



Analisis Keamanan Rekam Medis Elektronik pada *Telemedicine* Menggunakan *Blockchain* dan *Smart Contract*

Stephanie

Universitas Mikroskil

Alvin Winata

Universitas Mikroskil

Satria Kelana Surbakti

Universitas Mikroskil

Louis Winata

Universitas Mikroskil

Susanti

Universitas Mikroskil

Edward Kerry Mahchristo

Universitas Mikroskil

Joosten

Universitas Mikroskil

Alamat: Jl. M.H Thamrin No.140, Pusat Ps., Kec. Medan Kota, Kota Medan, Sumatera Utara 20212

Korespondensi penulis: 221120813@students.mikroskil.ac.id

Abstrak. *The advancement of digital technology has significantly impacted the healthcare sector, particularly through the implementation of telemedicine, which involves the storage of sensitive patient data and faces challenges related to data security, ethics, and legal compliance. This study aims to provide a theoretical contribution by developing a conceptual framework for health data security based on blockchain and smart contracts, as well as a practical contribution to assist healthcare providers in establishing telemedicine systems that are more secure, transparent, and aligned with ethical and regulatory principles. The research employs a descriptive qualitative method by collecting data from scientific journals and other relevant sources. The application of electronic medical record security using blockchain and smart contracts offers advantages such as secure and remotely controlled data exchange, along with enhanced patient control over data access rights.*

Keywords: *Blockchain; Smart Contract, Telemedicine.*

Abstrak. Kemajuan teknologi pada era digital telah membawa dampak besar bagi sektor kesehatan, terutama melalui implementasi *telemedicine* yang melibatkan penyimpanan data sensitif pasien dan menghadapi tantangan dalam aspek keamanan, etika, serta kepatuhan terhadap regulasi hukum. Penelitian ini bertujuan memberikan kontribusi teoretis berupa pengembangan kerangka konseptual keamanan data kesehatan berbasis *blockchain* dan *smart contract*, sekaligus kontribusi praktis bagi penyedia layanan kesehatan dalam menciptakan sistem *telemedicine* yang lebih aman, transparan, serta sejalan dengan prinsip etika dan peraturan yang berlaku. Metode yang digunakan adalah penelitian kualitatif deskriptif dengan pengumpulan informasi dari berbagai jurnal ilmiah dan sumber relevan. Penerapan sistem keamanan rekam medis elektronik berbasis *blockchain* dan *smart contract* dinilai mampu menghadirkan keunggulan berupa pertukaran data yang aman dan terkontrol dari jarak jauh, serta memberikan hak kendali akses yang lebih besar kepada pasien.

Kata Kunci: *Blockchain; Smart Contract, Telemedicine.*

PENDAHULUAN

Perkembangan teknologi pada era digital telah membawa perubahan besar dalam bidang kesehatan, salah satunya adalah melalui *telemedicine*. *Telemedicine* merupakan layanan

kesehatan jarak jauh berbasis teknologi komunikasi yang memungkinkan interaksi antara pasien dan tenaga medis tanpa hambatan geografis. Layanan ini terbukti efektif dalam memperluas akses, terutama bagi pasien dengan keterbatasan mobilitas atau yang tinggal pada daerah terpencil (Solimini dkk., 2021).

Terlepas dari manfaatnya, *telemedicine* menghadapi berbagai tantangan terutama dalam aspek keamanan data, etika dan kepatuhan hukum. Rekam medis elektronik sebagai inti dari *telemedicine* menyimpan data sensitif pasien yang harus dijaga kerahasiaannya. Beberapa studi menunjukkan bahwa masih terdapat risiko pelanggaran privasi, akses tidak sah, serta lemahnya perlindungan data dalam praktik *telemedicine* (Alenoghena dkk., 2023), (Ftouni dkk., 2022). Selain itu, kerangka hukum dan regulasi di berbagai negara belum sepenuhnya mampu menjawab kompleksitas permasalahan baru yang timbul, seperti persoalan tanggung jawab hukum, perlindungan data lintas batas, dan standar interoperabilitas sistem (Solimini dkk., 2021).

Berdasarkan konteks ini, *blockchain* muncul sebagai teknologi potensial untuk mengatasi permasalahan-permasalahan yang disebutkan sebelumnya melalui sifatnya yang desentralistik, transparan, dan sulit dimanipulasi (Raimundo dkk., 2021). Lebih lanjut, penggunaan *smart contract* memungkinkan pengaturan otorisasi akses dan persetujuan pasien dilakukan secara otomatis dan akuntabel, sehingga mengurangi potensi penyalahgunaan data (Rodeck dkk., 2022). Meskipun sejumlah penelitian telah mengeksplorasi pemanfaatan *blockchain* di bidang kesehatan, sebagian besar masih terbatas pada aspek umum seperti manajemen data atau rantai pasok, sedangkan kajian spesifik terkait perlindungan rekam medis elektronik dalam *telemedicine* masih relatif sedikit.

Berdasarkan uraian tersebut, penelitian ini difokuskan pada analisis keamanan rekam medis elektronik pada *telemedicine* dengan memanfaatkan *blockchain* dan *smart contract*. Penelitian ini diharapkan mampu memberikan kontribusi teoretis berupa kerangka konseptual keamanan data kesehatan berbasis *blockchain*, serta kontribusi praktis dalam mendukung penyedia layanan kesehatan menghadirkan sistem *telemedicine* yang lebih aman, transparan, dan sesuai dengan prinsip regulasi maupun etika medis yang berlaku.

KAJIAN TEORI

1. *Telemedicine*

Telemedicine merupakan salah satu inovasi penting dalam dunia kesehatan modern. WHO mendefinisikan *telemedicine* sebagai penyediaan layanan kesehatan jarak jauh oleh tenaga medis dengan memanfaatkan teknologi informasi dan komunikasi untuk tujuan diagnosis, pengobatan, dan pencegahan penyakit ketika jarak menjadi faktor penghambat. Pada praktiknya, *telemedicine* memungkinkan pasien dan tenaga medis tetap terhubung melalui konsultasi daring, pemantauan kondisi kesehatan, hingga transfer data medis yang aman (Ezeamii dkk., 2024).

Penerapan *telemedicine* menawarkan sejumlah manfaat. Salah satunya adalah perluasan akses layanan kesehatan ke wilayah terpencil yang kekurangan tenaga medis. Selain itu, *telemedicine* juga meningkatkan efisiensi dengan mengurangi biaya perjalanan dan waktu tunggu pasien, serta mendukung kontinuitas perawatan bagi pasien dengan penyakit kronis. Tidak hanya itu, sistem ini juga memungkinkan kolaborasi lintas wilayah antara tenaga medis, sehingga meningkatkan kualitas keputusan medis.

Meskipun demikian, *telemedicine* masih menghadapi berbagai tantangan. Salah satunya adalah keterbatasan pemeriksaan fisik yang dapat memengaruhi akurasi diagnosis. Selain itu, kesenjangan infrastruktur teknologi, seperti keterbatasan akses internet di daerah tertentu, menjadi hambatan signifikan. Risiko keamanan dan privasi data pasien juga masih menjadi isu

yang sering dibahas. Di samping itu, banyak negara, termasuk Indonesia, masih berupaya menyusun regulasi yang jelas terkait aspek hukum dan etika *telemedicine* agar penggunaannya dapat berjalan lebih optimal (Haleem dkk., 2021).

2. Rekam Medis Elektronik (EMR/EHR)

Perkembangan *telemedicine* tidak dapat dilepaskan dari penggunaan rekam medis elektronik. *Electronic Medical Record* (EMR) merujuk pada catatan medis digital pasien yang dikelola oleh satu fasilitas kesehatan. Informasi yang terdapat di dalamnya mencakup riwayat penyakit, hasil laboratorium, resep obat, hingga catatan dokter (Lederman dkk., 2024). Sementara itu, *Electronic Health Record* (EHR) merupakan bentuk yang lebih luas dari EMR karena memungkinkan data pasien diakses lintas fasilitas, sehingga mendukung integrasi dan koordinasi antar tenaga kesehatan (Shen dkk., 2025).

Penggunaan EHR maupun EMR membawa berbagai manfaat. Salah satunya adalah peningkatan efisiensi karena akses informasi medis menjadi lebih cepat dibandingkan sistem berbasis dokumen fisik. Selain itu, sistem ini juga meningkatkan akurasi pencatatan medis, mendukung transparansi riwayat kesehatan pasien, serta menyediakan data yang berharga untuk riset dan analisis kesehatan masyarakat (Kim dkk., 2023).

Meski demikian, ada beberapa tantangan utama dalam penerapannya. Masalah keamanan dan privasi data menjadi perhatian penting karena rekam medis elektronik sering kali tersimpan dalam sistem terpusat yang rentan diretas atau dimanipulasi. Selain itu, interoperabilitas antar sistem EHR/EMR juga masih menjadi kendala akibat perbedaan standar dan format data. Tantangan lainnya adalah biaya implementasi yang tinggi, resistensi tenaga medis yang kesulitan beradaptasi dengan sistem baru, serta risiko yang muncul saat suatu institusi bermigrasi dari satu sistem EHR ke sistem lain (Miake-Lye dkk., 2023).

3. Blockchain

Blockchain merupakan teknologi basis data terdistribusi atau desentralisasi yang menyimpan informasi dalam blok-blok yang saling terhubung secara kriptografi. Setiap blok berisi sejumlah data transaksi yang disusun secara berurutan membentuk rantai (*chain*). Rangkaian blok tersebut berfungsi untuk memastikan integritas dan keamanan data, sehingga teknologi ini mengeliminasi kebutuhan akan entitas pusat. Sebaliknya, pengelolaan data dilakukan oleh jaringan *node* independen yang saling berkontribusi (Utomo, 2021).

Konsep dasar dari *blockchain* meliputi tiga prinsip utama. Pertama, desentralisasi, di mana data disimpan dan dikelola oleh banyak *node* dalam jaringan tanpa adanya otoritas pusat. Kedua, *immutability* atau ketidakberubahan, yaitu setiap data yang sudah direkam dalam blok tidak dapat diubah tanpa persetujuan dari seluruh jaringan. Ketiga, kriptografi, yaitu penggunaan enkripsi data dan fungsi *hash* yang berperan penting dalam menjaga keamanan sekaligus keaslian transaksi di setiap blok (Suryawijaya, 2023).

Dari sisi manfaat, *blockchain* mampu meningkatkan keamanan serta transparansi transaksi. Teknologi ini juga mengurangi risiko manipulasi maupun penipuan data karena sifatnya yang desentralisasi dan transparan. Selain itu, *blockchain* dapat meningkatkan efisiensi dengan menghilangkan kebutuhan perantara, sekaligus mendorong terciptanya interoperabilitas dalam ekosistem digital (Purnomo dkk., 2024).

Namun demikian, penerapan *blockchain* tidak terlepas dari sejumlah tantangan. Salah satunya adalah regulasi yang masih belum jelas dan belum merata di berbagai negara, termasuk Indonesia. Infrastruktur dan kesiapan sumber daya manusia juga menjadi hambatan yang signifikan. Di sisi lain, *blockchain* masih menghadapi isu skalabilitas dan ketergantungan pada jaringan internet.

Masalah interoperabilitas antar *blockchain* yang berbeda juga menjadi tantangan teknis yang perlu diselesaikan.

4. Smart Contract

Smart contract adalah program komputer otomatis yang berjalan di jaringan *blockchain* untuk mengotomatisasi pelaksanaan kontrak sesuai aturan yang telah ditentukan (Budiyanto, 2023). Konsep ini pertama kali diperkenalkan oleh Nick Szabo pada tahun 1994 sebagai perjanjian digital yang dapat dieksekusi secara mandiri tanpa memerlukan perantara. Dengan adanya *smart contract*, kontrak dapat dijalankan secara otomatis berdasarkan kondisi tertentu yang telah diprogram sebelumnya.

Konsep dasar *smart contract* mencakup tiga hal penting. Pertama, otomatisasi, yaitu kontrak dieksekusi secara otomatis ketika kondisi tertentu terpenuhi berdasarkan prinsip *if-then*. Kedua, kontrol akses, di mana hanya pihak berwenang yang dapat mengakses dan berinteraksi dengan kontrak. Ketiga, transparansi, karena seluruh catatan kontrak beserta pelaksanaannya dapat diakses serta diverifikasi oleh semua pihak yang terlibat.

Smart contract memberikan berbagai manfaat. Teknologi ini dapat menghemat waktu dan biaya dengan menghilangkan perantara dalam suatu transaksi (PuskoMedia Indonesia, 2025). Risiko pelanggaran kontrak juga dapat diminimalkan karena pelaksanaannya berlangsung secara otomatis dan sesuai kode yang telah diprogram. Selain itu, *smart contract* mampu meningkatkan transparansi serta akuntabilitas pelaksanaan perjanjian, sekaligus mempercepat proses transaksi maupun pengambilan keputusan.

Meskipun demikian, implementasi *smart contract* masih menghadapi sejumlah tantangan. Salah satu kendala terbesar adalah keterbatasan regulasi dan legalitas, khususnya di Indonesia. Dari sisi teknis, terdapat risiko kerentanan kode dan potensi kesalahan pemrograman yang dapat dimanfaatkan pihak tertentu (Lim dkk., 2024). Selain itu, masih terdapat ambiguitas hukum terkait penyelesaian sengketa berbasis teknologi yang belum matang secara menyeluruh.

METODE PENELITIAN

Penelitian ini menggunakan penelitian kualitatif deskriptif dengan memperoleh data melalui jurnal ilmiah, dan sumber relevan lainnya yang terkait dengan pembahasan. Teknik pengumpulan data dilakukan melalui penelusuran dan seleksi artikel berdasarkan kata kunci serta kriteria kelayakan. Data yang terkumpul dianalisis menggunakan metode analisis isi (*content analysis*) dengan cara mengidentifikasi, mengelompokkan, dan menyimpulkan temuan.

HASIL PENELITIAN DAN PEMBAHASAN

1. Analisis Risiko Keamanan Rekam Medis pada Telemedicine Konvensional

Telemedicine telah merevolusi cara pelayanan kesehatan diberikan, namun kemudahan ini diiringi dengan risiko keamanan yang signifikan terkait pengelolaan rekam medis elektronik (RME). Pada umumnya, sistem *telemedicine* konvensional mengandalkan server terpusat (*centralized server*) untuk menyimpan data pasien. Model ini secara inheren menciptakan titik tunggal kegagalan (*single point of failure*), di mana seluruh data berisiko hilang atau tidak dapat diakses jika server utama mengalami gangguan. Selain itu, arsitektur terpusat menjadikannya target utama bagi serangan siber yang dapat mengakibatkan pencurian atau manipulasi data medis sensitif. Isu fundamental lainnya adalah kurangnya integritas dan transparansi data. Permasalahan-permasalahan ini menjadi dasar bagi urgensi pengembangan sistem rekam medis elektronik yang lebih aman dan terintegrasi di Indonesia (Dhiya, 2024).

2. Blockchain sebagai Solusi Keamanan Rekam Medis

Menjawab tantangan besar dalam pengelolaan rekam medis, teknologi *blockchain* menawarkan sebuah paradigma baru untuk mengelola data rekam medis secara aman dan terdesentralisasi. *Blockchain* berfungsi sebagai buku besar digital yang terdistribusi (*distributed ledger*) dan tidak dapat diubah (*immutable*), di mana setiap transaksi dicatat dan diverifikasi oleh jaringan dan disimpan dalam bentuk blok-blok yang saling terhubung. Berbeda dengan sistem penyimpanan terpusat yang rentan diretas, kehilangan data, ataupun dimanipulasi oleh pihak yang tidak berwenang, *blockchain* mengatasi kelemahan tersebut melalui beberapa mekanisme inti.

Pertama, sifatnya yang terdesentralisasi menghilangkan adanya titik tunggal kegagalan (*single point of failure*) karena data direplikasi di seluruh jaringan. Jika salah satu jaringan mengalami gangguan atau diserang, salinan data tetap aman pada jaringan lainnya.

Kedua, *blockchain* menerapkan keamanan kriptografi tingkat tinggi. Setiap transaksi yang dicatat diamankan melalui *hash* kriptografi dan dihubungkan dalam sebuah rantai yang tidak dapat diubah, sehingga menjamin integritas rekam medis dari manipulasi. Artinya jika ada pihak yang mencoba mengubah transaksi dalam satu blok, maka seluruh rantai berikutnya akan terpengaruh dan perubahan tersebut langsung terdeteksi. Sifat *immutable* ini menjamin keaslian dan integritas rekam medis, sehingga risiko manipulasi atau penghapusan data dapat diminimalkan.

Implementasi teknis dari *blockchain* untuk tujuan keamanan data medis ini telah menjadi fokus dalam penelitian di Indonesia (Wikarsa dkk., 2022). Selain itu, teknologi ini juga mampu mendorong peningkatan interoperabilitas yang aman antar penyedia layanan kesehatan, menciptakan ekosistem data yang terpadu, mempercepat proses rujukan, mengurangi redundansi, dan lebih terpercaya dalam pencatatan medis (Dhiya, 2024).

3. Peran Smart Contract

Dalam konteks teknologi *blockchain*, *smart contract* digunakan untuk menjalankan transaksi tanpa perlu pihak ketiga secara otomatis. *Smart contract* menggunakan algoritma konsensus *Proof of Work* (PoW) untuk meningkatkan keamanan informasi dengan memastikan semua transaksi valid dan tidak dapat diubah. Cara kerja *smart contract* yaitu *smart contract* ditulis dalam kode dan diterapkan ke *blockchain* sesuai dengan kondisi yang ditentukan, ketika kondisi terpenuhi maka *smart contract* akan memicu transaksi. Untuk memastikan transaksinya valid, komputer yang terhubung dalam jaringan *blockchain* harus menyelesaikan teka-teki matematika yang dikenal sebagai *mining* (Rahmasari dkk., 2024).

Smart contract dalam *telemedicine* berperan dalam mengatur hak akses berbasis izin (*permissioned access*) yang berarti hanya pihak tertentu yang memiliki hak untuk mengakses data medis pasien seperti konsultasi, pembayaran maupun privasi pasien yang telah dienkripsi. *Smart contract* juga berperan untuk pembuatan jejak audit yang transparan (*Audit Trail Transparan*) dalam *telemedicine* secara otomatis yang artinya setiap kali terjadi penambahan, perubahan ataupun diakses pada data medis, maka *smart contract* akan mencatatnya secara permanen dalam *blockchain* secara jelas tanpa bisa dimanipulasi. Dengan adanya *smart contract* dalam *telemedicine*, semua pihak dapat melacak dan memverifikasi setiap perubahan yang dilakukan pada data medis, hal ini mengurangi kemungkinan terjadinya akses yang tidak sah ataupun manipulasi data. Peran ini memberikan semua pihak baik rumah sakit, pasien maupun regulator memiliki kepercayaan yang tinggi terhadap integritas data medis dan memungkinkan pengawasan yang lebih baik (Putra, 2025).

4. Manfaat Implementasi Teknologi Blockchain dan Smart Contract

Pemanfaatan teknologi *blockchain* dan *smart contract* dalam layanan *telemedicine* menawarkan berbagai manfaat yang signifikan, terutama terkait dengan keamanan, kontrol akses oleh pasien,

transparansi konsultasi dan pembayaran, efisiensi operasional tanpa pihak ketiga, serta interoperabilitas sistem kesehatan.

Dalam hal keamanan, data rekam medis pasien disimpan dalam bentuk yang telah dienkripsi di jaringan *blockchain* sehingga data tidak dapat dimanipulasi maupun diubah (*immutable*). Setiap perubahan atau akses data medis pasien secara otomatis dicatat, hal ini sangat berguna untuk mencegah risiko penyalahgunaan informasi, manipulasi data, dan memastikan bahwa rekam medis tersimpan dengan aman.

Dalam sisi kontrol akses oleh pasien, ini memberi pasien memiliki kendali penuh untuk menentukan siapa yang dapat mengakses data rekam medis mereka, dan hak akses tersebut dapat diberikan atau dicabut kapan saja tanpa campur tangan pihak lain. Ini penting untuk menjaga privasi pasien tetap terjamin.

Dalam aspek transparansi konsultasi dan pembayaran, penerapan teknologi *blockchain* dan *smart contract* secara otomatis mencatat setiap sesi konsultasi, resep, dan transaksi pembayaran. Dengan demikian, ini mengurangi kemungkinan terjadinya penipuan transaksi atau penagihan yang tidak jelas.

Dalam hal efisiensi operasional tanpa pihak ketiga, *smart contract* memungkinkan otomatisasi dalam layanan dan pembayaran secara langsung *peer-to-peer* tanpa melibatkan banyak pihak, sehingga ini bermanfaat untuk mengurangi biaya operasional dan mempercepat proses klaim dan pembayaran.

Dalam hal interoperabilitas sistem kesehatan, *blockchain* memungkinkan data rekam medis menjadi satu sumber referensi tunggal (*single source of truth*) yang dapat diakses dengan aman oleh berbagai sistem atau platform kesehatan yang berbeda, sehingga ini akan bermanfaat dalam hal rujukan dan perawatan lanjutan tanpa perlu mengisi ulang rekam medis pasien berkali-kali (Putra, 2025).

5. Tantangan Implementasi Teknologi Blockchain

Kendala pertama adalah Regulasi dan Hukum. Meskipun terdapat kerangka peraturan untuk RME (misalnya, Permenkes No. 24 Tahun 2022 di Indonesia), belum ada rancangan hukum yang spesifik untuk sistem desentralisasi seperti *blockchain*, dan kesenjangan regulasi nasional ini menciptakan ambiguitas terkait yurisdiksi serta tata kelola (Damayanti dkk., 2025). Selain itu, sifat utama *blockchain* yang *immutable*, data yang tercatat tidak bisa diubah atau dihapus, berpotensi berkonflik dengan hak pasien untuk menghapus data mereka (*right to be forgotten*), yang dijamin oleh undang-undang perlindungan data. Solusi yang sering dipakai untuk mengatasi konflik ini adalah menyimpan data sensitif di luar rantai (*off-chain*) dan hanya mencatat *hash* kriptografinya pada *blockchain* (Hambali dkk., 2025). Untuk layanan *telemedicine* yang menjangkau lintas negara, tantangan kepatuhan global juga muncul, karena fasilitas harus memastikan kepatuhan terhadap standar privasi data internasional yang ketat, seperti GDPR di Eropa atau HIPAA di AS, yang menambah kompleksitas hukum yang signifikan (Ahmad dkk., 2021).

Kendala berikutnya adalah Biaya dan Finansial. Pengembangan infrastruktur *blockchain* yang terdesentralisasi, termasuk perancangan dan audit *Smart Contract*, memerlukan investasi awal yang tinggi dan juga membutuhkan sumber daya manusia dengan keahlian khusus yang mahal, sehingga biaya ini jauh melampaui anggaran untuk sistem RME terpusat konvensional. Kemudian, isu latensi (penundaan waktu akses) dan biaya operasional juga harus diperhitungkan, sebab proses verifikasi data dan konsensus—bahkan pada model *permissioned blockchain* yang lebih efisien—masih dapat menghasilkan latensi yang kurang ideal untuk kebutuhan klinis yang

mendesak. Selain itu, setiap pembaruan data medis memerlukan biaya komputasi (*gas fee*) yang perlu dipertimbangkan untuk keberlanjutan operasional (Hambali dkk., 2025).

Terakhir, ada kendala Kesiapan Teknologi dan Sumber Daya Manusia (SDM). Efektivitas *blockchain* dalam berbagi data secara aman sangat bergantung pada standarisasi format data kesehatan, seperti HL7 FHIR. Namun, kurangnya standar data universal yang diadopsi secara luas menghambat kemampuan *blockchain* untuk berfungsi sebagai platform pertukaran data yang mulus antara berbagai penyedia layanan kesehatan. Selain itu, ketersediaan tenaga ahli di bidang teknologi *blockchain* dan kriptografi yang spesifik untuk sektor kesehatan masih sangat terbatas. Keberhasilan implementasi juga membutuhkan pelatihan intensif bagi tenaga kesehatan untuk memastikan mereka memiliki literasi digital yang memadai agar dapat menggunakan sistem RME berbasis teknologi baru ini secara efektif (Putri, 2023).

6. Diskusi dan Perbandingan Sistem

Pada dasarnya, sistem RME berbasis *blockchain* menawarkan keunggulan yang jauh lebih kuat dalam hal keamanan dan kontrol data yang berpusat pada pasien dibandingkan dengan sistem tradisional yang terpusat. Keunggulan ini sangat relevan untuk *telemedicine* karena memfasilitasi pertukaran data yang aman dan terkontrol jarak jauh. Meskipun demikian, manfaat ini hanya akan terwujud setelah fasilitas kesehatan berhasil mengatasi rintangan berupa biaya tinggi, kompleksitas teknis, dan adaptasi regulasi (Ahmad dkk., 2021). Perbandingan fitur utama antara kedua sistem tersebut dirangkum dalam tabel berikut:

Tabel 1 Perbandingan RME Tradisional dan RME Berbasis Blockchain

Fitur yang Dibandingkan	Sistem RME Tradisional (Terpusat)	RME Berbasis <i>Blockchain</i> & <i>Smart Contract</i>
Keamanan Data	Terpusat. Rentan terhadap serangan tunggal pada server pusat dan manipulasi oleh administrator.	Terdesentralisasi dan Tahan Manipulasi. Data dienkripsi, tersebar, dan diverifikasi oleh jaringan. Integritas data terjamin.
Kontrol Akses Pasien	Dikendalikan penuh oleh institusi kesehatan atau penyedia layanan.	Pasien sebagai Pemilik Kunci. Pasien dapat mengatur dan memberi izin akses data mereka secara otomatis melalui <i>Smart Contract</i> .
Integrasi Data	Rendah. Data cenderung terperangkap dalam silo dan sulit dibagi antar fasilitas yang berbeda.	Tinggi (Potensial). Menciptakan lapisan terpercaya untuk pertukaran data yang aman antar penyedia layanan.
Biaya Implementasi	Relatif lebih rendah dan mudah disesuaikan.	Tinggi. Memerlukan investasi awal yang besar untuk membangun infrastruktur yang terdesentralisasi.

KESIMPULAN

Keamanan Rekam Medis Elektronik (RME) pada *telemedicine* melalui penerapan teknologi *blockchain* dan *smart contract* terbukti menjadi solusi untuk mengatasi permasalahan utama terkait keamanan data, etika dan kepatuhan hukum. Teknologi ini memungkinkan pertukaran data yang aman dan terkontrol jarak jauh serta pemberian kendali akses kepada pasien, sehingga mampu meningkatkan perlindungan terhadap data kesehatan sensitif. Selain memberikan manfaat praktis, kerangka konseptual yang ditawarkan juga menjadi kontribusi teoretis dalam pengembangan sistem *telemedicine* yang lebih aman, transparan, serta selaras dengan regulasi dan etika medis yang berlaku. Dengan demikian, rekam medis elektronik berbasis *blockchain* dan *smart contract* dapat menjadi model inovatif untuk memperkuat keandalan dan integritas layanan *telemedicine*.

DAFTAR PUSTAKA

- Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. *International journal of medical informatics*, 148, 104399.
- Alenoghena, C. O., Ohize, H. O., Adejo, A. O., Onumanyi, A. J., Ohihoin, E. E., Balarabe, A. I., ... Alenoghena, B. (2023). Telemedicine: a survey of telecommunication technologies, developments, and challenges. *Journal of Sensor and Actuator Networks*, 12(2), 20.
- Budiyanto, A. E. (2023). Analisis yuridis penggunaan smart contract dalam perspektif asas kebebasan berkontrak. *Journal Sains Student Research*, 1(1), 815–827.
- Damayanti, P. S., Adiputra, I. M. S., & Pradnyantara, I. G. A. N. P. (2025). Tantangan penerapan Rekam Medis Elektronik (RME) berdasarkan regulasi Permenkes No. 24 Tahun 2022. *Health Sciences and Pharmacy Journal*, 9(1), 47–55.
- Dhiya, D. W. R. (2024). *PERAN TEKNOLOGI BLOCKCHAIN UNTUK MENINGKATKAN TRANSPARANSI DAN KEAMANAN PADA PEMUNGUTAN SUARA ELEKTRONIK*.
- Ezeamii, V. C., Okobi, O. E., Wambai-Sani, H., Perera, G. S., Zaynieva, S., Okonkwo, C. C., ... Obiefuna, N. G. (2024). Revolutionizing healthcare: how telemedicine is improving patient outcomes and expanding access to care. *Cureus*, 16(7).
- Ftouni, R., AlJardali, B., Hamdanieh, M., Ftouni, L., & Salem, N. (2022). Challenges of telemedicine during the COVID-19 pandemic: a systematic review. *BMC medical informatics and decision making*, 22(1), 207.
- Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors international*, 2, 100117.
- Hambali, I. P., Sabrina, S. S., Fawwaz, M. Z., & Alia, H. (2025). *Studi Literatur Implementasi Blockchain dalam Meningkatkan Keamanan Rekam Medis Elektronik pada Infrastruktur Cloud*.
- Kim, M. K., Roupheal, C., McMichael, J., Welch, N., & Dasarathy, S. (2023). Challenges in and opportunities for electronic health record-based data analysis and interpretation. *Gut and liver*, 18(2), 201.
- Lederman, R., Brainin, E., & Ben-Assuli, O. (2024). The Electronic Medical Record—A New Look at the Challenges and Opportunities. *Future Internet*, Vol. 16, hlm. 74. MDPI.
- 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.

- Miake-Lye, I. M., Cogan, A. M., Mak, S., Brunner, J., Rinne, S., Brayton, C. E., ... Weiner, M. (2023). Transitioning from one electronic health record to another: a systematic review. *Journal of General Internal Medicine*, 38(Suppl 4), 956–964.
- Purnomo, B. H., Rismayadi, D. A., & Thoriq, M. R. F. (2024). Adopsi Blockchain sebagai Solusi Keamanan dan Transparansi Transaksi Digital di Industri Fintech. *Jurnal Minfo Polgan*, 13(2), 2486–2492.
- PuskoMedia Indonesia. (2025). *Mengenal Smart Contract: Konsep Dasar di Balik Teknologi Blockchain*. Diambil dari <https://puskomedia.id/blog/mengenal-smart-contract-konsep-dasar-di-balik-teknologi-blockchain/>
- Putra, G. (2025). *PERAN TEKNOLOGI BLOCKCHAIN UNTUK MENINGKATKAN KEAMANAN DAN PRIVASI DATA MEDIS DI SEKTOR KESEHATAN*.
- Putri, A. T. D. (2023). Challenges in implementing electronic medical record in Indonesia healthcare facilities. *Jurnal Medika Utama*, 4(3), 3427–3431.
- Rahmasari, E. S., & Ardianto, A. F. (2024). Meningkatkan Keamanan Data Rekam Medis Puskesmas Gajahan Melalui Teknologi Blockchain dengan Impelementasi Penggunaan Metode Smart Contract dan Algoritma Konsesus Proof-of-Work. *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis*, 449–455.
- Raimundo, R., & Rosário, A. (2021). Blockchain system in the higher education. *European Journal of Investigation in Health, Psychology and Education*, 11(1), 276–293.
- Rodeck, D., & Curry, B. (2022). What is blockchain. *Forbes*.
- Shen, Y., Yu, J., Zhou, J., & Hu, G. (2025). Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: comprehensive review. *Journal of Medical Internet Research*, 27, e59024.
- Solimini, R., Busardò, F. P., Gibelli, F., Sirignano, A., & Ricci, G. (2021). Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic. *Medicina*, 57(12), 1314.
- Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55–68.
- Utomo, T. P. (2021). Implementasi teknologi blockchain di perpustakaan: Peluang, tantangan dan hambatan. *Buletin Perpustakaan*, 4(2), 173–200.
- Wikarsa, L., Suwanto, T., & Lengkey, C. (2022). Implementasi Algoritma Konsensus Proof-of-Work dalam Blockchain terhadap Rekam Medis. *Jurnal Pekommas*, 7(1), 41–52.