

PERAN TEKNOLOGI *BLOCKCHAIN* TERHADAP KEAMANAN DAN PRIVASI DATA SISTEM INFORMASI LAYANAN KESEHATAN: STUDI PUSTAKA

Irra Pratiwi¹⁾, Suprih Widodo^{2,*}

^{1, 2)}Pendidikan Sistem Teknologi dan Informasi, Universitas Pendidikan Indonesia

e-mail: irrapratiwi@upi.edu¹⁾, supri@upi.edu²⁾

*corresponding author

(Naskah masuk : 10 April 2025 Diterima untuk diterbitkan : 21 April 2025)

ABSTRAK

Meningkatnya minat untuk digitalisasi mendorong bertambahnya penggunaan penyimpanan identitas pasien dan rekam medis oleh penyedia layanan kesehatan. Dengan menerapkan konsep desentralisasi dan distribusi data, *blockchain* memberikan solusi untuk melindungi informasi kesehatan yang sangat sensitif dari risiko serangan siber dan manipulasi data yang sangat marak sekali terjadi. Selain itu, *blockchain* juga memiliki kunci dalam otentikasi identitas pasien serta menciptakan pelacakan riwayat medis yang aman. Metode yang digunakan dalam penelitian ini adalah studi pustaka untuk menggali literatur-literatur dari berbagai jurnal dan artikel terkait peran teknologi *blockchain* dalam meningkatkan keamanan dan privasi data sistem informasi kesehatan. Oleh karena itu, penelitian ini dapat memberikan pemahaman mendalam tentang dampak positif dan potensi tantangan dalam mengimplementasikan teknologi *blockchain* untuk keamanan data sistem informasi kesehatan. Teknologi *blockchain* dapat membantu mengurangi terjadinya kehilangan atau kecurangan data, mengurangi biaya inventasi rumah sakit, serta dapat mengintegrasikan sistem yang berbeda dengan cepat.

Kata Kunci: *Blokchain, Keamanan Data, Sistem Informasi Kesehatan.*

ABSTRACT

The growing interest in digitization is driving the increasing use of patient identity storage and medical records by healthcare providers. By applying the concept of decentralization and data distribution, *blockchain* provides a solution to protect highly sensitive health information from the risk of cyberattacks and data manipulation, which is very prevalent. In addition, *blockchain* also has the key to authenticating patient identity and creating secure medical history tracking. The method used in this research is a literature study to explore literature from various journals and articles related to the role of *blockchain* technology in improving the security and privacy of health information system data. Therefore, this research can provide an in-depth understanding of the positive impacts and potential challenges in implementing *blockchain* technology for health information system data security. *Blockchain* technology can help reduce the occurrence of data loss or fraud, reduce hospital inventory costs, and can quickly integrate disparate systems.

Keywords: *Blockchain, Data Security, Health Information System.*

I. PENDAHULUAN

Dalam beberapa tahun terakhir, teknologi *blockchain* telah mendapatkan perhatian yang signifikan di berbagai bidang, termasuk layanan kesehatan. Agar dapat menyesuaikan perkembangan zaman yang semakin modern terhadap teknologi sehingga perusahaan harus mampu menyesuaikan pola bisnisnya dengan mengukur seberapa besar dampak positif yang diberikan jika menerapkan sistem informasi, teknologi informasi dan seberapa tinggi peluang yang tersedia pada kegiatan operasional perusahaan tersebut. Dalam sistem layanan kesehatan, banyak data dibuat, diuji, disimpan, dan diakses setiap hari. Seperti data yang dibuat saat pasien menjalani beberapa tes yang akan dilihat oleh dokter, radiografer, dan tenaga medis lain. Setelah itu, hasilnya akan disimpan di rumah sakit dan dapat diakses sewaktu pasien membutuhkan. Namun, tidak semua rumah sakit tidak menerapkan kebijakan rekam medis elektronik. Meskipun teknologi ini membawa manfaat signifikan, tantangan utama yang dihadapi adalah keamanan dan privasi data pasien. Informasi medis yang bersifat pribadi dan sensitif memerlukan perlindungan yang kuat untuk mencegah akses yang tidak sah dan penyalahgunaan data

[1]. Selain itu, meskipun rekam medis elektronik dapat menghemat biaya jangka panjang, biaya awal implementasi bisa sangat tinggi. Pembelian perangkat lunak, pelatihan untuk tenaga medis, dan penyesuaian infrastruktur merupakan investasi yang signifikan bagi lembaga kesehatan.

Teknologi blockchain pertama kali dikenal sebagai infrastruktur pendukung mata uang kripto, telah muncul sebagai solusi yang menjanjikan untuk meningkatkan keamanan dan privasi data dalam layanan kesehatan. Keamanan dan privasi data merupakan hal yang penting dalam sistem informasi layanan kesehatan. Data kesehatan pasien yang disimpan di sistem informasi layanan kesehatan harus dilindungi dari penyalahgunaan, seperti pemalsuan identitas, pencurian data, atau akses tanpa izin. Teknologi blockchain menawarkan sistem terdistribusi yang aman, transparan, dan tak terubah, yang dapat merubah paradigma keamanan informasi di sektor layanan kesehatan. Dalam manajemen data seperti mencakup pengumpulan, pemrosesan, distribusi, pengambilan, perlindungan, dan penyimpanan data, terutama dalam lingkungan perawatan kesehatan, keamanan data tentu sangat penting. Oleh karena itu, diperlukan adanya penguatan keamanan database untuk tetap menjaga privasi data pasien. Teknologi blockchain dapat membuat solusi database terdistribusi dan aman tanpa memerlukan administrator tetap. Selain itu, teknologi blockchain berguna untuk meningkatkan keaslian dan transparansi data layanan kesehatan di rumah sakit dan institusi. Hal ini dapat mempertahankan izin Electronic Medical Record (EMR) dan membuat pemrosesan data pasien menjadi sederhana.

Menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo 20/2016) yaitu data perseorangan tertentu yang di simpan, di rawat, dan dijaga kebenarannya serta mendapatkan perlindungan atas kerahasiaannya. Adapun rekam medis pasien diregulasi oleh Kementerian Kesehatan Republik Indonesia nomor 269/MENKES/PER/III/2008 dan merupakan suatu dokumen yang sangat rahasia dan hanya boleh ditulis oleh dokter atau pihak tenaga kesehatan yang melakukan tindakan kepada pasien tersebut. Di Indonesia, penerapan blockchain dalam layanan kesehatan masih dalam tahap eksplorasi. Alasannya karena beberapa rumah sakit di Indonesia belum menerapkan rekam medis elektronik. Oleh karena itu, studi literatur ini bertujuan untuk memberikan pemahaman yang mendalam tentang peran teknologi blockchain terhadap keamanan dan privasi data dalam sistem informasi layanan kesehatan. Melalui merinci temuan-temuan dari penelitian dan literatur terkait, artikel ini akan menguraikan bagaimana blockchain dapat menjadi fondasi yang kokoh untuk melindungi integritas data, memberikan otorisasi akses yang terkontrol, dan menyederhanakan proses manajemen informasi kesehatan.

Saat ini, hanya ada beberapa penelitian yang mencoba mengimplementasikan penggunaan teknologi blockchain di bidang kesehatan. Dengan memfokuskan tinjauan literatur pada studi-studi kasus, riset-riset terbaru, dan pandangan pakar, artikel ini bertujuan untuk memberikan pandangan holistik tentang keefektifan blockchain dalam menjawab tantangan keamanan dan privasi yang dihadapi oleh sistem informasi layanan kesehatan. Melalui pemahaman yang lebih mendalam ini, diharapkan artikel ini dapat memberikan wawasan berharga bagi para profesional kesehatan, pengembang teknologi, dan pengambil keputusan dalam upaya mereka meningkatkan keamanan data pasien dan menjaga privasi dalam konteks layanan kesehatan yang terus berkembang. Sehingga dapat membantu penelitian selanjutnya baik terkait dengan pengimplementasian maupun efektivitas.

II. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kualitatif dengan metode studi Pustaka sebagai landasan metodologi. Studi pustaka mengacu pada pendekatan penelitian yang menggali berbagai kajian kepustakaan yang relevan dengan topik penelitian [2]. Pemanfaatan metode studi pustaka memungkinkan penelitian ini untuk merencanakan langkah awal tanpa perlu terjun langsung ke lapangan, sehingga data dan wawasan yang diperlukan dapat diperoleh dari sumber-sumber yang telah ada. Penelitian deskriptif adalah jenis penelitian yang meneliti gejala sosial dengan mendeskripsikan nilai variable berdasarkan indikator yang diteliti. Penelitian ini tidak melakukan hubungan atau perbandingan antara variable lain.

Setelah sumber data dari literatur berhasil dikumpulkan, penelitian ini menerapkan analisis isi (content analysis) untuk mengungkap makna dan informasi yang terkandung dalam teks-teks yang telah disusun. Analisis isi membantu dalam mengurai teks secara obyektif, tanpa campur tangan subjektif dari peneliti, sehingga gambaran yang objektif dapat dihasilkan [3]. Peneliti juga menggunakan metode

deskriptif analisis untuk mengumpulkan, mengidentifikasi, dan mengorganisasi data dengan sistematis guna memberikan pemahaman yang jelas kepada pembaca. Pengumpulan data penelitin ini menggunakan metode mencari sumber dan menkontruksi dari berbagai sumber, termasuk buku, jurnal, dan penelitian sebelumnya. Untuk mendukung proposisi dan gagasan, bahan pustaka yang diperoleh dari berbagai referensi harus dianalisis secara kritis. Analisis kritis merupakan suatu pandangan yang menyatakan peneliti bukanlah subyek yang bebas nilai ketika memandang penelitian. Dengan demikian, peneliti harus tetap bersifat netral.

Tabel 1. Penelitian Terkait

No	Judul Dan Tahun Penelitian	Metode Penelitian	Hasil Penelitian
1.	<i>Blockchain for Healthcare Systems: Architecture, Security Challenges, Trends and Future Directions</i> (Kumar et al, 2023)	Penelitian ini dilakukan dengan pendekatan kualitatif deskriptif melalui analisis pustaka terhadap berbagai artikel ilmiah, jurnal, dan publikasi terbaru yang berkaitan dengan implementasi teknologi <i>blockchain</i> dalam sistem layanan kesehatan.	Penelitian ini menemukan bahwa teknologi <i>blockchain</i> dapat meningkatkan keamanan dan privasi data dalam sistem layanan kesehatan melalui fitur desentralisasi, transparansi, dan kontrol akses berbasis <i>smart contract</i> . Namun, tantangan seperti skalabilitas, interoperabilitas, dan regulasi masih perlu diatasi agar implementasinya optimal dan berkelanjutan.
2.	<i>Blockchain for Healthcare Management: Enhancing Data Security and Transparency</i> (Fernandes et al. ,2023)	Penelitian ini menggunakan pendekatan kualitatif berbasis studi literatur, dengan menganalisis berbagai penelitian dan studi kasus terkait implementasi <i>blockchain</i> dalam manajemen data kesehatan. Penulis juga mengevaluasi arsitektur sistem dan fitur keamanan dari beberapa solusi berbasis <i>blockchain</i> yang telah dikembangkan.	Hasil penelitian menunjukkan bahwa <i>blockchain</i> dapat meningkatkan keamanan, transparansi, dan efisiensi dalam pengelolaan data medis. Teknologi ini memungkinkan kontrol akses yang ketat, pencatatan data yang tidak dapat diubah, serta otomatisasi proses medis menggunakan <i>smart contract</i> yang secara keseluruhan mengurangi risiko manipulasi dan kebocoran data.
3.	Peran Teknologi Blockchain dalam Keamanan dan Privasi Data Sistem Informasi Kesehatan: Studi Literatur, (Matulesi ,2023)	Penelitian ini menggunakan metode studi literatur, dengan menelaah berbagai jurnal, artikel ilmiah, dan laporan terkait penerapan teknologi <i>blockchain</i> dalam sistem informasi kesehatan, khususnya yang berfokus pada aspek keamanan dan privasi data.	Penelitian ini menegaskan bahwa meskipun <i>blockchain</i> menawarkan potensi besar, dukungan regulasi dan peningkatan infrastruktur sangat diperlukan agar teknologi ini dapat diadopsi secara efektif di Indonesia. Penelitian ini menunjukkan bahwa teknologi <i>blockchain</i> dapat secara signifikan meningkatkan keamanan dan privasi data dalam sistem informasi layanan kesehatan. <i>Blockchain</i> menawarkan beberapa keuntungan utama, seperti keamanan data yang lebih tinggi karena sifatnya yang tidak dapat diubah (<i>immutable</i>), yang mengurangi risiko manipulasi

No	Judul Dan Tahun Penelitian	Metode Penelitian	Hasil Penelitian
			atau kehilangan data medis pasien. Selain itu, privasi pasien dapat lebih terjaga dengan memberikan mereka kontrol penuh atas siapa saja yang bisa mengakses data medis mereka, menggunakan mekanisme otorisasi berbasis kriptografi.

Secara keseluruhan, penelitian ini mengadopsi desain literatur review, yang secara kritis mengevaluasi temuan, gagasan, dan pengetahuan yang terdapat dalam literatur akademik. Metode penelitian kepustakaan ini digunakan untuk menyusun konsep mengenai Produktivitas yang nantinya dapat digunakan sebagai pijakan dalam mengembangkan langkah-langkah praktis sebagai alternatif pendekatan manajemen. Sifatnya adalah analisis deskriptif yang sistematis, memungkinkan data yang ditemukan untuk diuraikan dan dipahami dengan baik oleh pembaca, sehingga membentuk landasan yang kokoh untuk pemahaman mendalam terhadap topik penelitian yang dibahas [3].

III. HASIL DAN PEMBAHASAN

Desentralisasi merupakan konsep utama dalam teknologi *blockchain* dengan menghilangkan kebutuhan akan otoritas terpusat dan memberikan kontrol yang lebih besar kepada individu atau organisasi yang menggunakannya. Ini penting untuk keamanan dan privasi data karena otoritas sentral rentan terhadap serangan siber. Data yang disimpan di berbagai simpul jaringan dalam sistem *blockchain* lebih tahan terhadap serangan dan akan sulit untuk dimanipulasi. Teknologi *blockchain* pertama kali hadir di tahun 2009, melalui mata uang kripto Bitcoin. *Blockchain* merupakan daftar catatan transaksi lengkap dan valid yang disusun dalam urutan kronologis blok. Blok yang mendahului blok tertentu disebut sebagai blok induknya, dan blok pertama disebut sebagai blok asal. Rantai dibentuk karena setiap blok dihubungkan ke blok sebelumnya dengan referensi (nilai hash). Teknologi *blockchain* dapat digambarkan sebagai rekening publik yang mencatat transaksi sebagai basis data aset yang dapat dibagi antara berbagai lokasi, organisasi, atau tempat.

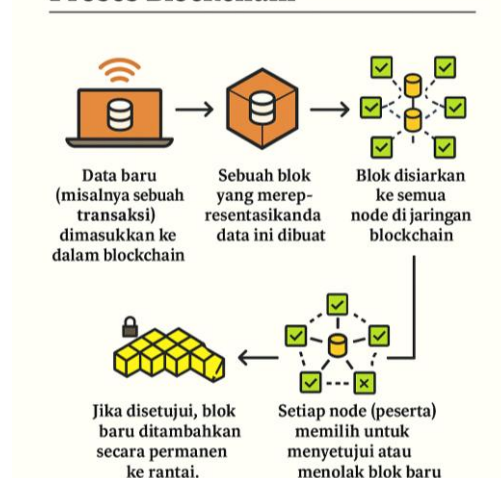
Blockchain hadir sebagai teknologi inovatif dengan potensi besar untuk mengubah berbagai industri, memberikan solusi untuk keamanan data, transparansi, dan pengelolaan informasi secara lebih efisien. Desentralisasi yang dimaksud dalam teknologi *blockchain* yaitu Informasi pada *blockchain* disimpan di berbagai node (komputer) di seluruh jaringan, bukan di satu entitas central [4]. Hal ini dapat memastikan distribusi dan ketergantungan yang merata. Seluruh riwayat pencatatan di *blockchain* dapat diakses dan diverifikasi oleh setiap peserta jaringan. Transaksi dienkripsi menggunakan kunci kriptografi yang kuat, memastikan keamanan dan integritas data. Sistem dengan mengimplementasikan *blockchain* akan otomatis mengeksekusi perjanjian atau kondisi tertentu saat dipenuhi, tanpa intervensi pihak ketiga. Oleh karena itu *blockchain* dapat meningkatkan sistem dengan kepercayaan dan transparansi.

Teknologi *blockchain* memiliki data yang disimpan dalam jaringan yang tersebar, sehingga jika salah satu node rusak, data masih dapat tetap diakses melalui node lain [5]. Hal ini dapat dipastikan bahwa data tetap tersedia dan diakses meskipun terjadi gangguan pada salah satu node dalam jaringan. Data yang sudah tersimpan masih tetap bisa diakses kapanpun tanpa gangguan. Karena data *blockchain* transparan dan dapat diakses oleh siapa saja, maka dapat memastikan bahwa data yang disimpan sudah akurat dan terpercaya. Sehingga membantu mengurangi terjadinya risiko penyalahgunaan serta pemalsuan data.

Selain itu, semua informasi yang terekam dalam node *blockchain* hanya tersedia untuk seluruh jaringan node yang terhubung. Dengan demikian, semua pemangku kepentingan dapat menggunakannya sesuai dengan wewenangnya masing-masing serta tidak bisa diedit tanpa persetujuan dari seluruh node dalam jaringan. Sedangkan dalam database biasa, data disusun kedalam bentuk tabel, sedangkan *blockchain*, menyusun datanya ke dalam potongan-potongan (block), lalu dikaitkan satu

sama lain. Struktur data pada *blockchain* ini secara terstruktur membuat garis waktu data yang tidak dapat diubah ketika diimplementasikan pada sistem yang terdesentralisasi [6].

Proses Blockchain



Gambar 1. Proses Blockchain

Teknologi *blockchain* terbagi menjadi berbagai tipe yaitu *public blockchain*, *private blockchain*, dan *semi-private blockchain*. *Public blockchain* merupakan jaringan terdistribusi yang terbuka untuk semua entitas yang berpartisipasi dalam jaringan dan bersifat open source sehingga entitas dapat mendistribusikannya [7]. *Private blockchain* merupakan *blockchain* yang bersifat tertutup dan hanya digunakan untuk pertukaran informasi internal. Hal ini mencegah pihak yang tidak berkepentingan untuk melihat apa yang sedang dilakukan di dalam *blockchain* [8]. Sistem informasi Kesehatan dapat menerapkan dua jenis *blockchain* tersebut, baik *public blockchain* maupun *private blockchain*.

Salah satu keunggulan utama teknologi *blockchain* yaitu keamanan data yang tinggi. Karena dalam teknologi *blockchain* harus melewati proses validasi yang ketat. Privasi data merujuk pada hak individu untuk mengontrol dan melindungi informasi pribadi. Informasi tersebut mencakup sejumlah prinsip dan praktik yang dirancang untuk memastikan bahwa data pribadi seseorang dijaga dari akses atau penggunaan yang tidak sah. Keamanan data merujuk pada konsep yang luas yang mencakup berbagai upaya dan praktik untuk melindungi integritas, kerahasiaan, dan ketersediaan data. Di Indonesia, kesadaran akan perlunya perlindungan data pribadi akan semakin meningkat, seiring dengan pertumbuhan. Berdasarkan UUD 1945 Pasal 28G Ayat (1), warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta miliknya [4].

Teknologi *blockchain* memiliki peran penting untuk melindungi keamanan dan privasi data. Hal ini melibatkan penerapan langkah-langkah keamanan teknis, kebijakan, dan prosedur untuk mencegah kebocoran, manipulasi, atau penghancuran data. Aspek keamanan data meliputi kontrol akses, enkripsi, pemantauan aktivitas sistem. Salah satu aspek yang perlu dilindungi dalam sistem informasi Kesehatan yaitu dalam aspek rekam medis elektronik. Rekam medis elektronik dapat menunjang perekaman, penyimpanan, pengolahan data, serta penyajian informasi kesehatan [9].

Dengan demikian, banyak sekali data yang perlu dilindungi. Jika sistem yang digunakan tidak menerapkan teknologi *blockchain*, maka akan memudahkan data untuk dimanipulasi dan dicurangi. Karena rekam medis elektronik harus disajikan dengan lengkap dan akurat. Keamanan data dalam sistem informasi kesehatan merupakan kombinasi antara teknologi dengan organisasi. Keamanan data dalam sistem informasi kesehatan sangat penting untuk menjaga integritas dan konfidensialitas informasi kesehatan yang terkandung serta melindungi privasi pasien dan memenuhi kepastian perlindungan hukum bagi pasien, tenaga medis, dan institusi kesehatan.

Bentuk keamanan data dalam sistem informasi kesehatan yaitu seperti otentikasi, integritas, serta penyimpanan dan transmisi data yang aman [10]. Dalam sistem informasi kesehatan, Otentikasi merupakan proses verifikasi identitas pasien untuk memastikan bahwa pasien tersebut yang memiliki

hak akses pada suatu sistem. Penerapan sistem otentikasi dapat melibatkan penggunaan dua atau lebih metode otentikasi sekaligus, seperti penggunaan password, kode SMS, atau pengenalan sidik jari. sampai *face ID*. Hal ini meningkatkan tingkat keamanan karena membutuhkan lebih dari satu tipe verifikasi. Sedangkan teknologi blockchain sudah memenuhi prinsip bentuk keamanan data dalam sistem informasi kesehatan. Namun, tidak menutup kemungkinan akan tetap terjadinya kebocoran data atau kecurangan lain. Karena jika pemahaman terkait teknologi blockchain masih kurang, penerapan blockchain sebagai keamanan dan privasi data tidak akan optimal. Teknologi blockchain dapat memfasilitasi berbagi data kesehatan yang aman dan efisien. Data kesehatan dapat dibagikan dengan berbagai pihak yang berkepentingan, seperti dokter, perawat, dan rumah sakit, tanpa khawatir data tersebut akan disalahgunakan. Hal ini dapat mempercepat proses diagnosis dan pengobatan pasien [11].

Implementasi teknologi blockchain dalam layanan kesehatan berpotensi merevolusi industri kesehatan, terdapat beberapa tantangan yang harus diatasi sebelum dapat diadopsi secara luas. Salah satu tantangan utama ialah kurangnya standarisasi dan interoperabilitas dalam industri kesehatan [8]. Sistem informasi kesehatan di Indonesia masih belum banyak yang menerapkan teknologi blockchain. Oleh karena itu, seringkali terjadinya manipulasi dan pemalsuan identitas pasien dan tenaga medis ataupun rekam medis lainnya. Penerapan sistem blockchain membutuhkan peran stakeholder, pemangku kebijakan untuk merancang sebuah tameng khusus terkait keamanan siber yang berorientasi pada era disrupsi terhadap perlindungan data [12]. Dalam menerapkan teknologi blockchain, perlu adanya tim pengembang yang paham dengan implementasi teknologi blockchain. Biaya implementasi dapat meningkat jika instansi memiliki tim khusus dengan pengalaman pengembangan blockchain yang tepat.

Adapun potensi tantangan yang akan terjadi ketika menerapkan teknologi blockchain dalam sistem informasi kesehatan. Blockchain, terutama yang terkait dengan cryptocurrency seperti Bitcoin dan Ethereum, telah mengalami masalah skalabilitas [13]. Jika dalam konteks sistem informasi kesehatan yang membutuhkan penanganan volume data yang besar, skalabilitas menjadi tantangan yang perlu dihadapi. Oleh karena itu, diperlukan solusi blockchain yang scalable untuk dapat mengakomodasi volume data yang besar. Untuk tetap menjaga integritas dengan berbagai sistem instansi yang lain, sistem informasi kesehatan terdiri dari berbagai macam aplikasi yang harus dapat berkomunikasi satu sama lain. Oleh sebab itu, perlu memastikan interoperabilitas antara sistem yang sudah ada dengan solusi berbasis blockchain dapat menjadi kompleks.

Teknologi blockchain dapat digunakan untuk meningkatkan keandalan data pasien, karena data yang tersimpan di blockchain tidak dapat diubah atau dihapus serta meningkatkan efisiensi berbagi data pasien, karena data pasien dapat diakses oleh berbagai pihak yang berkepentingan secara aman dan terpercaya [8]. Salah satu contoh penerapan teknologi untuk keamanan dan privasi data adalah sistem rekam medis elektronik (EMR). Teknologi blockchain dapat digunakan untuk menyimpan rekam medis pasien secara aman dan terpercaya. Dengan demikian, data pasien dapat diakses oleh berbagai pihak yang berkepentingan, seperti dokter, perawat, dan rumah sakit, tanpa khawatir data tersebut akan disalahgunakan.



Gambar 2. Tantangan Blockchain

Selain itu, menurut penelitian sebelumnya teknologi blockchain masih rentan terhadap serangan siber. Oleh karena itu, diperlukan keamanan siber yang kuat untuk melindungi sistem blockchain. Hal-hal yang dapat mengatasi tantangan penerapan blockchain dalam sistem informasi kesehatan bisa melalui penetapan standarisasi dan interoperabilitas dalam sistem informasi kesehatan [14]. Hal ini akan memudahkan integrasi sistem blockchain dengan sistem yang sudah ada. Untuk memastikan bahwa teknologi blockchain dapat diterapkan dan dikelola dengan aman dan efektif, instansi dapat melakukan suatu pelatihan dan pengembangan sumber daya manusia yang memang menjadi stakeholder dari sistem informasi kesehatan tersebut.

Teknologi blockchain juga dapat mengalami masalah skalabilitas, terutama jika digunakan untuk menangani volume data yang besar. Hal ini disebabkan oleh sifat blockchain yang terdesentralisasi. Setiap node di jaringan blockchain harus menyimpan salinan lengkap dari semua data yang ada di blockchain. Jika volume data yang ada di blockchain terlalu besar, maka dapat menyebabkan kinerja sistem blockchain menjadi menurun [15]. Instansi dapat bekerja sama dengan pakar keamanan siber untuk mengembangkan keamanan siber yang kuat untuk sistem blockchain. Sehingga dapat dilakukan dengan melibatkan pakar keamanan siber dari berbagai bidang.

IV. KESIMPULAN

Dalam konteks teknologi blockchain, desentralisasi memegang peran kunci dalam mengubah paradigma keamanan dan privasi data. Hal ini tidak hanya meningkatkan keamanan data dengan mengurangi kerentanan terhadap serangan siber, tetapi juga memastikan transparansi dan integritas data. Konsep desentralisasi dalam blockchain menjelaskan bahwa data disimpan di berbagai simpul jaringan, mengurangi risiko manipulasi dan memberikan ketahanan terhadap serangan. Dengan struktur rantai blok yang menyusun catatan transaksi, blockchain menciptakan basis data yang dapat dibagi secara terdistribusi.

Kejelasan dan aksesibilitas data yang tinggi juga membantu meminimalkan risiko penyalahgunaan dan pemalsuan data. Struktur data yang unik pada blockchain, dengan blok-blok yang terkait melalui nilai hash, memastikan integritas dan keberlanjutan catatan transaksi. Selain itu, implementasi blockchain memastikan bahwa data hanya dapat diakses dan diedit dengan persetujuan seluruh jaringan node, menghindari risiko perubahan yang tidak sah. Teknologi blockchain berperan penting dalam melindungi keamanan dan privasi data dalam sistem informasi kesehatan. Melibatkan langkah-langkah teknis, kebijakan, dan prosedur untuk mencegah kebocoran, manipulasi, atau penghancuran data.

Implementasi teknologi blockchain dalam layanan kesehatan memiliki potensi untuk meningkatkan efisiensi, keamanan, dan transparansi. Namun, terdapat beberapa tantangan yang harus diatasi sebelum dapat diadopsi secara luas. Tantangan utama dari implementasi teknologi blockchain yaitu sistem informasi kesehatan di berbagai instansi masih belum memiliki standarisasi yang sama. Hal ini dapat menyebabkan kendala dalam interoperabilitas antara sistem yang berbeda. Untuk mengatasi tantangan-tantangan tersebut, diperlukan kerja sama dari berbagai pihak, termasuk pemerintah, pemangku kepentingan, dan penyedia teknologi.

Meskipun memiliki potensi besar dalam meningkatkan keamanan dan privasi data, teknologi blockchain masih rentan terhadap serangan siber. Oleh karena itu, perlindungan sistem blockchain memerlukan keamanan siber yang kuat untuk mengatasi ancaman siber yang mungkin timbul. Tantangan dalam penerapan blockchain di sistem informasi kesehatan dapat diatasi melalui penetapan standarisasi dan interoperabilitas. Dengan adanya standar yang jelas, integrasi antara sistem blockchain dengan sistem lain dapat dilakukan dengan lebih lancar dan efisien. Untuk memastikan pengelolaan blockchain dengan aman dan efektif, pelatihan dan pengembangan sumber daya manusia menjadi krusial. Stakeholder sistem informasi kesehatan perlu memiliki pemahaman yang mendalam tentang teknologi blockchain dan keamanan siber untuk memaksimalkan potensinya.

DAFTAR PUSTAKA

- [1] A. Gunawan, *PENGANTAR SISTEM INFORMASI KESEHATAN*. [Daring]. Tersedia pada: www.penerbitlitnus.co.id

- [2] Q. Aini, P. Abas Sunarya, N. Azizah, dan A. A. Putri, “Pemanfaatan Teknologi Blockchain pada Bidang Kesehatan dengan Sistematis Literatur Review.”
- [3] T. D. Cahyono dan W. Hadikurniawati, “BLOCKCHAIN UNTUK APLIKASI IOT HEALTHCARE: STUDI LITERATUR,” vol. 28, no. 2, hlm. 2023.
- [4] P. Hukum dkk., “Endison Ravlindo & Ariawan Gunadi PERLINDUNGAN HUKUM TERHADAP DATA KESEHATAN MELALUI DATA PRIBADI,” vol. 4, no. 2, hlm. 2021.
- [5] J. Oliver, Y. Tampubolon, A. Bhawiyuga, dan R. A. Siregar, “Implementasi Blockchain berbasis BigchainDB untuk Menjamin Keamanan Data dalam Sistem Pencatatan Rekam Medis,” 2022. [Daring]. Tersedia pada: <http://j-ptiik.ub.ac.id>
- [6] P. Rizkia Wardhani dan M. Irwan Padli Nasution, “Peran Teknologi Blockchain dalam Keamanan dalam Privasi Data.”
- [7] E. Abou Maroun, J. Daniel, D. Zowghi, dan A. Talaei-Khoei, “Blockchain in Supply Chain Management: Australian Manufacturer Case Study,” dalam *Lecture Notes in Business Information Processing*, Springer, 2019, hlm. 93–107. doi: 10.1007/978-3-030-32242-7_8.
- [8] M. Teguh Budiyo, “Implementasi Blockchain dalam Sistem Layanan Kesehatan Sebuah Kajian Regulasi.”
- [9] D. Apriani dkk., “Optimasi Transparansi Data dalam Rantai Pasokan melalui Integrasi Teknologi Blockchain,” vol. 2, no. 1, hlm. 1–10, 2023, doi: 10.34306/mentari.v2i1.326.
- [10] I. Elan Maulani, T. Herdianto, D. Febri Syawaludin, dan M. Oga Laksana, “Dwi Febri Syawaludin,” *Medika Oga Laksana Jurnal Sosial dan Teknologi (SOSTECH)*, vol. 3, no. 2, hlm. 2023.
- [11] E. Yulianingsih, H. Yudiastuti, F. Sains Teknologi, J. A. Jenderal Yani No, dan S. Selatan, “Evaluasi Sistem Delivery Obat (SIDEBAT) ... 853.”
- [12] U. Rahardja, F. Budiarty, dan U. Raharja, “PENGARUH TEKNOLOGI BLOCKCHAIN TERHADAP KEABSAHAN IJAZAH,” vol. 2, no. 1, 2021.
- [13] D. Pengampu dan D. Sentot Imam Wahjono, “POTENSI TEKNOLOGI BLOCKCHAIN PADA PERUSAHAAN KURIR ANTERAJA BAGUS AJI PUTRA,” 2023. [Daring]. Tersedia pada: <https://infokomputer.grid.id/read/121800839/nih-manfaat-teknologi-blockchain-untuk-industri->
- [14] H. Yulianton, R. Candra, N. Santi, K. Hadiono, dan S. Mulyani, *IMPLEMENTASI SEDERHANA BLOCKCHAIN*. 2018.
- [15] A. R. Tjipto dan G. Dewantoro, “Kajian Peran Internet of Thing dalam Topik Healthcare,” 2022.