

ANALISIS KEAMANAN KOMUNIKASI DATA PADA SISTEM TERDISTRIBUSI MENGGUNAKAN BLOCKCHAIN

PENULIS

¹⁾Erlina Wati Br Lase, ²⁾Alfi Syahrin Ritonga, ³⁾Halimatul Sakdiah Bancin,
⁴⁾M. Fahrizal

ABSTRAK

Perkembangan sistem terdistribusi, seperti komputasi awan dan Internet of Things (IoT), meningkatkan kebutuhan akan mekanisme keamanan komunikasi data yang mampu melindungi kerahasiaan, integritas, dan ketersediaan informasi. Namun, arsitektur terdistribusi konvensional masih rentan terhadap serangan seperti penyadapan, manipulasi data, dan pemalsuan identitas. Penelitian ini bertujuan menganalisis peran teknologi Blockchain dalam meningkatkan keamanan komunikasi data pada sistem terdistribusi melalui penerapan kriptografi asimetris, fungsi hash, dan mekanisme konsensus. Penelitian menggunakan metode studi kepustakaan dengan menganalisis literatur ilmiah yang diterbitkan pada periode 2019–2025 dari Google Scholar, IEEE Xplore, dan ScienceDirect. Hasil kajian menunjukkan bahwa enkripsi kunci publik mampu menjaga kerahasiaan komunikasi antar node, struktur Blockchain yang didukung Merkle tree menjamin integritas data terhadap perubahan yang tidak sah, sedangkan mekanisme konsensus seperti Proof of Work dan Proof of Stake meningkatkan ketahanan sistem terhadap serangan Sybil dan mengurangi risiko single point of failure. Meskipun demikian, Blockchain masih menghadapi tantangan berupa keterbatasan skalabilitas dan potensi serangan 51%. Penelitian ini menyimpulkan bahwa Blockchain merupakan pendekatan yang efektif untuk memperkuat keamanan komunikasi data pada sistem terdistribusi serta berpotensi menjadi dasar pengembangan sistem yang lebih aman dan andal di berbagai bidang.

Kata Kunci

Blockchain; Keamanan Data; Sistem Terdistribusi;

AFILIASI

Prodi, Fakultas

¹⁻⁴⁾ Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi
Informasi

Nama Institusi

¹⁻⁴⁾ Universitas Budi Darma

Alamat Institusi

¹⁻⁴⁾ Jl. Sisingamangaraja No. 338, Kelurahan Siti Rejo I, Kecamatan Medan Kota,
Kota Medan, Sumatera Utara 20219, Indonesia.

KORESPONDENSI

Penulis

Erlina Wati Br Lase

Email

erlinawatibrase@gmail.com

LICENSE



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

I. PENDAHULUAN

Pada pertengahan tahun 2023, sebuah penyedia layanan cloud besar di Asia Tenggara mengalami kebocoran data pelanggan akibat serangan man-in-the-middle (MITM) yang menyusup ke jalur komunikasi antar server internal. Penyerang berhasil membaca, menyalin, dan bahkan mengubah sejumlah data transaksi keuangan sebelum akhirnya dikenali oleh sistem pemantauan. Insiden ini memperpanjang daftar kasus serangan siber yang menargetkan infrastruktur terdistribusi, sekaligus menegaskan bahwa arsitektur yang bertumpu pada otoritas terpusat atau replikasi data tanpa verifikasi kriptografis yang kukuh sangat rentan terhadap penyusupan yang sulit dideteksi secara dini. Fenomena tersebut mencerminkan tantangan mendasar dalam keamanan komunikasi data pada sistem terdistribusi. Sistem terdistribusi, yang terdiri atas sejumlah komputer otonom yang saling terhubung melalui jaringan, menawarkan keunggulan skalabilitas dan ketahanan terhadap kegagalan satu titik. Akan tetapi, sifat alaminya yang tersebar justru membuka banyak permukaan serangan, terutama pada lapisan komunikasi data. Data yang melintas antar node dapat disadap, dimodifikasi, atau dihambat oleh pihak yang tidak berwenang, sehingga mempertaruhkan aspek kerahasiaan, integritas, maupun ketersediaan Layanan [1]. Selain itu, dalam lingkungan yang melibatkan banyak pihak tanpa kepercayaan penuh, seperti pada sistem kesehatan digital, rantai pasok, atau kota cerdas, kebutuhan akan mekanisme keamanan yang tidak bergantung pada otoritas tunggal menjadi semakin mendesak.

Blockchain merupakan teknologi yang dibangun berdasarkan prinsip kriptografi dengan menerapkan konsep distributed ledger, yaitu sistem pencatatan data yang didistribusikan ke seluruh node dalam jaringan tanpa bergantung pada otoritas pusat. Melalui penerapan fungsi hash kriptografi, tanda tangan digital (digital signature), dan mekanisme konsensus, setiap transaksi yang tercatat dapat diverifikasi oleh seluruh peserta jaringan sehingga menjamin integritas, autentikasi, dan ketahanan data terhadap manipulasi. Karakteristik tersebut menjadikan Blockchain mampu menyediakan sistem penyimpanan dan pertukaran data yang lebih aman, transparan, serta sulit diubah (immutable), sehingga banyak dimanfaatkan untuk meningkatkan keamanan pada berbagai bidang, termasuk perlindungan data, Internet of Things (IoT), aplikasi web, dan sistem keamanan siber secara umum [7]. Blockchain menggabungkan primitif kriptografi seperti fungsi hash dan kunci asimetris dengan mekanisme konsensus yang memungkinkan sekumpulan node mencapai kesepakatan tanpa harus saling percaya. Konsep ini membuka peluang untuk membangun lapisan keamanan komunikasi data yang tidak bergantung pada otoritas pusat, sehingga setiap pertukaran informasi tervalidasi oleh seluruh jaringan. Tinjauan mutakhir terhadap penerapan teknologi Blockchain dalam protokol kriptografis memperkuat pandangan ini dengan menunjukkan bahwa sifat Blockchain yang tidak dapat diubah (immutability), transparansi, dan kemampuan pemrograman melalui kontrak pintar secara signifikan memperkuat keamanan dan kepercayaan dalam pertukaran data terdistribusi [2]. Meskipun demikian, penerapan Blockchain untuk mengamankan komunikasi data pada sistem terdistribusi bukanlah perkara yang sepenuhnya sederhana. Diperlukan pemahaman mendalam tentang bagaimana elemen-elemen kriptografi dan protokol konsensus bekerja secara sinergis untuk menangkal ancaman spesifik pada jalur komunikasi. Literatur teknis yang mengulas Blockchain kerap terfokus pada ranah mata uang kripto, sementara analisis mengenai kontribusinya terhadap aspek fundamental keamanan data yakni kerahasiaan, integritas, dan ketersediaan—dalam komunikasi antar node sistem terdistribusi masih memerlukan pengkajian yang lebih terstruktur dan mendalam.

Berdasarkan fenomena-fenomena yang telah peneliti uraikan diatas, artikel ini merumuskan pertanyaan penelitian berikut: bagaimana penerapan mekanisme kriptografi dan prinsip distributed ledger pada Blockchain dapat mengatasi ancaman terhadap kerahasiaan, integritas, dan ketersediaan data dalam proses komunikasi pada sistem terdistribusi? Adapun tujuan penelitian ini mencakup tiga hal: (1) menjelaskan cara kerja enkripsi asimetris, fungsi hash, dan mekanisme konsensus dalam konteks komunikasi data terdistribusi Berbasis Blockchain; (2) mengkaji peran masing-masing mekanisme tersebut dalam menjaga tiga aspek utama keamanan data; serta (3) membandingkan tingkat ketahanan antara sistem terdistribusi konvensional dan sistem Berbasis Blockchain terhadap empat jenis serangan siber yang umum terjadi. Artikel ini disusun menggunakan pendekatan studi kepustakaan, sehingga seluruh analisis didasarkan pada sintesis teori dan temuan dari literatur ilmiah terkini. Dengan demikian, pembahasan berfokus pada penjelasan konseptual yang mendalam, bukan pada hasil eksperimen atau simulasi. Diharapkan artikel ini dapat menjadi rujukan awal bagi akademisi dan peneliti yang ingin memahami peran Blockchain dalam memperkuat keamanan komunikasi data di lingkungan terdistribusi.

II. METODE PENELITIAN

Penelitian ini menggunakan metode studi kepustakaan (library research), yaitu pendekatan penelitian yang berfokus pada pengumpulan, pengkajian, dan sintesis berbagai sumber literatur ilmiah yang relevan untuk memperoleh pemahaman yang komprehensif mengenai keamanan komunikasi data pada sistem terdistribusi berbasis Blockchain. Metode ini dipilih karena topik penelitian lebih menitikberatkan pada analisis konseptual terhadap perkembangan teori, mekanisme teknologi, serta hasil-hasil penelitian terdahulu dibandingkan dengan pengujian melalui eksperimen secara langsung. Dengan demikian, pendekatan studi kepustakaan dinilai mampu memberikan gambaran yang sistematis mengenai penerapan teknologi Blockchain dalam meningkatkan aspek kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data pada sistem terdistribusi.

Proses pengumpulan data dilakukan melalui identifikasi dan penelusuran berbagai sumber literatur yang memiliki kredibilitas tinggi, meliputi artikel jurnal internasional dan nasional, prosiding konferensi ilmiah, buku akademik, laporan teknis, serta publikasi ilmiah lainnya yang diterbitkan pada rentang tahun 2019–2025. Pemilihan rentang waktu tersebut bertujuan agar kajian yang dilakukan mampu merepresentasikan perkembangan terbaru terkait implementasi Blockchain, mekanisme kriptografi modern, serta berbagai protocol konsensus yang saat ini banyak diterapkan dalam pengamanan komunikasi data pada sistem terdistribusi. Selain mempertimbangkan kebaruan publikasi, literatur yang digunakan juga dipilih berdasarkan relevansi substansi, kualitas publikasi, serta kesesuaian dengan fokus penelitian.

Penelusuran literatur dilakukan melalui beberapa basis data ilmiah yang telah diakui secara internasional, yaitu Google Scholar, IEEE Xplore, dan ScienceDirect. Ketiga basis data tersebut dipilih karena menyediakan publikasi ilmiah yang memiliki kualitas akademik tinggi dan banyak dijadikan rujukan dalam bidang keamanan informasi, jaringan komputer, sistem terdistribusi, serta teknologi Blockchain. Proses pencarian dilakukan menggunakan kombinasi kata kunci, antara lain "Blockchain for distributed system security", "cryptographic hash data integrity", "asymmetric encryption confidentiality", "consensus mechanism Sybil attack", serta beberapa kata kunci pendukung lainnya seperti distributed ledger technology, Merkle tree, Proof of Work, Proof of Stake, dan Blockchain security. Penggunaan kombinasi kata kunci tersebut bertujuan untuk memperoleh literatur yang lebih beragam sehingga mampu menggambarkan perkembangan penelitian secara lebih menyeluruh. Setelah seluruh literatur berhasil dikumpulkan, dilakukan proses seleksi Berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi mencakup publikasi yang membahas penerapan Blockchain dalam sistem terdistribusi, mekanisme kriptografi, fungsi hash, protokol konsensus, maupun keamanan komunikasi data. Sebaliknya, publikasi yang hanya membahas aspek ekonomi, mata uang kripto, atau implementasi Blockchain yang tidak berkaitan dengan keamanan komunikasi data tidak dijadikan sebagai sumber utama dalam penelitian ini. Tahapan seleksi tersebut bertujuan agar seluruh referensi yang dianalisis memiliki keterkaitan langsung dengan rumusan masalah serta tujuan penelitian.

Analisis data dilakukan secara kualitatif melalui teknik analisis isi (content analysis). Setiap literatur yang telah memenuhi kriteria dianalisis secara mendalam untuk mengidentifikasi konsep-konsep utama, mekanisme kerja kriptografi, fungsi struktur Merkle tree, serta karakteristik berbagai protokol konsensus yang digunakan dalam teknologi Blockchain. Selanjutnya, hasil analisis tersebut dikelompokkan berdasarkan tiga aspek utama keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability), sehingga diperoleh pemahaman mengenai kontribusi masing-masing mekanisme Blockchain dalam meningkatkan keamanan komunikasi data pada sistem terdistribusi. Tahap berikutnya adalah melakukan sintesis terhadap seluruh temuan dari berbagai literatur untuk membangun argumen ilmiah mengenai efektivitas penerapan Blockchain dalam menghadapi berbagai ancaman keamanan siber. Hasil sintesis tersebut kemudian digunakan sebagai dasar dalam menyusun pembahasan mengenai kemampuan teknologi Blockchain dalam mengatasi serangan man-in-the-middle, data tampering, Sybil attack, dan single point of failure. Selain itu, dilakukan pula analisis komparatif antara sistem terdistribusi konvensional dengan sistem berbasis Blockchain yang disajikan dalam bentuk tabel perbandingan sehingga memudahkan pembaca memahami perbedaan karakteristik keamanan dari kedua pendekatan tersebut.

Pendekatan studi kepustakaan dalam penelitian ini dipilih karena mampu menghasilkan pemetaan konsep yang komprehensif mengenai perkembangan teknologi Blockchain beserta implementasinya dalam keamanan komunikasi data tanpa memerlukan infrastruktur eksperimen yang kompleks. Selain lebih efisien dari sisi waktu

dan biaya, metode ini juga memungkinkan peneliti mengintegrasikan berbagai hasil penelitian terdahulu sehingga diperoleh pemahaman yang lebih luas mengenai kelebihan, keterbatasan, serta peluang pengembangan teknologi Blockchain dalam mendukung keamanan sistem terdistribusi di masa mendatang.

III. HASIL DAN PEMBAHASAN

Pada bagian ini, ketiga elemen keamanan data (kerahasiaan, integritas, dan ketersediaan) dianalisis secara terpisah untuk melihat kontribusi spesifik komponen Blockchain. Kemudian, perbandingan sistem terdistribusi konvensional dan sistem berbasis Blockchain disajikan dalam bentuk tabel.

3.1 Analisis Kerahasiaan: Peran Enkripsi Asimetris pada Komunikasi Antar Node

Kerahasiaan dalam komunikasi data pada sistem terdistribusi dijaga dengan memastikan bahwa hanya pihak tujuan yang dapat membaca isi pesan. Blockchain memanfaatkan sistem kriptografi kunci publik (kunci asimetris) yang telah dikaji secara khusus dalam konteks komunikasi terdistribusi. Setiap partisipan memiliki pasangan kunci: kunci privat yang dirahasiakan dan kunci publik yang disebarluaskan. Ketika node A ingin mengirim data sensitif kepada node B, A dapat mengenkripsi data tersebut menggunakan kunci publik B hanya B yang memiliki kunci privat yang sesuai sehingga mampu mendekripsinya. Dengan demikian, meskipun lalu lintas data disadap dalam serangan MITM, penyerang tidak dapat mengurai isi pesan. Lebih dari sekedar enkripsi, mekanisme kunci asimetris juga menyediakan autentikasi melalui tanda tangan digital. Node A dapat menandatangani pesan dengan kunci privatnya, dan semua node lain dapat memverifikasi tanda tangan tersebut dengan kunci publik A. Verifikasi ini membuktikan dua hal sekaligus: pesan benar-benar berasal dari A (autentikasi) dan tidak dimodifikasi setelah ditandatangani (integritas). Studi terkini tentang enkripsi asimetris dalam Blockchain mengonfirmasi bahwa algoritma kurva eliptis (ECC) memberikan keamanan yang setara dengan RSA menggunakan ukuran kunci yang jauh lebih kecil, sehingga lebih efisien untuk diimplementasikan pada sistem IoT terdistribusi [9].

Perlu dicatat bahwa Blockchain publik umumnya tidak mengenkripsi data transaksi yang tersimpan di dalam blok agar dapat diverifikasi oleh semua node. Oleh karena itu, banyak implementasi menggabungkan pendekatan hibrida: data sensitif disimpan dalam bentuk terenkripsi di luar rantai (off-chain), sedangkan Blockchain hanya menyimpan jejak hash, bukti keberadaan, atau kebijakan akses berbasis kontrak pintar. Di lingkungan kesehatan, misalnya, data rekam medis dapat dibagikan dengan pihak ketiga melalui mekanisme proxy re-encryption yang dikendalikan oleh pasien, sementara Blockchain mencatat izin akses dan log permintaan data untuk audit[5]. Pada perangkat IoT dengan sumber daya terbatas, kerahasiaan sering kali dijaga dengan enkripsi simetris yang efisien pada saluran komunikasi, sedangkan verifikasi identitas Perangkat dilakukan melalui sertifikat yang ditanamkan di Blockchain. Pendekatan-pendekatan ini menunjukkan bahwa Blockchain paling efektif menjaga kerahasiaan jika dipadukan dengan skema enkripsi dan manajemen akses yang sesuai dengan karakteristik sistem.

3.2 Analisis Integritas: Fungsi Hash dan Merkle tree sebagai Penjaga Keaslian Data

Integritas data dalam komunikasi terdistribusi mensyaratkan bahwa setiap perubahan data, sekecil apapun, dapat segera terdeteksi oleh penerima. Blockchain merancang hal ini secara inheren melalui rantai blok dan struktur Merkle tree. Saat data dikemas dalam blok baru, hash dari blok tersebut dihitung dan dicantumkan di header blok berikutnya. Akibatnya, apabila seorang penyerang mencoba mengubah isi satu transaksi yang telah dikonfirmasi, ia harus menghitung ulang hash blok yang dimodifikasi serta seluruh blok sesudahnya—sekali-gus mengalahkan mekanisme konsensus untuk membuat rantai palsu diakui sebagai rantai terpanjang. Kompleksitas komputasi yang luar biasa besar, terutama pada jaringan dengan daya hash tinggi, membuat Upaya ini secara praktis mustahil.

Pada level komunikasi langsung antar node, penggunaan fungsi hash juga memungkinkan deteksi kerusakan data akibat gangguan jaringan atau serangan data tampering. Sebelum mengirim data, node pengirim dapat menghasilkan hash dari data tersebut dan mengirimkannya bersama data melalui jalur terpisah. Penerima kemudian menghitung hash dari data yang diterima dan membandingkannya; ketidakcocokan mengindikasikan bahwa data telah berubah selama transit. Skema pemeriksaan integritas data jarak jauh berbasis Blockchain yang dirancang untuk perangkat IoT dalam jaringan 5G membuktikan bahwa mekanisme hash terdistribusi ini mampu memverifikasi integritas data berskala besar tanpa bergantung pada auditor pihak ketiga yang terpusat, sehingga secara konseptual selaras dengan prinsip desentralisasi yang menjadi fondasi keamanan komunikasi terdistribusi.

[10].

Struktur Merkle tree juga meningkatkan efisiensi verifikasi integritas dalam konteks komunikasi berskala besar. Misalkan sebuah blok berisi ribuan transaksi; node yang hanya berkepentingan pada satu transaksi tidak perlu mengunduh dan memeriksa seluruh transaksi. Cukup dengan menyediakan jalur Merkle (beberapa hash perantara), node tersebut dapat memverifikasi bahwa transaksi tertentu memang tercakup dalam Merkle root yang sah. Hal ini sangat bermanfaat untuk perangkat dengan sumber daya terbatas dalam sistem terdistribusi, seperti sensor IoT. Dalam konteks audit dan ketertelusuran, Blockchain juga memungkinkan pencatatan setiap versi perubahan data (data provenance), sehingga integritas riwayat data dapat dipertanggungjawabkan secara transparan.

Dengan demikian, fungsi hash dan Merkle tree tidak hanya menjaga integritas penyimpanan data, tetapi juga memungkinkan pengamanan integritas komunikasi data secara efisien. Perubahan sekecil apa pun akan menghasilkan hash yang sepenuhnya berbeda (efek avalanche), sehingga integritas dapat diverifikasi secara sederhana namun andal.

3.3 Tabel Kecocokan

Ketersediaan sistem terdistribusi berarti bahwa layanan dan data tetap dapat diakses meskipun terjadi gangguan atau serangan. Pada sistem terdistribusi konvensional, ketersediaan sering bergantung pada server pusat atau sekelompok node koordinator; kegagalan pada komponen kritis ini berpotensi melumpuhkan keseluruhan sistem. Serangan Sybil, di sisi lain, terjadi ketika satu entitas membuat banyak identitas palsu untuk mendominasi jaringan dan memanipulasi proses pengambilan keputusan, yang dapat berujung pada penyensoran transaksi atau penghentian layanan.

Mekanisme konsensus pada Blockchain dirancang untuk mengatasi kedua ancaman ini secara fundamental. Karena tidak ada otoritas tunggal, tidak ada titik kegagalan tunggal. Selama mayoritas node yang jujur tetap beroperasi dan mengikuti protokol, layanan penulisan dan verifikasi data akan terus berjalan. Kajian komprehensif terhadap mekanisme konsensus dalam ekosistem Blockchain menemukan bahwa PoW dan PoS merupakan dua paradigma fundamental yang mampu memberikan ketahanan terhadap serangan Sybil dalam jaringan permissionless, meskipun masing-masing menawarkan karakteristik ketahanan yang berbeda [4]. Pada PoW, pengaruh tidak ditentukan oleh jumlah identitas, melainkan oleh daya komputasi yang dimiliki; pada PoS, pengaruh sebanding dengan jumlah aset yang dipertaruhkan, sehingga menciptakan penghalang ekonomi yang tinggi].

Ketahanan terhadap serangan penolakan layanan (DoS) juga meningkat karena lalu lintas data disebar keseluruh jaringan peer-to-peer. Tidak ada server pusat yang dapat dibanjiri permintaan. Setiap node menjalankan fungsi verifikasi secara mandiri; jika satu atau beberapa node dimatikan, node lain tetap melanjutkan operasi. Lebih lanjut, sejumlah arsitektur Blockchain modern mengintegrasikan mekanisme deteksi anomali berbasis kecerdasan buatan dan kontrol akses adaptif untuk memperkuat ketahanan terhadap serangan yang lebih canggih.

Namun, perlu digarisbawahi bahwa ketersediaan ini tidak mutlak. Ancaman serangan 51% tetap ada: jika satu entitas berhasil menguasai mayoritas daya hash atau aset yang dipertaruhkan, ia dapat menyensor transaksi, membatalkan blok, bahkan melakukan pengeluaran ganda. Selain itu, dalam jaringan Blockchain publik dengan ukuran blok terbatas, lonjakan volume komunikasi dapat menyebabkan kemacetan dan peningkatan biaya transaksi, yang secara fungsional menurunkan ketersediaan. Oleh karena itu, efektivitas Blockchain dalam menjaga ketersediaan sangat dipengaruhi oleh desain konsensus, distribusi partisipan, dan parameter jaringan yang dipilih.

3.4 Normalisasi

Untuk memberikan gambaran yang lebih konkret, berikut disajikan tabel perbandingan antara sistem terdistribusi konvensional (berbasis replikasi server dengan koordinator pusat) dan sistem terdistribusi Berbasis Blockchain dalam menghadapi empat jenis serangan

Tabel 1. Perbandingan Ketahanan terhadap Serangan

Jenis Serangan	Sistem Terdistribusi Konvensional	Sistem Berbasis Blockchain	Keterangan
Man-in-the-middle (MITM)	Rentan apabila saluran komunikasi tidak dilengkapi enkripsi end-to-end; autentikasi bergantung pada otoritas sertifikat terpusat.	Tahan. Komunikasi diamankan melalui kriptografi kunci publik; tanda tangan digital memungkinkan verifikasi keaslian pengirim tanpa pihak ketiga tepercaya.	Blockchain memanfaatkan kriptografi asimetris sehingga data yang disadap tidak dapat dibaca, dan integritas pengirim terverifikasi secara kriptografis.
Data Tampering	Deteksi mengandalkan checksum atau audit log yang masih dapat dimodifikasi apabila penyerang memperoleh akses ke server pusat.	Sangat tahan. Setiap perubahan data mengubah hash blok dan merusak keterkaitan rantai, sehingga node akan menolak data yang tidak valid.	Struktur Blockchain berbasis hash berantai dan <i>Merkle tree</i> menjamin integritas data yang sulit dimanipulasi tanpa menguasai mayoritas jaringan.
Sybil Attack	Rentan pada sistem yang bergantung pada identitas atau voting berbasis jumlah node; penyerang dapat membuat banyak identitas palsu untuk memengaruhi keputusan.	Relatif tahan (bergantung pada mekanisme konsensus). Pada PoW pengaruh ditentukan oleh daya komputasi; pada PoS oleh aset yang dipertaruhkan, sehingga serangan menjadi mahal secara ekonomi.	Mekanisme konsensus menggeser masalah Sybil dari "jumlah identitas" menjadi "biaya ekonomi untuk menguasai jaringan".
Single Point of Failure	Sangat rentan. Kegagalan server pusat atau koordinator dapat menyebabkan sistem berhenti atau kehilangan fungsi utama.	Sangat tahan. Tidak terdapat otoritas tunggal; sistem tetap berjalan selama mayoritas node jujur tetap aktif, meskipun sebagian node mengalami kegagalan.	Desentralisasi menghilangkan ketergantungan pada satu titik kegagalan, namun tetap perlu mempertimbangkan risiko serangan mayoritas (51%).

Tabel tersebut memperlihatkan bahwa arsitektur berbasis Blockchain menawarkan ketahanan yang unggul pada keempat jenis serangan, berkat kombinasi kriptografi yang kuat dan mekanisme konsensus yang terdesentralisasi. Namun, keunggulan ini bukan tanpa biaya; kompleksitas komputasi dan kebutuhan penyimpanan yang terus bertambah menjadi pertimbangan penting dalam implementasi nyata.

VI. SIMPULAN

Berdasarkan analisis yang telah dilakukan, Blockchain memberikan kontribusi signifikan dalam meningkatkan keamanan komunikasi data pada sistem terdistribusi melalui pemanfaatan primitif kriptografi dan protokol konsensus yang terdesentralisasi. Pada aspek kerahasiaan, enkripsi asimetris dan tanda tangan digital memungkinkan komunikasi yang aman antar node tanpa ketergantungan pada otoritas sertifikat pusat. Pada aspek integritas, fungsi hash dan struktur Merkle tree menjamin bahwa setiap perubahan data—baik selama penyimpanan maupun transit—dapat segera terdeteksi dan ditolak oleh jaringan. Pada aspek ketersediaan, mekanisme konsensus seperti Proof of Work dan Proof of Stake secara fundamental menghilangkan titik kegagalan tunggal dan membuat serangan Sybil menjadi tidak ekonomis, sehingga layanan dapat terus beroperasi meskipun sebagian node mengalami gangguan.

Meskipun demikian, Blockchain bukanlah solusi sempurna. Potensi serangan 51%, masalah skalabilitas yang berdampak pada latensi dan kapasitas transaksi, serta konsumsi energi yang tinggi pada PoW menjadi tantangan yang belum sepenuhnya terselesaikan. Dalam konteks komunikasi data real-time, overhead consensus mungkin menyebabkan penundaan yang tidak dapat diterima untuk aplikasi tertentu. Oleh karena itu, pemilihan jenis Blockchain (publik, privat, atau konsorsium) dan desain parameter jaringan harus disesuaikan dengan kebutuhan keamanan dan kinerja spesifik.

Untuk penelitian selanjutnya, disarankan agar dilakukan studi simulasi menggunakan platform Blockchain bersifat konsorsium seperti Hyperledger Fabric. Simulasi tersebut dapat mengukur secara kuantitatif parameter kualitas layanan (latensi, throughput, dan tingkat keberhasilan verifikasi) ketika mekanisme keamanan Blockchain diterapkan pada skenario komunikasi data terdistribusi dengan jumlah node terbatas. Selain itu, eksplorasi terhadap teknik penskalaan lapis kedua, seperti state channel atau sidechain, menarik untuk dikaji guna mengatasi keterbatasan throughput tanpa mengorbankan keamanan. Integrasi dengan pendekatan Zero Trust dan deteksi anomali berbasis kecerdasan buatan juga dapat menjadi arah pengembangan yang menjanjikan untuk memperkuat ketahanan sistem terhadap ancaman yang semakin adaptif. Dengan demikian, kajian konseptual ini dapat menjadi landasan bagi pengembangan prototipe yang aplikatif.

REFERENSI

- [1] A. Anggraeni, J. G. A. Ginting, and S. Ikhwan, "Implementation of intrusion prevention system (IPS) to analysis triad cia on network security attacks on web server," *JURNAL INFOTEL*, vol. 14, no. 4, pp. 277–286, Nov. 2022, doi: 10.20895/infotel.v14i4.813.
- [2] T. Dan Hambatan, "IMPLEMENTASI TEKNOLOGI BLOCKCHAIN DI," *Buletin Perpustakaan Universitas Islam Indonesia*, vol. 4, no. 2, pp. 173–200.
- [3] X. Luo, X. Chen, X. Chen, and Q. Cheng, "A survey on the application of Blockchain in cryptographic protocols," *Cybersecurity*, vol. 7, no. 1, Dec. 2024, doi: 10.1186/s42400-024-00324-7.
- [4] O. Kuznetsov, A. Rusnak, A. Yezhov, K. Kuznetsova, D. Kanonik, and O. Domin, "Merkle trees in Blockchain: A Study of collision probability and security implications," Jul. 01, 2024, Elsevier B.V. doi: 10.1016/j.iot.2024.101193.
- [5] Z. Liu, L. Ren, Y. Feng, S. Wang, and J. Wei, "Data Integrity Audit Scheme Based on Quad Merkle tree and Blockchain," *IEEE Access*, vol. 11, pp. 59263–59273, 2023, doi: 10.1109/ACCESS.2023.3240066.
- [6] C. F. Ikenga-Metuh and A. Yeboah-Ofori, "Blockchain Security Using Confidentiality, Integrity, and Availability for Secure Communication," *Blockchains*, vol. 4, no. 1, p. 3, Feb. 2026, doi: 10.3390/Blockchains4010003..
- [7] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 6(2), 147–156. <https://doi.org/10.1016/j.dcan.2019.01.005>.
- [8] J. Jayabalan and N. Jeyanthi, "Scalable Blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, Jun. 2022, doi: 10.1016/j.jpdc.2022.03.009.
- [9] H. Wang, D. He, J. Yu, N. N. Xiong, and B. Wu, "RDIC: A Blockchain-based remote data integrity checking scheme for IoT in 5G networks," *J. Parallel Distrib. Comput.*, vol. 152, pp. 1–10, Jun. 2021, doi: 10.1016/j.jpdc.2021.02.012.
- [10] M. Platt and P. McBurney, "Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance," Jan. 01, 2023, MDPI. doi: 10.3390/a16010034.