

Blockchain untuk Keamanan Data Kesehatan dalam Rekam Medis Elektronik

Dina Sonia^{1*}, Daniel Happy Putra¹, Mieke Nurmalasari²

¹Program Studi Rekam Medis dan Informasi Kesehatan, Fakultas Ilmu-Ilmu Kesehatan,
Universitas Esa Unggul

dina.sonia@esaunggul.ac.id, daniel.putra@esaunggul.ac.id

²Program Studi Manajemen dan Informasi Kesehatan, Fakultas Ilmu-Ilmu Kesehatan,
Universitas Esa Unggul
mieke.nurmalasari@esaunggul.ac.id

Keywords:

*Blockchain,
Health Data Security,
Electronic Medical Records,
Systematic Literature Review*

ABSTRACT

The digital transformation of healthcare through Electronic Medical Records (EMRs) has improved the efficiency and continuity of clinical information management but has also raised significant concerns regarding data security and privacy. The increasing frequency of cyberattacks and the limitations of conventional data protection mechanisms, particularly in developing countries such as Indonesia, highlight the need for more reliable security solutions. This study explores the potential of blockchain technology to enhance EMR security through a Systematic Literature Review (SLR) following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. A total of 13 peer-reviewed articles published within the last five years were systematically reviewed. The findings indicate that blockchain can serve as an additional security layer by improving data integrity and auditability through immutable ledgers, cryptographic hashing, and distributed consensus mechanisms. Data confidentiality is strengthened through patient-centered decentralized access control and advanced cryptographic techniques, while data availability is supported by hybrid architectures using off-chain storage. However, blockchain implementation still faces challenges, including scalability, cryptographic key management, system integration, and regulatory constraints. Overall, blockchain demonstrates strong potential to enhance security and trust within the EMR ecosystem, although it is better positioned as a complementary technology rather than a standalone solution.

Kata Kunci

*Blockchain,
Keamanan Data Kesehatan,
Rekam Medis Elektronik,
Systematic Literature Review*

ABSTRAK

Transformasi digital layanan kesehatan melalui penerapan Rekam Medis Elektronik (RME) meningkatkan efisiensi dan kesinambungan informasi klinis, tetapi juga menimbulkan tantangan terkait keamanan dan privasi data kesehatan. Tingginya risiko serangan siber serta keterbatasan mekanisme perlindungan data, khususnya di negara berkembang seperti Indonesia, mendorong kebutuhan akan teknologi yang lebih andal. Penelitian ini bertujuan mengeksplorasi potensi teknologi blockchain dalam meningkatkan keamanan RME melalui metode *Systematic Literature Review* (SLR) dengan pendekatan *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) terhadap 13 artikel ilmiah bereputasi yang diterbitkan dalam lima tahun terakhir. Hasil kajian menunjukkan bahwa blockchain berkontribusi signifikan sebagai lapisan keamanan tambahan dengan

memperkuat integritas dan auditabilitas data melalui mekanisme *immutable ledger*, *hashing*, dan konsensus terdistribusi. Kerahasiaan data didukung oleh kontrol akses terdesentralisasi berbasis pasien yang dipadukan dengan skema kriptografi lanjutan, sedangkan ketersediaan data bergantung pada penerapan arsitektur *hybrid* dengan penyimpanan *off-chain*. Namun, implementasi blockchain masih menghadapi tantangan berupa skalabilitas, manajemen kunci kriptografi, integrasi sistem, dan regulasi. Secara keseluruhan, blockchain berpotensi memperkuat keamanan dan kepercayaan dalam ekosistem RME, tetapi lebih tepat diposisikan sebagai teknologi pendukung daripada solusi tunggal.

Korespondensi Penulis:

Dina Sonia,
Universitas Esa Unggul,
Jl. Arjuna Utara No. 9, Kebon Jeruk, Jakarta Barat
Telepon: (021) 39529950
Email: dina.sonia@esaunggul.ac.id

Submitted : 08-01-2026; Accepted : 16-04-2026;
Published : 28-06-2026

Copyright (c) 2026 The Author (s)

This article is distributed under a Creative Commons
Attribution-ShareAlike 4.0 International License (CC BY-SA
4.0)

1. PENDAHULUAN

Transformasi digital dalam bidang kesehatan telah mendorong adopsi Rekam Medis Elektronik (RME) secara luas sebagai bagian dari upaya meningkatkan efisiensi layanan, kesinambungan informasi klinis, dan mutu pelayanan kesehatan. Namun, digitalisasi data kesehatan secara simultan juga meningkatkan risiko keamanan dan privasi karena rekam medis mengandung informasi sensitif yang bernilai tinggi serta menjadi target utama kejahatan siber. Berdasarkan laporan keamanan data yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN), sektor kesehatan termasuk infrastruktur informasi kritis yang paling rentan terhadap serangan siber, seperti *ransomware*, pencurian data pasien, dan gangguan operasional layanan yang berpotensi berdampak langsung terhadap keselamatan pasien [1].

Permasalahan keamanan RME semakin relevan dalam konteks Indonesia seiring dengan meningkatnya digitalisasi layanan kesehatan dan masih berkembangnya kapasitas keamanan siber nasional. Berdasarkan *National Cyber Security Index* (NCSI), pada tahun 2023 Indonesia berada pada peringkat ke-49 dunia dengan skor 63,64 dalam aspek keamanan siber. Kondisi tersebut menunjukkan masih adanya kesenjangan yang signifikan dalam perlindungan layanan digital dan tata kelola keamanan siber, khususnya pada sektor publik strategis seperti kesehatan [2]. Hal ini mengindikasikan bahwa meskipun regulasi perlindungan data pribadi telah tersedia, mekanisme teknis untuk menjamin integritas, kerahasiaan, dan ketersediaan data kesehatan masih belum optimal.

Berdasarkan penelitian sebelumnya, teknologi blockchain dipandang sebagai pendekatan yang potensial untuk mengatasi permasalahan keamanan data kesehatan. Blockchain didefinisikan sebagai *distributed ledger* yang bersifat *tamper-evident* dan *tamper-resistant*, dimana setiap transaksi dicatat secara kriptografis dan divalidasi melalui mekanisme konsensus terdistribusi sehingga sulit dimodifikasi tanpa persetujuan jaringan. Karakteristik utama blockchain yang dapat dimanfaatkan untuk menjamin integritas dan jejak audit data RME meliputi desentralisasi, imutabilitas, transparansi terbatas, dan kriptografi [3].

Penelitian lain yang membahas blockchain dalam bidang kesehatan umumnya berfokus pada aspek konseptual atau studi kasus tertentu, seperti peningkatan interoperabilitas, manajemen akses pasien, dan efisiensi pertukaran data klinis. Blockchain dimanfaatkan untuk meningkatkan kontrol pasien terhadap data medis serta mendukung pendekatan *patient-centered care*. Namun, penelitian-penelitian tersebut belum secara sistematis membandingkan efektivitas mekanisme keamanan blockchain dalam mengatasi berbagai tantangan keamanan RME secara komprehensif [4]. Di sisi lain, sebagian penelitian masih berfokus pada penjelasan prinsip dasar blockchain, jenis-jenis blockchain, dan mekanisme konsensus tanpa mengaitkannya secara spesifik dengan kebutuhan serta risiko pada sektor kesehatan, terutama dalam konteks negara berkembang [5].

Berdasarkan telaah terhadap penelitian sebelumnya, belum teridentifikasi adanya sintesis sistematis yang menganalisis penerapan teknologi blockchain dalam meningkatkan keamanan RME, termasuk model arsitektur yang digunakan, mekanisme keamanan yang dominan seperti *hashing*, *smart contract*, dan *access control*, serta berbagai keterbatasan implementasinya, seperti isu skalabilitas,

regulasi, dan integrasi dengan sistem kesehatan yang telah ada. Selain itu, penelitian di Indonesia masih belum banyak mengaitkan temuan-temuan tersebut dengan konteks kebijakan dan tingkat kesiapan keamanan siber nasional.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengeksplorasi secara sistematis potensi teknologi blockchain dalam meningkatkan keamanan data kesehatan pada RME melalui metode *Systematic Literature Review* (SLR). Penelitian ini berfokus pada identifikasi kontribusi blockchain terhadap aspek keamanan utama RME, meliputi kerahasiaan, integritas, ketersediaan, dan auditabilitas data, sekaligus menganalisis keterbatasan serta tantangan implementasinya. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi ilmiah berupa sintesis bukti berbasis literatur yang dapat menjadi landasan konseptual dan praktis bagi pengembangan sistem RME yang lebih aman, adaptif, dan selaras dengan kebutuhan keamanan siber di sektor kesehatan.

2. METODE PENELITIAN

2.1 Desain Penelitian

Metode yang digunakan dalam penelitian ini adalah studi literatur yang bertujuan untuk mengumpulkan, menganalisis, dan mengevaluasi berbagai sumber ilmiah, baik berupa buku referensi maupun artikel jurnal. Melalui pendekatan ini, penelitian dapat membahas secara mendalam potensi teknologi blockchain dalam meningkatkan keamanan Rekam Medis Elektronik (RME) yang adaptif dan selaras dengan kebutuhan keamanan siber di bidang kesehatan.

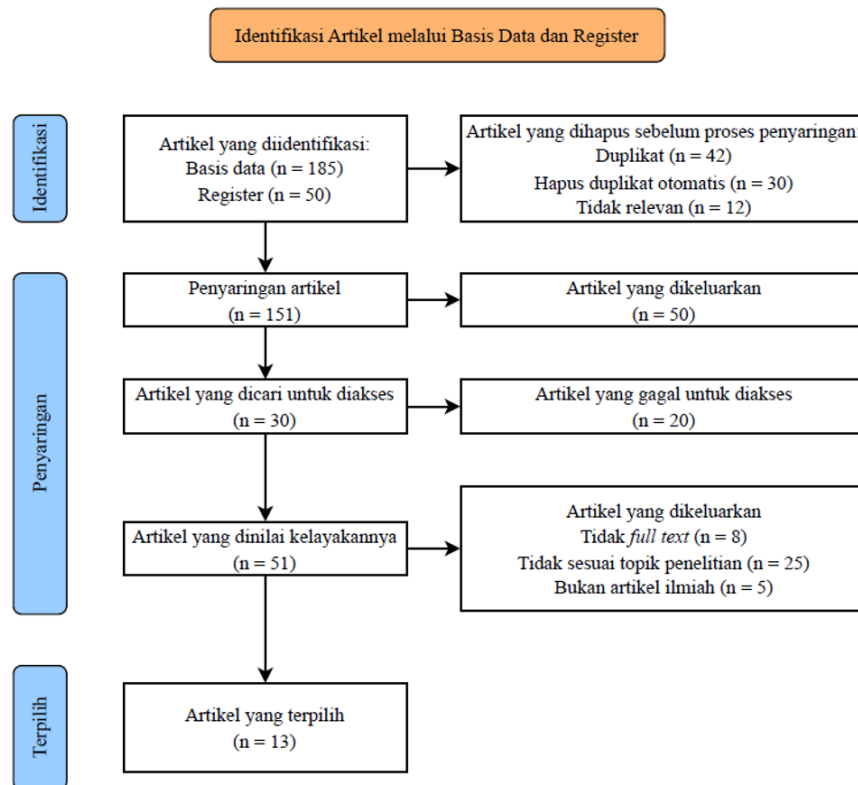
Pengumpulan data dilakukan dengan mengidentifikasi, menelaah, dan mengevaluasi artikel ilmiah yang relevan dengan topik penelitian. Pendekatan yang digunakan adalah *Systematic Literature Review* (SLR) dengan metode *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). Pencarian artikel dilakukan melalui beberapa basis data ilmiah, yaitu *Google Scholar*, *Scopus*, dan *CrossRef*, menggunakan kombinasi kata kunci “blockchain”, “*electronic medical record*”, “*electronic health record security*”, dan “*healthcare data security*”.

Artikel yang diperoleh kemudian diseleksi berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Kriteria inklusi meliputi artikel yang dipublikasikan dalam jurnal bereputasi, diterbitkan dalam lima tahun terakhir, tersedia dalam bentuk teks lengkap (*full text*), ditulis dalam bahasa Inggris, serta memiliki relevansi dengan topik blockchain dan keamanan data pada RME. Sementara itu, kriteria eksklusi meliputi artikel yang hanya tersedia dalam bentuk abstrak, tidak relevan dengan variabel penelitian, atau bukan merupakan artikel ilmiah.

2.2 Prosedur Penelitian

Prosedur penelitian diawali dengan proses seleksi literatur yang dilakukan secara sistematis menggunakan perangkat lunak *Covidence* untuk mempermudah proses penyaringan, pengelompokan, dan evaluasi artikel secara efisien. Seleksi artikel dilakukan berdasarkan tahapan PRISMA yang meliputi *identification* (identifikasi dan pengumpulan artikel sesuai kata kunci yang telah ditentukan), *screening* (penyaringan artikel berdasarkan judul dan abstrak untuk menilai relevansinya dengan topik penelitian), *eligibility* (penilaian kelayakan artikel melalui penelaahan teks lengkap), dan *included* (penetapan artikel yang memenuhi seluruh kriteria inklusi untuk dianalisis dalam penelitian) [6], [7].

Melalui tahapan tersebut, diperoleh artikel yang paling relevan dan sesuai dengan tujuan penelitian untuk dianalisis lebih lanjut. Adapun hasil proses pengumpulan dan seleksi literatur menggunakan metode PRISMA ditunjukkan pada Gambar 1.



Gambar 1. Diagram Alir Seleksi Artikel Menggunakan Metode PRISMA

Berdasarkan Gambar 1, diperoleh 13 artikel ilmiah yang memenuhi kriteria inklusi berdasarkan tahapan PRISMA. Proses analisis data dilakukan menggunakan analisis tematik secara kualitatif. Peneliti terlebih dahulu melakukan ekstraksi data dari setiap artikel terpilih dengan mengidentifikasi informasi penting, seperti tujuan penelitian, metode yang digunakan, jenis teknologi blockchain yang diterapkan, serta kontribusinya terhadap keamanan RME.

Selanjutnya, temuan dari masing-masing artikel dikelompokkan berdasarkan empat aspek utama keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan auditabilitas (*auditability*). Pada tahap ini, peneliti melakukan proses kategorisasi dan perbandingan hasil penelitian untuk mengidentifikasi pola, persamaan, serta perbedaan pendekatan yang digunakan dalam penerapan blockchain pada sistem RME. Selain itu, analisis juga dilakukan dengan menelaah berbagai tantangan dan keterbatasan implementasi yang dilaporkan dalam setiap studi, seperti isu skalabilitas, integrasi sistem, dan manajemen kunci kriptografi. Hasil analisis kemudian disintesis secara deskriptif untuk memberikan gambaran yang komprehensif mengenai peran teknologi blockchain dalam memperkuat keamanan data kesehatan pada sistem RME.

3. HASIL DAN ANALISIS

3.1 Kontribusi Blockchain terhadap Keamanan RME

Dalam penelitian ini, blockchain didefinisikan sebagai teknologi digital terdistribusi yang memungkinkan pencatatan data atau transaksi secara aman, transparan, dan tidak dapat diubah oleh pihak yang tidak berwenang. Data yang dicatat dalam blockchain disimpan dalam bentuk blok yang saling terhubung melalui mekanisme kriptografi dan diverifikasi oleh jaringan komputer melalui proses konsensus. Dengan mekanisme tersebut, setiap perubahan data dapat terdeteksi secara langsung.

Karakteristik utama blockchain meliputi desentralisasi, transparansi, keamanan berbasis kriptografi, serta sifat *immutable*, yaitu kondisi ketika data yang telah tercatat tidak dapat dimodifikasi atau dihapus tanpa meninggalkan jejak perubahan. Dalam konteks sistem RME, blockchain tidak dimaksudkan untuk menggantikan sistem informasi kesehatan yang telah ada, melainkan berfungsi sebagai lapisan keamanan tambahan (*security and trust layer*) yang terintegrasi dengan sistem RME untuk memperkuat perlindungan data kesehatan.

Melalui mekanisme pencatatan transaksi yang transparan, pengelolaan akses berbasis kriptografi, serta arsitektur jaringan terdistribusi, teknologi blockchain berpotensi meningkatkan keamanan dan

kepercayaan dalam pengelolaan data medis. Potensi tersebut terutama terlihat dalam upaya menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), serta keterlacakan (*traceability*) aktivitas terhadap data RME [8], [9].

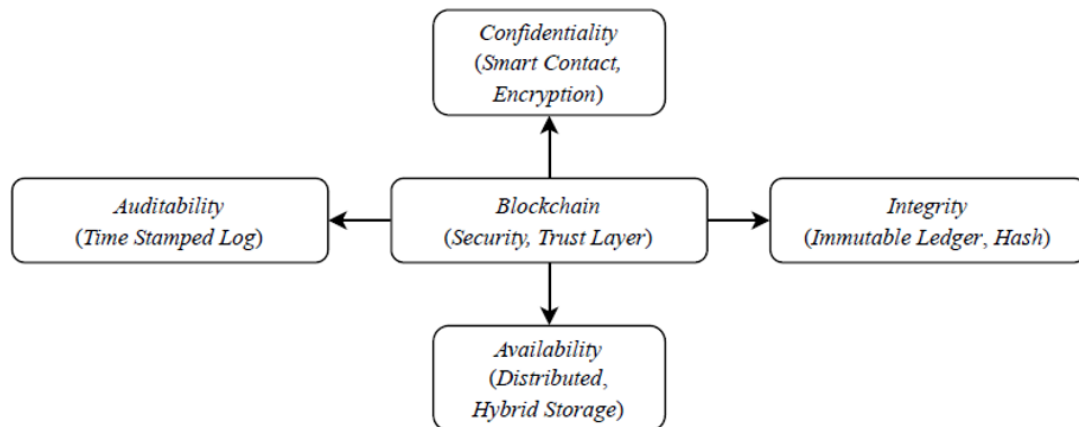
Analisis data dalam penelitian ini dilakukan melalui analisis tematik secara kualitatif terhadap 13 artikel ilmiah yang telah memenuhi kriteria inklusi berdasarkan tahapan PRISMA. Daftar artikel yang terpilih untuk dianalisis dalam penelitian ini disajikan pada Tabel 1.

Tabel 1. Karakteristik Artikel yang Diinklusi dalam Systematic Literature Review

No	Penulis (Tahun)	Desain Penelitian	Judul Artikel
1	Lee <i>et al.</i> (2022) [10]	Perancangan sistem	<i>Privacy Preservation in Patient Information Exchange Systems Based on Blockchain</i>
2	Yakubu <i>et al.</i> (2024) [11]	Penelitian eksperimen	<i>PatCen: A Blockchain Based Patient Centric Mechanism for The Granular Access Control of Infectious Disease Related Test Records</i>
3	Psarra <i>et al.</i> (2024) [12]	Pengembangan sistem	<i>Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records</i>
4	Al-Khasawneh <i>et al.</i> (2024) [13]	Pemodelan sistem	<i>A Secure Blockchain Framework for Healthcare Records Management Systems</i>
5	Haddad <i>et al.</i> (2024) [14]	Pemodelan sistem	<i>E2EE Enhanced Patient Centric Blockchain Based System for EHR Management</i>
6	Zhao dan Tian (2025) [15]	Pengembangan pemodelan sistem	<i>Secure Sharing of Electronic Medical Records Based on Blockchain and Searchable Encryption</i>
7	Shahzad <i>et al.</i> (2024) [16]	Research and Development	<i>A Robust Algorithm for Authenticated Health Data Access via Blockchain and Cloud Computing</i>
8	Alabdulatif (2025) [17]	Pengembangan pemodelan sistem	<i>Blockchain Based Privacy Preserving Authentication and Access Control Model for E-Health Users</i>
9	Kasyapa dan Vanmathi (2024) [18]	Literature Review	<i>Blockchain Integration in Healthcare: a Comprehensive Investigation of Use Cases, Performance Issues, and Mitigation Strategies</i>
10	Mole dan Shaji (2024) [19]	Research and Development	<i>Ethereum Blockchain for Electronic Health Records: Securing and Streamlining Patient Management</i>
11	Costa <i>et al.</i> (2022) [20]	Research and Development	<i>Blockchain Based Architecture Design for Personal Health Record</i>
12	Xiao <i>et al.</i> (2021) [21]	Penelitian pengembangan	<i>The Healthchain Blockchain for Electronic Health Records</i>
13	Fang <i>et al.</i> (2021) [22]	Systematic Literature Review	<i>Blockchain Personal Health Records: Systematic Review</i>

Hasil analisis sistematis terhadap 13 artikel ilmiah menunjukkan bahwa teknologi blockchain memberikan kontribusi yang signifikan dalam memperkuat keamanan RME, terutama pada aspek kerahasiaan, integritas, ketersediaan, dan auditabilitas data. Kontribusi tersebut dapat dipetakan ke dalam empat aspek utama keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan auditabilitas (*auditability*). Selain itu, berbagai penelitian juga melaporkan sejumlah keterbatasan implementasi blockchain yang masih menjadi tantangan dalam penerapannya pada sistem RME.

Berdasarkan hasil sintesis literatur, gambaran kontribusi teknologi blockchain terhadap keamanan RME disajikan sebagai berikut:



Gambar 2. Kontribusi Blockchain terhadap Keamanan RME

Secara konseptual, posisi blockchain dalam ekosistem RME digambarkan sebagai lapisan keamanan tambahan (*security and trust layer*) yang terintegrasi dengan sistem RME yang telah ada serta teknologi penyimpanan *off-chain*. Gambar 2 mengilustrasikan bagaimana blockchain berinteraksi dengan sistem RME dan media penyimpanan eksternal untuk memperkuat empat aspek utama keamanan informasi tanpa menggantikan fungsi inti sistem informasi kesehatan. Adapun peran blockchain pada masing-masing aspek keamanan dijelaskan sebagai berikut.

1. Kerahasiaan Data

Pada aspek kerahasiaan, blockchain mendukung penerapan kontrol akses terdesentralisasi yang berorientasi pada pasien sebagai pemilik data. Hak akses terhadap data medis ditentukan secara eksplisit oleh pasien dan dieksekusi secara otomatis melalui *smart contract*, sehingga mengurangi ketergantungan pada administrator sistem terpusat [10], [11], [12]. Untuk memperkuat mekanisme tersebut, berbagai penelitian mengombinasikan blockchain dengan skema kriptografi lanjutan, seperti *Attribute-Based Encryption* (ABE), *Proxy Re-Encryption* (PRE), *secret sharing*, dan *end-to-end encryption* [10], [12], [13], [14]. Integrasi teknologi tersebut memungkinkan pengelolaan hak akses yang lebih fleksibel, termasuk perubahan maupun pencabutan izin akses tanpa perlu memodifikasi data medis yang telah tersimpan. Dengan demikian, risiko kebocoran data akibat akses tidak sah dapat diminimalkan secara signifikan [15], [16], [17].

2. Integritas Data

Integritas data merupakan aspek keamanan yang paling konsisten diperkuat oleh teknologi blockchain. Karakteristik *ledger* pada blockchain menunjukkan bahwa catatan transaksi disimpan secara transparan dan dapat diverifikasi oleh seluruh pihak yang memiliki hak akses dalam jaringan. Selain itu, sifat *immutable* pada blockchain memastikan bahwa data yang telah dicatat tidak dapat diubah, dihapus, atau dimodifikasi tanpa meninggalkan jejak perubahan, sehingga keaslian data tetap terjaga [13], [18], [19].

Keterkaitan antarblok melalui kode unik (*hash*) memungkinkan setiap perubahan data terdeteksi secara langsung dan mencegah manipulasi data medis tanpa jejak. Sebagian besar penelitian menerapkan pendekatan penyimpanan hash dan metadata medis pada blockchain, sementara data klinis disimpan di luar blockchain (*off-chain*) [10], [18], [20]. Strategi ini memungkinkan proses verifikasi keaslian data dilakukan secara berkelanjutan tanpa membebani jaringan blockchain dengan data berukuran besar. Selain itu, mekanisme konsensus dan validasi transaksi memastikan bahwa hanya data yang berasal dari entitas terotorisasi yang dapat dicatat dalam sistem, sehingga meningkatkan keandalan informasi klinis [14], [18], [21].

3. Ketersediaan Data

Kontribusi blockchain terhadap ketersediaan data RME terutama berkaitan dengan penerapan arsitektur sistem terdistribusi. Dengan menghilangkan ketergantungan pada satu titik penyimpanan (*single point of failure*), sistem RME berbasis blockchain menjadi lebih tahan terhadap gangguan layanan, kegagalan infrastruktur, maupun serangan siber [11], [12], [18]. Sebagian besar penelitian mengadopsi arsitektur hibrida (*hybrid architecture*), yaitu blockchain digunakan untuk pencatatan transaksi dan pengelolaan akses, sedangkan data medis disimpan melalui teknologi penyimpanan *off-chain* seperti *InterPlanetary File System* (IPFS) atau layanan cloud storage [10], [12], [22]. IPFS merupakan sistem

penyimpanan data terdistribusi yang menyimpan file pada banyak komputer dalam jaringan sehingga data dapat diakses dari berbagai lokasi tanpa bergantung pada satu server pusat. Meskipun pendekatan tersebut meningkatkan ketersediaan data secara konseptual, beberapa studi melaporkan bahwa keterbatasan performa blockchain, terutama terkait latensi dan *throughput*, masih menjadi kendala dalam implementasi klinis berskala besar [11], [14], [21].

4. Auditabilitas dan Akuntabilitas

Auditabilitas merupakan salah satu aspek keamanan yang paling menonjol diperkuat oleh blockchain. Teknologi ini mampu menyediakan jejak audit permanen terhadap seluruh aktivitas yang berkaitan dengan RME, termasuk pembuatan data, pemberian dan pencabutan hak akses, serta pertukaran data antarentitas yang terlibat dalam pelayanan kesehatan, seperti rumah sakit, klinik, laboratorium, dokter, dan institusi kesehatan lainnya [13], [17], [18].

Dalam konteks RME, mekanisme tersebut memungkinkan informasi medis pasien diakses oleh tenaga kesehatan yang berwenang untuk mendukung proses diagnosis, pengobatan, maupun rujukan layanan secara lebih efektif. Selain itu, setiap transaksi dicatat secara *time-stamped*, yaitu dilengkapi dengan penanda waktu yang menunjukkan kapan suatu data dibuat, diakses, atau diperbarui. Karena catatan tersebut tidak dapat dihapus, proses penelusuran aktivitas pengguna dapat dilakukan secara transparan dan terverifikasi. Karakteristik ini memberikan nilai tambah yang signifikan bagi manajemen fasilitas kesehatan, auditor internal, maupun regulator dalam memastikan kepatuhan terhadap kebijakan dan regulasi perlindungan data kesehatan [14], [18].

Berdasarkan hasil analisis terhadap 13 artikel ilmiah, distribusi fokus aspek keamanan RME yang meliputi kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan auditabilitas (*auditability*) disajikan pada Tabel 2 dan Gambar 3.

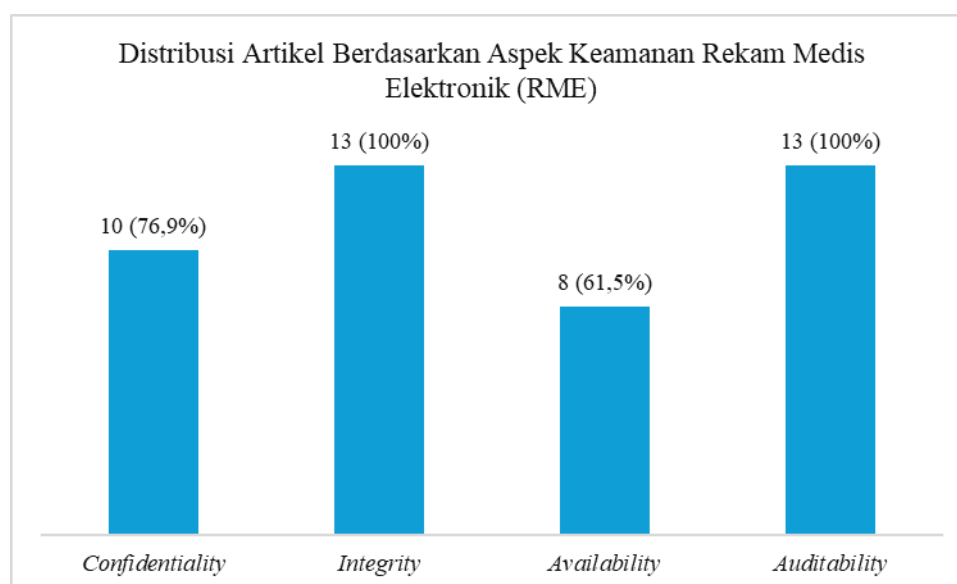
Tabel 2. Pemetaan Artikel Berdasarkan Aspek Keamanan Rekam Medis Elektronik (RME)

No	Judul Artikel	Kerahasiaan	Integritas	Ketersediaan	Auditabilitas
1	<i>Privacy Preservation in Patient Information Exchange Systems Based on Blockchain</i> [10]	√	√	√	
2	<i>PatCen: A Blockchain Based Patient Centric Mechanism for The Granular Access Control of Infectious Disease Related Test Records</i> [11]	√		√	
3	<i>Permissioned Blockchain Network for Proactive Access Control to Electronic Health Records</i> [12]	√		√	
4	<i>A Secure Blockchain Framework for Healthcare Records Management Systems</i> [13]	√	√		√
5	<i>E2EE Enhanced Patient Centric Blockchain Based System for EHR Management</i> [14]	√	√	√	√
6	<i>Secure Sharing of Electronic Medical Records Based on Blockchain and Searchable Encryption</i> [15]	√			
7	<i>A Robust Algorithm for Authenticated Health Data Access via Blockchain and Cloud Computing</i> [16]	√			
8	<i>Blockchain Based Privacy Preserving Authentication and Access Control Model for E-Health Users</i> [17]	√			√
9	<i>Blockchain Integration in Healthcare: a Comprehensive Investigation of Use Cases, Performance Issues, and Mitigation Strategies</i> [18]		√	√	√
10	<i>Ethereum Blockchain for Electronic Health Records: Securing and Streamlining Patient Management</i> [19]		√		
11	<i>Blockchain Based Architecture Design for Personal Health Record</i> [20]		√		
12	<i>The Healthchain Blockchain for Electronic Health Records</i> [21]		√		
13	<i>Blockchain Personal Health Records: Systematic Review</i> [22]			√	

Berdasarkan Tabel 2, hasil analisis terhadap 13 artikel ilmiah menunjukkan bahwa teknologi blockchain paling dominan digunakan untuk memperkuat aspek integritas dan auditabilitas data dalam sistem RME. Seluruh artikel yang dianalisis membahas aspek integritas, yang menunjukkan bahwa karakteristik blockchain, seperti *immutable ledger*, *hashing*, dan mekanisme konsensus, efektif dalam menjaga keutuhan serta mencegah manipulasi data medis.

Selain itu, sebagian besar penelitian juga menyoroti aspek kerahasiaan data melalui penerapan kontrol akses terdesentralisasi dan skema kriptografi untuk memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang. Sementara itu, aspek ketersediaan data dibahas dalam jumlah artikel yang lebih sedikit karena umumnya bergantung pada integrasi blockchain dengan mekanisme penyimpanan eksternal, seperti *off-chain storage* atau layanan *cloud storage*.

Hal ini menunjukkan bahwa blockchain berperan utama dalam menjamin integritas dan keterlacakan data kesehatan, sedangkan ketersediaan data memerlukan dukungan arsitektur sistem yang lebih luas. Adapun persentase distribusi aspek keamanan RME berdasarkan hasil analisis terhadap 13 artikel ilmiah adalah sebagai berikut:



Gambar 3. Distribusi Artikel Berdasarkan Aspek Keamanan Rekam Medik Elektronik (RME)

Berdasarkan Gambar 3, seluruh artikel yang dianalisis membahas aspek integritas (*integrity*) dan auditabilitas (*auditability*) data, dengan persentase masing-masing sebesar 100%. Temuan ini menunjukkan peran dominan teknologi blockchain dalam menjamin integritas dan keterlacakan data medis. Sementara itu, aspek kerahasiaan (*confidentiality*) dibahas dalam 10 artikel (76,9%), sedangkan aspek ketersediaan (*availability*) dibahas dalam 8 artikel (61,5%). Hasil tersebut mengindikasikan bahwa ketersediaan data masih lebih banyak bergantung pada integrasi blockchain dengan mekanisme penyimpanan *off-chain* dibandingkan pada teknologi blockchain itu sendiri.

3.2 Keterbatasan dan Tantangan Implementasi

Berdasarkan hasil analisis terhadap 13 artikel ilmiah, berbagai keterbatasan dan tantangan masih ditemukan dalam implementasi teknologi blockchain pada sistem RME. Adapun keterbatasan dan tantangan implementasi blockchain pada sistem RME adalah sebagai berikut:

Tabel 3. Tantangan dan Keterbatasan Implementasi Blockchain dalam Rekam Medik Elektronik (RME)

Kategori Tantangan	Deskripsi Tantangan			Implikasi terhadap Implementasi
Skalabilitas dan Performa	Latensi tinggi dan terbatas	dan <i>throughput</i>		Hambatan penerapan klinis berskala besar
Manajemen Kunci	Kompleksitas pengelolaan kunci kriptografi			Risiko kehilangan akses data
Integrasi Sistem	Ketidakselarasan dengan eksisting	dengan RME		Biaya dan kompleksitas implementasi

Regulasi dan Hukum	Konflik dengan kebijakan	Kebutuhan arsitektur <i>hybrid</i>
Sumber Daya Manusia (SDM) dan Organisasi	Keterbatasan kompetensi teknis	Retensi adopsi teknologi

Berdasarkan Tabel 3, teknologi blockchain menunjukkan potensi yang kuat dalam meningkatkan keamanan data pada sistem RME. Namun, beberapa artikel juga menyoroti berbagai keterbatasan dan tantangan dalam implementasinya. Tantangan utama yang diidentifikasi meliputi keterbatasan skalabilitas dan performa jaringan blockchain, kompleksitas pengelolaan kunci kriptografi, serta kesulitan integrasi dengan sistem RME yang telah ada [11], [20], [21].

Selain tantangan teknis, aspek hukum dan regulasi juga menjadi perhatian penting. Sifat blockchain yang permanen (*immutable*) berpotensi menimbulkan konflik dengan kebijakan penghapusan atau koreksi data yang berlaku dalam beberapa regulasi perlindungan data. Oleh karena itu, banyak penelitian merekomendasikan penerapan arsitektur hibrida (*hybrid architecture*) serta tata kelola data yang adaptif untuk mengatasi tantangan tersebut [10], [16], [22].

4. KESIMPULAN

Berdasarkan hasil *Systematic Literature Review* terhadap 13 artikel ilmiah, penelitian ini menunjukkan bahwa teknologi blockchain memiliki potensi yang signifikan dalam meningkatkan keamanan sistem RME, terutama pada aspek kerahasiaan, integritas, ketersediaan, dan auditabilitas data. Blockchain berperan dalam memperkuat kontrol akses, menjaga integritas data melalui mekanisme kriptografi dan *immutable ledger*, meningkatkan keterlacakan aktivitas pengguna, serta mendukung ketersediaan data melalui arsitektur sistem terdistribusi.

Namun, implementasinya masih menghadapi berbagai tantangan, seperti keterbatasan skalabilitas, kompleksitas pengelolaan kunci kriptografi, integrasi dengan sistem yang telah ada, serta aspek regulasi. Oleh karena itu, blockchain lebih tepat diposisikan sebagai teknologi pendukung untuk meningkatkan keamanan dan kepercayaan dalam ekosistem RME. Berdasarkan temuan tersebut, penerapan blockchain pada sistem RME perlu dilakukan secara bertahap dengan mempertimbangkan integrasi, interoperabilitas, dan tata kelola data kesehatan yang sesuai. Penelitian selanjutnya disarankan untuk mengembangkan model implementasi yang lebih aplikatif serta mengevaluasi kinerja blockchain pada lingkungan pelayanan kesehatan yang nyata guna mendukung penerapannya secara efektif dan berkelanjutan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Esa Unggul atas dukungan dan pendanaan yang diberikan sehingga penelitian ini dapat terlaksana dengan baik. Penulis juga menyampaikan apresiasi kepada seluruh anggota tim peneliti yang telah berkontribusi dalam perencanaan, pelaksanaan, dan analisis penelitian ini.

REFERENSI

- [1] Badan Siber dan Sandi Negara, *Buku Putih Keamanan Siber Sektor Kesehatan*. Jakarta: Direktorat Proteksi Infrastruktur Informasi Kritis Nasional, 2020.
- [2] Badan Siber dan Sandi Negara, "NCIS: National Cyber Security Index." [Online]. Available: <https://ncsi.ega.ee/>
- [3] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Gaithersburg, MD, Oct. 2018. doi: 10.6028/NIST.IR.8202.
- [4] K. Ramadhani, "Penerapan Teknologi Blockchain dalam Sistem Manajemen Kesehatan Elektronik," *J. Sos. dan Teknol.*, vol. 4, no. 2, pp. 116–119, 2024.
- [5] M. Charalambous and T. Damvakeraki, *Blockchain for Beginners - Basic Guiding Principles*. European Blockchain Observatory and Forum, 2023.
- [6] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, pp. 1–9, Mar. 2021, doi: 10.1136/bmj.n71.
- [7] M. J. Page *et al.*, "PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews," *BMJ*, pp. 1–36, Mar. 2021, doi: 10.1136/bmj.n160.
- [8] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare*, vol. 7, no. 2, pp. 1–30, Apr. 2019, doi: 10.3390/healthcare7020056.
- [9] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," *Symmetry (Basel)*, vol. 10, no. 10, pp. 1–22, Oct. 2018, doi:

- 10.3390/sym10100470.
- [10] S. -Lee, J. Kim, Y. Kwon, T. Kim, and S. Cho, "Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study," *J. Med. Internet Res.*, vol. 24, no. 3, pp. 1–20, Mar. 2022, doi: 10.2196/29108.
 - [11] B. M. Yakubu, S. M. Ali, M. I. Khan, and P. Bhattachakosol, "PatCen: A blockchain-based patient-centric mechanism for the granular access control of infectious disease-related test records," *PLoS One*, vol. 19, no. 9, pp. 1–35, Sep. 2024, doi: 10.1371/journal.pone.0310407.
 - [12] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas, "Permissioned blockchain network for proactive access control to electronic health records," *BMC Med. Inform. Decis. Mak.*, vol. 24, no. 1, pp. 1–22, Oct. 2024, doi: 10.1186/s12911-024-02708-8.
 - [13] M. A. Al-Khasawneh, M. Faheem, A. A. Alarood, S. Habibullah, and A. Alzahrani, "A secure blockchain framework for healthcare records management systems," *Healthc. Technol. Lett.*, vol. 11, no. 6, pp. 461–470, Dec. 2024, doi: 10.1049/htl2.12092.
 - [14] A. Haddad, M. H. Habaebi, E. A. A. Elsheikh, M. R. Islam, S. A. Zabidi, and F. E. M. Suliman, "E2EE enhanced patient-centric blockchain-based system for EHR management," *PLoS One*, vol. 19, no. 4, pp. 1–21, Apr. 2024, doi: 10.1371/journal.pone.0301371.
 - [15] A. Zhao and H. Tian, "Secure Sharing of Electronic Medical Records Based on Blockchain and Searchable Encryption," *Electronics*, vol. 14, no. 13, pp. 1–15, Jul. 2025, doi: 10.3390/electronics14132679.
 - [16] A. Shahzad, W. Chen, M. Shaheen, Y. Zhang, and F. Ahmad, "A robust algorithm for authenticated health data access via blockchain and cloud computing," *PLoS One*, vol. 19, no. 9, pp. 1–25, Sep. 2024, doi: 10.1371/journal.pone.0307039.
 - [17] A. Alabdulatif, "Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users," *Information*, vol. 16, no. 3, pp. 1–27, Mar. 2025, doi: 10.3390/info16030219.
 - [18] M. S. B. Kasyapa and C. Vanmathi, "Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies," *Front. Digit. Heal.*, vol. 6, pp. 1–24, Apr. 2024, doi: 10.3389/fdgth.2024.1359858.
 - [19] J. S. S. Mole and R. S. Shaji, "Ethereum blockchain for electronic health records: securing and streamlining patient management," *Front. Med.*, vol. 11, pp. 1–17, Sep. 2024, doi: 10.3389/fmed.2024.1434474.
 - [20] T. B. da S. Costa, L. Shinoda, R. A. Moreno, J. E. Krieger, and M. Gutierrez, "Blockchain-Based Architecture Design for Personal Health Record: Development and Usability Study," *J. Med. Internet Res.*, vol. 24, no. 4, pp. 1–15, Apr. 2022, doi: 10.2196/35013.
 - [21] Y. Xiao, B. Xu, W. Jiang, and Y. Wu, "The HealthChain Blockchain for Electronic Health Records: Development Study," *J. Med. Internet Res.*, vol. 23, no. 1, pp. 1–13, Jan. 2021, doi: 10.2196/13556.
 - [22] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain Personal Health Records: Systematic Review," *J. Med. Internet Res.*, vol. 23, no. 4, pp. 1–19, Apr. 2021, doi: 10.2196/25094.