "Collision-Aware Routing Using Multi-Objective Seagull Optimization Algorithm for WSN-Based IoT," *Sensors*, vol. 21, no. 24, p. 8496, Dec. 2021, doi: 10.3390/s21248496.

[4] O. Gurewitz, M. Shifrin, and E. Dvir, "Data Gathering Techniques in WSN: A Cross-Layer View," *Sensors*, vol. 22, no. 7, p. 2650, Mar. 2022, doi: 10.3390/s22072650.

[5] S. Tumula *et al.*, "An opportunistic energy-efficient dynamic self-configuration clustering algorithm in WSN-based IoT networks," *International Journal of Communication Systems*, vol. 37, no. 1, Jan. 2024, doi: 10.1002/dac.5633.

[6] R. Ramya and T. Brindha, "Fuzzy-Driven Cluster Head Selection and Deep Learning Prediction on the Basis of Hybrid Optimization Algorithm for Multiobjective Routing in WSN-IoT," *International Journal of Communication Systems*, vol. 38, no. 12, Aug. 2025, doi: 10.1002/dac.70162.

[7] A. Salim, W. Osamy, A. Aziz, and A. M. Khedr, "SEEDGT: Secure and energy efficient data gathering technique for IoT applications based WSNs," *Journal of Network and Computer Applications*, vol. 202, p. 103353, Jun. 2022, doi: 10.1016/j.jnca.2022.103353.

[8] M. Krishnan and Y. Lim, "Reinforcement learning-based dynamic routing using mobile sink for data collection in WSNs and IoT applications," *Journal of Network and Computer Applications*, vol. 194, p. 103223, Nov. 2021, doi: 10.1016/j.jnca.2021.103223.

[9] M. Krishnan and Y. Lim, "Reinforcement learning-based dynamic routing using mobile sink for data collection in WSNs and IoT applications," *Journal of Network and Computer Applications*, vol. 194, p. 103223, Nov. 2021, doi: 10.1016/j.jnca.2021.103223.

[10] D. Gopika and R. Panjanathan, "WITHDRAWN: Energy efficient routing protocols for WSN based IoT applications: A review," *Mater Today Proc*, Nov. 2020, doi: 10.1016/j.matpr.2020.10.137.

[11] M. Shahid *et al.*, "Link-Quality-Based Energy-Efficient Routing Protocol for WSN in IoT," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4645–4653, Feb. 2024, doi: 10.1109/TCE.2024.3356195.

[12] N. R. Patel, S. Kumar, and S. K. Singh, "Energy and Collision Aware WSN Routing Protocol for Sustainable and Intelligent IoT Applications," *IEEE Sens J*, vol. 21, no. 22, pp. 25282–25292, Nov. 2021, doi: 10.1109/JSEN.2021.3076192.

[13] M. Shafiq *et al.*, "Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3505–3521, 2021, doi: 10.32604/cmc.2021.015533.

[14] R. B. Pedditi and K. Debasis, "Energy Efficient Routing Protocol for an IoT-Based WSN System to Detect Forest Fires," *Applied Sciences*, vol. 13, no. 5, p. 3026, Feb. 2023, doi: 10.3390/app13053026.

[15] G. Arya, A. Bagwari, and D. S. Chauhan, "Performance Analysis of Deep Learning-Based Routing Protocol for an Efficient Data Transmission in 5G WSN Communication," *IEEE Access*, vol. 10, pp. 9340–9356, 2022, doi: 10.1109/ACCESS.2022.3142082.

[16] H. Benyezza, M. Bouhedda, R. Kara, and S. Rebouh, "Smart platform based on IoT and WSN for monitoring and control of a greenhouse in the context of precision agriculture," *Internet of Things*, vol. 23, p. 100830, Oct. 2023, doi: 10.1016/j.iot.2023.100830.

[17] H. Benyezza, M. Bouhedda, R. Kara, and S. Rebouh, "Smart platform based on IoT and WSN for monitoring and control of a greenhouse in the context of precision agriculture," *Internet of Things*, vol. 23, p. 100830, Oct. 2023, doi: 10.1016/j.iot.2023.100830.

[18] U. Panahi and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications," *Ain Shams Engineering Journal*, vol. 14, no. 2, p. 101866, Mar. 2023, doi: 10.1016/j.asej.2022.101866.

[19] K. Ramana, A. Revathi, A. Gayathri, R. H. Jhaveri, C. V. L. Narayana, and B. N. Kumar, "WOGRU-IDS — An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks," *Comput Commun*, vol. 196, pp. 195–206, Dec. 2022, doi: 10.1016/j.comcom.2022.10.001.

[20] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System," *IEEE Internet Things J*, vol. 10, no. 17, pp. 15087–15099, Sep. 2023, doi: 10.1109/JIOT.2023.3264565.

[21] T. Saba, K. Haseeb, A. A. Shah, A. Rehman, U. Tariq, and Z. Mehmood, "A Machine-Learning-Based Approach for Autonomous IoT Security," *IT Prof*, vol. 23, no. 3, pp. 69–75, May 2021, doi: 10.1109/MITP.2020.3031358.

[22] F. P. E. Putra, U. Ubaidi, A. Hamzah, W. A. Pramadi, and A. Nuraini, "Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 348–355, Jul. 2024, doi: 10.47709/brilliance.v4i1.4227.

[23] F. P. E. Putra, U. Ubaidi, A. B. Tamam, and R. W. Efendi, "Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 340–347, Jul. 2024, doi: 10.47709/brilliance.v4i1.4199.

[24] S. M. Hussein, J. A. López Ramos, and A. M. Ashir, "A Secure and Efficient Method to Protect Communications and Energy Consumption in IoT Wireless Sensor Networks," *Electronics (Basel)*, vol. 11, no. 17, p. 2721, Aug. 2022, doi: 10.3390/electronics11172721.

[25] S. Nagaraj *et al.*, "Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks," *Energies (Basel)*, vol. 16, no. 1, p. 8, Dec. 2022, doi: 10.3390/en16010008.

[26] S. Hriez, S. Almajali, H. Elgala, M. Ayyash, and H. B. Salameh, "A Novel Trust-Aware and Energy-Aware Clustering Method That Uses Stochastic Fractal Search in IoT-Enabled Wireless Sensor Networks," *IEEE Syst J*, vol. 16, no. 2, pp. 2693–2704, Jun. 2022, doi: 10.1109/JSYST.2021.3065323.

[27] F. P. E. Putra, R. M. Ilhamsyah, S. A. Efendy, and A. Rizki, "Implementation And Evaluation Of Zerotier-Based Virtual Network For Device Connectivity," *Brilliance: Research of Artificial Intelligence*, vol. 5, no. 1, pp. 281–290, Jun. 2025, doi: 10.47709/brilliance.v5i1.5966.

[28] F. P. E. Putra, N. Ramadhani, F. Fauzan, and Moh. Mursidi, "Service Quality Analysis of RFID-Based Smart Door Lock in Front One Azana Style Hotel Area," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 372–381, Jul. 2024, doi: 10.47709/brilliance.v4i1.4292.

[29] D. Antony Joseph Rajan and E. R. Naganathan, "Trust based anonymous intrusion detection for cloud assisted WSN-IOT," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 104–108, Jun. 2022, doi: 10.1016/j.gltp.2022.04.022.

[30] F. P. E. Putra, Moh. Irfan, M. Aziz, and R. N. Saputra, "Wireless Network Design at Pamekasan Regency Public Library," *Brilliance: Research of Artificial Intelligence*, vol. 5, no. 1, pp. 144–150, May 2025, doi: 10.47709/brilliance.v5i1.5876.

[31] F. P. E. Putra, F. Mu'minin, A. Nuraini, S. N. R. Barokah, and K. Khairurrozi, "Designing an Information System for Student Admissions at SMAN 1 Pademawu Using the Waterfall Method," *Brilliance: Research of Artificial Intelligence*, vol. 5, no. 1, pp. 582–591, Jul. 2025, doi: 10.47709/brilliance.v5i1.6508.

[32] H. Yu and Y. Bin Zikria, "Cognitive Radio Networks for Internet of Things and Wireless Sensor Networks," *Sensors*, vol. 20, no. 18, p. 5288, Sep. 2020, doi: 10.3390/s20185288.

[33] G. Gardašević, K. Katzis, D. Bajić, and L. Berbakov, "Emerging Wireless Sensor Networks and Internet of Things Technologies—Foundations of Smart Healthcare," *Sensors*, vol. 20, no. 13, p. 3619, Jun. 2020, doi: 10.3390/s20133619.

[34] S. Shankar, G. Deepika, G. Devi, S. Ramesh, S. Srivastava, and S. S. Kumar, "Development of Efficient Wireless Sensor Network for IoT Applications," in *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*, IEEE, Jun. 2023, pp. 1419–1424. doi: 10.1109/ICPCSN58827.2023.00237.

[35] S. Ghorpade, M. Zennaro, and B. S. Chaudhari, "Towards green computing: intelligent bio-inspired agent for IoT-enabled wireless sensor networks," *International Journal of Sensor Networks*, vol. 35, no. 2, p. 121, 2021, doi: 10.1504/IJSNET.2021.113632.

[36] M. Z. Ghawy *et al.*, "An Effective Wireless Sensor Network Routing Protocol Based on Particle Swarm Optimization Algorithm," *Wirel Commun Mob Comput*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/8455065.

[37] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," *Optik (Stuttg)*, vol. 273, p. 170419, Feb. 2023, doi: 10.1016/j.ijleo.2022.170419.

[38] J. N. Ndunagu, K. E. Ukhurebor, M. Akaaza, and R. B. Onyancha, "Development of a Wireless Sensor Network and IoT-based Smart Irrigation System," *Appl Environ Soil Sci*, vol. 2022, pp. 1–13, Jun. 2022, doi: 10.1155/2022/7678570.

[39] E. Hajian, M. R. Khayyambashi, and N. Movahhedinia, "A Mechanism for Load Balancing Routing and Virtualization Based on SDWSN for IoT Applications," *IEEE Access*, vol. 10, pp. 37457–37476, 2022, doi: 10.1109/ACCESS.2022.3164693.

[40] C. Jothikumar, K. Ramana, V. D. Chakravarthy, S. Singh, and I.-H. Ra, "An Efficient Routing Approach to Maximize the Lifetime of IoT-Based Wireless Sensor Networks in 5G and Beyond," *Mobile Information Systems*, vol. 2021, pp. 1–11, Jul. 2021, doi: 10.1155/2021/9160516.

[41] S. Rajasoundaran *et al.*, "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks," *Comput Commun*, vol. 187, pp. 71–82, Apr. 2022, doi: 10.1016/j.comcom.2022.02.004.

[42] F. P. E. Putra, U. Ubaidi, M. A. Huda, H. Hasbullah, and A. Rohman, "Computer Network Management Optimization Through Big Data Analysis Using Time Series Analysis Method," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 434–442, Aug. 2024, doi: 10.47709/brilliance.v4i1.4373.

[43] 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," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 413–421, Aug. 2024, doi: 10.47709/brilliance.v4i1.4357.

[44] F. P. E. Putra, U. Ubaidi, R. O. F. Kusuma, A. M. Syam, and S. A. Efendy, "Effect Of Distance On Wi-Fi Signal Quality In The Home Environment," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 391–398, Aug. 2024, doi: 10.47709/brilliance.v4i1.4319.

[45] A. F. Rachman, F. P. E. Putra, S. Syirofi, and D. Wahid, "Case Study of Computer Network Development for the Internet Of Things (IoT) Industry in an Urban Environment," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 399–407, Aug. 2024, doi: 10.47709/brilliance.v4i1.4302.

[46] T. M. Bandara, W. Mudiyanselage, and M. Raza, "Smart farm and monitoring system for measuring the Environmental condition using wireless sensor network - IOT Technology in farming," in *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, IEEE, Nov. 2020, pp. 1–7. doi: 10.1109/CITISIA50690.2020.9371830.

[47] J. R. Arunkumar, S. Velmurugan, B. Chinnaiah, G. Charulatha, M. Ramkumar Prabhu, and A. Prabhu Chakkaravarthy, "Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT," *Computer Systems Science and Engineering*, vol. 45, no. 3, pp. 2635–2645, 2023, doi: 10.32604/csse.2023.031605.

[48] R. Cheour, S. Khriji, M. abid, and O. Kanoun, "Microcontrollers for IoT: Optimizations, Computing Paradigms, and Future Directions," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, IEEE, Jun. 2020, pp. 1–7. doi: 10.1109/WF-IoT48130.2020.9221219.

[49] Md. N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie, and T. Shongwe, "Internet of Things and Wireless Sensor Networks for Smart Agriculture Applications: A Survey," *IEEE Access*, vol. 11, pp. 145813–145852, 2023, doi: 10.1109/ACCESS.2023.3346299.

[50] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr Comput*, vol. 32, no. 21, Nov. 2020, doi: 10.1002/cpe.4946.