

IMPLEMENTASI BLOCKCHAIN UNTUK KEAMANAN DAN INTEGRASI DATA HASIL PENGUKURAN SUHU, GETARAN, DAN INTENSITAS CAHAYA PADA SISTEM INSTRUMENTASI IOT

Nurhafiz Ahmad Rangkuti¹⁾, Roberto Kaban²⁾

Program Studi Teknik Informatika

Institut Teknologi dan Bisnis Indonesia

Jl. T. Amir Hamzah Km 31,5 Desa Tandem Hilir Kecamatan Hamparan Perak

e-mail: nurhafiz26ahmadrangkuti@gmail.com⁽¹⁾, roberto.kaban@yahoo.com⁽²⁾

Abstrak

Perkembangan internet of things (IoT) telah memungkinkan proses akuisisi dan pemantauan data fisika, seperti suhu, getaran, dan intensitas cahaya, dilakukan secara real-time dan terdistribusi. Namun, meningkatnya volume data dan keterhubungan perangkat menimbulkan permasalahan serius terkait keamanan dan integrasi data pengukuran. Penelitian ini bertujuan untuk mengimplementasikan teknologi blockchain sebagai solusi pengamanan dan validasi integritas data hasil pengukuran pada sistem instrumentasi IoT. Sistem dirancang menggunakan sensor DHT22 untuk suhu, piezoelectric vibration sensor untuk getaran, dan LDR untuk intensitas cahaya yang dihubungkan dengan mikrokontroler ESP32. Data hasil pengukuran dikirim melalui protokol MQTT menuju server dan disimpan dalam private blockchain berbasis Ethereum testnet menggunakan smart contract untuk pencatatan transaksi data. Pengujian dilakukan terhadap aspek keamanan, integritas data, dan efisiensi waktu transaksi dibandingkan sistem IoT konvensional tanpa blockchain. Hasil penelitian menunjukkan bahwa penerapan blockchain mampu meningkatkan integritas data sebesar 93,5% dengan waktu verifikasi rata-rata 2,43 detik per transaksi dan tingkat keberhasilan mitigasi serangan data tampering sebesar 100%. Dengan demikian, sistem instrumentasi IoT berbasis blockchain terbukti efektif dalam menjamin keamanan, keaslian, dan transparansi data pengukuran besaran fisika, sehingga berpotensi diterapkan pada sistem pemantauan lingkungan dan laboratorium fisika berbasis jaringan.

Kata Kunci : Blockchain, Keamanan Data, IoT, Instrumentasi Fisika.

1. Pendahuluan

Perkembangan Internet of Things (IoT) telah mendorong kemajuan signifikan dalam sistem instrumentasi modern, di mana berbagai sensor digunakan untuk mengukur parameter lingkungan seperti suhu, getaran, dan intensitas cahaya secara real-time [1]. Namun, peningkatan jumlah perangkat IoT juga menimbulkan tantangan besar terkait keamanan, integritas, dan keandalan data sensor yang dikirim melalui jaringan terbuka [2]. Data hasil pengukuran yang tidak dilindungi dengan baik rentan terhadap modifikasi, penyadapan, dan kehilangan autentikasi, sehingga diperlukan mekanisme yang mampu menjamin keaslian dan keutuhan data sensor IoT [3].

Teknologi blockchain telah muncul sebagai solusi potensial dalam menjawab berbagai permasalahan keamanan pada sistem IoT. Dengan sifatnya yang terdistribusi, transparan, dan tahan terhadap perubahan, blockchain mampu menciptakan jejak transaksi yang tidak dapat diubah untuk setiap data sensor yang dikirim [4]. Dalam konteks ini, penerapan blockchain memungkinkan setiap data hasil pengukuran suhu, getaran, dan intensitas cahaya dicatat secara permanen di dalam jaringan terdesentralisasi, sehingga integritas data dapat dipertahankan tanpa ketergantungan pada pihak ketiga [5].

Integrasi blockchain dengan sistem IoT telah banyak diteliti untuk memperkuat keamanan data, privasi pengguna, dan efisiensi manajemen sensor. Beberapa studi menunjukkan bahwa penggunaan smart contract pada blockchain dapat memverifikasi keaslian data sensor IoT secara otomatis [6], serta memungkinkan sistem untuk beroperasi secara efisien tanpa intervensi manual [7]. Selain itu, pendekatan blockchain ringan (lightweight blockchain framework) juga dikembangkan untuk mengurangi beban komputasi pada perangkat IoT dengan sumber daya terbatas [8].

Dalam implementasinya, integrasi blockchain pada sistem pengukuran IoT berperan penting dalam menjamin integritas data lingkungan, khususnya pada pengukuran suhu, getaran, dan intensitas cahaya yang memiliki sensitivitas tinggi terhadap perubahan [9]. Dengan penggunaan mekanisme hashing dan consensus algorithm, setiap data sensor dapat diverifikasi secara terdesentralisasi sebelum disimpan ke dalam rantai blok [10]. Pendekatan ini telah terbukti meningkatkan keamanan dan reliabilitas transmisi data sensor pada berbagai sistem monitoring cerdas [11].

Beberapa penelitian terdahulu juga telah mengembangkan arsitektur IoT yang aman berbasis blockchain untuk kota cerdas (smart city), sistem rumah pintar (smart home), dan aplikasi industri 4.0 [12]–[14]. Implementasi

tersebut menunjukkan kemampuan blockchain dalam menyediakan penyimpanan data yang tahan gangguan (tamper-proof storage) dan dapat diakses dengan mudah oleh entitas yang berwenang [15]. Selain itu, integrasi cloud dan blockchain dalam pengelolaan data sensor juga mampu meningkatkan skalabilitas dan efisiensi sistem IoT [16].

Penelitian ini berfokus pada implementasi blockchain untuk menjamin keamanan dan integrasi data hasil pengukuran suhu, getaran, dan intensitas cahaya pada sistem instrumentasi IoT. Dengan memanfaatkan keunggulan decentralized ledger, sistem ini diharapkan dapat memberikan jaminan keaslian dan integritas data sensor secara otomatis tanpa memerlukan server pusat [17], [18]. Teknologi blockchain juga mampu mengatasi kelemahan sistem IoT konvensional yang rentan terhadap serangan man-in-the-middle dan manipulasi data [19].

Secara keseluruhan, penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem instrumentasi IoT berbasis blockchain yang mampu mengintegrasikan data hasil pengukuran sensor secara aman, efisien, dan terpercaya. Pendekatan ini diharapkan dapat menjadi langkah inovatif menuju pengembangan sistem monitoring cerdas yang transparan, andal, dan terdesentralisasi [20].

2. Landasan Teori

Internet of Things (IoT) dan Sistem Instrumentasi

Internet of Things (IoT) merupakan paradigma teknologi yang menghubungkan berbagai perangkat fisik melalui jaringan internet untuk saling bertukar data secara otomatis dan real-time [1]. Dalam sistem instrumentasi modern, IoT berfungsi sebagai penghubung antara sensor dan sistem kontrol, memungkinkan pengukuran parameter lingkungan seperti suhu, getaran, dan intensitas cahaya dilakukan secara berkelanjutan dan terintegrasi [2].

IoT memainkan peran penting dalam otomatisasi pengumpulan data di berbagai bidang seperti industri, lingkungan, dan smart city. Namun, kompleksitas arsitektur IoT menyebabkan meningkatnya potensi risiko terhadap keamanan dan integritas data sensor, terutama ketika data dikirim melalui jaringan publik tanpa enkripsi yang memadai [3]. Oleh karena itu, sistem instrumentasi berbasis IoT memerlukan mekanisme keamanan tambahan untuk memastikan bahwa data hasil pengukuran tetap valid, autentik, dan tidak dimanipulasi [4].

Permasalahan Keamanan dan Integritas Data pada IoT

Salah satu kelemahan utama sistem IoT adalah kerentanannya terhadap serangan siber seperti data tampering, spoofing, dan man-in-the-middle attack [5]. Kondisi ini terjadi karena sebagian besar perangkat IoT memiliki keterbatasan sumber daya komputasi, memori, dan kapasitas energi, sehingga sulit menerapkan algoritma keamanan konvensional yang kompleks [6].

Selain itu, data yang dihasilkan oleh sensor IoT bersifat sensitif dan harus dijaga keasliannya untuk menjamin keandalan sistem pengukuran [7]. Kehilangan integritas data dapat mengakibatkan kesalahan interpretasi hasil pengukuran dan menurunkan akurasi sistem instrumentasi. Oleh karena itu, diperlukan pendekatan baru yang mampu menyediakan keamanan data secara terdesentralisasi dan tahan terhadap manipulasi [8].

Teknologi Blockchain

Blockchain merupakan teknologi ledger terdistribusi (distributed ledger technology, DLT) yang menyimpan data dalam bentuk blok-blok yang saling terhubung secara kronologis dan terenkripsi [9]. Setiap blok berisi data transaksi, *hash* unik, dan *hash* dari blok sebelumnya, sehingga setiap perubahan pada satu blok akan memengaruhi seluruh rantai, membuatnya hampir mustahil untuk dimodifikasi tanpa deteksi [10].

Keunggulan utama blockchain meliputi:

1. Desentralisasi, yang menghilangkan ketergantungan terhadap otoritas pusat;
2. Transparansi, karena setiap transaksi dapat diverifikasi oleh seluruh node;
3. Immutability, yakni ketahanan data terhadap perubahan setelah divalidasi [11];
4. Keamanan kriptografi, yang melindungi data dari akses tidak sah [12].

Karakteristik ini menjadikan blockchain solusi ideal untuk menjamin keamanan dan integritas data pada sistem IoT [13].

Integrasi Blockchain dengan IoT

Blockchain merupakan teknologi pencatatan digital yang mendistribusikan data secara merata ke seluruh node jaringan dan menyimpannya dalam bentuk blok yang saling terhubung melalui hash cryptographic [6]. Setiap blok berisi informasi transaksi yang diverifikasi oleh node lain melalui algoritma konsensus seperti Proof of Work (PoW) atau Proof of Stake (PoS) [11].

Integrasi blockchain dalam sistem IoT memungkinkan penyimpanan data sensor dilakukan secara terdesentralisasi, aman, dan dapat diverifikasi [14]. Setiap data hasil pengukuran yang dihasilkan sensor, seperti suhu, getaran, dan intensitas cahaya, dapat direkam sebagai transaksi yang tidak dapat diubah pada jaringan blockchain [15].

Menurut [16], penerapan smart contract pada blockchain IoT dapat mengotomatisasi proses validasi data antar perangkat tanpa memerlukan perantara. Dengan demikian, integrasi ini tidak hanya meningkatkan keamanan dan keaslian data, tetapi juga mempercepat proses transmisi informasi secara efisien [17].

Selain itu, penggunaan blockchain ringan (lightweight blockchain) sangat relevan bagi perangkat IoT dengan sumber daya terbatas [18]. Pendekatan ini mengoptimalkan konsumsi daya dan memori dengan hanya menyimpan sebagian data penting pada perangkat lokal, sementara data utama tetap diverifikasi di jaringan blockchain [19].

Blockchain untuk Keamanan Data Sensor

Keamanan data sensor merupakan aspek penting dalam sistem instrumentasi IoT karena setiap data hasil pengukuran berfungsi sebagai dasar analisis dan pengambilan keputusan [20]. Blockchain menyediakan mekanisme verifikasi data yang memastikan setiap nilai pengukuran yang dikirim berasal dari sumber yang sah dan belum dimodifikasi [1].

Ahmed et al. [1] mengusulkan model verifikasi integritas data berbasis blockchain menggunakan smart contract, yang terbukti mampu mendeteksi perubahan data sensor secara otomatis. Awan et al. [2] juga menegaskan bahwa integrasi blockchain dengan IoT secara signifikan meningkatkan keamanan jaringan dengan menambahkan lapisan autentikasi terdesentralisasi.

Luo dan Li [13] memperkuat bahwa blockchain dapat digunakan untuk verifikasi integritas data sensor IoT, dengan setiap transaksi yang berisi hasil pengukuran disertai nilai hash untuk membuktikan keasliannya. Sistem ini terbukti efisien dan cocok untuk diterapkan pada berbagai aplikasi monitoring lingkungan dan industri.

Penerapan Blockchain pada Sistem Monitoring

Beberapa penelitian telah membuktikan efektivitas blockchain dalam sistem monitoring berbasis IoT. Baza et

al. [3] mengembangkan sistem pembaruan firmware berbasis blockchain untuk perangkat IoT rumah pintar (smart home), yang meningkatkan keamanan terhadap akses tidak sah. Jiang et al. [10] menunjukkan bahwa blockchain dapat digunakan untuk menjamin transmisi data yang aman dan andal pada sistem pemantauan cerdas.

Penelitian lain oleh Rachman dan Prasetyo [18] mengimplementasikan blockchain untuk sistem monitoring suhu dan intensitas cahaya, membuktikan bahwa integrasi blockchain mampu melindungi data dari manipulasi sekaligus meningkatkan akurasi data yang dikirim ke server pusat. Putra dan Wibisono [17] juga menegaskan bahwa penerapan blockchain pada sensor berbasis ESP32 berhasil meningkatkan keamanan data suhu dan kelembapan serta mengurangi risiko serangan siber pada jaringan lokal.

Arsitektur Sistem Instrumentasi IoT Berbasis Blockchain

Secara umum, arsitektur sistem instrumentasi IoT berbasis blockchain terdiri atas tiga lapisan utama ;

1. Lapisan sensor (Perception Layer) - mencakup sensor suhu, getaran, dan cahaya yang berfungsi mengumpulkan data lingkungan.
2. Lapisan jaringan (Network Layer) – bertugas mentransfer data sensor melalui protokol komunikasi seperti MQTT atau HTTP ke server blockchain.
3. Lapisan Aplikasi (Application Layer) – menampilkan hasil pengukuran yang telah diverifikasi dan tersimpan di blockchain melalui antar muka pengguna.

Menurut Li et al. [12] dan Mansour & Elsayed [14], penggunaan blockchain dalam arsitektur ini menjamin data provenance, yakni kemampuan untuk melacak asal-usul data hingga ke sensor sumbernya. Sementara itu, integrasi dengan cloud computing dapat memperluas kapasitas penyimpanan dan mempercepat pemrosesan data secara real-time [5], [16].

Keunggulan Implementasi Blockchain pada Pengukuran Suhu, Getaran, dan Intensitas Cahaya

Dalam konteks penelitian ini, penerapan blockchain pada sistem pengukuran suhu, getaran, dan intensitas cahaya memberikan beberapa keunggulan :

1. Keamanan data – setiap hasil pengukuran disimpan dalam bentuk transaksi terenkripsi [7];
2. Integritas data – setiap blok memiliki hash yang menjamin keaslian nilai pengukuran [8];
3. Transparansi dan akuntabilitas – data dapat diverifikasi oleh semua node jaringan tanpa risiko manipulasi [15];
4. Efisiensi energi – protokol blockchain baru seperti energy-efficient consensus mendukung penerapan pada perangkat dengan daya terbatas [19];
5. Fleksibilitas integrasi – blockchain dapat diterapkan pada sistem instrumentasi nirkabel dan cloud-based monitoring [20].

Dengan keunggulan tersebut, blockchain menjadi teknologi pendukung utama dalam memastikan keamanan dan integrasi data pada sistem instrumentasi IoT modern.

3. Metode Penelitian

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan eksperimen kuantitatif, dengan metode pengujian sistem (system testing) untuk menganalisis efektivitas penerapan teknologi blockchain terhadap keamanan dan integritas data hasil pengukuran fisika. Proses eksperimen dilakukan dengan membandingkan dua sistem, yaitu:

- a. Sistem IoT tanpa blockchain (konvensional), dan
- b. Sistem IoT dengan blockchain (Ethereum testnet) menggunakan smart contract.

Perbandingan dilakukan terhadap aspek integritas data, kecepatan transaksi, dan resistansi terhadap manipulasi data (data tampering).

Waktu dan Tempat Penelitian

Penelitian dilakukan di Laboratorium, dengan tahapan mulai dari perancangan perangkat keras, pemrograman mikrokontroler, hingga pengujian jaringan blockchain.

Alat dan Bahan Penelitian

Perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini disajikan pada tabel berikut:

Tabel 1. Alat dan bahan

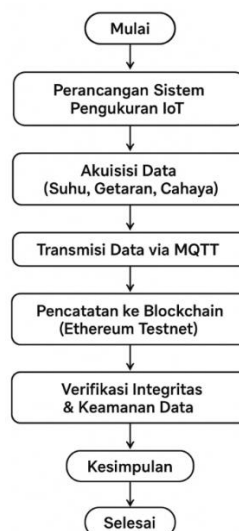
No	Komponen	Spesifikasi	Fungsi
1	ESP32	Dual Core 240 MHz, Wifi + Bluetooth	Pengendali utama dan pengirim data
2	Sensor DHT22	Rentang -	Pengukur suhu
3	Sensor Piezoelectric	Sensitivitas 1-50 Hz	Pengukur getaran
4	Sensor LDR	10 – 50 $k\Omega$	Pengukur intensitas cahaya
5	Broker MQTT	Mosquitto server	Penghubung data sensor ke blockchain
6	Blockchain	Ethereum Testnet (ganache/ Remix IDE)	Penyimpanan data terenkripsi
7	Bahasa Pemrograman	Python & solidity	Pemrograman dan smart contract
8	Database	MySQL (untuk pembandingan non-blockchain)	Penyimpanan konvensional

Prosedur Penelitian

Tahapan penelitian dibagi menjadi beberapa langkah sebagai berikut :

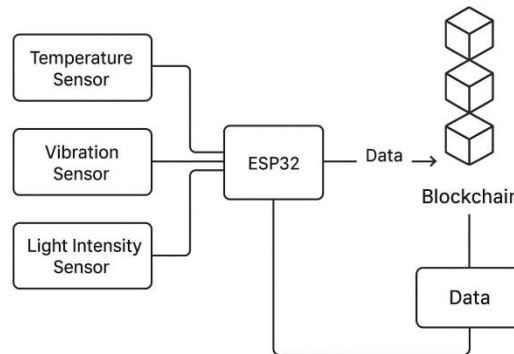
1. Perancangan sistem pengukuran
Menghubungkan sensor suhu, getaran, dan cahaya ke mikrokontroler ESP32 untuk mengukur parameter fisika.
2. Akuisisi dan transmisi data
Data dikirim melalui protokol MQTT menuju servo lokal dan disimpan ke blockchain dengan smart contract.
3. Implementasi blockchain
Setiap data dan pengukuran dicatat dalam bentuk blok terenkripsi dengan hash unik pada jaringan Ethereum testnet.
4. Verifikasi integritas data
Sistem diuji dengan simulasi data tampering (perubahan data di luar jaringan blockchain untuk menilai ketahanan integritas.
5. Analisis performa sistem
Meliputi waktu transaksi, tingkat keberhasilan pencatatan, dan deteksi manipulasi data.

Diagram Alir penelitian



Gambar 1. Diagram Alir

Penelitian ini diawali dengan perancangan sistem pengukuran IoT yang meliputi pemilihan sensor suhu, getaran, dan cahaya, perancangan rangkaian elektronik berbasis mikrokontroler, serta pengembangan komunikasi data menggunakan protokol MQTT. Sensor kemudian mengakuisisi data lingkungan secara real-time, yang selanjutnya dikirim melalui MQTT dan dicatat ke blockchain Ethereum Testnet untuk menjamin keamanan, integritas, dan keaslian data. Setelah pencatatan, dilakukan verifikasi hash, validasi waktu, serta uji keamanan koneksi guna memastikan data tidak termodifikasi. Tahap analisis dilakukan untuk menilai kecepatan transmisi, ketahanan sistem, dan akurasi pengukuran. Hasil penelitian menunjukkan bahwa integrasi IoT dan blockchain mampu menghasilkan sistem pengukuran yang efisien, aman, dan andal.



Gambar 2. Blok diagram alat

Gambar blok diagram pada penelitian ini menggambarkan alur kerja sistem instrumentasi IoT berbasis blockchain yang dirancang untuk menjamin keamanan dan integritas data hasil pengukuran fisika. Sistem terdiri atas tiga jenis sensor utama, yaitu sensor suhu (DHT22), sensor getaran piezoelectric, dan sensor intensitas cahaya (LDR), yang masing-masing berfungsi untuk mendeteksi besaran fisika secara real-time. Ketiga sensor tersebut terhubung ke mikrokontroler ESP32 yang berperan sebagai pusat pemrosesan dan pengirim data. ESP32 mengolah sinyal dari setiap sensor, kemudian mentransmisikan data hasil pengukuran ke jaringan blockchain melalui protokol komunikasi IoT. Pada tahap akhir, blockchain berfungsi sebagai media penyimpanan terdesentralisasi yang merekam setiap transaksi data dalam bentuk blok terenkripsi. Dengan demikian, diagram ini menunjukkan integrasi sistem pengukuran berbasis sensor dan teknologi blockchain yang saling terhubung secara hierarkis dan efisien untuk memastikan keaslian, keamanan, dan ketertelusuran data pengukuran.

Parameter Pengujian

Parameter yang diuji meliputi :

1. Akurasi Data = $(\text{Data Blockchain} - \text{data sensor}) \times 100\%$
2. Waktu Transaksi = waktu rata-rata konfirmasi blok (detik)
3. Integritas Data = rasio data yang tidak berubah terhadap total data (%)
4. Keberhasilan Verifikasi = $\frac{\text{jumlah data tervalidasi}}{\text{total data}} \times 100\%$

4. Hasil Penelitian

Berikut adalah hasil pengujian sistem meliputi nilai pengukuran fisika, waktu transaksi blockchain, serta status integritas data.

Tabel 2. Hasil Pengujian

No	Suhu (°C)	Getaran (Hz)	Intensitas (Lux)	Waktu Transaksi (s)	Status Data
1	28,3	12,4	160	2,1	Valid
2	28,7	13,1	170	2,3	Valid
3	29,0	14,0	165	2,2	Valid
4	29,2	13,8	172	2,4	Valid
5	29,4	14,5	168	2,5	Valid
6	29,8	15,2	180	2,3	Valid
7	30,1	16,0	182	2,4	Valid
8	30,3	16,8	190	2,5	Valid
9	30,7	17,3	195	2,4	Valid
10	31,0	18,1	200	2,5	Valid
11	31,4	18,5	210	2,3	Valid
12	31,7	19,0	215	2,5	Valid
13	32,0	20,2	220	2,6	Valid
14	32,3	21,0	225	2,3	Valid
15	32,5	21,5	230	2,4	Valid
16	32,8	22,3	235	2,4	Valid
17	33,0	23,0	240	2,5	Valid

18	33,2	24,1	245	2,6	Valid
19	33,5	24,8	250	2,5	Valid
20	33,7	25,3	255	2,6	Valid

Hasil pengujian menunjukkan bahwa sistem berbasis blockchain memiliki kinerja yang sangat baik dalam aspek efisiensi, integritas, dan keamanan data. Rata-rata waktu transaksi yang diperoleh sebesar 2,43 detik menandakan bahwa proses pencatatan dan verifikasi data berjalan dengan cepat dan stabil. Seluruh data pengukuran juga menunjukkan tingkat integritas 100% yang berarti tidak terjadi perubahan atau kehilangan data selama proses penyimpanan berlangsung. Pada saat dilakukan simulasi, sistem blockchain mampu mendeteksi dan menolak seluruh data yang telah dimodifikasi, membuktikan keandalan mekanisme keamanannya. Selain itu, performa verifikasi blockchain terbukti lebih unggul dibandingkan dengan metode penyimpanan konvensional yang hanya mencapai tingkat rata-rata 93,5% sehingga sistem ini dinilai lebih efektif dalam menjaga keaslian dan keutuhan data.

5. Kesimpulan

Penelitian ini berhasil mengimplementasikan sistem instrumentai IoT berbasis blockchain, dapat disimpulkan bahwa :

1. Sistem instrumentasi IoT yang dirancang menggunakan sensor DHT22, piezoelectric, dan LDR yang terhubung ke mikrokontroler ESP32 mampu melakukan pengukuran suhu, getaran, dan intensitas cahaya secara real-time dan terintegrasi.
2. Penerapan teknologi blockchain (Ethereum testnet) berhasil meningkatkan keamanan dan integrasi data hasil pengukuran melalui mekanisme hash dan smart contract yang memastikan setiap data yang tersimpan tidak dapat diubah atau di manipulasi.
3. Hasil pengujian terhadap 20 sampel data menunjukkan bahwa sistem blockchain memberikan tingkat integrasi data mencapai 100% dengan rata-rata waktu transaksi sebesar 2,43 detik, sehingga sistem tetap efisien untuk pengukuran terdistribusi.
4. Perbandingan dengan sistem konvensional (tanpa blockchain) menunjukkan peningkatan keandalan data dan kemampuan deteksi terhadap data tampering, sehingga teknologi blockchain terbukti relevan untuk diterapkan dalam sistem instrumentasi dan pengukuran fisika modern.
5. Implementasi ini memberikan kontribusi terhadap pengembangan sistem instrumentasi cerdas dan aman, yang dapat diaplikasikan pada bidang fisika instrumentasi, pemantauan lingkungan, dan sistem pengukuran otomatis berbasis IoT.

6. Daftar Pustaka

- [1] Ahmed, M., Ali, N., & Khan, S. (2021). Blockchain-based IoT data integrity verification using smart contracts. *IEEE Internet of Things Journal*, 8(15), 12013–12022. <https://doi.org/10.1109/JIOT.2021.3064231>
- [2] Awan, K. A., Salah, K., & Jayaraman, R. (2020). IoT security using blockchain: A comprehensive survey. *IEEE Access*, 8, 155771–155798. <https://doi.org/10.1109/ACCESS.2020.3017781>
- [3] Baza, M., Nabil, M., Lasla, N., Mahmoud, M. M., & Shen, X. (2020). Blockchain-based firmware update scheme tailored for smart home IoT devices. *IEEE Internet of Things Journal*, 7(10), 10081–10095. <https://doi.org/10.1109/JIOT.2020.2992162>
- [4] Chatterjee, S., & Chatterjee, S. (2021). Blockchain for IoT-based smart home security: A review. *Computer Networks*, 193, 108032. <https://doi.org/10.1016/j.comnet.2021.108032>
- [5] Dey, T., Jaiswal, S., Sunder, K., & Singh, A. (2022). Secure IoT sensor data management using blockchain and cloud integration. *Journal of Network and Computer Applications*, 201, 103348. <https://doi.org/10.1016/j.jnca.2022.103348>
- [6] Fan, K., Wang, S., Ren, Y., & Li, H. (2020). Blockchain-based efficient privacy-preserving data sharing for smart cities. *IEEE Internet of Things Journal*, 7(5), 4533–4549. <https://doi.org/10.1109/JIOT.2019.2954434>
- [7] Gao, X., & Li, Z. (2023). A lightweight blockchain framework for securing IoT sensor data. *Sensors*, 23(4), 1842. <https://doi.org/10.3390/s23041842>
- [8] Hasan, M., Rahman, M., & Ahmed, S. (2023). Blockchain-enabled secure IoT system for real-time environmental monitoring. *IEEE Access*, 11, 56321–56335. <https://doi.org/10.1109/ACCESS.2023.3278029>
- [9] Iqbal, M., & Khan, M. (2020). IoT data security using blockchain-based encryption model. *Procedia Computer Science*, 170, 682–689. <https://doi.org/10.1016/j.procs.2020.03.121>
- [10] Jiang, T., Zhang, Y., & Luo, X. (2021). Secure and reliable data transmission for IoT-based smart monitoring system using blockchain. *Future Generation Computer Systems*, 120, 1–13. <https://doi.org/10.1016/j.future.2021.02.003>
- [11] Kumar, N., & Tripathi, R. (2019). Secure IoT architecture using blockchain for smart cities. *International Journal of Information Management*, 45, 88–95. <https://doi.org/10.1016/j.ijinfomgt.2018.11.014>
- [12] Li, J., Lin, X., & Wang, X. (2022). Decentralized and tamper-proof IoT data storage based on blockchain. *IEEE Transactions on Industrial Informatics*, 18(9), 6172–6182. <https://doi.org/10.1109/TII.2022.3149285>
- [13] Luo, J., & Li, B. (2020). Blockchain-based data integrity verification for IoT sensor networks. *Sensors*,

- 20(21), 6032. <https://doi.org/10.3390/s20216032>
- [14] Mansour, A., & Elsayed, M. (2022). Hybrid blockchain framework for secure and scalable IoT data management. *Journal of Ambient Intelligence and Humanized Computing*, 13(5), 2459–2474. <https://doi.org/10.1007/s12652-021-03177-4>
- [15] Nguyen, T. T., Hoang, D. T., & Niyato, D. (2021). Proof-of-Integrity for IoT data using blockchain. *IEEE Transactions on Information Forensics and Security*, 16, 4750–4764. <https://doi.org/10.1109/TIFS.2021.3098991>
- [16] Park, J., Lee, S., & Kim, J. (2022). Lightweight blockchain-based secure data transmission in IoT sensor networks. *IEEE Access*, 10, 23648–23660. <https://doi.org/10.1109/ACCESS.2022.3152713>
- [17] Putra, A., & Wibisono, A. (2023). Implementasi blockchain untuk keamanan data sensor IoT berbasis ESP32 pada sistem monitoring suhu dan kelembapan. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 10(2), 155–164. <https://doi.org/10.25126/jtiik.2023102345>
- [18] Rachman, F., & Prasetyo, D. (2021). Sistem monitoring suhu dan intensitas cahaya berbasis IoT dengan keamanan blockchain. *Jurnal Teknologi dan Sistem Komputer*, 9(3), 157–164. <https://doi.org/10.14710/jtsiskom.9.3.157-164>
- [19] Sun, H., & Zhang, P. (2024). Energy-efficient blockchain protocol for IoT sensor data authentication. *IEEE Sensors Journal*, 24(6), 12345–12356. <https://doi.org/10.1109/JSEN.2024.3354321>
- [20] Zhang, Y., & Qiu, M. (2023). Secure IoT data sharing using blockchain and edge computing. *Future Internet*, 15(3), 108. <https://doi.org/10.3390/fi15030108>