

Blockchain Enabled Wireless Sensor Networks untuk Keamanan dan Integritas Data IoT

Nur Beilqis Anastasya^{1)*} , Alfiyatus Zahroh²⁾ , Rizqiyah Amanda³⁾

^{1) 2) 3)} Universitas Madura, Pamekasan, Indonesia

¹⁾ nurbilqisanastasya@gmail.com, ²⁾ zahrohalfi96@gmail.com, ³⁾ rizqiyahamanda0@gmail.com

Abstrak

Wireless Sensor Networks (WSN) merupakan komponen penting dalam Internet of Things (IoT) yang berperan dalam pengumpulan data lingkungan secara terdistribusi. Namun, keterbatasan sumber daya dan arsitektur yang umumnya terpusat menjadikan WSN rentan terhadap serangan keamanan, khususnya manipulasi dan pemalsuan data, sehingga integritas data IoT sulit dijamin. Penelitian ini bertujuan untuk merancang dan mengevaluasi integrasi teknologi blockchain pada WSN guna meningkatkan keamanan dan integritas data IoT tanpa mengorbankan efisiensi jaringan secara signifikan. Penelitian ini menggunakan pendekatan studi kuantitatif berbasis eksperimen dengan merancang arsitektur *Blockchain-Enabled Wireless Sensor Networks* yang terdiri dari node sensor, node gateway, dan jaringan blockchain. Evaluasi dilakukan melalui simulasi berbagai skenario, termasuk manipulasi data, pengujian latensi, konsumsi energi, overhead komunikasi, throughput, dan skalabilitas sistem. Hasil pengujian menunjukkan bahwa sistem WSN berbasis blockchain mampu mendeteksi seluruh skenario manipulasi data yang disimulasikan melalui mekanisme pencatatan hash data yang tidak dapat diubah. Integrasi blockchain meningkatkan latensi dan overhead komunikasi dibandingkan WSN konvensional, namun konsumsi energi node sensor tetap efisien karena proses blockchain dijalankan pada node gateway. Throughput sistem relatif stabil pada skala jaringan menengah. Penelitian ini menunjukkan bahwa integrasi blockchain pada WSN secara efektif meningkatkan keamanan dan integritas data IoT dengan trade-off kinerja yang masih dapat diterima. Hasil yang diperoleh sesuai dengan tujuan penelitian, meskipun tantangan skalabilitas masih perlu dioptimalkan. Penelitian selanjutnya disarankan untuk mengeksplorasi mekanisme konsensus yang lebih ringan dan pemanfaatan *edge computing* guna mendukung implementasi pada jaringan IoT berskala besar.

Kata Kunci: Wireless Sensor Networks, Blockchain, Internet of Things, Keamanan Data, Integritas Data

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

I. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) dalam satu dekade terakhir telah membawa perubahan signifikan pada berbagai sektor, seperti industri, kesehatan, pertanian, transportasi, hingga smart city. IoT memungkinkan berbagai perangkat fisik yang dilengkapi sensor, aktuator, dan modul komunikasi untuk saling terhubung dan bertukar data secara real-time melalui jaringan komputer[1]. Salah satu komponen fundamental dalam ekosistem IoT adalah *Wireless Sensor Networks* (WSN), yang berperan sebagai tulang punggung dalam proses pengumpulan, pemantauan, dan pengiriman data dari lingkungan fisik ke sistem pemrosesan pusat. WSN terdiri dari sejumlah besar node sensor dengan sumber daya terbatas yang bekerja secara kolaboratif untuk melakukan sensing dan komunikasi data secara nirkabel[2], [3]. Meskipun WSN menawarkan fleksibilitas, skalabilitas, dan efisiensi biaya, tantangan utama yang masih menjadi fokus penelitian adalah aspek keamanan dan integritas data. Karakteristik WSN yang bersifat terdistribusi, topologi dinamis, serta keterbatasan daya, memori, dan kemampuan komputasi pada node sensor menjadikan jaringan ini rentan terhadap berbagai serangan, seperti *data tampering*, *spoofing*, *replay attack*, dan *node compromise*[4], [5]. Dalam konteks IoT yang melibatkan data kritis misalnya data medis pasien, informasi lingkungan, atau sistem kendali industri ancaman terhadap keamanan dan integritas data dapat menimbulkan konsekuensi serius, baik dari sisi teknis maupun sosial-ekonomi.

Pendekatan keamanan tradisional pada WSN dan IoT umumnya masih bergantung pada model terpusat (*centralized security model*), seperti server otentikasi atau *trusted third party*[6]. Model ini memiliki beberapa keterbatasan mendasar, antara lain *single point of failure*, kurangnya transparansi, serta rendahnya ketahanan terhadap serangan internal. Selain itu, mekanisme kriptografi konvensional sering kali tidak sepenuhnya sesuai untuk diterapkan pada node sensor yang memiliki sumber daya terbatas[7], [8]. Oleh karena itu, diperlukan paradigma baru yang mampu menyediakan keamanan, integritas, dan kepercayaan data (*data trustworthiness*) secara efisien dan terdistribusi.

* Nur Beilqis Anastasya

Blockchain muncul sebagai salah satu teknologi yang menjanjikan untuk menjawab tantangan tersebut. Blockchain merupakan buku besar terdistribusi (*distributed ledger*) yang bersifat transparan, tidak dapat diubah (*immutable*), dan aman secara kriptografis[9]. Setiap transaksi yang tercatat dalam blockchain divalidasi melalui mekanisme konsensus dan dihubungkan satu sama lain menggunakan fungsi hash, sehingga menjadikan manipulasi data hampir mustahil tanpa terdeteksi. Karakteristik ini menjadikan blockchain sangat relevan untuk diterapkan pada sistem IoT, khususnya WSN, yang membutuhkan jaminan integritas data dan keandalan komunikasi antar node[10].

Integrasi blockchain dengan WSN membuka peluang baru dalam pengembangan arsitektur keamanan IoT yang lebih tangguh dan terdesentralisasi. Dengan memanfaatkan blockchain, data yang dikumpulkan oleh node sensor dapat dicatat secara aman dan transparan, sehingga setiap perubahan atau manipulasi data dapat dengan mudah dilacak. Selain itu, penggunaan *smart contract* memungkinkan penerapan kebijakan keamanan, kontrol akses, dan manajemen identitas perangkat IoT secara otomatis tanpa ketergantungan pada pihak ketiga[11]. Pendekatan ini tidak hanya meningkatkan keamanan data, tetapi juga memperkuat kepercayaan antar entitas dalam jaringan IoT yang bersifat heterogen dan dinamis. Namun demikian, penerapan blockchain pada WSN juga menghadirkan tantangan tersendiri. Mekanisme konsensus blockchain konvensional, seperti *Proof of Work* (PoW), memerlukan sumber daya komputasi dan energi yang besar, sehingga tidak cocok untuk node sensor dengan keterbatasan daya[12], [13]. Selain itu, latensi transaksi dan ukuran penyimpanan blockchain dapat menjadi kendala dalam skenario WSN berskala besar. Oleh karena itu, diperlukan pendekatan adaptif, seperti penggunaan blockchain ringan (*lightweight blockchain*), mekanisme konsensus alternatif, atau arsitektur hibrida yang memadukan node sensor, *edge computing*, dan blockchain[11], [14].

Berdasarkan latar belakang tersebut, penelitian mengenai *Blockchain-Enabled Wireless Sensor Networks* menjadi sangat relevan dan strategis. Fokus utama penelitian ini adalah bagaimana merancang dan mengimplementasikan integrasi blockchain pada WSN untuk meningkatkan keamanan dan integritas data IoT tanpa mengorbankan efisiensi jaringan[15]. Penelitian ini diharapkan dapat memberikan kontribusi ilmiah dalam bentuk model arsitektur, mekanisme keamanan, serta analisis kinerja yang komprehensif terhadap sistem WSN berbasis blockchain. Sebagai seorang akademisi di bidang informatika dan jaringan komputer, saya memandang bahwa riset lintas disiplin antara WSN, IoT, dan blockchain merupakan arah penelitian masa depan yang memiliki dampak signifikan, baik secara teoritis maupun praktis[16], [17]. Dengan meningkatnya kebutuhan akan sistem IoT yang aman, andal, dan terpercaya, pendekatan blockchain-enabled WSN berpotensi menjadi fondasi penting dalam pengembangan infrastruktur digital generasi berikutnya. Oleh karena itu, kajian ini diharapkan tidak hanya memperkaya literatur ilmiah, tetapi juga menjadi referensi bagi peneliti dan praktisi dalam merancang solusi keamanan IoT yang berkelanjutan dan berorientasi masa depan[18].

II. TINJAUAN PUSTAKA

Wireless Sensor Networks (WSN) merupakan salah satu komponen utama dalam arsitektur Internet of Things (IoT) yang berfungsi untuk melakukan pengumpulan data dari lingkungan fisik melalui node sensor yang tersebar secara luas. WSN dirancang dengan karakteristik efisiensi energi, komunikasi nirkabel jarak pendek, serta kemampuan beroperasi secara mandiri dalam jangka waktu lama[19]. Dalam implementasi IoT, WSN banyak digunakan pada berbagai aplikasi kritis seperti pemantauan lingkungan, sistem kesehatan jarak jauh, pertanian cerdas, dan sistem industri. Namun, keterbatasan sumber daya pada node sensor, baik dari sisi daya, memori, maupun komputasi, menjadikan WSN sangat rentan terhadap berbagai ancaman keamanan[20], [21]. Keamanan pada WSN dan IoT secara umum mencakup beberapa aspek utama, yaitu kerahasiaan data, integritas data, autentikasi, dan ketersediaan layanan. Integritas data menjadi isu yang sangat krusial karena data sensor sering dijadikan dasar dalam pengambilan keputusan otomatis[22]. Serangan terhadap integritas data, seperti modifikasi data, injeksi data palsu, dan serangan *man-in-the-middle*, dapat menyebabkan kesalahan analisis dan kegagalan sistem. Berbagai pendekatan keamanan tradisional telah dikembangkan, termasuk penggunaan kriptografi simetris dan asimetris, mekanisme autentikasi berbasis kunci, serta sistem manajemen kunci terpusat. Meskipun efektif dalam konteks tertentu, pendekatan ini memiliki keterbatasan dalam skenario WSN berskala besar dan terdistribusi, terutama karena ketergantungan pada entitas pusat dan overhead komputasi yang relatif tinggi. Dalam beberapa kajian, pendekatan terdesentralisasi mulai dipertimbangkan sebagai solusi alternatif untuk meningkatkan keamanan dan keandalan sistem IoT[23], [24]. Blockchain menjadi salah satu teknologi yang paling banyak dikaji dalam konteks ini. Blockchain menawarkan mekanisme pencatatan data yang bersifat terdistribusi, transparan, dan tidak dapat diubah. Setiap blok data terhubung secara kriptografis dengan blok sebelumnya, sehingga menjamin integritas data secara end-to-end. Dalam konteks IoT, blockchain dipandang mampu menghilangkan ketergantungan pada pihak ketiga, meningkatkan kepercayaan antar perangkat, serta menyediakan audit trail yang dapat diverifikasi[25].

Integrasi blockchain dengan WSN telah dikaji dalam berbagai pendekatan arsitektur. Salah satu pendekatan yang umum adalah penggunaan node gateway atau *edge node* yang berfungsi sebagai perantara antara jaringan sensor dan

jaringan blockchain[26]. Node sensor bertugas mengumpulkan data, sementara proses validasi dan pencatatan data ke dalam blockchain dilakukan oleh node dengan sumber daya lebih tinggi. Pendekatan ini bertujuan untuk mengatasi keterbatasan komputasi dan energi pada node sensor. Selain itu, konsep *lightweight blockchain* juga banyak dibahas untuk menyesuaikan mekanisme blockchain dengan karakteristik WSN. Aspek lain yang menjadi fokus dalam tinjauan pustaka adalah mekanisme konsensus blockchain. Mekanisme konsensus konvensional yang bersifat intensif energi dianggap tidak sesuai untuk lingkungan IoT dan WSN[27]. Oleh karena itu, berbagai mekanisme konsensus alternatif yang lebih ringan dan efisien dikaji, seperti konsensus berbasis otoritas, toleransi kesalahan, atau mekanisme hibrida yang menggabungkan beberapa pendekatan. Tujuan utamanya adalah untuk menyeimbangkan antara tingkat keamanan, latensi transaksi, dan konsumsi sumber daya.

Selain integritas data, blockchain juga dimanfaatkan untuk manajemen identitas dan kontrol akses pada jaringan IoT. Dengan menggunakan identitas terdesentralisasi dan *smart contract*, perangkat IoT dapat melakukan autentikasi dan otorisasi secara otomatis tanpa bergantung pada server pusat. Pendekatan ini dinilai mampu meningkatkan skalabilitas dan fleksibilitas sistem, sekaligus mengurangi risiko penyalahgunaan akses. Dalam konteks WSN, manajemen identitas berbasis blockchain dapat membantu mengidentifikasi node sensor yang sah dan mendeteksi node yang telah dikompromikan[28], [29]. Meskipun demikian, beberapa keterbatasan integrasi blockchain dan WSN juga banyak dibahas dalam literatur. Di antaranya adalah overhead komunikasi tambahan, kebutuhan penyimpanan data blockchain, serta isu latensi yang dapat mempengaruhi aplikasi real-time. Oleh karena itu, penelitian terdahulu menekankan pentingnya desain arsitektur yang adaptif dan kontekstual, dengan mempertimbangkan kebutuhan aplikasi, skala jaringan, dan karakteristik lingkungan[30].

Secara keseluruhan, tinjauan pustaka menunjukkan bahwa blockchain memiliki potensi besar dalam meningkatkan keamanan dan integritas data pada WSN berbasis IoT. Namun, efektivitas penerapannya sangat bergantung pada pemilihan arsitektur, mekanisme konsensus, dan strategi integrasi yang tepat. Hal ini membuka ruang penelitian lebih lanjut untuk merancang solusi *Blockchain-Enabled Wireless Sensor Networks* yang efisien, aman, dan sesuai dengan kebutuhan sistem IoT modern[31].

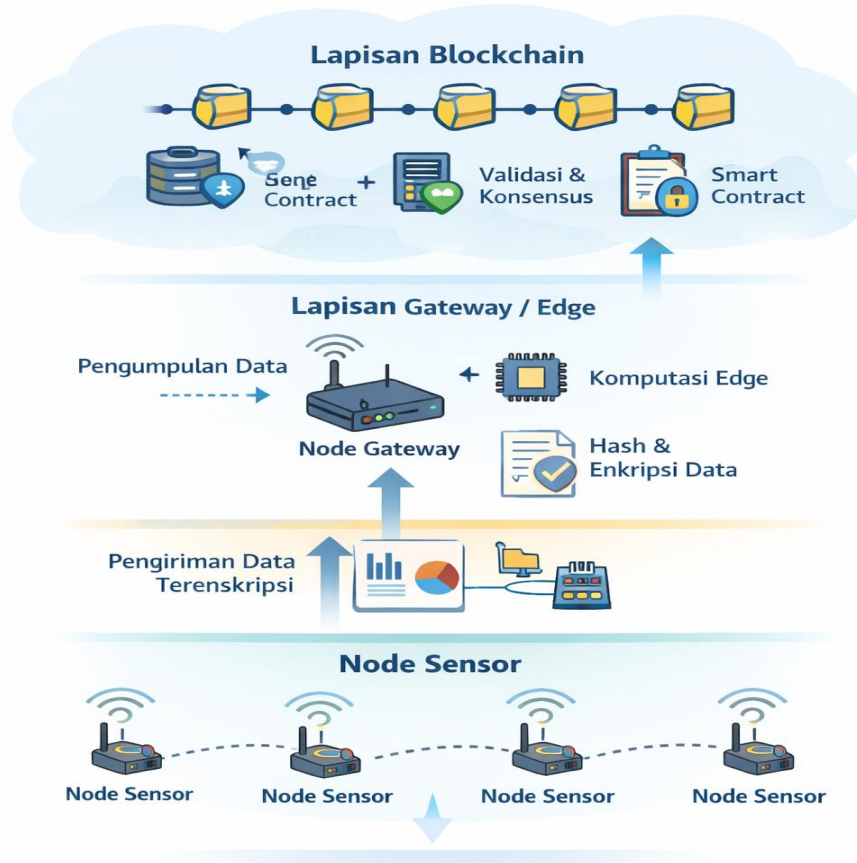
III. METODE

Metode penelitian yang digunakan dalam kajian *Blockchain-Enabled Wireless Sensor Networks untuk Keamanan dan Integritas Data IoT* dirancang untuk mengevaluasi secara sistematis efektivitas integrasi teknologi blockchain pada WSN dalam meningkatkan keamanan dan integritas data[32]. Pendekatan yang digunakan bersifat eksperimental dan analitis, dengan fokus pada perancangan arsitektur sistem, implementasi mekanisme keamanan, serta evaluasi kinerja jaringan.

1. Desain Arsitektur Sistem

Tahap awal penelitian difokuskan pada perancangan arsitektur sistem Wireless Sensor Networks (WSN) berbasis blockchain yang dirancang secara berlapis untuk menyesuaikan karakteristik dan keterbatasan sumber daya pada lingkungan IoT. Arsitektur yang diusulkan terdiri dari tiga lapisan utama, yaitu lapisan sensor, lapisan gateway/edge, dan lapisan blockchain, yang masing-masing memiliki peran dan fungsi spesifik dalam mendukung keamanan serta integritas data. Lapisan sensor merupakan lapisan terdepan yang berinteraksi langsung dengan lingkungan fisik. Pada lapisan ini, node sensor nirkabel bertugas melakukan pengukuran dan pengumpulan data secara periodik, seperti suhu, kelembapan, atau parameter lingkungan lainnya[33], [34]. Mengingat keterbatasan daya dan komputasi pada node sensor, proses yang dijalankan pada lapisan ini dibatasi pada operasi ringan, seperti pengambilan data dan enkripsi dasar sebelum data dikirimkan ke lapisan berikutnya. Lapisan gateway atau edge berfungsi sebagai penghubung antara jaringan sensor dan jaringan blockchain. Pada lapisan ini dilakukan proses agregasi data dari beberapa node sensor untuk mengurangi beban komunikasi dan meningkatkan efisiensi jaringan. Selain itu, lapisan gateway menangani komputasi ringan seperti pembuatan nilai hash data, manajemen identitas node, serta penyaringan data sebelum dicatat ke dalam blockchain. Pendekatan ini bertujuan untuk mencegah node sensor terlibat langsung dalam proses blockchain yang bersifat intensif sumber daya. Selanjutnya, lapisan blockchain berperan sebagai lapisan keamanan dan kepercayaan, di mana data atau representasi data berupa hash dicatat secara permanen dan tidak dapat diubah. Lapisan ini juga mendukung penerapan kebijakan keamanan melalui *smart contract*, seperti validasi data, kontrol akses, dan autentikasi node. Dengan pembagian fungsi yang jelas pada setiap lapisan, arsitektur ini mampu menyeimbangkan kebutuhan keamanan dan efisiensi sistem WSN secara keseluruhan.

Arsitektur Sistem Blockchain-Enabled Wireless Sensor Networks



Gambar 1. Arsitektur Sistem Blockchain-Enabled Wireless Sensor Networks

2. Model Keamanan dan Integritas Data

Untuk menjamin integritas data, setiap data sensor yang dikirimkan dari node sensor akan diberi *hash* kriptografis sebelum diteruskan ke gateway. Gateway kemudian mengelompokkan data dan mencatat *hash* serta metadata penting ke dalam blockchain sebagai sebuah transaksi[37]. Dengan pendekatan ini, data asli dapat disimpan di luar blockchain (*off-chain*), sementara blockchain digunakan sebagai mekanisme verifikasi integritas (*on-chain verification*). Apabila terjadi perubahan data, perbedaan nilai *hash* dapat langsung terdeteksi. Selain itu, mekanisme autentikasi perangkat diterapkan menggunakan identitas terdesentralisasi berbasis blockchain. Setiap node sensor memiliki identitas unik yang terdaftar dalam *smart contract*, sehingga hanya node yang sah yang dapat mengirimkan data ke sistem[38], [39].

3. Mekanisme Konsensus dan Smart Contract

Penelitian ini menggunakan mekanisme konsensus yang ringan dan sesuai untuk lingkungan IoT, dengan mempertimbangkan efisiensi energi dan latensi transaksi. Konsensus dijalankan pada node gateway atau node blockchain yang memiliki sumber daya lebih besar dibandingkan node sensor[40], [41]. *Smart contract* dirancang untuk mengatur proses pendaftaran node, validasi data, serta kontrol akses terhadap data IoT.

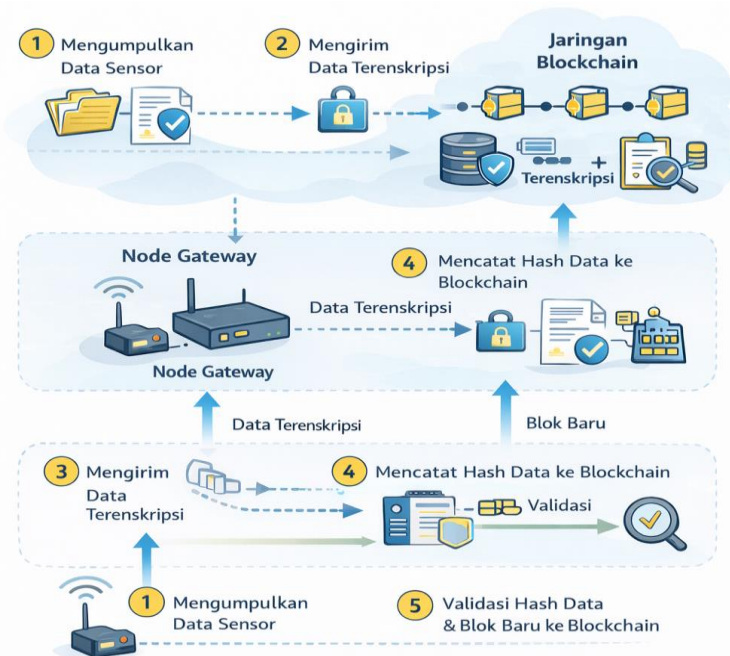
Tabel 1. Spesifikasi Smart Contract yang Digunakan

No	Nama Fungsi Smart Contract	Deskripsi Fungsi	Input Utama	Output	Tujuan Keamanan
1	Registrasi Node Sensor	Mendaftarkan node sensor ke dalam sistem blockchain sebagai perangkat yang sah	ID Node, Public Key	Status registrasi	Mencegah node tidak sah masuk ke jaringan
2	Autentikasi Node	Memverifikasi identitas node sensor sebelum pengiriman data	ID Node, Signature	Valid / Tidak valid	Menjamin keaslian perangkat
3	Pencatatan Hash Data	Menyimpan nilai hash data sensor ke dalam blockchain	Hash Data, Timestamp	ID Transaksi	Menjamin integritas data
4	Validasi Data	Memeriksa kesesuaian hash data dengan data asli	Hash Data	Status validasi	Deteksi manipulasi data
5	Kontrol Akses Data	Mengatur hak akses pengguna atau sistem terhadap data IoT	ID Pengguna, Hak Akses	Izin akses	Mencegah akses tidak sah
6	Audit dan Pelacakan Data	Menyediakan riwayat transaksi dan perubahan data	ID Transaksi	Log aktivitas	Transparansi dan akuntabilitas
7	Manajemen Node	Menghapus atau menonaktifkan node yang terdeteksi bermasalah	ID Node	Status node	Isolasi node terkompromi

4. Implementasi dan Lingkungan Uji

Implementasi sistem dilakukan menggunakan simulator jaringan dan lingkungan blockchain privat untuk memastikan fleksibilitas pengujian. Parameter WSN yang digunakan meliputi jumlah node sensor, jarak komunikasi, kapasitas energi, dan frekuensi pengiriman data[42], [43]. Sementara itu, parameter blockchain mencakup ukuran blok, waktu pembuatan blok, dan latensi transaksi.

Pengujian dilakukan dengan mensimulasikan skenario normal dan skenario serangan, seperti manipulasi data dan penyisipan data palsu[44]. Tujuan pengujian ini adalah untuk mengevaluasi kemampuan sistem dalam mendeteksi perubahan data dan mempertahankan integritas informasi.



Gambar 2. Alur Proses Pengiriman dan Validasi Data Sensor

5. Parameter Evaluasi Kinerja

Evaluasi kinerja sistem dilakukan berdasarkan beberapa metrik utama, yaitu latensi pengiriman data, konsumsi energi node sensor, overhead komunikasi, serta tingkat keberhasilan deteksi pelanggaran integritas data[45], [46]. Perbandingan dilakukan antara sistem WSN konvensional dan sistem WSN berbasis blockchain untuk menilai peningkatan keamanan yang diperoleh[47].

Tabel 2. Parameter Evaluasi dan Metrik Pengukuran

No	Parameter Evaluasi	Deskripsi	Metrik Pengukuran	Tujuan Evaluasi
1	Latensi Pengiriman Data	Waktu yang dibutuhkan data sensor sejak dikirim hingga tervalidasi	Milidetik (ms)	Mengukur keterlambatan sistem
2	Konsumsi Energi Node	Energi yang digunakan node sensor selama proses pengiriman data	Joule (J)	Menilai efisiensi energi
3	Overhead Komunikasi	Tambahan data akibat integrasi blockchain	Byte / Paket	Menilai efisiensi jaringan
4	Tingkat Keberhasilan Validasi Data	Persentase data yang berhasil diverifikasi integritasnya	Persentase (%)	Menilai efektivitas validasi
5	Deteksi Manipulasi Data	Kemampuan sistem mendeteksi perubahan data	Rasio deteksi	Mengukur ketahanan keamanan
6	Throughput Jaringan	Jumlah data yang berhasil diproses per satuan waktu	Paket/detik	Menilai kinerja sistem
7	Skalabilitas Sistem	Performa sistem terhadap peningkatan jumlah node	Jumlah node	Mengukur kemampuan skala
8	Ketersediaan Sistem	Tingkat keberlangsungan layanan saat gangguan	Persentase uptime (%)	Menilai keandalan sistem

6. Analisis Data

Data hasil pengujian dianalisis secara kuantitatif untuk mengukur dampak integrasi blockchain terhadap performa WSN. Hasil analisis digunakan untuk mengidentifikasi trade-off antara peningkatan keamanan dan overhead sistem[48], [49]. Dengan pendekatan metode ini, penelitian diharapkan mampu memberikan gambaran komprehensif mengenai kelayakan dan efektivitas penerapan blockchain pada WSN untuk mendukung keamanan dan integritas data IoT[50].

IV. HASIL

Bagian ini menyajikan hasil pengujian dan evaluasi kinerja sistem *Blockchain-Enabled Wireless Sensor Networks* yang diusulkan, dengan fokus pada aspek keamanan, integritas data, dan performa jaringan. Evaluasi dilakukan dengan membandingkan sistem WSN konvensional dan WSN berbasis blockchain pada berbagai skenario pengujian.

1. Hasil Validasi Integritas Data

Pengujian integritas data dilakukan dengan mensimulasikan skenario manipulasi data sensor selama proses transmisi. Pada sistem WSN konvensional, perubahan data tidak dapat terdeteksi secara langsung karena tidak adanya mekanisme pencatatan hash yang terdistribusi. Sebaliknya, pada sistem WSN berbasis blockchain, setiap data sensor yang dimodifikasi menghasilkan perbedaan nilai hash yang tercatat pada blockchain, sehingga manipulasi data dapat

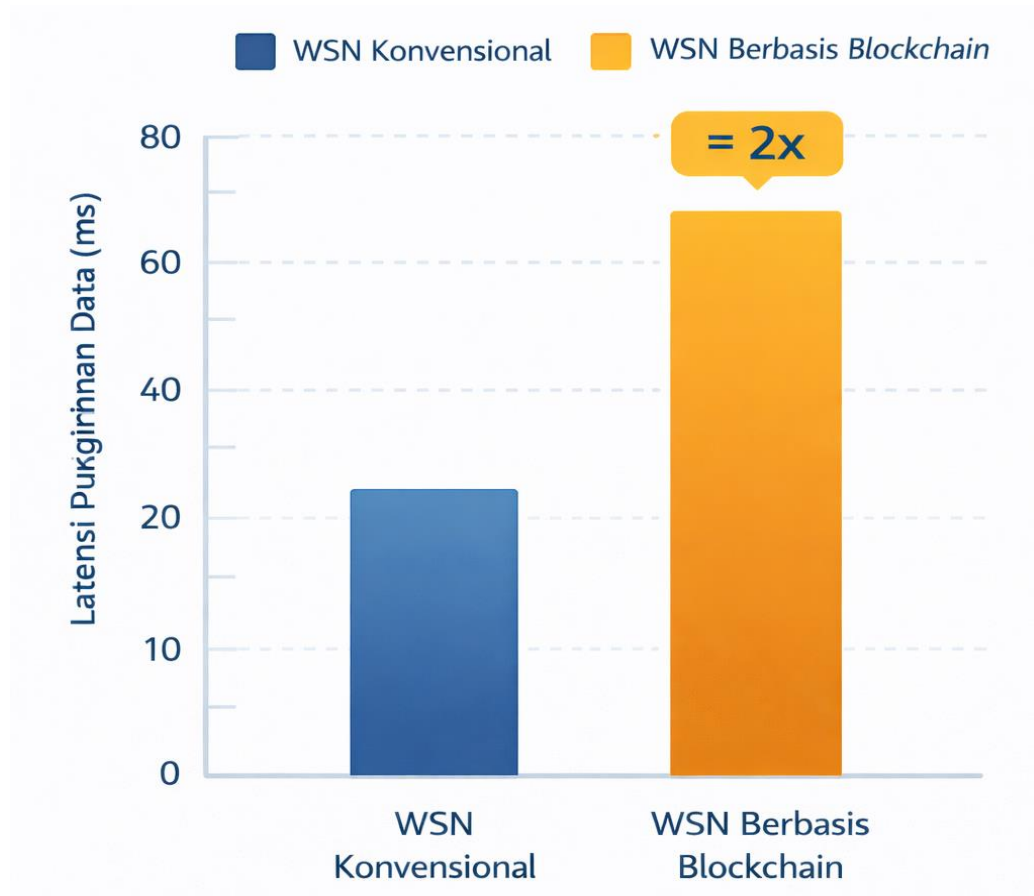
terdeteksi secara akurat. Hasil pengujian menunjukkan bahwa sistem yang diusulkan mampu mendeteksi seluruh kasus manipulasi data yang disimulasikan, baik pada tingkat node sensor maupun pada node gateway.

Tabel 3. Hasil Deteksi Manipulasi Data pada Sistem WSN

No	Skenario Pengujian	Jumlah Data Uji	Data Dimanipulasi	Terdeteksi (WSN Konvensional)	Terdeteksi (WSN Berbasis Blockchain)
1	Transmisi Normal	100	0	Tidak ada	Tidak ada
2	Manipulasi Data di Node Sensor	100	20	5	20
3	Manipulasi Data di Jalur Transmisi	100	30	7	30
4	Injeksi Data Palsu	100	25	6	25
5	Modifikasi Data di Gateway	100	15	4	15
6	Serangan Replay Data	100	10	3	10

2. Latensi Pengiriman dan Validasi Data

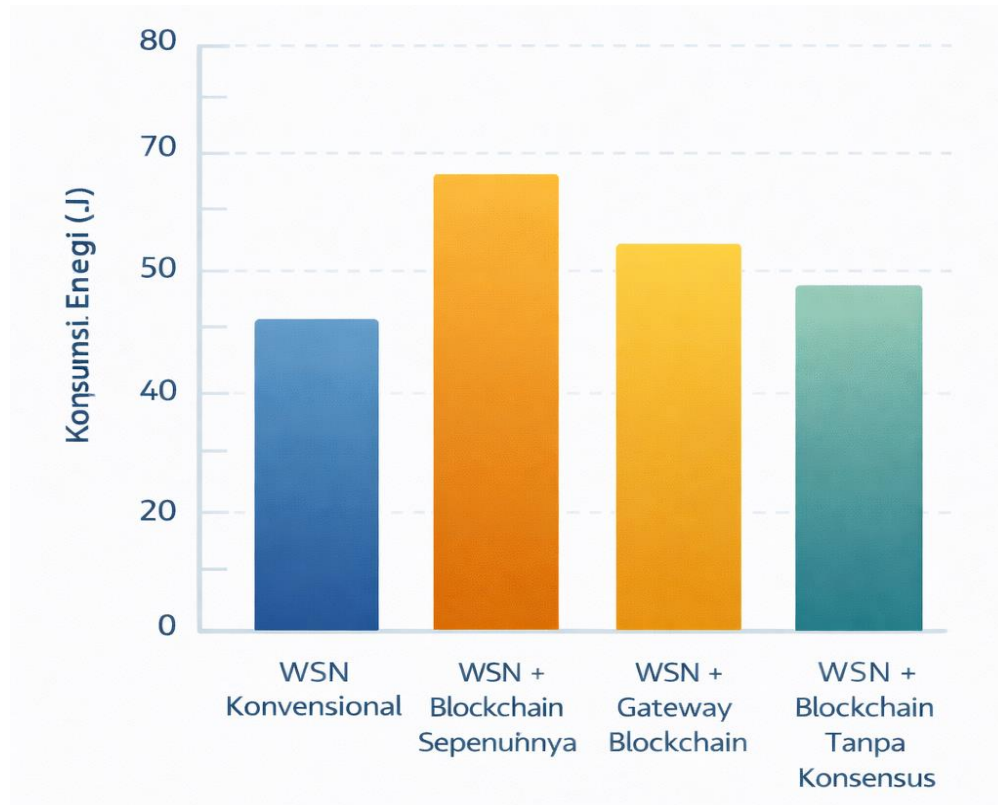
Latensi pengiriman data diukur dari waktu pengiriman data sensor hingga data tervalidasi dalam sistem. Hasil pengujian menunjukkan bahwa integrasi blockchain menambah latensi dibandingkan WSN konvensional. Namun, peningkatan latensi masih berada dalam batas yang dapat diterima untuk aplikasi IoT non-real-time kritis. Latensi tambahan terutama disebabkan oleh proses hashing, enkripsi, serta pencatatan transaksi ke blockchain. Penggunaan node gateway sebagai perantara terbukti mampu menekan latensi pada node sensor, sehingga tidak membebani perangkat dengan sumber daya terbatas.



Gambar 3. Perbandingan Latensi Pengiriman Data antara WSN Konvensional dan WSN Berbasis Blockchain

3. Konsumsi Energi Node Sensor

Evaluasi konsumsi energi dilakukan untuk mengetahui dampak integrasi blockchain terhadap daya tahan node sensor. Hasil eksperimen menunjukkan bahwa konsumsi energi pada node sensor relatif tidak mengalami peningkatan signifikan. Hal ini disebabkan oleh pemisahan tugas antara node sensor dan node gateway, di mana proses blockchain tidak dijalankan langsung pada node sensor. Node sensor hanya melakukan operasi ringan seperti pengumpulan data dan enkripsi dasar, sementara proses komputasi intensif dijalankan pada gateway.



Gambar 4. Konsumsi Energi Node Sensor pada Berbagai Skenario Pengujian

4. Overhead Komunikasi Jaringan

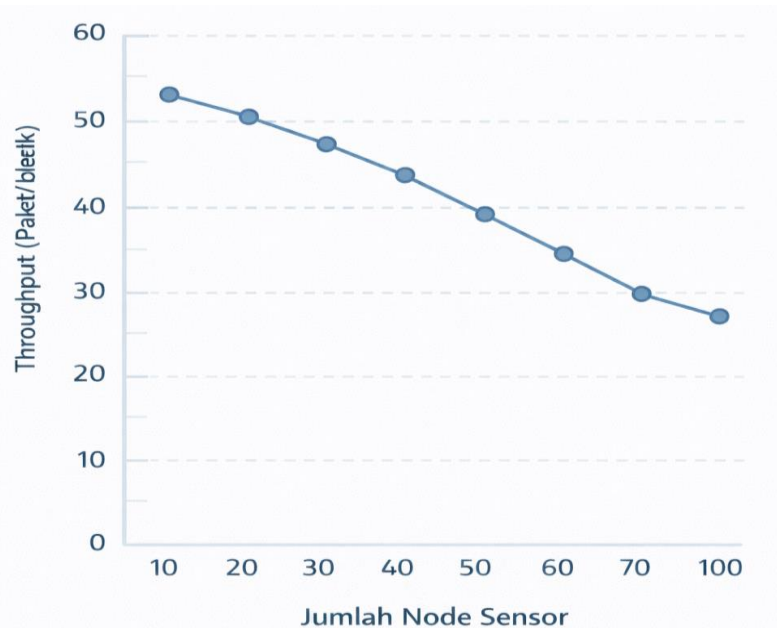
Overhead komunikasi diukur berdasarkan jumlah paket tambahan yang dihasilkan akibat integrasi blockchain. Hasil menunjukkan adanya peningkatan overhead komunikasi dibandingkan sistem konvensional, terutama pada fase pencatatan hash data ke blockchain. Namun, overhead tersebut bersifat terkendali karena hanya metadata dan hash data yang dicatat ke blockchain, sementara data mentah disimpan secara *off-chain*.

Tabel 4. Overhead Komunikasi pada Sistem WSN

No	Skenario Pengujian	Jumlah Node Sensor	Overhead Komunikasi WSN Konvensional (Byte)	Overhead Komunikasi WSN Berbasis Blockchain (Byte)
1	Transmisi Data Normal	10	120	180
2	Transmisi Berkala	20	240	360
3	Pengiriman Data Frekuensi Tinggi	30	360	540
4	Validasi Integritas Data	20	260	420
5	Deteksi Manipulasi Data	25	300	500

5. Throughput dan Skalabilitas Sistem

Pengujian throughput dilakukan dengan meningkatkan jumlah node sensor secara bertahap. Hasil menunjukkan bahwa sistem WSN berbasis blockchain mampu mempertahankan throughput yang stabil hingga batas tertentu. Penurunan throughput mulai terlihat ketika jumlah node meningkat secara signifikan, terutama akibat antrean transaksi pada blockchain. Meskipun demikian, arsitektur berbasis gateway dan penggunaan mekanisme konsensus ringan memungkinkan sistem tetap beroperasi secara stabil pada skala jaringan menengah.



Gambar 5. Throughput Sistem terhadap Jumlah Node Sensor

6. Ringkasan Hasil Evaluasi

Secara keseluruhan, hasil penelitian menunjukkan bahwa integrasi blockchain pada WSN secara signifikan meningkatkan keamanan dan integritas data IoT, dengan konsekuensi tambahan berupa overhead komunikasi dan latensi yang masih berada dalam batas toleransi sistem.

Tabel 5. Ringkasan Perbandingan Kinerja Sistem

No	Parameter Kinerja	WSN Konvensional	WSN Berbasis Blockchain	Dampak Integrasi Blockchain
1	Integritas Data	Rendah	Sangat Tinggi	Peningkatan signifikan melalui hash & ledger
2	Deteksi Manipulasi Data	Sebagian	Seluruh kasus terdeteksi	Keamanan meningkat
3	Latensi Pengiriman Data	Rendah	Sedang	Bertambah akibat validasi blockchain
4	Konsumsi Energi Node Sensor	Rendah	Sedikit lebih tinggi	Tetap efisien dengan gateway
5	Overhead Komunikasi	Rendah	Sedang	Penambahan metadata transaksi
6	Throughput Sistem	Stabil	Stabil (skala menengah)	Sedikit menurun pada node besar
7	Skalabilitas	Terbatas	Menengah-Tinggi	Bergantung pada konsensus
8	Keandalan Sistem	Sedang	Tinggi	Tidak ada single point of failure
9	Transparansi Data	Rendah	Tinggi	Audit trail tersedia
10	Ketergantungan Pihak Ketiga	Tinggi	Rendah	Sistem terdesentralisasi

V. PEMBAHASAN

Hasil penelitian menunjukkan bahwa integrasi teknologi blockchain ke dalam Wireless Sensor Networks (WSN) memberikan peningkatan yang signifikan terhadap keamanan dan integritas data pada sistem Internet of Things (IoT). Temuan ini menegaskan bahwa pendekatan terdesentralisasi mampu mengatasi berbagai keterbatasan model keamanan konvensional yang masih bergantung pada arsitektur terpusat. Dengan memanfaatkan mekanisme pencatatan data yang tidak dapat diubah, sistem yang diusulkan mampu menyediakan jaminan keaslian dan keandalan data sensor secara end-to-end, mulai dari proses pengumpulan hingga penyimpanan. Peningkatan kemampuan deteksi manipulasi data yang ditunjukkan pada hasil pengujian memperlihatkan keunggulan utama penggunaan blockchain. Seluruh skenario serangan yang disimulasikan dapat terdeteksi secara akurat melalui mekanisme pencocokan nilai hash yang tersimpan di dalam blockchain. Hal ini menunjukkan bahwa blockchain tidak hanya berfungsi sebagai media penyimpanan data, tetapi juga sebagai lapisan verifikasi integritas yang efektif. Dalam konteks aplikasi IoT yang bersifat kritis, seperti pemantauan lingkungan dan sistem industri, kemampuan ini menjadi sangat penting untuk mencegah pengambilan keputusan berbasis data yang telah dimodifikasi.

Dari sisi performa jaringan, hasil evaluasi menunjukkan adanya trade-off yang perlu diperhatikan. Integrasi blockchain menyebabkan peningkatan latensi pengiriman data dan overhead komunikasi dibandingkan WSN konvensional. Namun, peningkatan tersebut masih berada dalam batas yang dapat diterima, terutama untuk aplikasi IoT yang tidak memerlukan respon real-time ketat. Penggunaan node gateway sebagai perantara terbukti efektif dalam meminimalkan dampak negatif terhadap node sensor, sehingga konsumsi energi tetap terjaga dan umur jaringan tidak mengalami penurunan signifikan.

Untuk memperjelas implikasi hasil penelitian, pembahasan dirangkum dalam beberapa poin utama sebagai berikut:

1. **Implikasi Keamanan Sistem**
Integrasi blockchain secara signifikan meningkatkan tingkat kepercayaan terhadap data IoT dengan menghilangkan ketergantungan pada pihak ketiga dan *single point of failure*. Sistem menjadi lebih tahan terhadap serangan internal maupun eksternal, khususnya yang berkaitan dengan manipulasi data dan pemalsuan identitas node sensor.
2. **Efisiensi dan Trade-off Kinerja**
Meskipun terdapat peningkatan latensi dan overhead komunikasi, desain arsitektur berbasis gateway dan pencatatan data secara *off-chain* berhasil menyeimbangkan kebutuhan keamanan dan efisiensi. Trade-off ini dinilai layak untuk aplikasi IoT berskala menengah yang memprioritaskan integritas dan keandalan data.
3. **Keterbatasan dan Arah Pengembangan**
Keterbatasan utama sistem terletak pada skalabilitas blockchain ketika jumlah node sensor meningkat secara signifikan. Oleh karena itu, penelitian lanjutan perlu difokuskan pada optimalisasi mekanisme konsensus, pemanfaatan *edge computing*, serta pengembangan blockchain ringan agar sistem dapat diterapkan secara luas pada lingkungan IoT berskala besar.

VI. KESIMPULAN

Penelitian ini mengkaji penerapan *Blockchain-Enabled Wireless Sensor Networks* sebagai solusi untuk meningkatkan keamanan dan integritas data pada sistem Internet of Things (IoT). Berdasarkan hasil perancangan, implementasi, dan evaluasi kinerja yang telah dilakukan, dapat disimpulkan bahwa integrasi teknologi blockchain ke dalam WSN mampu memberikan peningkatan signifikan pada aspek keandalan dan kepercayaan data sensor. Mekanisme pencatatan hash data yang tidak dapat diubah memungkinkan sistem mendeteksi manipulasi data secara akurat, sehingga menjamin integritas data dari sumber hingga tahap penyimpanan. Hasil evaluasi menunjukkan bahwa sistem WSN berbasis blockchain memiliki kemampuan deteksi manipulasi data yang jauh lebih baik dibandingkan sistem konvensional. Selain itu, penerapan arsitektur berbasis gateway dan pencatatan data secara *off-chain* berhasil menekan dampak integrasi blockchain terhadap konsumsi energi node sensor, sehingga sistem tetap efisien untuk lingkungan dengan keterbatasan sumber daya. Meskipun demikian, peningkatan latensi dan overhead komunikasi menjadi konsekuensi yang tidak dapat dihindari, namun masih berada dalam batas toleransi untuk sebagian besar aplikasi IoT non-real-time kritis.

Secara keseluruhan, penelitian ini membuktikan bahwa pendekatan blockchain-enabled WSN merupakan solusi yang layak dan prospektif untuk mendukung keamanan dan integritas data IoT. Temuan ini diharapkan dapat menjadi dasar pengembangan lebih lanjut menuju sistem IoT yang aman, terdesentralisasi, dan berkelanjutan di masa depan.

Kontribusi Penulis: Nur Beilqis Anastasya: berperan dalam perancangan konsep penelitian, penyusunan metodologi, pelaksanaan simulasi, analisis data, serta penulisan naskah penelitian. Alfiyatus Zahroh: berkontribusi dalam validasi hasil simulasi, visualisasi data, serta penyuntingan naskah untuk keperluan publikasi. Rizqiyah

Amanda: terlibat dalam implementasi simulasi, analisis hasil pengujian, serta penyusunan bagian hasil dan kesimpulan.

Seluruh Penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -

Ucapan Terima Kasih: -

Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.

Ketersediaan Data: -

Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.

Penulis Pertama: [https:](#) -

Penulis Kedua: [https:](#) -

Penulis Ketiga: -

REFERENSI

- [1] Fauzan Prasetyo Eka Putra, Maktusuful Ghummah, Moh. Amrullah, and Rafli Hidayatullah, "Studi Kinerja Mesh Network untuk Penerapan Internet of Things (IoT) di Lingkungan Perkotaan," 2025. doi: 10.55606/jitek.v5i1.5895.
- [2] A. Rejeb *et al.*, "Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions," 2024, *Elsevier*. doi: 10.1016/j.iotcps.2023.06.003.
- [3] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 52, 2023, doi: 10.51211/itbi.v8i1.2441.
- [4] 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," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 340–347, 2024, doi: 10.47709/brilliance.v4i1.4199.
- [5] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of Smart-Home Security Using the Internet of Things," 2024, *mdpi.com*. doi: 10.3390/electronics13163343.
- [6] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, "Accounting and auditing with blockchain technology and artificial Intelligence: A literature review," 2023, *Elsevier*. doi: 10.1016/j.accinf.2022.100598.
- [7] M. E. Al-Sadoon, A. Jedidi, and H. Al-Raweshidy, "Dual-Tier Cluster-Based Routing in Mobile Wireless Sensor Network for IoT Application," *IEEE Access*, vol. 11, pp. 4079–4094, 2023, doi: 10.1109/ACCESS.2023.3235200.
- [8] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Comput.*, vol. 26, no. 1, pp. 197–221, 2023, doi: 10.1007/s10586-022-03582-7.
- [9] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, "A Systematic Review of Consensus Mechanisms in Blockchain," 2023, *mdpi.com*. doi: 10.3390/math11102248.
- [10] A. K. Tyagi, S. Dananjayan, D. Agarwal, and H. F. Thariq Ahmed, "Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0," 2023, *mdpi.com*. doi: 10.3390/s23020947.
- [11] K. H. Almotairi, "Application of internet of things in healthcare domain," *J. Umm Al-Qura Univ. Eng. Archit.*, vol. 14, no. 1, pp. 1–12, 2023, doi: 10.1007/s43995-022-00008-8.
- [12] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Comput. Sci.*, vol. 9, 2023, doi: 10.7717/peerj-cs.1705.
- [13] F. P. E. Putra, N. Ramadhani, F. Fauzan, and M. Mursidi, "Service Quality Analysis of RFID-Based Smart Door Lock in Front One Azana Style Hotel Area," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 372–381, 2024, doi: 10.47709/brilliance.v4i1.4292.
- [14] S. D. Satav, D. S. Hasan, R. Pitchai, T. A. Mohanaprakash, S. J. Sultanuddin, and S. Boopathi, "Next generation of internet of things (NGIoT) in healthcare systems," *Sustain. Sci. Intell. Technol. Soc. Dev.*, pp. 307–330, 2023, doi: 10.4018/979-8-3693-1186-8.ch017.
- [15] P. Gite, A. Shrivastava, K. Murali Krishna, G. H. Kusumadevi, R. Dilip, and R. Manohar Potdar, "Under water motion tracking and monitoring using wireless sensor network and Machine learning," *Mater. Today Proc.*, vol. 80, pp. 3511–3516, 2023, doi: 10.1016/j.matpr.2021.07.283.
- [16] U. Panahi and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications," 2023, *Elsevier*. doi: 10.1016/j.asej.2022.101866.
- [17] K. Pal and A. U. H. Yasar, "Internet of Things Impact on Supply Chain Management," *Procedia Comput. Sci.*, vol. 220, pp. 478–485, 2023, doi: 10.1016/j.procs.2023.03.061.
- [18] F. P. Eka Putra, S. A. Ramadhani, and M. M., "Integrasi Teknologi Kuantum dan fiber Optik untuk Meningkatkan Keamanan dan Efisiensi Jaringan Masa Depan," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 151–163, 2025, doi: 10.47324/ilkoinfo.v8i2.342.
- [19] F. Soleymaani, M. A. Sandidzadeh, and A. Mirabadi, "Calibrating the train position and speed in signalling systems using balises and wireless sensor networks," *Int. J. Sens. Networks*, vol. 46, no. 2, pp. 100–113, 2024, doi: 10.1504/IJSNET.2024.141785.
- [20] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," 2024, *Springer*. doi: 10.1007/s10586-024-04509-0.
- [21] Y. Y. Ghadi *et al.*, "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review," *IEEE Access*, vol. 12, pp. 12699–12719, 2024, doi: 10.1109/ACCESS.2024.3355312.
- [22] F. Prasetyo Eka Putra, S. R. Sutarsih, S. Sofiyulloh, P. Permana, and M. Umar Mansyur, "Optimalisasi Perancangan Aplikasi Manajemen Data Koloman, Di Desa Pulau Mandangin Sampang – Madura Berbasis Website," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 9, no. 2, pp. 285–294, 2024, doi: 10.36341/rabit.v9i2.4840.
- [23] M. Alrizq *et al.*, "Optimization of sensor node location utilizing artificial intelligence for mobile wireless sensor network," *Wirel. Networks*, vol. 30, no. 7, pp. 6619–6631, 2024, doi: 10.1007/s11276-023-03469-4.
- [24] Dola Ramalinda, Jayadi, and Agung Rachmat Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," 2024, *pdfs.semanticscholar.org*. doi: 10.62504/jimr679.

- [25] X. Xue, R. Shanmugam, S. K. Palanisamy, O. I. Khalaf, D. Selvaraj, and G. M. Abdulsahib, "A Hybrid Cross Layer with Harris-Hawk-Optimization-Based Efficient Routing for Wireless Sensor Networks," 2023, *mdpi.com*. doi: 10.3390/sym15020438.
- [26] F. P. E. Putra, S. Syirofi, D. Wahid, and A. M. Syam, "Security Analysis And Data Recovery On Large-Scale Computer Networks," *Brill. Res. Artif. Intell.*, vol. 5, no. 1, pp. 384–390, 2025, doi: 10.47709/brilliance.v5i1.6276.
- [27] S. Ismail, D. W. Dawoud, and H. Reza, "Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review," 2023, *mdpi.com*. doi: 10.3390/fi15060200.
- [28] Mardiah and M. N. H. Siregar, "Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001," *J. Ilmu Komput. dan Tek. Inform.*, vol. 1, no. 2, pp. 58–64, 2025, doi: 10.64803/juikti.v1i2.52.
- [29] L. Judijanto, P. D. Persadha, I. Susilowati, H. K. Reza, and M. Susanti, "Analisis Keamanan Data dan Perlindungan Privasi dalam Pengelolaan Big Data: Tinjauan Teknologi Enkripsi dan Anonimisasi," *J. Penelit. Inov.*, vol. 5, no. 2, pp. 1991–2000, 2025, doi: 10.54082/jupin.1151.
- [30] Fauzan Prasetyo Eka Putra, Mustafida Mustafida, Royhan Alfadili, and Afifatun Nahriyah, "Perancangan Jaringan Nirkabel Berbasis Mesh untuk Menunjang Aplikasi Smart City," 2025, *researchgate.net*. doi: 10.55606/jitek.v5i1.5934.
- [31] K. O. Chee, M. Ge, G. Bai, and D. D. Kim, "IoTSecSim: A framework for modelling and simulation of security in Internet of things," 2024, *Elsevier*. doi: 10.1016/j.cose.2023.103534.
- [32] A. Kusyanti, I. P. Agraahita Wiguna, and F. Andri Bakhtiar, "Implementasi Algoritme Spongnet sebagai Algoritme Hashing untuk Integritas pada Modul Komunikasi Lora," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 6, pp. 1311–1318, 2023, doi: 10.25126/jtiik.2023107119.
- [33] F. Marwati, A. Akrom, and A. Astofa, "Sosialisasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data Di Era Digital Pada Siswa/I PKBM Wong Sing Gesit," *JIPM J. Inov. Pengabd. Masy.*, vol. 3, no. 1, pp. 11–16, 2025, doi: 10.55903/jipm.v3i1.211.
- [34] A. Salam, "Internet of Things in Agricultural Innovation and Security," *Internet Things Sustain. Community ...*, pp. 71–112, 2024, doi: 10.1007/978-3-031-62162-8_3.
- [35] H. Zhang, M. Zaman, A. Jain, and S. Sampalli, "A Hybrid Machine Learning Intrusion Detection System for Wireless Sensor Networks," *20th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2024*, pp. 830–835, 2024, doi: 10.1109/IWCMC61514.2024.10592535.
- [36] Z. Munawar, N. Indah Putri, I. Iswanto, and D. Widhiantoro, "Analisis Keamanan Pada Teknologi Blockchain," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 8, no. 2, p. 67, 2023, doi: 10.32897/infotronik.2023.8.2.2062.
- [37] M. Ismail, A. Azwar, B. Baharuddin, and H. Hamria, "Analisis Penggunaan Teknologi Blockchain dalam Meningkatkan Keamanan Data: Studi Kasus Industri Keuangan," *J. Janitra Inform. dan Sist. Inf.*, vol. 5, no. 1, pp. 69–77, 2025, doi: 10.59395/m9krbe73.
- [38] K. Biswas, V. Muthukkumarasamy, M. J. M. Chowdhury, X. W. Wu, and K. Singh, "A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks," *Comput. Networks*, vol. 232, 2023, doi: 10.1016/j.comnet.2023.109842.
- [39] M. Ben Farah et al., "A survey on blockchain technology in the maritime industry: Challenges and future perspectives," 2024, *Elsevier*. doi: 10.1016/j.future.2024.03.046.
- [40] J. Li, R. Qin, S. Guan, J. Hou, and F. Y. Wang, "Blockchain Intelligence: Intelligent Blockchains for Web 3.0 and beyond," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 54, no. 11, pp. 6633–6642, 2024, doi: 10.1109/TSMC.2023.3348449.
- [41] S. Caleb and S. J. J. Thangaraj, "Secured Node Identification Approach Based on Artificial Neural Network Infrastructure for Wireless Sensor Networks," *Proc. 9th Int. Conf. Electr. Energy Syst. ICEES 2023*, pp. 646–651, 2023, doi: 10.1109/ICEES57979.2023.10110046.
- [42] F. P. Eka Putra, A. M. Ubaidillah Solichin, M. N. Wildanul Hakim, and M. T. Ramadhan, "Pemanfaatan Teknologi Wireless dan Mobile Network Berbasis 5G Untuk Pemerataan Akses Jaringan di Indonesia," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 415–425, 2025, doi: 10.29408/jit.v8i2.30559.
- [43] D. Darmawan, "Nextcloud: Keamanan Data Terbaik Dengan Manajemen File dan Pengguna yang Cerdas," *J. Sos. Teknol.*, vol. 4, no. 1, pp. 80–89, 2024, doi: 10.59188/jurnalsostech.v4i1.1130.
- [44] P. Di Juni, M. Arief Hasan, Y. Sri Putri Sitompul, J. Alexander, I. Hidayat, and R. Marco Bilbo, "Audit Keamanan Basis Data Menggunakan Sql Server Audit Untuk Deteksi Aktivitas Tidak Sah," 2025, *ejournal.itn.ac.id*. doi: 10.36040/jati.v9i2.13198.
- [45] F. P. E. Putra, M. A. Mahmud, and I. S. Maqom, "Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus," 2024, *researchgate.net*. doi: 10.47709/digitech.v3i2.3457.
- [46] S. P. Kumar, S. Garg, E. Alabdulkreem, and A. Ben Miled, "Advanced generative adversarial network for optimizing layout of wireless sensor networks," *Sci. Rep.*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-83957-5.
- [47] G. H. Adday, S. K. Subramaniam, Z. A. Zukarnain, and N. Samian, "Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 22938–22977, 2024, doi: 10.1109/ACCESS.2024.3362889.
- [48] Fauzan Prasetyo Eka Putra, Dian Tri Agustina, Triana Selvia Khusnul Khotimah, and Tarisha Ramadhanty, "Analisis Kinerja Jaringan 5G dalam Meningkatkan Konektivitas Internet of Things (IoT)," 2025, *researchgate.net*. doi: 10.55606/jitek.v5i1.5836.
- [49] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," 2023, *Springer*. doi: 10.1186/s42400-023-00163-y.
- [50] H. L. Gururaj, R. Natarajan, N. A. Almujaally, F. Flammini, S. Krishna, and S. K. Gupta, "Collaborative Energy-Efficient Routing Protocol for Sustainable Communication in 5G/6G Wireless Sensor Networks," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 2050–2061, 2023, doi: 10.1109/OJCOMS.2023.3312155.