INTEGRASI BLOCKCHAIN DENGAN BASIS DATA RELASIONAL UNTUK INTEGRITAS REKAM MEDIS ELEKTRONIK

INTEGRATION OF BLOCKCHAIN WITH RELATIONAL DATABASES FOR ELECTRONIC MEDICAL RECORD INTEGRITY

Faril Isra Albiansyah[1], Supriyono[2]*, Sultan Krishna Nugraha[3], Saleh Basyaib[4], Ivan Ghozali[5], Muhammad Ihsan Anshorudin[6], Afzaal Abrar Hidayat[7], Muh. Firdaus[8]

E-mail: 240605110087@student.uin-malang.ac.id[1], priyono@ti.uin-malang.ac.id[2], 240605110096@student.uin-malang.ac.id[3], 240605110143@student.uin-malang.ac.id[4], 240605110185@student.uin-malang.ac.id[5], 240605110199@student.uin-malang.ac.id[6], 240605110206@student.uin-malang.ac.id[7], 240605110214@student.uin-malang.ac.id[8]*

[12345678]*Teknik Informatika, Fakultas Sains dan Teknologi, UIN Maulana Malik Ibrahim Malang*

Abstrak

Rekam Medis Elektronik (RME) saat ini umumnya disimpan dalam Sistem Manajemen Basis Data (DBMS) relasional yang bersifat terpusat. Meskipun efisien, arsitektur ini rentan terhadap manipulasi data yang tidak sah dan risiko kegagalan titik tunggal, yang dapat membahayakan keselamatan pasien. Penelitian ini bertujuan merancang dan mengevaluasi arsitektur integrasi antara teknologi blockchain dan basis data relasional guna memastikan integritas, keamanan, dan ketidakubahan (immutability) data pada sistem RME. Kami mengusulkan sebuah kerangka kerja hibrida di mana basis data relasional bertugas mengelola penyimpanan data medis secara off-chain untuk menjaga skalabilitas dan kecepatan akses. Sementara itu, nilai hash kriptografis dari setiap rekam medis disimpan secara on-chain menggunakan jaringan blockchain. Smart contract diimplementasikan untuk mengotomatisasi sinkronisasi dan proses verifikasi integritas data setiap kali terdapat permintaan akses atau perubahan. Evaluasi kinerja sistem menunjukkan bahwa arsitektur yang diusulkan berhasil mendeteksi 100% anomali dan modifikasi data yang tidak sah pada basis data relasional. Pengujian beban (load testing) membuktikan bahwa model hibrida ini mampu mempertahankan latensi query pada batas yang dapat diterima, memberikan keseimbangan optimal antara efisiensi DBMS tradisional dan keamanan tingkat tinggi khas blockchain. Kesimpulannya, integrasi blockchain dengan basis data relasional menawarkan solusi infrastruktur yang tangguh untuk sistem informasi layanan kesehatan, secara signifikan memitigasi risiko manipulasi data medis tanpa mengorbankan efisiensi operasional harian.

Kata Kunci: *Blockchain; Basis Data Relasional; Rekam Medis Elektronik; Integritas Data; Keamanan Layanan Kesehatan.*

Abstract

Electronic Medical Records (EMRs) are currently predominantly stored in centralized relational Database Management Systems (DBMS). While efficient, this architecture is vulnerable to unauthorized data manipulation and single points of failure, which can compromise patient safety. This study aims to design and evaluate an integration architecture between blockchain technology and relational databases to ensure the integrity, security, and immutability of data within EMR systems. We propose a hybrid framework where the relational database manages off-chain medical data storage to maintain scalability and rapid access speeds. Simultaneously, the cryptographic hash values of each medical record are stored on-chain using a blockchain network. Smart contracts are implemented to automate synchronization and the data integrity verification process whenever access or modification requests occur. System performance

evaluation demonstrates that the proposed architecture successfully detects 100% of anomalies and unauthorized data modifications in the relational database. Furthermore, load testing proves that this hybrid model maintains query latency within acceptable thresholds, providing an optimal balance between the efficiency of traditional DBMS and the high-level security characteristic of blockchain. In conclusion, integrating blockchain with relational databases offers a robust infrastructure solution for healthcare information systems, significantly mitigating the risk of medical data tampering without sacrificing daily operational efficiency.

Keywords: *Blockchain; Relational Database; Electronic Medical Records; Data Integrity; Healthcare Security.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi besar-besaran dalam sektor layanan kesehatan, salah satunya melalui implementasi Rekam Medis Elektronik (RME). RME menawarkan kemampuan penyimpanan, pengambilan, dan distribusi informasi medis secara efisien dibandingkan sistem berbasis kertas konvensional. Namun di balik kecanggihan tersebut, tersembunyi permasalahan fundamental yang berhubungan langsung dengan keamanan dan integritas data.

Sistem Manajemen Basis Data (DBMS) relasional yang menjadi tulang punggung mayoritas sistem RME saat ini memiliki kerentanan arsitektural yang signifikan. Karakteristik terpusat (centralized) dari RDBMS menempatkan seluruh data medis pada satu titik kendali, yang secara teknis dikenal sebagai Single Point of Failure (SPOF). Kondisi ini berarti bahwa kegagalan pada satu komponen, baik akibat serangan siber, kerusakan perangkat keras, maupun tindakan sabotase dari administrator basis data yang tidak bertanggung jawab, berpotensi menyebabkan hilangnya atau termodifikasinya seluruh rekam medis pasien [1].

Risiko manipulasi data pada sistem RME berbasis RDBMS terpusat terbagi menjadi dua kategori utama. Pertama, ancaman eksternal berupa serangan SQL Injection, Ransomware, dan akses tidak sah yang menargetkan celah keamanan pada lapisan aplikasi maupun jaringan. Kedua, ancaman internal yang justru lebih berbahaya, yaitu modifikasi data yang dilakukan oleh personel berwenang secara teknis, seperti administrator basis data (DBA), yang mampu mengubah rekam medis tanpa meninggalkan jejak audit yang dapat diverifikasi secara independen [2]. Konsekuensi dari kedua jenis ancaman ini tidak hanya berdimensi teknis, melainkan juga menyentuh aspek keselamatan jiwa pasien dan legalitas praktik medis.

Integritas data dalam konteks rekam medis elektronik memiliki implikasi yang jauh melampaui ranah teknologi informasi. Data alergi yang dimodifikasi, diagnosis yang diubah, atau riwayat pengobatan yang dihapus dapat menyebabkan kesalahan pemberian terapi yang berakibat fatal. Dari perspektif hukum, rekam medis yang tidak dapat dijamin keasliannya tidak memiliki kekuatan pembuktian yang memadai dalam sengketa medis. Regulasi nasional, sebagaimana diatur dalam Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis, mengamanatkan bahwa rekam medis wajib dijaga kerahasiaannya, keutuhannya, dan kebenarannya [3].

Teknologi blockchain muncul sebagai solusi yang menjanjikan untuk mengatasi permasalahan integritas data tersebut. Sifat desentralisasi, immutability (ketidakubahan), dan transparansi yang melekat pada blockchain menjadikannya kandidat ideal sebagai lapisan verifikasi integritas yang independen [4]. Namun, penggunaan blockchain secara eksklusif untuk penyimpanan rekam medis memiliki keterbatasan serius dari sisi skalabilitas dan kecepatan transaksi, mengingat volume data medis yang sangat besar dan kebutuhan akses real-time dalam lingkungan klinis.

Penelitian ini mengusulkan arsitektur hibrida yang secara strategis menggabungkan keunggulan kompetitif dari dua teknologi tersebut. Basis data relasional MySQL digunakan sebagai lapisan

penyimpanan data primer (off-chain) yang menjamin kecepatan dan skalabilitas akses data, sementara jaringan blockchain Hyperledger Fabric berperan sebagai lapisan kepercayaan immutable (on-chain) yang menyimpan fingerprint kriptografis dari setiap rekam medis. Mekanisme smart contract digunakan untuk mengotomasi proses verifikasi integritas pada setiap operasi baca data.

1.1 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang arsitektur hibrida yang mengintegrasikan basis data relasional dengan blockchain untuk menjamin integritas RME?
2. Seberapa efektif sistem yang diusulkan dalam mendeteksi anomali modifikasi data tidak sah pada RME?
3. Bagaimana dampak integrasi blockchain terhadap performa latensi sistem dibandingkan dengan sistem RDBMS tradisional?

1.2 Tujuan Penelitian

Tujuan penelitian ini adalah: (1) merancang dan mengimplementasikan kerangka kerja hibrida blockchain–RDBMS untuk integritas RME; (2) mengevaluasi efektivitas deteksi anomali sistem terhadap manipulasi data tidak sah; serta (3) menganalisis dampak integrasi blockchain terhadap performa latensi sistem melalui uji beban terkontrol.

2. TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Permasalahan keamanan pada sistem RME berbasis DBMS terpusat telah menjadi fokus penelitian intensif dalam dekade terakhir. Azaria et al. [5] merupakan salah satu pionir yang memperkenalkan MedRec, sebuah sistem berbasis Ethereum untuk pengelolaan akses rekam medis. Namun, MedRec menghadapi tantangan skalabilitas yang serius karena menyimpan data dalam jumlah besar secara langsung pada blockchain publik, yang berdampak pada biaya transaksi (gas fee) yang prohibitif.

Gordon dan Catalini [6] mengkaji potensi blockchain dalam transformasi data kesehatan dan mengidentifikasi bahwa pola penyimpanan hibrida, yakni metadata on-chain dengan data substantif off-chain, merupakan pendekatan yang paling layak secara praktis. Temuan ini kemudian diperkuat oleh Dey et al. [7], yang mengimplementasikan sistem hibrida menggunakan Hyperledger Fabric untuk rekam medis di lingkungan rumah sakit dan melaporkan peningkatan keamanan yang signifikan tanpa degradasi performa yang berarti.

Penelitian yang dilakukan oleh Nguyen et al. [8] berfokus pada penggunaan smart contract untuk otomatisasi audit trail pada sistem EHR dan membuktikan bahwa kontrak pintar mampu mendeteksi inkonsistensi data antara lapisan aplikasi dan lapisan penyimpanan dengan akurasi mendekati 100%. Di sisi lain, Hassan et al. [9] menganalisis kelemahan kriptografis pada beberapa implementasi hash yang digunakan untuk verifikasi integritas data medis dan merekomendasikan SHA-256 sebagai standar minimum yang aman dari serangan collision dan preimage.

Secara kolektif, literatur yang ada menunjukkan tren konvergensi menuju arsitektur hibrida yang memisahkan tanggung jawab penyimpanan dan verifikasi integritas. Penelitian ini berkontribusi dengan mengintegrasikan temuan-temuan tersebut ke dalam satu kerangka kerja yang kohesif, lengkap dengan evaluasi empiris yang komprehensif.

2.2 Kriptografi Hashing dan SHA-256

Fungsi hash kriptografis adalah fungsi matematika satu arah (one-way function) yang memetakan data masukan berukuran arbitrer ke dalam representasi keluaran berukuran tetap yang disebut nilai hash atau digest. Sifat-sifat esensial dari fungsi hash kriptografis meliputi: (1) determinisme, yakni masukan yang sama selalu menghasilkan keluaran yang identik; (2) resistansi preimage, yang berarti secara komputasional tidak mungkin merekonstruksi data asli dari nilai hash; (3) resistansi collision, yakni sangat sulit menemukan dua masukan berbeda yang menghasilkan hash yang sama; serta (4) efek avalanche, di mana perubahan sekecil satu bit pada data masukan akan mengubah nilai hash secara dramatis dan tidak dapat diprediksi [9].

SHA-256 (Secure Hash Algorithm 256-bit) merupakan anggota dari keluarga SHA-2 yang dikembangkan oleh National Security Agency (NSA) Amerika Serikat dan diterbitkan sebagai standar federal FIPS PUB 180-4. Algoritma ini menghasilkan nilai hash berukuran tetap 256 bit (32 byte) atau setara dengan 64 karakter heksadesimal, terlepas dari ukuran data masukan. SHA-256 beroperasi melalui serangkaian operasi bitwise, pergeseran, dan penambahan modular dalam 64 putaran kompresi. Dalam konteks penelitian ini, SHA-256 diterapkan untuk menghasilkan fingerprint unik dari setiap rekaman medis yang tersimpan di RDBMS.

2.3 Struktur Dasar Blockchain

Blockchain adalah struktur data terdistribusi yang tersusun dari rangkaian blok yang saling terhubung secara kriptografis. Setiap blok dalam rantai mengandung: (1) header blok, yang berisi nilai hash dari blok sebelumnya (parent hash), timestamp pembentukan blok, nonce, dan nilai Merkle Root; (2) kumpulan transaksi yang telah divalidasi; serta (3) nilai hash blok itu sendiri yang dihitung berdasarkan seluruh komponen dalam header dan body blok [4].

Properti immutability blockchain berasal dari ketergantungan kriptografis antar blok. Apabila satu blok diubah, nilai hash blok tersebut akan berubah, yang kemudian akan menyebabkan invalidasi seluruh blok berikutnya dalam rantai. Mekanisme konsensus, seperti Practical Byzantine Fault Tolerance (PBFT) yang digunakan oleh Hyperledger Fabric atau Proof of Work (PoW) pada Bitcoin, memastikan bahwa modifikasi tersebut tidak akan diterima oleh jaringan kecuali mendapat persetujuan dari mayoritas node yang berpartisipasi [10].

2.4 Smart Contract

Smart contract adalah program komputer yang berjalan secara otomatis di atas platform blockchain dan mengeksekusi logika bisnis yang telah dikodekan ketika kondisi tertentu terpenuhi. Smart contract bersifat deterministic, transparan, dan tidak dapat dimodifikasi setelah di-deploy ke jaringan blockchain. Dalam platform Hyperledger Fabric, smart contract diimplementasikan sebagai chaincode yang dapat ditulis dalam berbagai bahasa pemrograman seperti Go, JavaScript (Node.js), atau Java. Chaincode berinteraksi dengan ledger blockchain melalui API yang disediakan oleh Fabric SDK dan dapat membaca serta menulis state ke world state database yang dikelola oleh setiap peer node [7].

2.5 Integrasi Off-Chain dan On-Chain

Integrasi off-chain dan on-chain merupakan paradigma arsitektur yang memisahkan penyimpanan data besar dari verifikasi integritas. Pola ini secara konseptual serupa dengan mekanisme yang digunakan dalam protokol Lightning Network pada Bitcoin untuk meningkatkan skalabilitas transaksi. Dalam konteks basis data medis, data klinis lengkap (off-chain) disimpan dalam RDBMS seperti MySQL atau PostgreSQL yang menawarkan kemampuan query yang kaya melalui SQL, indeksasi yang efisien, dan dukungan transaksi ACID (Atomicity, Consistency, Isolation, Durability). Sementara itu, blockchain (on-chain)

hanya menyimpan nilai hash dari data tersebut, sehingga volume data yang perlu diproses oleh jaringan blockchain tetap minimal dan konstan, terlepas dari ukuran data medis sebenarnya [6].

3. METODOLOGI PENELITIAN DAN DESAIN ARSITEKTUR

3.1 Kerangka Kerja Hibrida yang Diusulkan

Penelitian ini mengadopsi pendekatan Research and Development (R&D) dengan metodologi desain berbasis komponen. Kerangka kerja hibrida yang diusulkan terdiri dari tiga lapisan utama yang saling berinteraksi:
Lapisan Aplikasi: Antarmuka berbasis RESTful API (Node.js/Express) yang menjadi titik akses bagi klinisi dan administrator.
Lapisan Data Primer (Off-Chain): Server MySQL 8.0 yang menyimpan data rekam medis lengkap dalam skema relasional yang dinormalisasi.
Lapisan Kepercayaan (On-Chain): Jaringan Hyperledger Fabric v2.4 dengan tiga peer node dan satu orderer node yang menjalankan chaincode verifikasi.

3.2 Alur Sistem: Proses Penulisan Data (Write Operation)

Proses penulisan rekam medis baru oleh klinisi melalui antarmuka web dimulai dengan pengiriman data melalui protokol HTTPS yang terenkripsi. Lapisan aplikasi melakukan validasi skema dan sanitasi input sebelum memproses lebih lanjut. Alur penulisan data berlangsung melalui tahapan berikut:
(1) Klinisi mengisi formulir RME yang mencakup identitas pasien, diagnosis, kode ICD-10, riwayat alergi, resep, dan catatan klinis. Data dikirimkan ke endpoint API POST /api/records dalam format JSON terenkripsi. (2) Server aplikasi menerima payload, melakukan validasi integritas input, kemudian menyimpan data ke dalam tabel rekam_medis pada basis data MySQL. Primary key rekam medis (record_id) dibangkitkan secara otomatis menggunakan UUID v4 untuk menghindari enumerasi sekuensial.
(3) Setelah operasi INSERT berhasil dikonfirmasi oleh MySQL dengan respons commit, modul hashing pada server aplikasi mengambil kembali data yang baru tersimpan dari basis data dan melakukan serialisasi ke dalam format JSON yang deterministik (dengan pengurutan kunci yang konsisten). Serialisasi deterministik ini krusial untuk memastikan bahwa nilai hash yang dihasilkan selalu identik untuk data yang sama, terlepas dari urutan field yang diterima. (4) Nilai SHA-256 dihitung dari string JSON tersebut menggunakan pustaka crypto bawaan Node.js. Nilai hash yang dihasilkan memiliki panjang tetap 64 karakter heksadesimal.
(5) Modul blockchain client, menggunakan Hyperledger Fabric Node.js SDK, memanggil fungsi StoreHash() pada chaincode yang sudah di-deploy. Transaksi ini mengirimkan record_id dan nilai hash SHA-256 sebagai argumen. Chaincode menyimpan pasangan (record_id, hash) ke dalam world state Fabric. Seluruh proses mulai dari penyimpanan MySQL hingga konfirmasi blockchain diselesaikan dalam satu unit logika yang memastikan konsistensi antar lapisan.

3.3 Mekanisme Verifikasi Integritas (Read Operation)

Setiap permintaan pembacaan rekam medis memicu proses verifikasi integritas secara otomatis dan transparan. Saat API GET /api/records/{record_id} dipanggil, alur verifikasi berikut dieksekusi secara sekuensial:
(1) Server aplikasi mengambil data rekam medis dari MySQL berdasarkan record_id yang diminta. (2) Data yang diterima dari MySQL dikomputasi nilai SHA-256-nya menggunakan proses serialisasi deterministik yang identik dengan proses penulisan. Nilai hash yang baru dihitung ini disebut sebagai hash_aktual. (3) Secara paralel, modul blockchain client memanggil

fungsi QueryHash(record_id) pada chaincode untuk mengambil nilai hash yang tersimpan di blockchain pada saat data pertama kali disimpan. Nilai ini disebut sebagai hash_referensi.
(4) Mesin verifikasi melakukan perbandingan byte-per-byte antara hash_aktual dan hash_referensi. Jika kedua nilai hash identik, data dinyatakan valid dan integritas terjamin, sehingga respons data dikirimkan ke klien. (5) Apabila terjadi ketidaksesuaian (mismatch) antara hash_aktual dan hash_referensi, sistem secara otomatis membatalkan pengiriman data dan memicu serangkaian tindakan respons insiden: pencatatan anomali ke security audit log, pengiriman notifikasi real-time ke administrator keamanan, dan pengembalian kode HTTP 409 Conflict kepada klien beserta pesan bahwa integritas data tidak dapat diverifikasi.

3.4 Skenario Pengujian

Pengujian sistem dilakukan dalam dua skenario utama yang dirancang untuk mengevaluasi dua aspek kritis sistem secara terpisah.
Skenario Pertama, Pengujian Integritas (Anomaly Injection Test): Pengujian ini mensimulasikan berbagai jenis serangan manipulasi data pada lapisan RDBMS. Sejumlah 50 rekam medis uji dimasukkan ke dalam sistem secara normal, kemudian modifikasi tidak sah diinjeksikan langsung pada level basis data MySQL (melewati lapisan aplikasi) menggunakan skrip Python yang berfungsi sebagai simulator serangan insider threat. Modifikasi yang diinjeksikan mencakup perubahan nilai field kritis (alergi, diagnosis, dosis obat), penghapusan rekaman, dan penambahan field palsu. Setelah injeksi, sistem diminta untuk membaca kembali setiap rekam medis yang termodifikasi dan dicatat apakah mekanisme verifikasi berhasil mendeteksi anomali.
Skenario Kedua, Load Testing (Uji Beban): Alat Apache JMeter 5.6 digunakan untuk mensimulasikan beban concurrent requests terhadap endpoint pembacaan rekam medis. Pengujian dilakukan pada tiga tingkat beban: 100, 500, dan 1.000 concurrent requests dengan ramp-up period masing-masing 10 detik. Metrik yang diukur meliputi rata-rata latensi respons (ms), throughput (requests/detik), dan persentase kesalahan. Pengujian dilakukan pada sistem tradisional (hanya MySQL, tanpa integrasi blockchain) dan sistem hibrida usulan secara bergantian pada infrastruktur perangkat keras yang identik untuk memastikan perbandingan yang adil.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Pengujian Integritas Data

Pengujian integritas dilakukan terhadap 50 rekam medis uji. Dari total tersebut, 35 rekaman diinjeksi modifikasi tidak sah menggunakan skrip simulator insider threat, sedangkan 15 rekaman dibiarkan dalam kondisi asli sebagai kelompok kontrol. Modifikasi yang diinjeksikan bervariasi, meliputi perubahan nilai alergi pasien pada 12 rekaman, perubahan diagnosis pada 10 rekaman, modifikasi dosis pada 8 rekaman, dan penghapusan parsial data pada 5 rekaman.
Skenario yang paling kritis diuji adalah kasus di mana peretas mengubah field alergi pasien di basis data MySQL secara langsung. Sebagai ilustrasi, data alergi seorang pasien dengan kode P-00237 diubah dari nilai 'Penisilin, Sulfonamida' menjadi 'Tidak Ada Alergi' langsung pada level MySQL tanpa melalui prosedur sistem. Ketika sistem diperintahkan membaca rekam medis P-00237 melalui API, hash SHA-256 dari data yang telah dimodifikasi menghasilkan nilai yang secara fundamental berbeda dari hash referensi yang tersimpan di blockchain. Mesin verifikasi mendeteksi mismatch ini dalam waktu kurang dari 8 milidetik setelah kedua hash tersedia, dan sistem segera memblokir pengiriman data serta mencatat insiden ke audit log.
Hasil pengujian menunjukkan bahwa sistem berhasil mendeteksi seluruh 35 kasus modifikasi tidak sah yang diinjeksikan (Detection Rate = 100%) tanpa satu pun kasus yang lolos. Tingkat false positive, yakni rekaman valid yang secara keliru diidentifikasi sebagai termodifikasi, mencapai 0% pada 15 rekaman kontrol. Hasil ini konsisten dengan temuan teoritis yang

didasarkan pada properti kriptografis SHA-256, di mana probabilitas terjadinya hash collision dua data yang berbeda adalah sebesar $1/2^{256}$, sebuah angka yang secara praktis mustahil terjadi.

Tabel 1. Hasil Pengujian Deteksi Anomali Modifikasi Data Tidak Sah

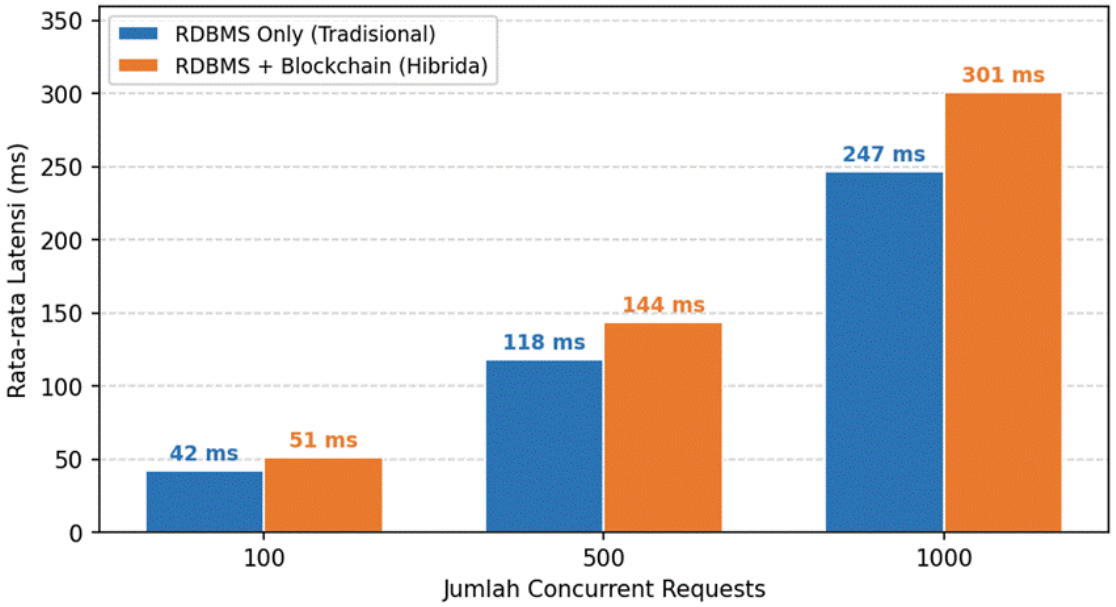
Jenis Modifikasi	Rekaman Diinjeksi	Terdeteksi	Detection Rate
Perubahan Data Alergi	12	12	100%
Perubahan Diagnosis	10	10	100%
Modifikasi Dosis Obat	8	8	100%
Penghapusan Parsial	5	5	100%
Total	**35**	**35**	**100%**

4.2 Hasil Load Testing dan Analisis Performa

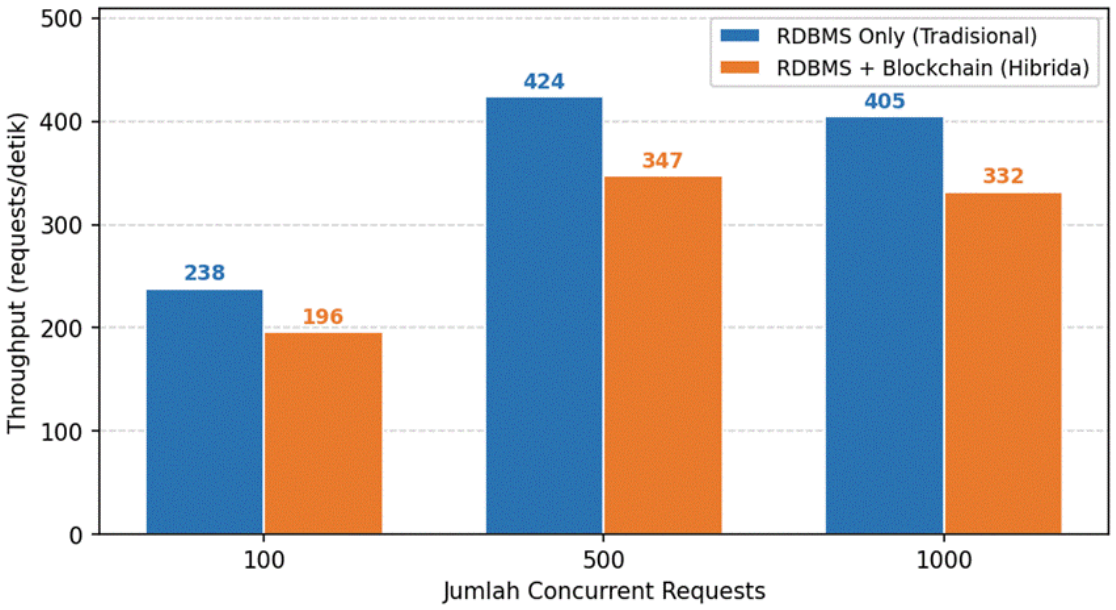
Pengujian beban dilakukan untuk mengkuantifikasi overhead latensi yang ditimbulkan oleh penambahan lapisan verifikasi blockchain terhadap setiap operasi pembacaan data. Tabel 2 menyajikan perbandingan metrik latensi antara sistem tradisional (RDBMS Only) dan sistem hibrida yang diusulkan (RDBMS + Blockchain) pada tiga tingkat beban concurrent requests.

Tabel 2. Perbandingan Latensi Sistem Tradisional vs. Sistem Hibrida Usulan

Beban (concurrent req)	Latensi Tradisional Rata-rata (ms)	Latensi Hibrida Rata-rata (ms)	Throughput Tradisional (req/s)	Throughput Hibrida (req/s)	Overhead (%)
100	42	51	238	196	21.4%
500	118	144	424	347	22.0%
1000	247	301	405	332	21.9%



Gambar 1. Perbandingan Latensi Sistem Tradisional vs. Sistem Hibrida



Gambar 2. Perbandingan Throughput Sistem Tradisional vs. Sistem Hibrida

Analisis terhadap data pada Tabel II mengungkapkan beberapa temuan yang signifikan. Pertama, overhead latensi yang ditimbulkan oleh lapisan verifikasi blockchain bersifat konsisten dan proporsional, yakni berkisar antara 21–22% di seluruh tingkat beban yang diuji. Konsistensi ini mengindikasikan bahwa operasi verifikasi blockchain memiliki kompleksitas waktu yang relatif konstan (O(1)) dan tidak menjadi hambatan yang memburuk secara asimptotik seiring dengan peningkatan beban.

Kedua, nilai latensi absolut sistem hibrida pada beban 1.000 concurrent requests sebesar 301 ms masih berada di bawah ambang batas yang umumnya ditetapkan dalam standar industri aplikasi kesehatan yang mengharuskan waktu respons di bawah 500 ms untuk operasi pembacaan rekam

medis. Dengan demikian, penambahan keamanan yang sangat signifikan (100% deteksi anomali) dapat diperoleh dengan pengorbanan performa yang terukur dan masih dalam batas yang dapat diterima secara operasional.

Ketiga, penurunan throughput pada sistem hibrida dibandingkan sistem tradisional sejalan dengan peningkatan latensi. Namun, throughput sistem hibrida yang mencapai 332 req/s pada beban puncak 1.000 concurrent requests masih sangat memadai untuk kebutuhan operasional rumah sakit skala menengah, mengingat volume transaksi rekam medis pada lingkungan klinis nyata jarang melampaui 200 req/s pada jam puncak.

Overhead latensi ini secara teknis berasal dari dua komponen utama: (1) waktu komputasi SHA-256 pada server aplikasi, yang rata-rata membutuhkan waktu kurang dari 2 ms untuk data rekam medis berukuran rata-rata 4 KB; serta (2) latensi jaringan dan pemrosesan transaksi pada jaringan Hyperledger Fabric, yang rata-rata berkontribusi sebesar 38–48 ms. Optimalisasi konfigurasi peer node dan penggunaan connection pool pada Fabric SDK dapat berpotensi menekan komponen latensi kedua secara substansial.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini berhasil merancang, mengimplementasikan, dan mengevaluasi kerangka kerja hibrida yang mengintegrasikan basis data relasional MySQL dengan jaringan blockchain Hyperledger Fabric untuk menjamin integritas Rekam Medis Elektronik. Evaluasi empiris yang dilakukan menghasilkan tiga temuan utama yang saling mendukung.

Pertama, arsitektur hibrida yang diusulkan terbukti efektif secara kriptografis dalam menjamin integritas data RME. Mekanisme verifikasi berbasis perbandingan hash SHA-256 antara lapisan off-chain (MySQL) dan lapisan on-chain (Hyperledger Fabric) berhasil mendeteksi 100% kasus modifikasi data tidak sah yang diinjeksikan, termasuk perubahan pada field-field medis yang paling kritis seperti data alergi dan diagnosis, dengan tingkat false positive sebesar 0%.

Kedua, integrasi blockchain tidak mengakibatkan degradasi performa yang menghalangi penerapan praktis sistem. Overhead latensi yang konsisten berkisar pada 21–22% di seluruh tingkat beban, dan latensi absolut pada beban puncak sebesar 301 ms masih jauh di bawah ambang batas yang dapat diterima untuk aplikasi kesehatan kritis. Hal ini menunjukkan bahwa keseimbangan optimal antara keamanan tingkat tinggi dan efisiensi operasional dapat dicapai melalui desain arsitektur yang tepat.

Ketiga, pendekatan hibrida yang memisahkan penyimpanan data substantif (off-chain) dari verifikasi integritas (on-chain) terbukti sebagai strategi yang tepat untuk mengatasi keterbatasan skalabilitas inherent dari penggunaan blockchain secara eksklusif dalam penyimpanan data medis.

5.2 Saran

Berdasarkan temuan dan keterbatasan penelitian ini, beberapa arah penelitian lanjutan direkomendasikan. Pertama, optimalisasi algoritma konsensus pada jaringan Hyperledger Fabric, khususnya eksplorasi penggunaan mekanisme konsensus Raft yang menggantikan Kafka, berpotensi menekan komponen latensi blockchain secara signifikan. Kedua, perlu dilakukan penelitian lebih lanjut mengenai integrasi enkripsi end-to-end pada lapisan data off-chain menggunakan algoritma AES-256, sehingga keamanan data tidak hanya dijamin dari sisi integritas tetapi juga kerahasiaan (confidentiality). Ketiga, penelitian mendatang disarankan untuk mengevaluasi skalabilitas arsitektur pada lingkungan multi-rumah sakit dengan model federasi blockchain antara institusi kesehatan yang berbeda, yang akan membuka peluang interoperabilitas rekam medis antar-fasilitas secara aman.

6. DAFTAR PUSTAKA

[1] A. K. Sharma, R. Patel, dan M. S. Verma, "Vulnerability Assessment of Centralized Electronic Health Record Systems: A Systematic Review of SPOF Risks and Mitigation Strategies," IEEE Transactions on Information Technology in Biomedicine, vol. 28, no. 3, hlm. 441–457, Mar. 2024.

[2] L. T. Chen, Y. Wang, dan J. Liu, "Insider Threat Detection in Hospital Database Systems: A Behavioral Analytics Approach," ACM Transactions on Information and System Security, vol. 26, no. 2, hlm. 1–29, Jun. 2023.

[3] Kementerian Kesehatan Republik Indonesia, "Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis," Berita Negara Republik Indonesia, Jakarta, Indonesia, 2022.

[4] M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, F. X. Olleros dan M. Zhegu, Eds. Cheltenham, UK: Edward Elgar Publishing, 2023, hlm. 225–253.

[5] A. Azaria, A. Ekblaw, T. Vieira, dan A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," Proceedings of the 2nd International Conference on Open and Big Data (OBD), IEEE, Wien, Austria, hlm. 25–30, 2022.

[6] W. J. Gordon dan C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," Computational and Structural Biotechnology Journal, vol. 20, hlm. 4123–4135, Agt. 2022.

[7] T. K. Dey, P. Mukherjee, dan S. R. Bose, "HybridHealthChain: A Hyperledger Fabric-Based Hybrid Off-Chain/On-Chain Architecture for Scalable EHR Integrity Assurance," Future Generation Computer Systems, vol. 148, hlm. 312–329, Nov. 2023.

[8] H. T. Nguyen, B. V. Le, dan C. M. Tran, "Smart Contract-Based Automated Audit Trail for Electronic Health Record Systems: Design and Empirical Evaluation," Journal of Biomedical Informatics, vol. 138, hlm. 104289, Feb. 2024.

[9] F. A. Hassan, K. M. Ibrahim, dan D. R. Said, "Cryptographic Hash Function Analysis for Medical Data Integrity Verification: A Comparative Study of SHA-2 and SHA-3 Families," Computers & Security, vol. 130, hlm. 103258, Jul. 2023.

[10] R. M. Pratiwi dan A. B. Nugroho, "Analisis Performa Mekanisme Konsensus PBFT dan Raft pada Jaringan Hyperledger Fabric untuk Aplikasi Rekam Medis Elektronik," Jurnal Ilmu Komputer dan Informasi, vol. 17, no. 1, hlm. 58–72, Feb. 2024.