Jurnal Informatika dan Tekonologi Komputer
E-ISSN: 2809-9230
P-ISSN: 2809-9249

Blockchain sebagai Pilar Keamanan IoT: Tinjauan Sistematis tentang Mekanisme Otentikasi dan Integritas Data

Nur Sa'diah Nasution [1]*, Adelia Mestika Kusuma W [1], Bela Sukma Yani [1], Indah Oktavia Ramadhani [1], May Utami[1], Mucklas Arya Qodri [1], Nurul Annisa [1]

[1] Program Studi Sistem Informasi, Universitas Mikroskil, Sumatera Utara; Indonesia
* Corresponding Author : Nur Sa'diah Nasution, email: nasutionnursadiah@gmail.com

Abstract: *This study explores the significance of Blockchain technology in bolstering the security of Internet of Things (IoT) systems, particularly concerning authentication and data integrity mechanisms. Utilizing a systematic literature review (SLR) approach, the research involves formulating research questions, performing extensive literature searches, setting inclusion and exclusion criteria, selecting pertinent studies, and processing and analyzing the data to draw conclusions. The findings indicate that Blockchain considerably enhances IoT security by offering robust authentication techniques that ensure only authorized devices gain network access, in addition to improving data integrity through unalterable transaction records. Furthermore, the decentralized nature of Blockchain reduces single points of failure and increases system resilience against cyberattacks. These results highlight Blockchain's potential to address security weaknesses within IoT frameworks. In summary, this research emphasizes the critical role of Blockchain in securing IoT ecosystems and building trust among users and stakeholders. Future investigations should aim to tackle scalability and interoperability issues, as well as evaluate real-world implementations, to maximize the effectiveness of Blockchain in IoT security.*

Keywords: *Authentication; Blockchain; Data Integration; Internet of Things (IoT); Security*

Abstrak: Penelitian ini mengkaji pentingnya teknologi Blockchain dalam memperkuat keamanan sistem Internet of Things (IoT), khususnya terkait mekanisme autentikasi dan integritas data. Dengan menggunakan pendekatan tinjauan literatur sistematis (SLR), penelitian ini melibatkan penyusunan pertanyaan penelitian, pencarian literatur yang komprehensif, penetapan kriteria inklusi dan eksklusi, pemilihan studi yang relevan, serta pengolahan dan analisis data untuk menarik kesimpulan. Hasil penelitian menunjukkan bahwa Blockchain secara signifikan meningkatkan keamanan IoT dengan menyediakan teknik autentikasi yang tangguh, memastikan hanya perangkat yang berwenang yang dapat mengakses jaringan, serta meningkatkan integritas data melalui catatan transaksi yang tidak dapat diubah. Selain itu, sifat desentralisasi Blockchain mengurangi titik kegagalan tunggal dan meningkatkan ketahanan sistem terhadap serangan siber. Hasil ini menyoroti potensi Blockchain dalam mengatasi kelemahan keamanan dalam kerangka kerja IoT. Secara ringkas, penelitian ini menekankan peran kritis Blockchain dalam mengamankan ekosistem IoT dan membangun kepercayaan di antara pengguna dan pemangku kepentingan. Penelitian masa depan sebaiknya fokus pada mengatasi masalah skalabilitas dan interoperabilitas, serta mengevaluasi implementasi dunia nyata, untuk memaksimalkan efektivitas Blockchain dalam keamanan IoT.

Kata kunci: BlockChain; Integrasi Data; Internet of Things (IoT); Keamanan; Otentitkasi

Naskah Masuk: 19 Desember 2025
Revisi: 23 Desember 2025
Diterima: 30 Maret 2026
Terbit: 31 Maret 2026
Ver. Skrg.: 31 Maret 2026

1. Pendahuluan

Internet of Things (IoT) merupakan konsep jaringan perangkat fisik yang saling terhubung mulai dari peralatan rumah tangga, sensor wearable, hingga mesin industri yang mampu berkomunikasi dan bertukar data melalui internet tanpa memerlukan intervensi manusia secara langsung. Dalam satu dekade terakhir, perkembangan IoT berlangsung sangat pesat dan menjadi salah satu pilar utama transformasi digital di berbagai sektor, seperti kesehatan, manufaktur, pertanian, transportasi, dan smart city. International Data Corporation (IDC) memproyeksikan bahwa jumlah perangkat IoT yang terhubung akan melampaui 41 miliar unit pada tahun 2025, yang menunjukkan besarnya skala dan potensi teknologi ini dalam mengubah aktivitas manusia maupun proses industri [1].

Teknologi IoT memungkinkan pemantauan secara real-time, otomatisasi, serta optimalisasi proses sehingga dapat meningkatkan efisiensi dan menekan biaya operasional. Dalam konteks rumah pintar, IoT memungkinkan pengendalian jarak jauh terhadap sistem pencahayaan, keamanan, dan pengaturan suhu. Sementara itu, pada sektor industri, IoT mendukung penerapan predictive maintenance serta efisiensi manajemen rantai pasok. Namun demikian, pertumbuhan perangkat yang terhubung secara masif juga menimbulkan berbagai risiko baru, khususnya terkait keamanan dan privasi data. Perangkat IoT umumnya mengumpulkan dan memproses data sensitif, seperti data pribadi, rekam medis, maupun transaksi keuangan, sehingga menjadikannya target yang rentan terhadap serangan siber.

Berbagai penelitian menunjukkan bahwa sebagian besar perangkat IoT masih memiliki tingkat kerentanan yang tinggi. Bhalfaqih et al. mengungkapkan bahwa lebih dari 70% perangkat IoT rentan terhadap berbagai ancaman siber, seperti akses tidak sah, pencurian data, injeksi malware, serta serangan Distributed Denial of Service (DDoS) [2]. Kerentanan ini semakin diperparah oleh karakteristik jaringan IoT yang bersifat terdistribusi dan heterogen, di mana perangkat beroperasi dengan kemampuan perangkat keras, protokol komunikasi, dan standar keamanan yang berbeda-beda. Kondisi tersebut menjadikan penerapan autentikasi yang aman, integritas data, dan komunikasi tepercaya antarperangkat sebagai tantangan utama dalam pengembangan sistem IoT.

Salah satu teknologi yang dinilai memiliki potensi besar untuk mengatasi permasalahan keamanan tersebut adalah Blockchain. Blockchain merupakan sistem buku besar terdistribusi dan terdesentralisasi yang mencatat transaksi secara aman dan transparan dengan memanfaatkan teknik kriptografi [3]. Berbeda dengan sistem terpusat, Blockchain tidak bergantung pada satu otoritas tunggal dalam proses validasi data, melainkan menggunakan mekanisme konsensus antar node jaringan. Karakteristik ini menjadikan data yang telah tercatat bersifat immutable, sehingga tidak dapat diubah atau dihapus, dan sangat relevan untuk meningkatkan kepercayaan serta keamanan dalam ekosistem IoT.

Dalam implementasinya pada IoT, Blockchain mampu menyediakan mekanisme autentikasi yang aman dengan memberikan identitas digital unik bagi setiap perangkat, sehingga hanya perangkat yang terverifikasi yang dapat bergabung dan berinteraksi dalam jaringan. Selain itu, Blockchain mendukung integritas dan keterlacakan data dengan mencatat seluruh transaksi antarperangkat ke dalam ledger yang tahan terhadap manipulasi. Sejumlah penelitian sebelumnya menunjukkan bahwa integrasi Blockchain dan IoT dapat mengurangi risiko keamanan, menekan potensi serangan siber, serta meningkatkan kepercayaan pengguna terhadap sistem berbasis teknologi cerdas. Arsitektur terdesentralisasi Blockchain juga mengurangi ketergantungan pada server terpusat yang kerap menjadi single point of failure.

Meskipun menawarkan berbagai keunggulan, penerapan Blockchain pada sistem IoT masih menghadapi sejumlah tantangan. Isu skalabilitas menjadi perhatian utama karena Blockchain harus menangani volume data yang sangat besar dari miliaran perangkat IoT. Proses validasi transaksi dan mekanisme konsensus membutuhkan sumber daya komputasi yang tinggi, sementara sebagian besar perangkat IoT memiliki keterbatasan daya dan kapasitas pemrosesan. Selain itu, permasalahan interoperabilitas, konsumsi energi, latensi transaksi, biaya implementasi, serta belum adanya standar global untuk integrasi Blockchain–IoT turut menghambat adopsi secara luas.

Oleh karena itu, penelitian ini dilakukan dengan menggunakan pendekatan Systematic Literature Review (SLR) untuk mengkaji peran teknologi Blockchain dalam meningkatkan keamanan, integritas data, dan keandalan operasional sistem IoT. Kajian ini menganalisis penelitian-penelitian relevan yang dipublikasikan pada periode 2020–2025 guna mengidentifikasi mekanisme yang telah dikembangkan, menilai efektivitasnya, serta mengungkap celah penelitian dan arah pengembangan di masa depan, khususnya terkait mekanisme autentikasi, integritas data, dan strategi implementasi yang skalabel.

2. Kajian Pustaka atau Penelitian Terkait

Internet of Things (IoT) merupakan konsep jaringan perangkat fisik yang saling terhubung dan mampu berkomunikasi serta bertukar data melalui internet secara otomatis tanpa keterlibatan manusia secara langsung. Perangkat IoT memiliki kemampuan untuk mengumpulkan, mengirim, dan memproses data secara real-time, sehingga banyak dimanfaatkan dalam berbagai sektor. Namun, karakteristik IoT yang bersifat heterogen, terdistribusi, dan memiliki keterbatasan sumber daya menjadikannya rentan terhadap berbagai ancaman keamanan [4].

Keamanan sistem IoT merujuk pada upaya perlindungan terhadap perangkat, jaringan, dan data dari akses tidak sah, penyalahgunaan, serta serangan siber. Aspek utama dalam keamanan IoT meliputi autentikasi, integritas data, dan keandalan sistem. Autentikasi berfungsi untuk memastikan bahwa hanya perangkat atau entitas yang sah yang dapat mengakses dan berinteraksi dalam jaringan IoT, sedangkan integritas data bertujuan untuk menjamin bahwa data tidak mengalami perubahan selama proses pengiriman maupun penyimpanan [5].

Blockchain merupakan teknologi buku besar terdistribusi dan terdesentralisasi yang mencatat transaksi secara aman dan transparan dengan memanfaatkan kriptografi dan mekanisme konsensus. Setiap data yang telah dicatat dalam Blockchain bersifat tidak dapat diubah (immutable), sehingga mampu meningkatkan kepercayaan antar entitas dalam jaringan. Karakteristik tersebut menjadikan Blockchain relevan sebagai solusi alternatif dalam meningkatkan keamanan sistem yang bersifat terdistribusi, termasuk IoT [6].

Dalam konteks IoT, Blockchain berperan sebagai mekanisme pengaman yang mampu menyediakan autentikasi perangkat berbasis identitas digital serta menjamin integritas data melalui pencatatan transaksi yang tahan terhadap manipulasi. Integrasi Blockchain dan IoT diharapkan dapat mengurangi ketergantungan pada sistem terpusat, meningkatkan transparansi, serta memperkuat keandalan dan keamanan komunikasi antarperangkat.

3. Metode yang Diusulkan

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk mengeksplorasi peran teknologi Blockchain dalam meningkatkan keamanan sistem Internet of Things (IoT). Metode SLR dipilih karena kemampuannya untuk memberikan gambaran komprehensif tentang penelitian yang ada dan mengidentifikasi celah dalam literatur saat ini. Menurut Stefanescu dkk. (2022), SLR adalah metode terstruktur dan transparan untuk mengidentifikasi, mengevaluasi, dan menafsirkan semua penelitian relevan pada topik tertentu, sehingga memberikan landasan yang kokoh untuk pengambilan keputusan [7]. Berikut adalah tahapan metode tersebut :

3.1 Rumusan Masalah

a. RQ1 : Bagaimana teknologi Blockchain dapat meningkatkan keamanan sistem IoT, terutama dalam hal autentikasi?
b. RQ2 : Mekanisme apa yang digunakan Blockchain untuk meningkatkan integritas data dalam sistem IoT?

c. RQ3 : Membahas tantangan utama yang dihadapi dalam implementasi Blockchain di lingkungan IoT, seperti keterbatasan sumber daya perangkat, kompleksitas sistem, dan persyaratan skalabilitas.

3.2 Pencarian literatur

Pencarian dilakukan di berbagai basis data akademik, termasuk IEEE Xplore, SpringerLink, dan ScienceDirect, dengan menggunakan kata kunci relevan seperti "Blockchain," "Internet of Things," "keamanan," "otentikasi," dan "integritas data." Pencarian sistematis dan komprehensif sangat penting untuk memastikan bahwa semua penelitian yang relevan teridentifikasi dan dianalisis. Selain itu, penelitian oleh Yang dkk. (2025) menunjukkan bahwa penggunaan kata kunci yang tepat dan relevan dapat meningkatkan kualitas dan relevansi hasil pencarian, memungkinkan peneliti untuk menemukan artikel yang paling sesuai dengan topik mereka [8].

3.3 Pemilihan literatur

Menetapkan kriteria inklusi dan eksklusi sangat penting dalam memilih studi yang akan dimasukkan ke dalam tinjauan. Kriteria ini sangat penting untuk memastikan bahwa hanya studi berkualitas tinggi yang dimasukkan ke dalam analisis. Menurut [8], memiliki kriteria inklusi dan eksklusi yang jelas membantu meminimalkan bias dalam pemilihan studi dan memastikan bahwa hasil tinjauan literatur dapat diandalkan [9].

Tabel 1 Pemilihan Literatur

Kriteria Inklusi	Kriteria Eksklusi
Semua artikel harus diterbitkan antara tahun 2020 dan 2025	Artikel yang diterbitkan sebelum tahun 2020 atau setelah tahun 2025 akan dikecualikan.
Artikel ilmiah harus diterbitkan dalam bahasa Inggris dan oleh jurnal internasional.	Artikel yang tidak ditulis dalam bahasa Inggris atau diterbitkan di jurnal non-internasional akan dikecualikan
Setiap artikel harus secara eksplisit membahas penerapan Blockchain dalam konteks Internet of Things (IoT).	Artikel yang tidak secara khusus membahas penerapan Blockchain dalam IoT, seperti yang fokus hanya pada Blockchain dalam bidang kesehatan, keuangan, atau manajemen data umum, akan dikecualikan.
Artikel yang dipilih harus secara kolektif menyoroti aspek keamanan, integrasi, atau efisiensi sistem IoT melalui implementasi Blockchain.	Artikel yang tidak memberikan kontribusi signifikan terhadap aspek keamanan, integrasi, atau efisiensi sistem IoT melalui Blockchain akan dikecualikan.
Semua jurnal harus terdiri dari artikel ilmiah yang direview oleh rekan sejawat, termasuk tinjauan literatur, survei, dan studi eksperimental, dengan metodologi yang jelas	Artikel dari sumber yang tidak direview oleh rekan sejawat, seperti majalah, blog, white paper perusahaan, atau prosiding konferensi yang tidak terverifikasi, akan dikecualikan.

Setelah proses penyaringan ini, artikel yang lolos akan dievaluasi lebih lanjut melalui Penilaian Kualitas (QA) dengan merujuk pada Pertanyaan Penelitian (RQ) untuk memastikan relevansi dan kualitas akademiknya.

Tabel 2 Penilaian Kualitas

Kode	Penilaian Kualitas
QA1	Apakah artikel ini membahas penerapan Blockchain dalam konteks keamanan IoT, khususnya terkait autentikasi?
QA2	Apakah artikel ini membahas mekanisme Blockchain untuk meningkatkan integritas data dalam IoT?
QA3	Apakah artikel ini mengeksplorasi tantangan dan strategi dalam menerapkan Blockchain untuk meningkatkan keamanan IoT?

Penilaian dilakukan dengan memberikan tanda "✓" jika artikel memenuhi kriteria dan dianggap relevan. Artikel yang lolos semua tiga kriteria QA akan dikategorikan sebagai "Studi Terpilih" dan digunakan sebagai dasar pada tahap Penyajian Data untuk analisis lebih lanjut.

4. Hasil dan Pembahasan

4.1 Hasil

Penelitian ini berfokus pada tiga aspek utama implementasi Blockchain dalam konteks Internet of Things (IoT):

a. Mekanisme autentikasi: Bagaimana Blockchain meningkatkan autentikasi perangkat IoT.
b. Integritas data: Sejauh mana Blockchain memastikan keaslian dan integritas data.
c. Tantangan implementasi: Hambatan teknis dan non-teknis yang dihadapi saat mengintegrasikan Blockchain dengan IoT.

Ulasan literatur dilakukan menggunakan basis data IEEE Xplore, SpringerLink, dan ScienceDirect, dengan menggunakan frasa kunci seperti Blockchain, Internet of Things, Keamanan IoT, autentikasi, dan integritas data. Pencarian awal menghasilkan sekitar 50 artikel yang relevan dengan topik penelitian. Dengan menerapkan kriteria inklusi dan eksklusi, 25 artikel diidentifikasi sebagai relevan dengan fokus penelitian.

Tabel 3 Kriteria Inklusi

Kriteria Inklusi	**Jumlah Artikel**
Semua artikel harus diterbitkan antara tahun 2020 dan 2025.	50
Artikel literatur harus diterbitkan dalam bahasa Inggris dan oleh jurnal internasional.	50
Setiap artikel harus secara eksplisit membahas penerapan Blockchain dalam konteks Internet of Things (IoT).	40
Artikel yang dipilih harus secara kolektif menyoroti aspek keamanan, integrasi, atau efisiensi sistem IoT melalui implementasi Blockchain	35
Semua jurnal harus terdiri dari artikel ilmiah yang direview oleh rekan sejawat, termasuk tinjauan literatur, survei, dan studi eksperimental, dengan metodologi yang jelas	25

Berdasarkan tabel inklusi data artikel di atas, hasil menunjukkan bahwa 25 artikel dilanjutkan ke tahap berikutnya dan 25 jurnal dikecualikan dan tidak dilanjutkan ke tahap berikutnya. Penilaian Kualitas (QA) dilakukan pada 25 artikel yang termasuk, berdasarkan kriteria yang telah ditetapkan. Akibatnya, 7 artikel memenuhi semua standar kualitas dan diklasifikasikan sebagai Studi Terpilih. Artikel-artikel terpilih ini menjadi dasar utama untuk analisis yang disajikan dalam penelitian ini.

Tabel 4. Artikel terpilih

Author	Title	QA1	QA2	QA3	Result
Dlimi et al., 2021 (Et. Al., 2021)	Kerangka Kerja Blockchain Ringan untuk Integrasi IoT di Kota Cerdas	✓	✓	✓	V
Stefanescu et al., 2022 (Stefanescu et al., 2022)	Tinjauan Literatur Sistematis tentang Blockchain Ringan untuk IoT	✓	✓	✓	V
Alzoubi, 2024 (Alzoubi, 2024)	Blockchain dalam IoT: Keamanan, Aplikasi, Teknologi, dan Tantangan	✓	✓	✓	V
Singh et al., 2023 (Kumar et al., 2023)	Kontrol Akses Berbasis Blockchain untuk Mencegah Serangan Siber dalam IoT: Tinjauan Literatur Sistematis	✓	✓	✓	V
Chen et al., 2023 (Chen et al., 2023)	Arsitektur Keamanan IoT Berbasis Blockchain dan Aplikasinya	✓	✓	✓	V
Saidu et al., 2023 (Saidu et al., 2025)	Menjelajahi Konvergensi Blockchain–IoT untuk Pelacakan Logistik	✓	✓	✓	V
Ali et al., 2025 (Guma Ali et al., 2025)	Integrasi Blockchain, IoT, Kecerdasan Buatan, dan Robotika untuk Pengelolaan Sampah yang Efisien di Kota Cerdas	✓	✓	✓	V

4.2 Pembahasan

Wawasan yang diperoleh dari studi-studi terpilih memberikan gambaran tentang cara Blockchain dapat memperkuat otentikasi, memastikan integritas data, dan mengatasi tantangan yang terkait dengan implementasi Blockchain dalam lingkungan IoT.

4.2.1. RQ1 – Bagaimana Teknologi Blockchain Dapat Meningkatkan Keamanan Sistem IoT, Terutama dalam Hal Otentikasi?

Studi-studi yang ditinjau secara konsisten menunjukkan bahwa Blockchain secara signifikan meningkatkan mekanisme autentikasi dalam sistem IoT. Autentikasi merupakan aspek yang sangat penting dalam keamanan IoT karena menjamin bahwa hanya perangkat yang memiliki otorisasi yang dapat terhubung ke jaringan. Dlimi et al. memperkenalkan kerangka kerja Blockchain ringan yang dirancang untuk integrasi IoT dalam lingkungan smart city, yang memanfaatkan manajemen identitas terdesentralisasi untuk memverifikasi keaslian perangkat sehingga mengurangi ketergantungan pada otoritas pusat [9]. Model terdesentralisasi ini menurunkan risiko terjadinya *single point of failure*, sebagaimana dikemukakan oleh Zhang et al., yang menyatakan bahwa otoritas terpusat rentan terhadap serangan siber [10].

Singh et al. mengkaji berbagai strategi pengendalian akses berbasis Blockchain dan menunjukkan bahwa *smart contract* mampu mengotomatisasi proses autentikasi serta secara efektif mencegah akses tidak sah [11]. Temuan ini sejalan dengan penelitian Kumar dan Singh yang menegaskan bahwa *smart contract* meningkatkan keamanan dengan menegakkan aturan yang telah ditetapkan tanpa intervensi manusia, sehingga meminimalkan risiko kesalahan manusia [12]. Chen et al. mengembangkan arsitektur keamanan IoT berbasis Blockchain dan membuktikan bahwa penggunaan *ledger* yang bersifat *immutable* serta protokol kriptografi dapat menumbuhkan kepercayaan antarperangkat [13]. Hal ini diperkuat oleh Ullah yang menemukan bahwa transparansi yang ditawarkan oleh Blockchain meningkatkan kepercayaan dalam interaksi antarperangkat, terutama dalam lingkungan di mana perangkat beroperasi secara otonom [14].

Secara keseluruhan, temuan-temuan tersebut menegaskan bahwa Blockchain menyediakan mekanisme autentikasi yang kuat dan terdesentralisasi, sehingga mampu mengatasi salah satu kerentanan utama dalam jaringan IoT. Dengan memastikan bahwa hanya perangkat yang terautentikasi yang dapat berkomunikasi, teknologi Blockchain secara efektif mengurangi risiko akses tidak sah serta potensi terjadinya pelanggaran data.

4.2.2. RQ2 – Mekanisme Apa yang Digunakan Blockchain untuk Meningkatkan Integritas Data dalam Sistem IoT?

Literatur menunjukkan bahwa Blockchain berperan penting dalam menjamin integritas data melalui berbagai mekanisme. Stefanescu et al. mencatat bahwa kerangka kerja Blockchain ringan mampu menjaga pencatatan data IoT yang tahan terhadap manipulasi, sehingga integritas data tetap terjaga meskipun digunakan pada perangkat dengan sumber daya terbatas [15]. Hal ini sangat penting dalam situasi yang menuntut tingkat akurasi data yang tinggi, sebagaimana ditekankan oleh Alzoubi, yang menyatakan bahwa pemeliharaan integritas data merupakan aspek krusial dalam pengambilan keputusan pada aplikasi IoT [8].

Alzoubi juga menjelaskan bahwa penggunaan hashing kriptografi dan mekanisme konsensus memungkinkan data IoT bersifat *immutable*, sehingga mencegah terjadinya perubahan data tanpa otorisasi [4]. Penerapan hash kriptografi menjamin bahwa setiap perubahan terhadap data dapat segera terdeteksi, sehingga keaslian informasi tetap terjaga. Saidu et al. meneliti pemanfaatan Blockchain untuk keterlacakan logistik dalam sistem IoT dan menunjukkan bahwa sifat data yang tidak dapat diubah mendukung proses pelacakan dan audit yang andal [9]. Fitur ini sangat penting bagi industri yang bergantung pada akurasi data untuk memenuhi kepatuhan dan efektivitas operasional. Khan et al. memperkuat temuan tersebut dengan menunjukkan bahwa struktur terdesentralisasi Blockchain meningkatkan integritas data karena menghilangkan risiko kegagalan pada satu titik (*single point of failure*) yang dapat mengancam keakuratan data [16]. Mekanisme konsensus yang digunakan dalam Blockchain memastikan bahwa seluruh peserta jaringan mencapai kesepakatan terhadap validitas data, sehingga semakin memperkuat integritas data.

Studi-studi tersebut menunjukkan bahwa *ledger* Blockchain yang bersifat immutable dan mekanisme konsensusnya memberikan tingkat jaminan yang tinggi terhadap integritas data, yang sangat penting bagi aplikasi IoT yang bergantung pada data yang akurat dan andal. Dengan memastikan bahwa data tidak dapat dimodifikasi tanpa terdeteksi, teknologi Blockchain meningkatkan keandalan sistem IoT, yang krusial bagi berbagai aplikasi, mulai dari bidang kesehatan hingga manajemen rantai pasok.

4.2.3. RQ3 – Tantangan Apa Saja yang Dihadapi dalam Implementasi Teknologi Blockchain pada Konteks IoT?

Meskipun memiliki berbagai manfaat, integrasi teknologi Blockchain ke dalam sistem IoT menghadirkan sejumlah tantangan:

Keterbatasan Sumber Daya: Perangkat IoT berdaya rendah dapat mengalami kesulitan dalam menjalankan algoritma Blockchain secara efisien, sebagaimana disoroti oleh Ali et al. dalam konteks pengelolaan limbah smart city [7]. Permasalahan ini semakin diperkuat oleh temuan Saputhanthri et al. yang menyatakan bahwa banyak perangkat IoT tidak memiliki kapasitas komputasi yang dibutuhkan untuk menjalankan operasi kriptografi yang kompleks, sehingga menyulitkan implementasi solusi Blockchain secara efektif 5].

a. Skalabilitas: Kemampuan untuk mengelola volume data besar yang dihasilkan oleh perangkat IoT dapat menjadi kendala bagi jaringan Blockchain. Kerangka kerja ringan dan hibrida telah diusulkan untuk mengatasi tantangan ini [15]. Abbassi et al. juga menekankan pentingnya solusi yang skalabel dengan mengusulkan mekanisme konsensus hibrida yang dapat meningkatkan kinerja pada lingkungan dengan volume transaksi yang tinggi [3]. Tantangan skalabilitas ini menjadi semakin mendesak karena sistem IoT diproyeksikan akan berkembang dengan sangat cepat, sehingga memerlukan solusi yang mampu menangani peningkatan beban data tanpa mengorbankan kinerja.
b. Interoperabilitas: Integrasi berbagai platform IoT dengan teknologi Blockchain masih merupakan tugas yang kompleks. Alzoubi menekankan bahwa standardisasi dan kompatibilitas protokol merupakan area penting yang memerlukan kajian lebih lanjut [16]. Hal ini didukung oleh Kaveh yang menyatakan bahwa ketiadaan protokol standar dapat secara signifikan menghambat potensi penerapan Blockchain dalam IoT [17]. Kurangnya interoperabilitas dapat menyebabkan sistem yang terfragmentasi sehingga sulit dikelola dan diamankan.

Tantangan-tantangan tersebut menunjukkan bahwa meskipun Blockchain meningkatkan autentikasi dan integritas data, penelitian di masa depan perlu berfokus pada skalabilitas, efisiensi sumber daya, dan interoperabilitas lintas platform guna mendukung adopsi praktis dalam ekosistem IoT berskala besar. Mengatasi kendala-kendala ini akan menjadi faktor penting untuk membuka potensi penuh teknologi Blockchain dalam meningkatkan keamanan IoT.

5. Kesimpulan

Teknologi Blockchain terbukti mampu meningkatkan keamanan sistem Internet of Things (IoT) melalui penerapan mekanisme autentikasi yang terdesentralisasi. Dengan pendekatan ini, hanya perangkat yang memiliki identitas valid yang dapat mengakses jaringan, sehingga risiko akses tidak sah dapat diminimalkan. Selain itu, pengurangan ketergantungan pada otoritas terpusat juga membantu menghindari potensi *single point of failure* dalam sistem IoT.

Selain aspek autentikasi, Blockchain juga berperan penting dalam menjaga integritas data. Penggunaan *ledger* yang bersifat *immutable* serta teknik hashing kriptografi memastikan bahwa data yang tersimpan tidak dapat diubah tanpa terdeteksi. Hal ini menjadikan Blockchain sebagai solusi yang efektif dalam meningkatkan keandalan dan transparansi data pada berbagai aplikasi IoT, mulai dari sektor kesehatan hingga industri.

Meskipun demikian, implementasi Blockchain dalam lingkungan IoT masih menghadapi sejumlah tantangan. Keterbatasan sumber daya perangkat, permasalahan skalabilitas, serta kurangnya interoperabilitas antarplatform menjadi hambatan utama dalam penerapan secara luas. Oleh karena itu, diperlukan pendekatan dan inovasi lebih lanjut agar integrasi Blockchain dan IoT dapat berjalan secara optimal dan efisien.

Penelitian selanjutnya disarankan untuk berfokus pada pengembangan kerangka kerja Blockchain yang ringan dan efisien, sehingga dapat diimplementasikan pada perangkat IoT dengan keterbatasan sumber daya. Selain itu, diperlukan inovasi dalam mekanisme konsensus yang lebih hemat energi dan memiliki latensi rendah agar mampu mendukung kebutuhan sistem IoT yang bersifat real-time dan berskala besar.

Selain aspek teknis, penting juga untuk mengembangkan standar interoperabilitas yang memungkinkan integrasi yang lebih mudah antara berbagai platform IoT dan teknologi Blockchain. Penelitian di masa depan juga perlu melakukan pengujian empiris serta implementasi di dunia nyata guna mengevaluasi kinerja, skalabilitas, dan tingkat keamanan sistem secara menyeluruh dalam skala besar.

.

Daftar Pustaka

[1] Y. Abbassi and H. Benlahmer, "IoT and Blockchain combined: For decentralized security," *Procedia Computer Science*, vol. 191, pp. 337–342, 2021. https://doi.org/10.1016/j.procs.2021.07.045

[2] M. Almelhem Marah, S. Edit, and B. Laszlo, "The Role of Blockchain and IOT in Reverse Logistics: The Impacts on the Environmental and Economical Sustainability a Structured Literature Review," *Chemical Engineering Transactions*, vol. 107, pp. 433–438, 2023. https://doi.org/10.3303/CET23107073

[3] M. M. Alzoubi, "Blockchain in the IoT: Security, applications, technologies, and challenges," *International Journal of Blockchains and Cryptocurrencies*, vol. 5, no. 1, pp. 14–43, 2024. https://doi.org/10.1504/IJBC.2024.140162

[4] M. Balfaqih *et al.*, "A Blockchain-Enabled IoT Logistics System for Efficient Tracking and Management of High-Price Shipments: A Resilient, Scalable and Sustainable Approach to Smart Cities," *Sustainability*, vol. 15, no. 18, 13971, 2023. https://doi.org/10.3390/su151813971

[5] H. Chen *et al.*, "Blockchain-based internet of things security architecture and applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 12, pp. 16703–16714, 2023. https://doi.org/10.1007/s12652-023-04675-w

[6] D. Z. *et al.*, "A Lightweight Blockchain Framework for IoT Integration in Smart Cities," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 5, pp. 889–894, 2021. https://doi.org/10.17762/turcomat.v12i5.1731

[7] G. Ali *et al.*, "Fusion of Blockchain, IoT, Artificial Intelligence, and Robotics for Efficient Waste Management in Smart Cities," 2025. https://doi.org/10.15157/IJITIS.2025.8.3.388-495

[8] S. Kaveh, F. Ebrahimzadeh, and R. Safa, "Leveraging Blockchain and IoT for Secure and Scalable Healthcare Innovations," *Annals of Healthcare Systems Engineering*, vol. 2, no. 1, pp. 44–55, 2025. https://doi.org/10.22105/ahse.v2i1.27

[9] F. I. Khan and S. A. Abbasi, "Major accidents in process industries and an analysis of causes and consequences," *Journal of Loss Prevention in the Process Industries*, vol. 12, no. 5, pp. 361–378, 1999. https://doi.org/10.1016/S0950-4230(98)00062-X
[10] A. Kumar *et al.*, "Neuroadaptive Incentivization in Healthcare using Blockchain and IoT," *SN Computer Science*, vol. 5, no. 1, 13, 2023. https://doi.org/10.1007/s42979-023-02365-0
[11] W. M. Lim and S. Kumar, "Guidelines for interpreting the results of bibliometric analysis: A sensemaking approach," *Global Business and Organizational Excellence*, vol. 43, no. 2, pp. 17–26, 2024. https://doi.org/10.1002/joe.22229
[12] Y. Saidu *et al.*, "Exploring Blockchain–IoT Convergence for Logistics Traceability: A Systematic Review and Future Outlook," *IEEE Access*, vol. 13, pp. 112390–112416, 2025. https://doi.org/10.1109/ACCESS.2025.3583927
[13] A. Saputhanthri, C. De Alwis, and M. Liyanage, "Survey on Blockchain-Based IoT Payment and Marketplaces," *IEEE Access*, vol. 10, pp. 103411–103437, 2022. https://doi.org/10.1109/ACCESS.2022.3208688
[14] P. C. Sauer and S. Seuring, "How to conduct systematic literature reviews in management research: A guide in 6 steps and 14 decisions," *Review of Managerial Science*, vol. 17, no. 5, pp. 1899–1933, 2023. https://doi.org/10.1007/s11846-023-00668-3
[15] D. Stefanescu *et al.*, "A Systematic Literature Review of Lightweight Blockchain for IoT," *IEEE Access*, vol. 10, pp. 123138–123159, 2022. https://doi.org/10.1109/ACCESS.2022.3224222
[16] I. Ullah and P. J. M. Havinga, "Governance of a Blockchain-Enabled IoT Ecosystem: A Variable Geometry Approach," *Sensors*, vol. 23, no. 22, 9031, 2023. https://doi.org/10.3390/s23229031
[17] Y. Yang *et al.*, "A Survey of Blockchain Applications for Management in Agriculture and Livestock Internet of Things," *Future Internet*, vol. 17, no. 1, 40, 2025. https://doi.org/10.3390/fi17010040