TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

Potensi Penggunaan Blockchain untuk Meningkatkan Keamanan Jaringan: Telaah Literatur dan Implikasi Masa Depan

Syaif Nurul Ikhsan, Dimas Febriawan*

Fakultas Teknologi Industri dan Informatika, Teknik Informatika, Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia
Email: [1]syaif.noelaz.011@gmail.com, [2*]dimas.febriawan@uhamka.ac.id
Email Penulis Korespondensi: dimas.febriawan@uhamka.ac.id

Abstrak−Era digital telah melahirkan ketergantungan yang tinggi terhadap infrastruktur jaringan dan data, yang secara bersamaan memicu tantangan keamanan informasi yang kian kompleks. Serangan siber seperti DDoS, peretasan data, dan manipulasi informasi menjadi ancaman nyata. Sementara itu, solusi keamanan konvensional dinilai belum sepenuhnya mampu menangani serangan yang semakin canggih. Penelitian ini hadir untuk mengisi celah literatur dengan mengeksplorasi potensi teknologi blockchain dalam memperkuat sistem keamanan jaringan melalui pendekatan studi literatur sistematik terhadap 10 artikel ilmiah terkini. Penelitian ini bertujuan menganalisis kontribusi blockchain terhadap dimensi utama keamanan: autentikasi, integritas, ketersediaan, dan privasi. Metodologi yang digunakan adalah pendekatan kualitatif berbasis studi pustaka, dengan seleksi artikel menggunakan kriteria tahun publikasi, relevansi tema, dan validitas akademik. Hasil menunjukkan bahwa blockchain menawarkan solusi yang signifikan dalam hal pencatatan transaksi yang immutable, sistem autentikasi terdesentralisasi, dan model perlindungan privasi berbasis smart contract. Temuan ini memperkuat urgensi integrasi blockchain ke dalam arsitektur keamanan jaringan masa kini, sekaligus membuka jalan bagi pengembangan sistem hybrid yang menggabungkan blockchain dengan AI dan IDS.

Kata Kunci: Blockchain; Keamanan Jaringan; Studi Literatur; Autentikasi; Privasi; Desentralisasi

Abstract−The digital era has given rise to a high dependency on network infrastructure and data, which simultaneously triggers increasingly complex information security challenges. Cyber attacks such as DDoS, data hacking and information manipulation are real threats. Meanwhile, conventional security solutions are considered not yet fully capable of handling increasingly sophisticated attacks. This research is here to fill the literature gap by exploring the potential of blockchain technology in strengthening network security systems through a systematic literature study approach to 10 recent scientific articles. This research aims to analyze the contribution of blockchain to the main dimensions of security: authentication, integrity, availability and privacy. The methodology used is a qualitative approach based on literature study, with article selection using the criteria of year of publication, theme relevance and academic validity. The results show that blockchain offers significant solutions in terms of immutable transaction recording, decentralized authentication systems, and smart contract-based privacy protection models. These findings reinforce the urgency of integrating blockchain into today's network security architecture, while paving the way for the development of hybrid systems that combine blockchain with AI and IDS.

Keywords: Blockchain; Network Security; Literature Study; Authentication; Privacy; Decentralization

1. PENDAHULUAN

Transformasi digital telah menjadi pendorong utama dalam perkembangan teknologi informasi dan komunikasi di seluruh dunia (Bani, 2024). Inovasi digital telah menciptakan peluang baru dalam berbagai sektor, seperti keuangan, pemerintahan, pendidikan, kesehatan, dan industri (Saputra et al., 2023). Di sisi lain, pertumbuhan sistem informasi yang pesat ini juga diiringi dengan meningkatnya kerentanan terhadap berbagai bentuk serangan siber dan pelanggaran data (Ananta et al., 2024). Ketergantungan yang tinggi terhadap jaringan dan sistem digital mengharuskan adanya mekanisme keamanan yang tangguh dan adaptif. Dalam konteks ini, keamanan jaringan menjadi isu sentral yang tidak dapat diabaikan, baik oleh institusi pemerintah maupun sektor swasta (Budiyanto & Mabruri, 2025).

Ancaman terhadap keamanan jaringan kini tidak lagi bersifat konvensional, tetapi telah berkembang menjadi serangan yang kompleks, sistematis, dan bersifat lintas batas(Sadi & Nugraha, 2025). Fenomena seperti *Distributed Denial of Service* (DDoS), *ransomware, sniffing, spoofing,* dan *phishing* telah menimbulkan kerugian signifikan bagi individu, organisasi, bahkan negara (Pratama et al., 2024). Data menjadi aset yang paling berharga di era digital ini, namun juga menjadi sasaran utama dalam berbagai skenario serangan (Sumampouw & Sembiring, 2024). Berbagai laporan insiden menunjukkan bahwa sistem keamanan tradisional seperti firewall dan antivirus sudah tidak lagi cukup untuk melindungi integritas, kerahasiaan, dan ketersediaan data secara menyeluruh. Sistem yang bersifat terpusat juga berpotensi menjadi single point of failure yang rentan diserang (Adzimi et al., 2024).

Termasuk insiden nyata, kasus kebocoran data pada Pusat Data Nasional Sementara (PDNS) tahun 2024 menggaris bawahi lemahnya sistem keamanan nasional yang selama ini bergantung pada model terpusat (Indonesia, 2024). Dalam kasus tersebut, ribuan data sensitif dari institusi negara dan layanan publik terpapar dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Hal ini membuktikan bahwa sistem keamanan siber Indonesia belum sepenuhnya siap menghadapi tantangan era digital yang semakin kompleks dan dinamis. Oleh karena itu, pendekatan keamanan yang reaktif dan berbasis perlindungan perimeter perlu segera ditransformasikan menjadi pendekatan yang lebih proaktif, holistik, dan adaptif (Soetrisno et al., 2025).

Dalam konteks inilah, teknologi blockchain muncul sebagai salah satu alternatif yang menjanjikan. Blockchain merupakan teknologi pencatatan digital terdistribusi yang memiliki karakteristik desentralisasi, transparansi, dan imutabilitas (Nuraini, 2025). Teknologi ini memungkinkan pencatatan transaksi atau data yang tidak dapat diubah atau dimanipulasi, karena setiap entri divalidasi oleh jaringan dan disimpan dalam blok yang saling terhubung. Validasi

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

melalui konsensus ini mengeliminasi kebutuhan akan pihak ketiga sebagai otoritas pusat, sehingga meminimalkan risiko sentralisasi dan manipulasi data (Susanti, 2024). Blockchain juga menawarkan potensi besar dalam mendukung keandalan autentikasi, integritas data, dan privasi pengguna melalui smart contract dan enkripsi kriptografi tingkat tinggi (Hidayatullah & Saiin, 2025).

Secara konseptual, teknologi blockchain memiliki kemampuan untuk mengatasi beberapa tantangan utama dalam sistem keamanan jaringan. Dengan desentralisasi, blockchain mampu meniadakan titik pusat kegagalan yang umum terjadi dalam arsitektur tradisional (Ardyawin et al., 2024). Imutabilitas data pada blockchain menjamin bahwa setiap informasi yang tercatat tidak dapat diubah secara sewenang-wenang, yang berimplikasi langsung terhadap aspek integritas dan forensik digital. Selain itu, transparansi dan jejak audit yang dimiliki blockchain dapat meningkatkan kepercayaan pengguna terhadap sistem digital, sekaligus mempermudah proses pengawasan dan pemantauan keamanan jaringan (Afdilah et al., 2024).

Awalnya dikembangkan untuk mendukung mata uang kripto seperti Bitcoin dan Ethereum, aplikasi blockchain kini telah merambah berbagai bidang non-keuangan, termasuk dalam penguatan keamanan jaringan (Lim et al., 2024). Implementasi blockchain dalam sistem keamanan informasi dapat memberikan nilai tambah melalui pencatatan aktivitas log yang transparan dan tahan gangguan, pengelolaan identitas digital, serta penerapan sistem kontrol akses berbasis hak kepemilikan terverifikasi. Namun, tantangan implementasi tetap ada, seperti konsumsi energi, kecepatan transaksi, dan interoperabilitas dengan sistem eksisting, yang membutuhkan perhatian dalam proses adopsinya (Ramalinda & Raharja, 2024).

Penelitian sebelumnya telah menggaris bawahi manfaat blockchain dalam mendukung sistem keamanan informasi, namun sebagian besar masih berfokus pada studi kasus terbatas atau hanya menyoroti aspek teknis tertentu (Wulandari & Hwihanus, 2023). Masih terdapat kekosongan literatur yang mengkaji kontribusi blockchain secara komprehensif dalam kerangka keamanan jaringan berdasarkan dimensi-dimensi yang telah teruji secara teoritis. Oleh karena itu, kajian yang mendalam dan sistematis terhadap peran blockchain dalam mendukung empat aspek utama keamanan informasi yaitu autentikasi (authentication), integritas (integrity), ketersediaan (availability), dan privasi (confidentiality), atau dikenal dengan model (CIAA) menjadi sangat relevan dan mendesak (Gemawaty & Yuliani, 2024).

Penelitian ini dilakukan sebagai respons terhadap kebutuhan mendesak untuk mengevaluasi dan mengidentifikasi potensi penerapan blockchain dalam memperkuat arsitektur keamanan jaringan. Tujuan utama dari penelitian ini adalah untuk menganalisis sejauh mana kontribusi blockchain terhadap empat aspek utama keamanan informasi berdasarkan kajian literatur akademik yang valid dan mutakhir. Penelitian ini menggunakan metode studi literatur sistematis terhadap 10 artikel ilmiah nasional dan internasional yang relevan dan terkini, guna memperoleh sintesis ilmiah yang valid dan aplikatif.

Dengan demikian, penelitian ini diharapkan dapat mengisi kesenjangan literatur akademik mengenai integrasi teknologi blockchain dalam keamanan jaringan, serta memberikan rekomendasi strategis untuk pengembangan kebijakan dan teknologi keamanan digital di Indonesia. Selain itu, penelitian ini juga bertujuan memberikan wawasan bagi praktisi teknologi informasi dalam merancang dan mengimplementasikan sistem keamanan yang adaptif dan berkelanjutan dengan pendekatan teknologi blockchain.

2. METODOLOGI PENELITIAN

Metode penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur sistematis. Pendekatan kualitatif dipilih karena memungkinkan peneliti mengeksplorasi makna, konteks, dan pemahaman mendalam dari fenomena yang diteliti, dalam hal ini adalah peran teknologi blockchain dalam meningkatkan keamanan jaringan. Dengan demikian, pendekatan ini tidak bertujuan menghasilkan angka atau data statistik, tetapi pemahaman teoretis yang kaya dan relevan. Adapun tahapan penelitian dalam studi ini dijelaskan seperti pada Gambar 1.

Gambar 1. Tahapan Penelitian

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

2.1 Identifikasi Masalah

Tahapan awal penelitian ini difokuskan pada perumusan isu berdasarkan fenomena aktual, yakni meningkatnya ancaman siber dan kebutuhan akan sistem keamanan digital yang lebih aman dan transparan. Ancaman siber seperti pembobolan data, serangan ransomware, dan pencurian identitas kini menjadi ancaman serius. Oleh karena itu, peneliti mengkaji potensi teknologi blockchain sebagai solusi alternatif yang lebih tangguh dan terdistribusi.

2.2 Penulusuran Studi Literatur

Setelah fokus masalah ditentukan, peneliti melakukan pencarian literatur ilmiah secara sistematis dengan menggunakan tiga kata kunci utama: “blockchain”, “keamanan jaringan”, dan “cybersecurity”. Kata “blockchain” dipilih karena merupakan inti teknologi yang dikaji, sedangkan “keamanan jaringan” merepresentasikan konteks penerapan, dan “cybersecurity” digunakan sebagai istilah teknis global yang lebih luas. Ketiga kata kunci ini dipilih secara strategis agar relevan dengan topik penelitian sekaligus menjaga fokus pencarian, serta Penggunaan tiga kata kunci dianggap ideal karena mampu menyeimbangkan antara keluasan cakupan dan ketepatan hasil pencarian. Literatur diperoleh dari database akademik terpercaya seperti Google Scholar untuk memperoleh referensi yang mutakhir dan relevan dengan konteks penelitian.

2.3 Kriteria Seleksi Literatur

Penelitian ini menggunakan beberapa kriteria inklusi sebagai acuan dalam pemilihan literatur, yaitu:
a. Artikel atau jurnal yang diterbitkan dalam rentang waktu maksimal 5 tahun terakhir.
b. Publikasi yang memuat kata kunci yang sesuai dengan topik penelitian.
c. Artikel berupa full paper tanpa pembatasan pada jenis metode penelitian yang digunakan.
d. Artikel ditulis dalam bahasa Indonesia atau bahasa Inggris.

2.4. Analisis Temuan

Literatur yang terpilih dianalisis menggunakan pendekatan isi dan tematik. Peneliti terlebih dahulu melakukan pengkodean terbuka terhadap bagian-bagian penting dalam masing-masing artikel, kemudian mengelompokkan hasil kode tersebut ke dalam tema-tema utama yang berulang seperti autentikasi, integritas, ketersediaan, dan privasi. Pendekatan ini memfasilitasi pengidentifikasian pola argumentasi dan kontribusi dari tiap artikel dalam konteks teknologi blockchain pada keamanan jaringan. Proses ini dilakukan secara manual melalui pembacaan intensif dan pengorganisasian hasil dalam matriks tematik untuk mempermudah interpretasi dan penyusunan narasi ilmiah yang sistematis.

2.5 Penyusunan Temuan

Hasil analisis kemudian disusun dalam bentuk narasi yang runtut dan terstruktur. Setiap temuan dihubungkan dengan teori dan rumusan masalah yang telah dirancang sebelumnya, sehingga membentuk kerangka logis yang mudah dipahami oleh pembaca.

2.6 Penarikan Kesimpulan

Di tahap akhir, peneliti menyimpulkan hasil dari keseluruhan proses analisis untuk menjawab pertanyaan penelitian. Kesimpulan disusun secara reflektif dan argumentatif, serta dapat memberikan kontribusi teoritis maupun rekomendasi praktis terkait pemanfaatan blockchain dalam meningkatkan keamanan jaringan.

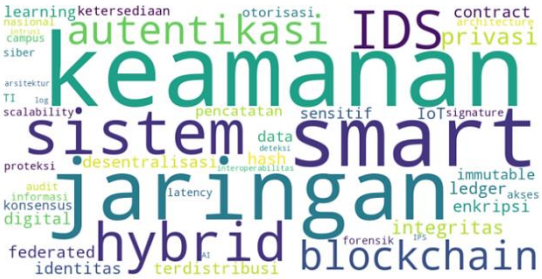
3. HASIL DAN PEMBAHASAN

Dalam proses penelitian ini, telah diperoleh sebanyak 173 artikel dari portal Google Scholar dengan menggunakan kata kunci utama “blockchain”, “keamanan jaringan”, dan “cybersecurity”. Setelah dilakukan proses penyaringan awal berdasarkan kriteria rentang waktu publikasi maksimal 5 tahun terakhir, jumlah artikel yang relevan disaring menjadi 166 artikel.

Setelah seleksi awal, 166 artikel dianalisis lebih lanjut. Dari hasil tersebut, 10 artikel dipilih karena memiliki pembahasan yang mendalam, relevan dengan dimensi keamanan seperti autentikasi, integritas, ketersediaan, dan privasi. Artikel dipilih dari berbagai konteks untuk memastikan cakupan analisis tetap luas dan relevan.

Dari keseluruhan proses seleksi dan analisis, akhirnya terpilih 10 artikel yang dianggap paling relevan, terdiri atas 8 jurnal nasional berbahasa Indonesia dan 2 jurnal internasional berbahasa Inggris. Kemudian, pada artikel yang terpilih tersebut disusun dan dipaparkan secara sistematis dalam bentuk tabel untuk memudahkan interpretasi dan pengelompokan data.

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838



Gambar 2. Visualisasi Worldcloud

Visualisasi Wordcloud pada Gambar 2. menunjukkan bahwa kata-kata seperti blockchain, keamanan, autentikasi, privasi, integritas, desentralisasi, Deteksi Intrusi dan Arsitektur Hybrid menjadi tema dominan dalam artikel yang dianalisis. Ini memperkuat temuan tematik yang diklasifikasikan dalam enam subtema utama pada bagian pembahasan.

Tabel 1. Hasil Studi Literatur

No	Pengarang, Tahun & Bahasa	Judul Jurnal	Nama Jurnal (ISSN/DOI)	Tujuan Penelitian	Metode Penelitian	Hasil Penelitian
1	Phillnov Yohanes Pinontoan & Irwan Sembiring (2022) Indonesia	Implementasi dan Analisis Deteksi Serangan Jaringan pada Web Server NFT Menggunakan Suricata	Jurnal Pendidikan Teknologi Informasi dan Komunikasi (DOI:10.53682/edutik.v4i1.9428)	Mengevaluasi efektivitas Suricata dalam mendeteksi serangan pada web server NFT	Eksperimen : port scan, DDoS, pentesting (NMap, Hping3, Nikto, Metasploit)	Suricata mampu mendeteksi serangan web scanning dan anomali, meskipun rule-set perlu diperbarui
2	Muhammad Fajar Sidiq, Akbari Indra Basuki, Halim Firdaus, & Muhammad Aldi Baihaqi (2020) Indonesia	Sentralisasi Pengawasan Informasi Jaringan Menggunakan Blockchain Ethereum	Jurnal Teknologi Informasi dan Ilmu Komputer (DOI:10.25126/jtiik.2020722662)	Membangun sistem monitoring konfigurasi jaringan terpusat dan aman	Purwarupa: controller jaringan, transaksi ke Ethereum blockchain	Sistem berhasil menjaga availability, integrity, confidentiality pada data flow jaringan
3	Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022) Internasional	A review of blockchain-based secure sharing of healthcare data	Applied Sciences (DOI:10.3390/app12157912)	Mengkaji dan merangkum pendekatan terkini dalam penerapan teknologi blockchain untuk berbagi data kesehatan secara aman	Studi literatur sistematis (review article)	Blockchain dapat meningkatkan keamanan, privasi, dan interoperabilitas data kesehatan. Teknologi ini berpotensi menyelesaikan masalah otentikasi, integritas data, dan kontrol akses dalam sistem

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

No	Pengarang, Tahun & Bahasa	Judul Jurnal	Nama Jurnal (ISSN/DOI)	Tujuan Penelitian	Metode Penelitian	Hasil Penelitian
						kesehatan digital.
4	Zakiyya Zulfa & Galih Salsabilah (2024) Indonesia	Pengembangan Sistem Keamanan Jaringan Berbasis Blockchain untuk Infrastruktur IoT	Prosiding Seminar Nasional Ilmu Matematika dan Sains 2024 (2024)	Mengembangkan sistem keamanan desentralisasi untuk IoT	Simulasi sistem autentikasi dan tracking data via blockchain	Sistem berhasil meningkatkan autentikasi dan pencegahan serangan pada IoT
5	Imam Santoso, Rahmat Nursiaga, Alfonso Sabatani Quiko, & Gunawan Santoso (2025) Indonesia	Model Transformasi Keamanan Digital dalam Jaringan Peer-to-Peer (P2P) Untuk Efisiensi Tinggi Smart Campus	Jurnal Jaringan dan Rekayasa Komputer (DOI:10.9020/jarekom.v1i1)	Mendesain sistem P2P cerdas berbasis blockchain dan IoE	Prototyping dan pengujian arsitektur	Penerapan smart contract berbasis blockchain mampu mendeteksi ancaman siber secara real-time. Jumlah insiden turun 60%, dan mitigasi meningkat hingga 77%, menunjukkan efektivitas tinggi terhadap serangan internal dan eksternal
6	Uky Zaza Agustiana (2024) Indonesia	Pemanfaatan Blockchain untuk Meningkatkan Keamanan Siber dalam Pembayaran Lintas Batas di Fintech	Jurnal Bisnis, Ekonomi Syariah, dan Pajak (DOI:10.61132/jbepv1i4.738)	Menelaah peran blockchain pada keamanan transaksi fintech lintas negara	Studi literatur & studi kasus	Blockchain meningkatkan transparansi dan mengurangi fraud, tantangan regulasi masih ada
7	Imam Riadi, Herman & Aulyah Zakilah Ifani (2021) Indonesia	Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Blockchain	Jurnal Informatika Sunan Kalijaga (DOI:10.14421/jiska.2021.6.3.139-148)	Meminimalkan resiko broken authentication pada web server	Desain sistem dengan blockchain sebagai otentikasi	Sistem menunjukkan peningkatan keamanan autentikasi pada web server
8	Rifky Mustaqim Handoko, Budi Aulyansyah Ahmad	Implementasi Blockchain untuk Keamanan Sistem Pembayaran	Jurnal Ilmu Teknik dan Informatika (DOI:10.51903/teknik.v4i2.589)	Menganalisis efisiensi dan keamanan blockchain di fintech Indonesia	Pendekatan deskriptif kualitatif berbasis studi literatur dan	Blockchain menurunkan fraud, meningkatkan efisiensi dan transparansi,

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

No	Pengarang, Tahun & Bahasa	Judul Jurnal	Nama Jurnal (ISSN/DOI)	Tujuan Penelitian	Metode Penelitian	Hasil Penelitian
	Trisna, Ryan Delon Pratama, & Jadiaman Parhusip (2024) Indonesia	Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia)			case	namun perlu dukungan regulasi
9	Puteri Ananda Khairunnisa, Norul Annisa, Yukandri, & Jadiaman Parhusip (2024) Indonesia	Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI(Studi Kasus di Indonesia)	Jurnal Ilmu Teknik dan Informatika (DOI:10.51903/teknik.v3i1.570)	Mendesain sistem IDS berbasis Snort + AI	Studi kasus & implementasi AI + IDS Snort dan Port Knocking	Sistem mampu meningkatkan deteksi threat dan mematuhi regulasi BSSN
10	Seyed Salar Sefati, Razvan Craciunescu, Bahman Arasteh, Simona Halunga, Octavian Fratu, & Irina Tal (2024) Internasional	Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT)	Smart Cities (DOI:10.3390/smartcities7050109)	Merancang sistem komunikasi IoT aman menggunakan blockchain dan Federated Learning	Simulasi teknis dan Proof	Blockchain memungkinkan data lokal tetap aman tanpa dikirim ke server pusat. Solusi ini mendukung efisiensi bandwidth, menjaga privasi, serta meningkatkan ketahanan sistem terhadap serangan jaringan

3.1 Pembahasan

Berdasarkan hasil seleksi dan telaah sistematis terhadap 10 artikel ilmiah terkini, dilakukan analisis tematik untuk mengidentifikasi kontribusi teknologi blockchain terhadap penguatan sistem keamanan jaringan. Analisis ini diarahkan pada 4 prinsip utama keamanan informasi : autentikasi (authentication), integritas (integrity), ketersediaan (availability), dan privasi (confidentiality) yang menjadi kerangka dasar dalam praktik keamanan siber. Melalui pendekatan tersebut, diperoleh 6 kelompok tematik utama yang merepresentasikan bagaimana blockchain dapat membentuk sistem keamanan jaringan yang adaptif, transparan, dan terdesentralisasi. Temuan ini menjadi landasan penting dalam mendukung relevansi penelitian ini, yakni kajian literatur tentang penggunaan blockchain untuk meningkatkan keamanan jaringan.

3.1.1 Penguatan Otentikasi Sistem Terdistribusi

Dalam studi yang dilakukan oleh (Riadi & Ifani, 2021) bahwa sistem login konvensional terbukti masih memiliki kelemahan serius terhadap serangan *broken authentication*, yaitu ketika kredensial pengguna dapat dimanipulasi atau dicuri oleh pihak tidak sah. Mereka mengusulkan pemanfaatan blockchain untuk menyimpan data POST dalam bentuk

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

hash terenkripsi di jaringan terdistribusi. Hasil implementasi menunjukkan bahwa pendekatan ini secara signifikan meningkatkan ketahanan sistem autentikasi karena tidak ada penyimpanan langsung informasi sensitif pada basis data terpusat yang rentan terhadap serangan.

Penelitian yang dilakukan oleh (Zulfa & Salsabilah, 2025) memperkuat kontribusi tersebut melalui pendekatan autentikasi perangkat IoT yang dicatat dalam *ledger* blockchain. Dengan menciptakan identitas digital unik untuk tiap perangkat, sistem memungkinkan validasi akses yang lebih aman dan akurat. Kontribusi dari kedua studi ini menunjukkan bahwa blockchain tidak hanya meningkatkan keamanan autentikasi, tetapi juga memperluas fleksibilitas kontrol akses dalam jaringan berskala besar dan heterogen.

Fleksibilitas kontrol akses yang dimaksud merujuk pada kemampuan sistem blockchain untuk menerapkan model otorisasi yang dinamis, di mana hak akses pengguna atau perangkat dapat disesuaikan berdasarkan kondisi tertentu, seperti waktu, lokasi, atau level otentikasi. Hal ini dilakukan melalui mekanisme smart contract yang mengeksekusi kebijakan akses secara otomatis tanpa perlu intervensi manusia atau otoritas pusat.

Namun demikian, tantangan tetap ada. Tidak semua sistem lama (legacy system) dapat langsung diintegrasikan dengan mekanisme autentikasi blockchain, terutama yang masih menggunakan protokol otentikasi sederhana seperti username-password tanpa enkripsi. Selain itu, pada jaringan berskala besar, penggunaan blockchain publik dapat menghadapi isu latency dan throughput, yang berdampak terhadap waktu verifikasi autentikasi. Menariknya, sebagian studi lain juga menyoroti bahwa blockchain memang memperkuat autentikasi, namun belum cukup fleksibel untuk konteks perangkat dengan keterbatasan daya dan konektivitas rendah, seperti dalam sistem IoT pedesaan. Hal ini menunjukkan bahwa efektivitas autentikasi berbasis blockchain masih bergantung pada infrastruktur jaringan yang mendukung.

Kontribusi dari temuan ini berkaitan langsung dengan permasalahan yang diangkat dalam pendahuluan, yaitu tingginya risiko peretasan data dan pencurian kredensial akibat sistem autentikasi terpusat. Dengan menyediakan mekanisme otentikasi terdistribusi dan tidak bergantung pada satu titik kegagalan, blockchain menjawab tantangan tersebut dengan pendekatan yang lebih resilien, transparan, dan dapat diaudit secara real-time.

3.1.2 Menjamin Integritas Data dalam Infrastruktur Jaringan

Menurut kajian yang dipaparkan oleh (Sidiq et al., 2020), integritas data jaringan dapat dijaga dengan optimal melalui *smart contract* berbasis *Ethereum* yang mencatat lalu lintas dan aktivitas sistem secara otomatis. Keunggulan sistem ini terletak pada pencatatan immutable yang membuat setiap perubahan dapat dilacak dan diverifikasi, sehingga mengurangi risiko manipulasi data baik dari internal maupun eksternal.

Sementara itu, dalam studi yang dipublikasikan oleh (Xi et al., 2022), integritas data medis dijaga melalui *hash-based verification* dalam struktur *hybrid on-chain* dan *off-chain*. Data sensitif disimpan secara eksternal, namun diverifikasi melalui pointer hash di blockchain, menjamin keutuhan tanpa mengekspos isi data. Kedua studi ini membuktikan bahwa blockchain menyediakan kerangka integritas data yang tangguh dan dapat diaudit dalam berbagai konteks sistem informasi.

Namun demikian, pendekatan hybrid yang mengandalkan penyimpanan *off-chain* menimbulkan tantangan tersendiri, terutama dalam hal verifikasi silang, potensi kerusakan atau kehilangan file asli, serta kesulitan menyelaraskan jejak hash jika terjadi migrasi server. Selain itu, proses verifikasi integritas berbasis blockchain memerlukan daya komputasi tambahan, yang berisiko memperlambat sistem jika tidak didukung infrastruktur yang andal.

Beberapa artikel tidak secara eksplisit menyebutkan kelemahan dari model ini, namun diam-diam mengasumsikan adanya kebutuhan tambahan dalam audit manual saat terjadi konflik data antara on-chain dan off-chain. Ini menunjukkan bahwa meskipun integritas dapat dijaga secara teknis, kesiapan ekosistem pendukung masih menjadi celah yang belum sepenuhnya dipecahkan.

Kontribusi ini sangat relevan dalam konteks serangan manipulasi data dan pemalsuan informasi yang dibahas pada pendahuluan. Kemampuan blockchain untuk merekam log aktivitas secara tidak dapat diubah menjadi solusi penting dalam pengawasan sistem, terutama untuk mencegah tindakan pencurian data oleh pengguna internal.

3.1.3 Perlindungan Privasi Data Sensitif

Menurut Penelitian yang dilakukan oleh (Xi et al., 2022) memberikan pemahaman mendalam tentang bagaimana blockchain dapat melindungi privasi data melalui mekanisme smart contract untuk manajemen akses dan pencatatan transaksi yang dapat diaudit. Dalam konteks sistem informasi kesehatan, pendekatan ini memungkinkan pelacakan aktivitas tanpa mengorbankan kerahasiaan data pasien yang bersifat pribadi.

Senada dengan itu, studi oleh (Sefati et al., 2024) menawarkan model yang mengintegrasikan *federated learning* dan blockchain untuk melatih sistem kecerdasan buatan tanpa perlu mentransfer data mentah. Data tetap berada di edge device, sementara proses pelatihan tetap transparan melalui pencatatan parameter di blockchain. Hal ini menunjukkan bahwa blockchain mampu menjawab tantangan privasi dalam jaringan cerdas yang skalabel dan berbasis kolaborasi.

Namun demikian, privasi yang dilindungi melalui *federated learning* tetap memiliki celah, seperti risiko model *inversion attacks* yang memungkinkan pelaku merekonstruksi data asli dari parameter yang tercatat. Beberapa artikel tidak membahas secara langsung kerentanan ini, namun menunjukkan bahwa integrasi sistem semacam itu masih memerlukan lapisan enkripsi tambahan yang belum selalu tersedia dalam protokol dasar blockchain.

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

Selain itu, *smart contract* yang mengelola hak akses juga rentan terhadap kesalahan pemrograman (contract vulnerability), yang jika tidak diuji dengan cermat, justru dapat membuka celah privasi baru. Hal ini menunjukkan bahwa meskipun blockchain memberikan lapisan perlindungan baru, tetap dibutuhkan *governance* dan audit berkelanjutan terhadap logika *smart contract* itu sendiri.

Dengan meningkatnya kasus kebocoran data, seperti insiden PDNS 2024 yang disinggung pada pendahuluan, sistem privasi berbasis blockchain dapat memberikan alternatif penting, selama risiko-risiko teknis tersebut dikelola secara sistematik.

3.1.4 Ketersediaan Sistem yang Stabil dan Efisien

Dalam kajiannya, (Agustiana, 2024) mengidentifikasi bahwa blockchain dapat mengatasi kendala ketersediaan sistem dalam transaksi lintas batas dengan mengeliminasi peran perantara. Penerapan *smart contract* mampu mempercepat transaksi, mengurangi biaya, dan meminimalisasi potensi *single point of failure*, yang sering kali menjadi titik lemah pada sistem terpusat.

Hasil serupa ditemukan dalam penelitian oleh (Handoko et al., 2024) yang menguji implementasi blockchain pada ekosistem fintech Indonesia. Sistem yang dibangun menciptakan transaksi yang lebih cepat, aman, dan transparan, serta mendorong efisiensi yang signifikan dalam proses operasional. Kedua kajian ini memperkuat bukti bahwa blockchain mendukung prinsip *availability* dengan menyediakan sistem yang selalu aktif dan tangguh terhadap gangguan teknis.

Namun, isu skalabilitas dan konsumsi energi menjadi perhatian utama dalam sistem blockchain publik. Studi-studi tersebut umumnya tidak menyoroti secara langsung bagaimana mekanisme konsensus seperti Proof of Work (PoW) berdampak pada latency dan energi, terutama saat beban transaksi tinggi. Meskipun beberapa sistem mulai mengadopsi Proof of Stake (PoS), peralihan ini masih menimbulkan tantangan interoperabilitas dan pengaturan teknis yang belum standar.

Tidak semua artikel menampilkan pandangan kritis ini, namun penting dicatat bahwa ketersediaan sistem tidak hanya soal uptime teknis, melainkan juga kemampuan sistem mempertahankan performa saat digunakan secara masif. Di sinilah blockchain perlu didampingi oleh desain arsitektur layer-2 atau teknologi tambahan seperti sidechain untuk menjaga skala dan performa.

Kontribusi ini berkorelasi langsung dengan isu DDoS dan sistem yang rawan mati total jika bergantung pada satu otoritas pusat. Blockchain mendistribusikan titik pengambilan keputusan, sehingga tetap aktif bahkan saat satu node gagal, namun perlu terus dioptimalkan dari sisi efisiensi.

3.1.5 Deteksi dan Pencegahan Intrusi secara Proaktif

Dalam kontribusinya, (Phillnov Yohanes Pinontoan, 2024) mengembangkan sistem deteksi intrusi yang menggabungkan IDS Suricata dan pencatatan berbasis blockchain NFT. Setiap aktivitas lalu lintas jaringan disimpan dalam ledger blockchain yang tidak dapat diubah, memungkinkan analisis forensik digital dan peningkatan respons terhadap serangan seperti *malware* dan DDoS secara real-time.

Pengembangan lebih lanjut dilakukan oleh (Khairunnisa et al., 2024) melalui sistem IDS nasional yang memadukan teknologi SNORT, AI, dan blockchain. Sistem ini tidak hanya adaptif terhadap ancaman siber, tetapi juga dirancang sesuai standar regulasi nasional dari BSSN. Temuan ini menunjukkan bahwa blockchain dapat memainkan peran aktif dalam pengawasan dan perlindungan sistem jaringan dari serangan yang terus berkembang.

Meski demikian, kedua studi cenderung berfokus pada integrasi sistem tanpa membahas risiko *false-positive* yang tinggi dalam IDS berbasis signature, atau keterbatasan AI dalam mengenali *zero-day* attack. Selain itu, pencatatan ke blockchain dapat menimbulkan overhead tinggi, yang justru memperlambat deteksi jika tidak dikombinasikan dengan sistem *buffer log* atau *off-chain processing*. Penting juga dicatat bahwa belum ada konsensus tentang standar format log keamanan untuk pencatatan di blockchain, sehingga interoperabilitas antar sistem keamanan masih menjadi isu yang belum terselesaikan.

Secara umum, blockchain mampu memperkuat lapisan respons insiden siber, tetapi harus didampingi oleh pengujian performa, validasi log, dan sistem redundansi untuk menjamin efektivitas nyata di lapangan.

3.1.6 Arsitektur Hybrid untuk Ketahanan Skala Besar

Dalam studi yang dilakukan oleh (Santoso et al., 2025), dirancang model arsitektur keamanan smart campus yang memadukan blockchain, AI, dan enkripsi adaptif secara *peer-to-peer*. Sistem ini dirancang untuk mempercepat mitigasi ancaman dan menurunkan insiden keamanan dengan tingkat efektivitas yang tinggi. Penerapannya menunjukkan keunggulan pendekatan hybrid dalam lingkungan yang dinamis dan padat pengguna seperti kampus digital.

Adapun dalam kajian oleh (Khairunnisa et al., 2024), dikembangkan model sistem keamanan TI nasional dengan struktur hybrid yang fleksibel, modular, dan tahan gangguan. Blockchain berperan sebagai pengatur akses dan pencatat transaksi antar entitas secara aman dan desentralistik. Keduanya menunjukkan bahwa blockchain tidak berdiri sendiri, tetapi dapat berfungsi sebagai tulang punggung sistem keamanan berskala besar dalam ekosistem hybrid modern.

Namun demikian, tantangan pada arsitektur hybrid terletak pada manajemen kerumitan sistem: semakin banyak lapisan teknologi yang digabung, semakin tinggi kebutuhan akan orkestrasi, monitoring, dan pemeliharaan sinkronisasi

TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

antar modul. Beberapa studi juga tidak membahas aspek keberlanjutan sistem dalam jangka panjang, terutama terkait kebutuhan daya dan audit kebijakan keamanan lintas platform.

Pendekatan hybrid menjadi sangat penting untuk menjawab tantangan keamanan jaringan yang kompleks dan bersifat dinamis seperti yang dibahas di pendahuluan. Ketika serangan terjadi secara multi-vektor (seperti DDoS dikombinasikan dengan malware dan rekayasa sosial), hanya sistem yang modular dan adaptif yang mampu merespons secara real-time dan resilien. Di sinilah blockchain menjadi fondasi utama karena fleksibilitas dan keterbukaan strukturnya.

Dari keseluruhan pembahasan ini, dapat disimpulkan bahwa teknologi blockchain memiliki potensi besar dalam memperkuat sistem keamanan jaringan, baik dari peran strategis dalam memperkuat empat dimensi utama keamanan informasi, yaitu autentikasi, integritas, ketersediaan, dan privasi (CIAA). Melalui mekanisme desentralisasi, pencatatan data yang immutable, dan validasi berbasis konsensus. Autentikasi diperkuat dengan identitas digital berbasis hash, integritas dijaga melalui smart contract, ketersediaan ditingkatkan lewat struktur jaringan terdistribusi, dan privasi didukung oleh teknik kriptografi serta integrasi dengan *federated learning*. Setiap artikel yang dianalisis memberikan kontribusi konseptual maupun teknis yang saling melengkapi, membentuk pemahaman komprehensif mengenai peran strategis blockchain dalam membentuk arsitektur keamanan jaringan yang adaptif, desentralistik, dan transparan.

4. KESIMPULAN

Berdasarkan telaah terhadap sepuluh artikel ilmiah yang relevan, penelitian ini menyimpulkan bahwa teknologi blockchain memiliki potensi yang signifikan dalam meningkatkan keamanan jaringan, serta telah terbukti efektif dalam mendukung aspek-aspek keamanan jaringan. Dalam aspek *authentication*, blockchain meningkatkan keandalan autentikasi pengguna dan perangkat melalui pencatatan identitas digital berbasis hash yang tidak dapat diubah, mengurangi risiko pemalsuan dan penyalahgunaan akses. Dari sisi *integrity*, blockchain menjamin keutuhan data melalui pencatatan transaksi yang immutable dan dapat diverifikasi secara otomatis menggunakan smart contract, efektif diterapkan dalam sistem jaringan maupun penyimpanan data sensitif. Pada dimensi *availability*, arsitektur terdesentralisasi blockchain mendukung ketersediaan sistem yang stabil, menghilangkan titik kegagalan pusat, dan meningkatkan efisiensi transaksi, khususnya di sektor keuangan digital. Dalam hal *confidentiality*, blockchain terutama saat diintegrasikan dengan federated learning mampu menjaga privasi data dengan memungkinkan proses komputasi tanpa perlu memindahkan data mentah. Blockchain efeketif mendukung sistem deteksi dan pencegahan intrusi (IDS/IPS) melalui pencatatan log keamanan real-time yang tidak dapat dimanipulasi, memperkuat sistem pemantauan dan respons terhadap ancaman siber. Pada skala besar, blockchain dapat diintegrasikan dalam arsitektur hybrid bersama AI dan IDS, membentuk sistem keamanan jaringan yang modular, skalabel, dan sesuai dengan kebutuhan infrastruktur digital nasional. Namun demikian, penelitian ini juga menyadari bahwa penerapan blockchain dalam keamanan jaringan masih menghadapi tantangan, termasuk dalam hal efisiensi energi, kompleksitas integrasi dengan sistem lama, serta belum meratanya kesiapan regulasi dan infrastruktur digital di berbagai sektor. Oleh karena itu, diperlukan studi lanjut yang bersifat empiris untuk menguji keefektifan blockchain dalam konteks operasional yang nyata serta simulasi implementasi lintas sektor. Penelitian ini diharapkan dapat menjadi dasar konseptual bagi akademisi, praktisi, dan pembuat kebijakan dalam memahami dan mengevaluasi peran blockchain sebagai inovasi teknologi yang tidak hanya relevan, tetapi juga esensial dalam membangun ekosistem keamanan jaringan yang tangguh dan berkelanjutan.

REFERENCES

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2024). Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian. *Journal of Internet and Software Engineering*, *1*(4), 12.

Afdilah, S., Agustina, N. S., Hani, I., & Gunawan, G. (2024). Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna. *Journal Software, Hardware and Information Technology*, *4*(2), 47–62.

Agustiana, U. Z. (2024). *Pemanfaatan Blockchain untuk Meningkatkan Keamanan Siber dalam Pembayaran Lintas Batas di Industri Fintech*.

Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, *9*(2), 113–118.

Ardyawin, I., Syaharuddin, S., & Iswanto, D. (2024). Peran Teknologi Blockchain dalam Meningkatkan Keamanan dan Akuntabilitas Data Di Perpustakaan: Potensi dan Tantangan. *SEMINAR NASIONAL LPPM UMMAT*, *3*, 65–74.

Bani, P. (2024). Blockchain dan Asuransi Mikro: Kajian Literatur tentang Peluang dan Tantangan Inovasi. *Premium Insurance Business Journal*, *11*(2), 1–12.

Budiyanto, D., & Mabruri, M. (2025). Pentingnya Keamanan Siber Dalam Era Digital:: Tinjauan Global Dan Kondisi Di Indonesia. *Prosiding Seminar Nasional Sains Dan Teknologi" SainTek"*, *2*(1), 981–994.

Gemawaty, C. A., & Yuliani, Y. (2024). Manajemen Identitas Dan Akses Dalam Keamanan Sistem Informasi (Pendekatan Literature Review). *Jurnal Manajamen Informatika Jayakarta*, *4*(4), 396–403.

Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi Blockchain untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 64–74.

Hidayatullah, R., & Saiin, A. (2025). Dinamika Hukum Wakaf di Indonesia Tantangan dan Solusi dalam Pengelolaan


TIN: Terapan Informatika Nusantara
Vol 6, No 2, July 2025, page 95-104
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i2.7838

Aset Wakaf Produktif. *Al Barakat: Jurnal Kajian Hukum Ekonomi Syariah*, *5*(01), 11–23.

Indonesia, C. (2024). Fakta-fakta Kebocoran Data PDNS, Dalang hingga Jumlah Tebusan. In *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20240624122531-185-1113359/fakta-fakta-kebocoran-data-pdns-dalang-hingga-jumlah-tebusan.

Khairunnisa, P. A., Annisa, N., & Parhusip, Y. J. (2024). *Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI : Studi Kasus di Indonesia*. *4*, 9–16.

Lim, W., Angkasa, S., & Wibowo, A. D. P. (2024). Smart Contracts: Validitas Hukum dan Tantangan di Masa Depan Indonesia. *Jurnal Kewarganegaraan*, *8*(1), 829–838.

Nuraini, F. N. (2025). Peran Teknologi Blockchain dalam Meningkatkan Keandalan Akuntansi. *Profit: Jurnal Manajemen, Bisnis Dan Akuntansi*, *4*(2), 303–312.

Phillnov Yohanes Pinontoan, I. S. (2024). Implementasi dan Analisis Deteksi Serangan Jaringan Pada Web Server NFT Menggunakan Suricata. *EduTIK: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, *4*, 65–78. https://repository.uksw.edu//handle/123456789/33686

Pratama, F., Avini, T., Saputra, I., Putri, M. K., & Imamfajri, S. (2024). Analisis Risiko Keamanan Pada Pengembangan Perangkat Lunak Berbasis Cloud. *Jurnal Kecerdasan Buatan Dan Teknologi Informasi*, *3*(2), 61–67.

Ramalinda, D., & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*.

Riadi, I., & Ifani, A. Z. (2021). Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Teknologi Blockchain. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *6*(3), 139–148.

Sadi, N. D., & Nugraha, I. F. (2025). Serangan Siber Pada Isiden Power Grid Tahun 2020 Dan Dampaknya Terhadap Hubungan India-Tiongkok. *Triwikrama: Jurnal Ilmu Sosial*, *8*(7), 31–40.

Santoso, I., Nursiaga, R., Quiko, A. S., & Santoso, G. (2025). *Model Transformasi Keamanan Digital dalam Jaringan Peer-to-Peer (P2P) Untuk Efisiensi Tinggi Smart Campus*. *01*(01), 12–21.

Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *5*(2), 159–187.

Sefati, S. S., Craciunescu, R., Arasteh, B., Halunga, S., Fratu, O., & Tal, I. (2024). Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT). *Smart Cities*, *7*(5), 2802–2841. https://doi.org/10.3390/smartcities7050109

Sidiq, M. F., Basuki, A. I., Firdaus, H., Baihaqi, M. A., Informatika, P. P., Ilmu, L., Indonesia, P., & Korespondensi, P. (2020). Centralized Monitoring of Network Information Using Ethereum. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(6), 1187–1196. https://doi.org/10.25126/jtiik.202072662

Soetrisno, W., Azhar, W. Y., Purba, A. B., Hilman, A., Lestari, V. A., & Mutawally, A. N. (2025). Meningkatkan Keamanan dan Mitigasi pada Arsitektur Software Defined Network. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *20*(1), 18–28.

Sumampouw, E. G. J., & Sembiring, I. (2024). Analisis Verifikasi Proof of Stake (POS) NFT dengan Teknologi Smart Contract. *Edutik: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, *4*(1), 15–28.

Susanti, W. F. E. (2024). Blockchain, Artificial Intelligence, dan Big Data: Teknologi yang Mengubah Wajah Akuntansi di Era Digital. *Jebital: Jurnal Ekonomi Dan Bisnis Digital*, *1*(4), 1–9.

Wulandari, I. W., & Hwihanus, H. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian Dan Penalaran Ilmu Manajemen*, *1*(1), 11–25.

Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A Review of Blockchain-Based Secure Sharing of Healthcare Data. *Applied Sciences (Switzerland)*, *12*(15). https://doi.org/10.3390/app12157912

Zulfa, Z. H., & Salsabilah, G. (2025). *Pengembangan Sistem Keamanan Jaringan Berbasis Blockchain untuk Infrastruktur IOT*. *1*, 40–43.