

ANALISIS PENERAPAN BLOCKCHAIN UNTUK KEAMANAN DATA MEDIS ELEKTRONIK

Bella Gusmita Sari¹, Diki Ananda², Anisa Dwi Arianti³, Indra Gunawan⁴

¹ bellagusmita17@gmail.com

² dddiki3937@gmail.com

³ anisadwiariantiii@gmail.com

⁴ indra@amiktunasbangsa.ac.id

Abstrak

Perkembangan teknologi digital di sektor kesehatan membawa tantangan besar terhadap keamanan dan privasi data medis elektronik (Electronic Medical Records/EMR). Data medis bersifat sangat sensitif dan bernilai tinggi, sehingga menjadi target utama serangan siber, kebocoran data, maupun manipulasi informasi. Teknologi blockchain dipandang sebagai salah satu solusi inovatif untuk meningkatkan keamanan, integritas, dan transparansi dalam pengelolaan data medis. Penelitian ini bertujuan untuk menganalisis potensi penerapan blockchain dalam melindungi data medis elektronik melalui studi literatur dari artikel ilmiah, prosiding, white paper, dan laporan industri yang terbit pada periode 2016–2024. Hasil analisis menunjukkan bahwa blockchain mampu menyediakan mekanisme enkripsi terdistribusi, otentikasi berbasis konsensus, serta pencatatan transaksi yang tidak dapat diubah (*immutable*). Dengan demikian, blockchain tidak hanya memperkuat keamanan data medis, tetapi juga meningkatkan kepercayaan antara pasien, tenaga medis, dan institusi kesehatan.

Kata kunci: Blockchain, keamanan data, rekam medis elektronik, kesehatan digital

ANALYSIS OF BLOCKCHAIN APPLICATIONS FOR ELECTRONIC MEDICAL DATA SECURITY

Abstract

The digital transformation in healthcare has introduced both opportunities and challenges, particularly in managing the security and privacy of electronic medical records (EMR). Medical data is highly sensitive and valuable, making it a prime target for cyberattacks, data breaches, and unauthorized manipulation. Blockchain technology has emerged as a promising solution to strengthen the security, integrity, and transparency of medical data management. This study aims to analyze the potential implementation of blockchain in protecting electronic medical data through a literature review of scientific articles, conference proceedings, white papers, and industry reports published between 2016 and 2024. The findings indicate that blockchain provides distributed encryption mechanisms, consensus-based authentication, and immutable transaction records. These features not only reinforce data security but also enhance trust among patients, healthcare professionals, and institutions.

Keywords: Blockchain, data security, electronic medical records, digital health

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa dampak signifikan di berbagai sektor, termasuk sektor kesehatan. Digitalisasi layanan kesehatan menjadi salah satu upaya untuk meningkatkan kualitas pelayanan, efisiensi, serta akurasi dalam pengelolaan data pasien (Ahuja et al., 2020). Salah satu wujud nyata dari digitalisasi ini adalah penerapan Electronic Medical Records (EMR) atau rekam medis elektronik, yang kini banyak digunakan oleh rumah sakit, klinik, maupun fasilitas kesehatan lainnya (WHO, 2020). EMR menyimpan informasi penting dan sangat sensitif, seperti identitas pasien, riwayat medis, hasil laboratorium, resep obat, hingga catatan tindakan medis (Hassan et al., 2019).

Meskipun EMR memberikan berbagai keuntungan seperti kemudahan akses, penghematan biaya administrasi, dan mendukung pengambilan keputusan berbasis data, sistem ini juga memiliki kelemahan serius. Data medis elektronik menjadi target utama serangan siber karena memiliki nilai ekonomi tinggi di pasar gelap (Kuo et al., 2021). Laporan Ponemon Institute (2021) menyebutkan bahwa rata-rata kerugian akibat kebocoran data medis mencapai lebih dari USD 9 juta per kasus — tertinggi di antara sektor lainnya. Selain itu, meningkatnya serangan ransomware, kebocoran identitas pasien, serta penyalahgunaan akses internal menambah kompleksitas ancaman terhadap sistem EMR (Agbo et al., 2019).

Permasalahan utama dari EMR konvensional adalah model penyimpanan data yang masih terpusat (centralized), menciptakan risiko single point of failure (Bhattacharya et al., 2022). Jika server utama diretas atau rusak, seluruh sistem berpotensi lumpuh. Selain itu, model ini menimbulkan masalah integritas data dan transparansi karena sulit menelusuri modifikasi yang terjadi. Dalam konteks ini, teknologi blockchain muncul sebagai solusi alternatif yang menawarkan paradigma baru dalam keamanan data. Dengan sifatnya yang terdesentralisasi, transparan, dan berbasis kriptografi, blockchain mampu menciptakan sistem pencatatan yang aman, terpercaya, dan sulit dimanipulasi (Nakamoto, 2008; Mettler, 2016).

Penelitian ini bertujuan untuk menganalisis penerapan blockchain dalam meningkatkan keamanan data medis elektronik, dengan meninjau potensi, manfaat, serta tantangan implementasinya. Kajian dilakukan melalui metode studi literatur terhadap publikasi ilmiah dan laporan industri terkini (2016–2024). Hasil penelitian diharapkan dapat memperkaya wacana akademik sekaligus menjadi rujukan praktis bagi pengembangan sistem kesehatan digital yang lebih aman dan terpercaya.

2. TINJAUAN PUSTAKA

2.1 Data Medis Elektronik (Electronic Medical Records/EMR)

Electronic Medical Records (EMR) adalah sistem digital untuk pencatatan, penyimpanan, dan pengelolaan data medis pasien (WHO, 2020). Keunggulannya meliputi efisiensi, integrasi layanan, dan kemudahan akses lintas fasilitas kesehatan (Hassan et al., 2019). Namun, kelemahannya terletak pada kerentanan terhadap serangan siber dan penyalahgunaan akses internal (Kuo et al., 2021). Model penyimpanan terpusat sering kali menciptakan risiko *data breach* dan kehilangan data akibat kegagalan sistem (Bhattacharya et al., 2022).

Beberapa penelitian menyoroti meningkatnya insiden serangan terhadap sistem EMR global (Ahuja et al., 2020; Ponemon Institute, 2021), yang menegaskan pentingnya solusi keamanan baru berbasis teknologi desentralisasi seperti *blockchain*.

Meskipun demikian, sistem EMR juga memiliki kelemahan yang signifikan. Kerentanan terhadap kebocoran data dan serangan siber menjadi tantangan besar, terutama karena sebagian besar sistem masih berbasis penyimpanan terpusat (centralized). Model ini berpotensi menciptakan *single point of failure*, sehingga jika server utama diretas atau rusak, seluruh data pasien dapat terancam hilang atau dimanipulasi. Selain itu, adanya risiko penyalahgunaan akses oleh pihak internal (insider threat) menambah kompleksitas tantangan keamanan EMR.

2.2 Teknologi Blockchain

Blockchain merupakan teknologi Distributed Ledger Technology (DLT) yang diperkenalkan oleh Nakamoto (2008). Setiap blok data pada blockchain diverifikasi melalui mekanisme konsensus dan dilindungi dengan kriptografi, menjadikannya sulit dimanipulasi (Zhang et al., 2018).

Karakteristik utama blockchain meliputi:

1. Desentralisasi

Tidak ada satu entitas tunggal yang mengendalikan seluruh data; informasi didistribusikan ke berbagai node dalam jaringan.

2. Transparansi

Setiap perubahan atau transaksi tercatat secara publik di dalam jaringan dan dapat diverifikasi oleh seluruh partisipan.

3. Imutabilitas

Data yang sudah tercatat di blockchain tidak dapat diubah atau dihapus, sehingga menjamin integritas.

4. Keamanan kriptografi

Blockchain menggunakan enkripsi dan tanda tangan digital untuk memastikan otentikasi dan kerahasiaan.

5. Smart contract

Kontrak digital yang berjalan secara otomatis sesuai aturan yang diprogram, sehingga mendukung pengelolaan akses tanpa campur tangan pihak ketiga. (Christidis & Devetsikiotis, 2016).

Dengan karakteristik tersebut, blockchain berkembang pesat tidak hanya pada bidang keuangan (*cryptocurrency*), tetapi juga pada berbagai sektor lain seperti logistik, pemerintahan, dan terutama kesehatan. Teknologi ini mulai diterapkan di sektor non-keuangan, termasuk kesehatan (Mettler, 2016; Ekblaw et al., 2017), karena kemampuannya menjamin keamanan dan keaslian data secara efisien (Roehrs et al., 2019).

2.3 Blockchain dalam Keamanan Data Medis

Penggunaan blockchain dalam konteks kesehatan menjadi perhatian para peneliti sejak pertengahan 2010-an. Menurut Mettler (2016), blockchain dapat menghadirkan jejak audit (audit trail) yang transparan, di mana setiap akses atau perubahan data pasien akan tercatat secara permanen dan dapat

ditelusuri. Hal ini meningkatkan akuntabilitas sekaligus meminimalisasi risiko manipulasi data.

Ekblaw et al. (2017) melalui proyek MedRec membuktikan bahwa blockchain dapat digunakan untuk mengelola data medis pasien secara terdesentralisasi. Sistem ini memungkinkan pasien sebagai pemilik sah data untuk mengontrol siapa saja yang dapat mengakses informasi kesehatan mereka. Dengan demikian, privasi pasien dapat lebih terlindungi dibandingkan sistem konvensional yang dikelola sepenuhnya oleh rumah sakit atau lembaga kesehatan.

Selain itu, studi lain menunjukkan bahwa blockchain mampu:

1. Meningkatkan keamanan data: Melalui enkripsi dan konsensus, blockchain mengurangi risiko peretasan.
2. Memperkuat privasi: Pasien dapat memberikan akses terbatas kepada pihak tertentu sesuai kebutuhan.
3. Mendukung interoperabilitas: Blockchain dapat menjadi platform yang memungkinkan pertukaran data medis antar rumah sakit dan klinik secara aman.
4. Mengurangi biaya administrasi: Dengan adanya smart contract, pengelolaan data dapat lebih efisien tanpa perlu perantara.

Mettler (2016) menyatakan bahwa blockchain dapat menghadirkan audit trail yang transparan, di mana setiap perubahan data pasien dapat ditelusuri secara permanen. Ekblaw et al. (2017) melalui proyek MedRec memperkenalkan sistem berbasis blockchain yang memungkinkan pasien mengontrol akses terhadap data medis mereka. Agbo et al. (2019) menegaskan bahwa blockchain mampu mendukung interoperabilitas antar rumah sakit melalui smart contract yang mengatur hak akses dengan aman.

Studi lanjutan oleh Zhuang et al. (2020) menunjukkan bahwa penggunaan blockchain dalam sistem EMR meningkatkan privasi pasien dan meminimalkan risiko kebocoran data. Selain itu, penggabungan blockchain dengan Internet of Medical Things (IoMT) memungkinkan integrasi data medis dari berbagai perangkat secara real time (Zhao et al., 2021). Namun, implementasi teknologi ini masih dihadapkan pada kendala seperti skalabilitas jaringan, biaya infrastruktur, dan kurangnya regulasi yang mendukung (Bhattacharya et al., 2022; Angraal et al., 2017).

Dengan demikian, blockchain berpotensi besar untuk menjadi pondasi keamanan data medis yang

lebih kuat, namun masih memerlukan standarisasi dan dukungan kebijakan yang memadai.

Namun, tantangan juga masih ada, antara lain terkait skalabilitas jaringan, kecepatan transaksi, serta regulasi hukum dan etika dalam penggunaan blockchain di sektor kesehatan. Oleh karena itu, analisis mendalam mengenai penerapan blockchain dalam keamanan data medis elektronik menjadi penting untuk memberikan gambaran yang lebih komprehensif.

3. METODOLOGI

Penelitian ini menggunakan pendekatan studi literatur dengan meninjau artikel ilmiah, prosiding konferensi, laporan industri, dan *white paper* yang terbit antara tahun 2016–2024. Kriteria inklusi mencakup publikasi yang membahas blockchain dalam konteks keamanan data medis, manajemen EMR, serta privasi pasien.

Analisis dilakukan secara deskriptif-kualitatif, dengan langkah-langkah sebagai berikut:

1. Mengidentifikasi masalah keamanan utama dalam EMR.
2. Mengkaji konsep dasar blockchain serta komponen yang relevan untuk pengamanan data medis.
3. Membandingkan hasil temuan dari berbagai penelitian terdahulu.
4. Menyusun analisis mengenai kelebihan, keterbatasan, serta potensi penerapan blockchain di sektor kesehatan.

4. HASIL DAN PEMBAHASAN

4.1 Keamanan dan Integritas Data

Salah satu keunggulan utama blockchain dalam konteks Electronic Medical Records (EMR) adalah kemampuannya menjaga integritas data. Setiap transaksi atau catatan medis yang dimasukkan ke dalam blockchain tersimpan dalam bentuk blok yang saling terhubung melalui algoritma kriptografi hash. Mekanisme ini menjadikan data bersifat tamper-proof, artinya perubahan sekecil apa pun pada data akan terdeteksi karena akan mengubah hash dari blok terkait.

Dengan demikian, blockchain mampu mencegah terjadinya pemalsuan data medis pasien, seperti manipulasi hasil laboratorium, perubahan identitas pasien, atau rekayasa catatan obat. Integritas data yang tinggi ini sangat penting dalam layanan kesehatan, mengingat akurasi data medis menjadi dasar pengambilan keputusan klinis yang berdampak langsung pada keselamatan pasien.

4.2 Kontrol Akses dan Privasi

Keamanan data medis tidak hanya terkait perlindungan dari serangan eksternal, tetapi juga dengan pengelolaan hak akses. Blockchain mendukung penggunaan smart contract, yaitu protokol digital yang secara otomatis menjalankan aturan yang telah diprogram. Dalam konteks EMR, smart contract memungkinkan pasien untuk menetapkan siapa saja yang memiliki izin melihat atau mengelola data medis mereka.

Sebagai contoh, pasien dapat memberikan akses hanya kepada dokter spesialis tertentu untuk melihat riwayat medis, sementara pihak asuransi hanya dapat mengakses informasi yang relevan dengan klaim. Mekanisme ini mendukung konsep patient-centric data ownership, di mana pasien memiliki kontrol penuh atas data pribadinya.

Selain itu, penerapan blockchain juga dapat membantu institusi kesehatan dalam memenuhi standar regulasi internasional seperti Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat atau General Data Protection Regulation (GDPR) di Uni Eropa, yang menekankan perlindungan data pribadi pasien.

4.3 Transparansi dan Audit Trail

Blockchain menyediakan jejak audit (audit trail) yang permanen dan transparan. Setiap aktivitas, baik berupa penambahan, pembaruan, maupun permintaan akses data, akan terekam secara kronologis di dalam jaringan blockchain. Transparansi ini memastikan adanya akuntabilitas dalam setiap interaksi terhadap data medis.

Bagi tenaga medis dan institusi kesehatan, keberadaan audit trail membantu dalam pelacakan akses data untuk mencegah penyalahgunaan. Misalnya, jika seorang staf rumah sakit mengakses data pasien tanpa otorisasi, aktivitas tersebut dapat langsung terdeteksi dan ditindaklanjuti. Dengan demikian, blockchain bukan hanya memberikan keamanan teknis, tetapi juga mendukung governance dalam pengelolaan data kesehatan.

4.4 Tantangan Implementasi

Meskipun memiliki potensi besar, penerapan blockchain dalam sistem EMR masih menghadapi sejumlah tantangan yang perlu diperhatikan:

1. Skalabilitas dan kinerja jaringan

Blockchain, terutama model publik, memiliki keterbatasan dalam hal kapasitas transaksi per detik. Hal ini menjadi kendala mengingat sistem kesehatan harus menangani jutaan catatan medis dalam waktu nyata.

2. Interoperabilitas

Saat ini, banyak rumah sakit dan klinik menggunakan sistem EMR yang berbeda-beda. Integrasi blockchain dengan berbagai platform tersebut membutuhkan standarisasi protokol data medis agar sistem dapat saling berkomunikasi secara efisien.

3. Biaya implementasi

Adopsi blockchain memerlukan investasi yang cukup besar, baik dalam bentuk infrastruktur teknologi, pelatihan tenaga medis, maupun pengembangan aplikasi yang sesuai dengan kebutuhan layanan kesehatan.

4. Regulasi dan hukum

Aspek hukum terkait kepemilikan data, tanggung jawab atas pelanggaran privasi, serta tata kelola jaringan blockchain di sektor kesehatan masih menjadi perdebatan. Perlu adanya regulasi yang jelas untuk memastikan penggunaan blockchain sejalan dengan etika medis dan hukum yang berlaku.

Dengan mempertimbangkan faktor-faktor tersebut, penelitian dan pengembangan lebih lanjut masih sangat dibutuhkan agar blockchain dapat diimplementasikan secara optimal dalam meningkatkan keamanan data medis elektronik.

5. KESIMPULAN

Berdasarkan hasil kajian, blockchain menawarkan solusi inovatif untuk meningkatkan keamanan data medis elektronik melalui mekanisme desentralisasi, enkripsi, kontrol akses berbasis *smart contract*, serta pencatatan transaksi yang imutabel. Teknologi ini berpotensi mengurangi risiko kebocoran data, meningkatkan transparansi, dan memperkuat kepercayaan antara pasien, tenaga medis, serta penyedia layanan kesehatan.

Namun, penerapan blockchain dalam sistem medis elektronik memerlukan kajian lebih lanjut terkait skalabilitas, interoperabilitas, dan regulasi. Penelitian lanjutan diharapkan dapat menguji model implementasi blockchain di berbagai konteks layanan kesehatan, sehingga manfaatnya dapat terealisasi secara optimal.

6. DAFTAR PUSTAKA

- Ahuja, S. P., Mani, S., & Zambrano, J. (2020). A Survey of the Application of Blockchain in Healthcare. *Healthcare Informatics Research*, 26(4), 263–269.
- Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare*, 7(2), 56.
- Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology: Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9), e003800.
- Bhattacharya, S., Tanwar, S., Tyagi, S., & Kumar, N. (2022). Blockchain for Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences*, 12(3), 1415.
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.
- Ekblaw, A., Azaria, A., Halamka, J., & Lippman, A. (2017). MedRec: Blockchain for Medical Data Access and Permission Management. MIT Media Lab.
- Hassan, N., Ali, S., & Islam, R. (2019). Electronic Medical Record Systems: Challenges and Opportunities in Developing Countries. *Health Informatics Journal*, 25(3), 1112–1123.
- Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2021). Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. *Journal of the American Medical Informatics Association*, 28(3), 534–544.
- Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. *IEEE Healthcom*, 1–4.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Ponemon Institute. (2021). Cost of a Data Breach Report 2021. IBM Security.
- Roehrs, A., da Costa, C. A., da Rosa Righi, R., & da Silva, V. F. (2019). Personal Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, 92, 103139.
- WHO. (2020). Electronic Health Records: Manual for Developing Countries. World Health Organization.
- Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain Technology Use Cases in Healthcare. *Advances in Computers*, 111, 1–41.
- Zhao, J., Bai, G., & Zhang, Z. (2021). Blockchain-Based Sharing and Tamper-Proof Framework of Electronic Health Records in Multi-Hospital Systems. *Information Processing & Management*, 58(4), 102539...