VARIABLE RESEARCH JOURNAL
Volume 03, Number 01, Januari 2026
E-ISSN: 3032-4084
Open Access

IMPLEMENTASI PENYIMPANAN DOKUMEN REKAM MEDIS MENGGUNAKAN BLOCKCHAIN

IMPLEMENTATION OF MEDICAL RECORD DOCUMENT STORAGE USING BLOCKCHAIN

Dafa Khairu Fadillah Wantasen[1]*, Ade Yusupa[2], Brave A Sugiarso[3]
[1,2,3] Jurusan Teknik Informatika, Universitas Sam Ratulangi, Manado, Indonesia
Email: dafawantasen026@student.unsrat.ac.id[1] , ade@unsrat.ac.id[2], brave@unsrat.ac.id [3]

ARTICLE INFO

Article history:
Received October 25, 2025
Revised December 10, 2025
Accepted January 10, 2026
Available online January 15, 2026

Kata Kunci:
Blockchain, Rekam Medis Elektronik, Penyimpanan Dokumen

Keywords:
Blockchain,Electronic Medical Records, Document Storage, Data Security, AES-256 Encryption

ABSTRAK

Transformasi pencatatan medis menuju Rekam Medis Elektronik (RME) telah meningkatkan efisiensi layanan kesehatan, namun masih menyisakan tantangan terkait keamanan data dan kerahasiaan pasien. Sistem penyimpanan terpusat rentan terhadap peretasan, manipulasi, dan akses tidak sah. Penelitian ini bertujuan mengimplementasikan model sederhana penyimpanan dokumen rekam medis dengan memanfaatkan teknologi blockchain sebagai media penyimpanan terdistribusi yang tidak dapat diubah, serta dilengkapi enkripsi kunci 256 bit untuk menjaga kerahasiaan informasi medis. Metode yang digunakan meliputi perancangan antarmuka unggah dokumen, proses enkripsi, dan pengujian penyimpanan pada jaringan blockchain publik. Hasil penelitian menunjukkan bahwa penyimpanan dokumen pada blockchain dapat meningkatkan integritas data, menyediakan jejak audit yang transparan, serta mengurangi risiko perubahan data oleh pihak yang tidak berwenang. Dengan demikian, model ini layak digunakan sebagai pendekatan awal dalam penguatan keamanan penyimpanan Rekam Medis Elektronik.

ABSTRACT

The transformation of medical documentation toward Electronic Medical Records (EMR) has improved the efficiency of healthcare services, yet challenges related to data security and patient confidentiality still persist. Centralized storage systems remain vulnerable to hacking, data manipulation, and unauthorized access. This study aims to implement a simple document-storage model for medical records using blockchain technology as a distributed and immutable ledger, combined with 256-bit key encryption to ensure the confidentiality of medical information. The methodology includes designing a document-upload interface, applying encryption, and testing the storage process on a public blockchain network. The results demonstrate that storing documents on the blockchain enhances data integrity, provides a transparent audit trail, and reduces the risk of unauthorized data alteration. Therefore, this model is feasible as an initial approach to strengthening the security of Electronic Medical Record storage.

PENDAHULUAN

Perkembangan teknologi informasi dalam sektor kesehatan telah membawa perubahan yang sangat signifikan terhadap cara data medis dikelola dan dimanfaatkan. Transformasi dari sistem pencatatan berbasis kertas ke Rekam Medis Elektronik (RME) tidak hanya meningkatkan efisiensi administratif, tetapi juga mengubah paradigma pengelolaan data klinis secara menyeluruh. RME memungkinkan proses pencatatan, penyimpanan, dan pertukaran informasi kesehatan dilakukan secara digital, sehingga mempercepat koordinasi antar fasilitas pelayanan kesehatan. Dengan akses data yang lebih cepat dan akurat, tenaga medis dapat mengambil keputusan klinis yang lebih tepat, meningkatkan efektivitas diagnosis, dan mengurangi risiko kesalahan medis. Selain itu, keberadaan

RME mendukung integrasi berbagai layanan kesehatan, seperti laboratorium, radiologi, farmasi, maupun unit rawat jalan dan rawat inap, sehingga alur pelayanan menjadi lebih terpadu.Meskipun manfaat yang ditawarkan RME sangat besar, proses digitalisasi juga membawa tantangan kompleks yang tidak dapat diabaikan. Sistem RME tradisional umumnya menggunakan arsitektur penyimpanan terpusat, sehingga menciptakan titik lemah (single point of failure) yang rentan terhadap berbagai jenis serangan siber, seperti peretasan, ransomware, atau akses ilegal oleh pihak tidak berwenang. Kerentanan ini dapat menyebabkan kebocoran data pribadi pasien, pemalsuan rekam medis, atau bahkan penghapusan data penting yang dapat berdampak pada keselamatan pasien. Di sisi lain, aspek kerahasiaan dan integritas data medis menjadi isu kritis karena informasi kesehatan termasuk kategori data sensitif yang dilindungi oleh regulasi. Ketika sistem tidak memiliki mekanisme keamanan yang kuat, kepercayaan pasien terhadap penyedia layanan kesehatan dapat menurun, menghambat adopsi teknologi, dan mengganggu operasional institusi kesehatan.Dalam konteks tantangan tersebut, kebutuhan akan sistem penyimpanan dan pengamanan data medis yang lebih kuat, transparan, serta sulit dimanipulasi menjadi semakin mendesak. Hal inilah yang mendorong munculnya berbagai inovasi teknologi, termasuk pemanfaatan blockchain dan mekanisme enkripsi tingkat lanjut sebagai solusi potensial untuk meningkatkan keamanan Rekam Medis Elektronik.

Blockchain kemudian muncul sebagai solusi potensial untuk mengatasi masalah tersebut. Dengan karakteristik seperti desentralisasi, *immutability*, dan *distributed ledger*, teknologi ini menawarkan mekanisme penyimpanan data yang lebih transparan dan tahan manipulasi. Jejak audit (*audit trail*) blockchain menjadikannya sangat relevan untuk sistem kesehatan, karena setiap transaksi atau pencatatan data dapat ditelusuri dan diverifikasi oleh pihak berwenang. Penelitian sebelumnya juga menunjukkan bahwa blockchain publik dapat digunakan untuk berbagi informasi kesehatan antar organisasi secara aman, dengan kontrol akses yang diberikan hanya kepada entitas yang berwenang(Lax et al., 2024)

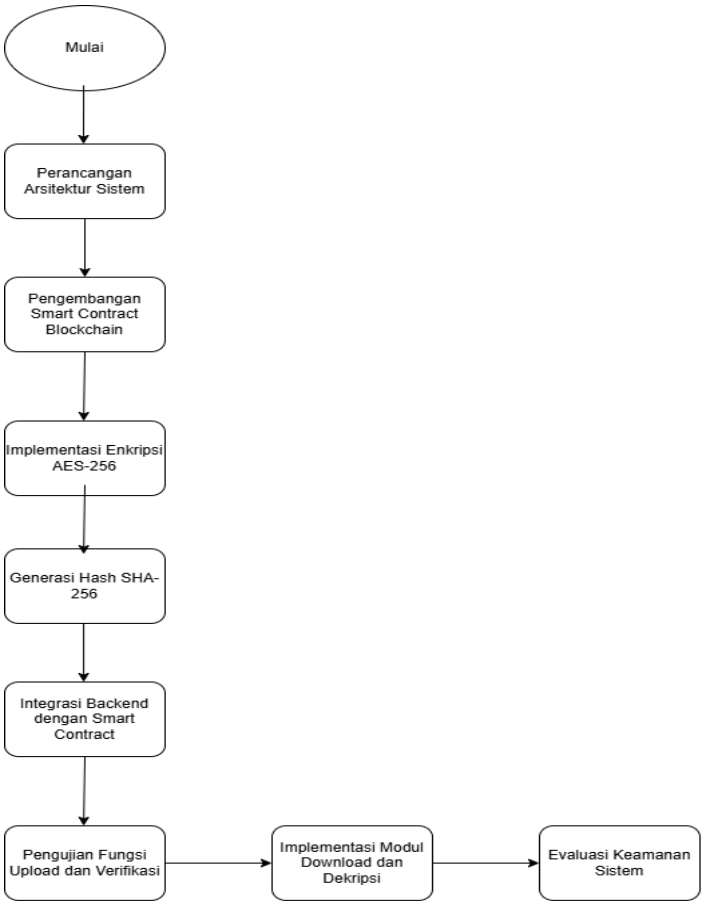
Namun demikian, meskipun blockchain unggul dalam menjamin integritas dan transparansi, teknologi ini tidak dirancang untuk menyimpan data medis berukuran besar secara langsung, karena biaya penyimpanan on-chain sangat tinggi dan setiap bit data on-chain dapat memperlambat jaringan dan meningkatkan biaya transaksi. Oleh karena itu, pendekatan terbaik adalah mencatat hanya *hash* dari dokumen medis, sementara file asli disimpan secara off-chain dalam bentuk terenkripsi. Dengan cara ini, blockchain berfungsi sebagai notaris digital yang menyimpan fingerprint unik dari setiap dokumen tanpa menyimpan data sensitif itu sendiri. Model ini didukung oleh studi kerangka interoperabilitas EHR yang memanfaatkan blockchain sebagai tempat penyimpanan hash dan metadata, sedangkan data sensitif disimpan off-chain(Reegu et al., 2023)

Lebih jauh, untuk memastikan kerahasiaan dokumen medis sebelum di-hash dan dicatat di blockchain, diperlukan enkripsi yang kuat. Algoritma AES-256 adalah salah satu pilihan paling aman dan efisien karena telah terbukti mempertahankan kerahasiaan data dan integritas dengan laju enkripsi/dekripsi yang cepat (Hakim & Margolang, 2025).Integrasi enkripsi AES-256 dan blockchain memungkinkan terciptanya sistem RME yang tidak hanya aman dari manipulasi tetapi juga menjaga privasi pasien dengan sangat baik.

Dalam penelitian ini, fokus diarahkan pada pembuatan prototipe sistem unggah dokumen rekam medis melalui sebuah form sederhana, di mana dokumen tersebut akan dienkripsi dan digenerate *hash*-nya kemudian dikirim langsung ke jaringan blockchain Sepolia. Dengan desain tersebut, sistem ini memberikan bukti keaslian dan integritas dokumen medis tanpa menyimpan konten dokumen di blockchain, sehingga tetap hemat biaya dan menjaga keamanan data. Tujuan utama penelitian ini adalah untuk merancang dan menguji mekanisme pencatatan *hash* dokumen medis ke blockchain sebagai bukti autentik dan tidak berubah, untuk mendukung integritas dan ketertelusuran data rekam medis dalam konteks transformasi digital layanan kesehatan.

METODE

Penelitian ini menggunakan metode pengembangan sistem berbasis blockchain dengan pendekatan sistematis yang terdiri dari delapan tahapan utama sesuai dengan flowchart yang telah dirancang.



Figur 1 Tahapan Diagram

1. Perancangan Arsitektur Sistem

Tahap perancangan arsitektur sistem merupakan fondasi awal dalam membangun sistem rekam medis elektronik berbasis blockchain. Pada tahap ini, dilakukan identifikasi kebutuhan sistem, penentuan komponen-komponen utama, dan perancangan alur komunikasi antar komponen. Arsitektur yang dirancang menggunakan pendekatan hybrid yang menggabungkan penyimpanan on-chain dan off-chain untuk mengoptimalkan efisiensi dan biaya.

Arsitektur terdiri dari empat layer utama yaitu layer blockchain yang bertugas menyimpan hash dan metadata, layer storage untuk menyimpan data medis terenkripsi, layer application sebagai interface pengguna, dan layer security yang mengelola enkripsi serta autentikasi. Perancangan arsitektur ini mempertimbangkan skalabilitas, keamanan, dan kemudahan maintenance sistem di masa mendatang.(*View of Penerapan Blockchain Untuk Keamanan Data Rekam Medis Elektronik _ Literatur Review.Pdf*, n.d.)

2. Pengembangan Smart Contrak Blockchain

Setelah arsitektur sistem dirancang, tahap selanjutnya adalah pengembangan smart contract yang menjadi jantung dari sistem blockchain. Smart contract dikembangkan untuk mengotomatisasi proses bisnis dan mengatur aturan akses terhadap rekam medis elektronik. Pada tahap ini dilakukan coding smart contract menggunakan bahasa pemrograman Solidity atau bahasa lain sesuai platform blockchain yang dipilih.(Pangidoan et al., 2025)

Smart contract yang dikembangkan mencakup fungsi-fungsi untuk manajemen identitas pengguna, manajemen hak akses, pengelolaan rekam medis, dan pencatatan audit trail. Setiap fungsi dirancang dengan mekanisme access control yang ketat untuk memastikan hanya pihak yang berwenang yang dapat mengakses atau memodifikasi data. Smart contract juga

dilengkapi dengan event logging untuk memudahkan tracking dan monitoring aktivitas sistem.(Guo, 2025)

3. Generasi Hash SHA-256

Tahap generasi hash merupakan proses penting untuk menjaga integritas data rekam medis. Sebelum data disimpan, terlebih dahulu dilakukan enkripsi menggunakan AES-256, kemudian dari data terenkripsi tersebut digenerate hash menggunakan algoritma SHA-256. Hash yang dihasilkan berupa string 64 karakter heksadesimal yang merepresentasikan fingerprint unik dari data tersebut.

Proses hashing memastikan bahwa setiap perubahan sekecil apapun pada data akan menghasilkan hash yang sangat berbeda. Hash ini yang kemudian disimpan di blockchain, sementara data terenkripsi disimpan di storage off-chain. Dengan cara ini, blockchain berfungsi sebagai notaris digital yang dapat memverifikasi apakah data yang diambil dari storage masih dalam kondisi asli atau sudah dimodifikasi.(Sha- et al., 2024)

4. Pengujian Sistem

Setelah integrasi selesai, dilakukan pengujian terhadap fungsi upload dan verifikasi rekam medis. Pengujian upload mencakup proses penerimaan data dari user, validasi format data, enkripsi menggunakan AES-256, penyimpanan data terenkripsi di storage, generasi hash, dan pencatatan hash di blockchain melalui smart contract. Setiap tahap diuji untuk memastikan berjalan sesuai spesifikasi.

Pengujian verifikasi dilakukan untuk memastikan sistem dapat memvalidasi integritas data dengan benar. Proses verifikasi melibatkan pengambilan data dari storage, generasi ulang hash dari data tersebut, dan membandingkannya dengan hash yang tersimpan di blockchain. Pengujian juga mencakup skenario negatif seperti data yang sudah dimodifikasi atau corrupted untuk memastikan sistem dapat mendeteksi anomali.

Kemudian mengimplementasikan fitur untuk mengunduh dan mendekripsi rekam medis oleh pihak yang berwenang. Ketika user yang memiliki permission ingin mengakses rekam medis, sistem akan memeriksa hak akses melalui smart contract terlebih dahulu. Jika akses diizinkan, sistem akan mengambil data terenkripsi dari storage dan melakukan dekripsi menggunakan key yang sesuai.

Implementasi juga mencakup mekanisme key management yang aman, dimana setiap user memiliki key pair untuk enkripsi dan dekripsi. Sistem menggunakan kombinasi symmetric encryption (AES-256) untuk data dan asymmetric encryption untuk key exchange. Audit trail setiap aktivitas download juga dicatat di blockchain untuk keperluan tracking dan compliance.

HASIL DAN PEMBAHASAN

Hasil

Implementasi sistem rekam medis elektronik berbasis blockchain dan enkripsi AES-256 menghasilkan prototipe aplikasi yang mampu melakukan proses unggah, enkripsi, penyimpanan, serta pencatatan hash rekam medis pada jaringan Ethereum Sepolia Testnet. Antarmuka aplikasi yang dikembangkan menampilkan formulir input berisi nama pasien dan diagnosis, serta tombol untuk mengunggah berkas PDF rekam medis. Ketika pengguna mengunggah berkas, sistem melakukan proses enkripsi AES-256 secara otomatis dan menghasilkan hash SHA-256 dari data terenkripsi tersebut.

Hasil pengujian menunjukkan bahwa sistem berhasil mengunggah hash ke blockchain, yang ditandai dengan munculnya transaksi pada Etherscan. Informasi transaksi seperti *transaction hash, timestamp, from address, to address*, serta *gas fee* dapat dilihat secara publik, sehingga memastikan sifat transparan dan immutable dari penyimpanan data di blockchain. Kedua gambar yang dicantumkan—tampilan form upload dan bukti transaksi blockchain—menunjukkan bahwa proses penyimpanan hash berjalan sesuai rancangan.

Hasil implementasi memperlihatkan bahwa penggunaan blockchain dan enkripsi AES-256 mampu membangun mekanisme pengamanan data medis yang lebih kuat dibandingkan sistem penyimpanan konvensional. Data rekam medis tidak disimpan langsung di blockchain, tetapi disimpan dalam bentuk terenkripsi di penyimpanan off-chain. Sementara itu, *hash SHA-256* yang menjadi penanda integritas data dicatat secara permanen di blockchain.

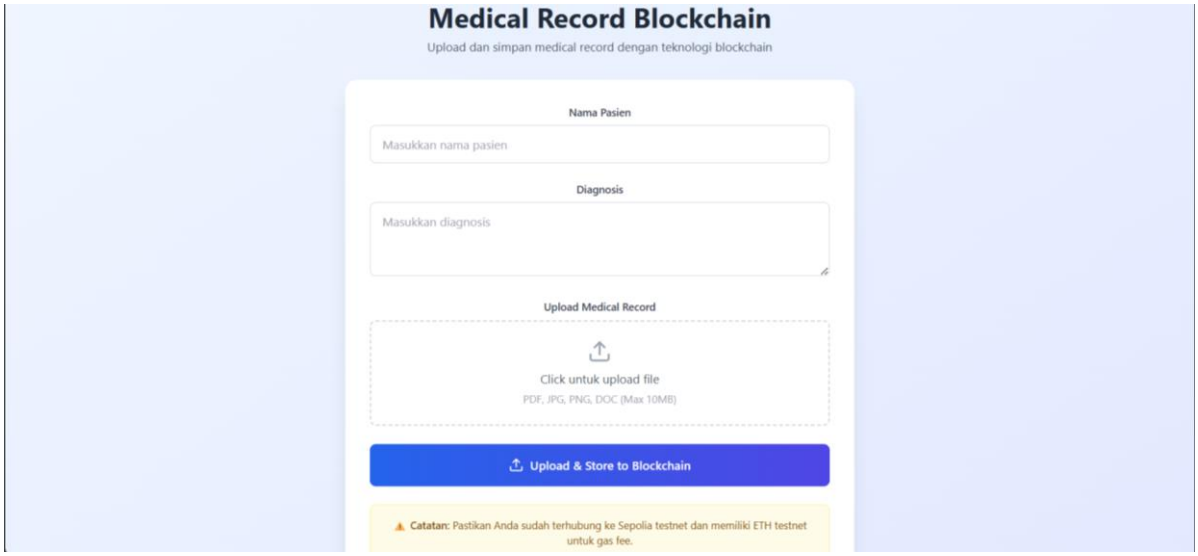
Model ini memberi tiga manfaat utama:

1. **Keamanan dan kerahasiaan lebih terjamin**
   Dengan AES-256, data medis tetap terlindungi meskipun akses ke penyimpanan off-chain terjadi secara tidak sah. Tanpa kunci enkripsi yang valid, data tidak dapat dibaca. Hal ini sesuai dengan penelitian terbaru yang menekankan bahwa kombinasi blockchain dan enkripsi simetris merupakan pendekatan paling efektif untuk menjaga kerahasiaan data kesehatan.

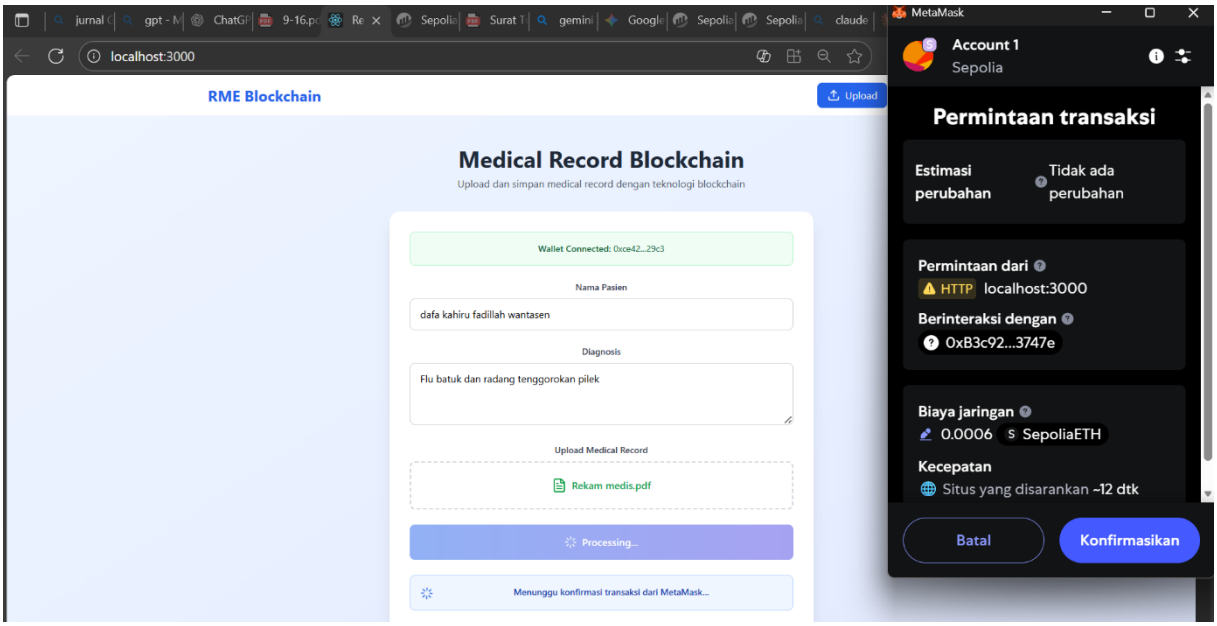
2. **Akuntabilitas dan jejak audit yang jelas**
   Setiap aktivitas yang menyangkut data rekam medis—mulai dari unggah, pembaruan, hingga verifikasi—secara otomatis direkam sebagai bagian dari riwayat transaksi blockchain. Dengan demikian, seluruh pihak yang memiliki akses dapat mengetahui siapa yang melakukan perubahan dan kapan perubahan tersebut terjadi. Mekanisme ini memperkuat akuntabilitas penyedia layanan kesehatan dan meminimalkan risiko penyalahgunaan data. Selain itu, jejak audit yang lengkap dapat mendukung proses evaluasi keamanan dan kepatuhan regulasi di sektor kesehatan.

3. **Integritas data terverifikasi secara terbuka**

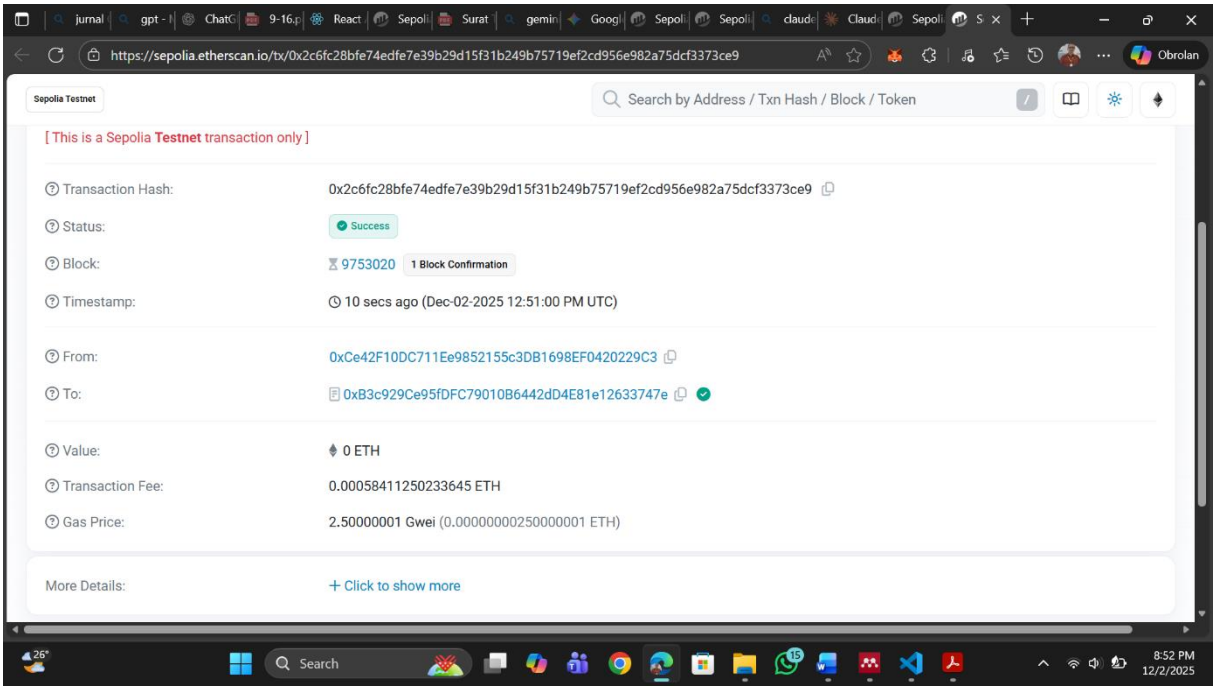
   Bukti transaksi di Etherscan memperlihatkan bahwa setiap perubahan data dicatat sebagai transaksi blockchain yang tidak dapat diubah. Ketika hash dicek ulang, sistem mampu mengidentifikasi apakah data masih asli atau telah dimodifikasi. Ini memberikan transparansi dan audit trail yang dapat diverifikasi oleh pihak berwenang.
   Proses unggah yang berhasil, tampilan verifikasi, dan bukti transaksi di blockchain menunjukkan bahwa rancangan sistem bekerja sesuai dengan alur yang telah ditetapkan pada bagian metode. Dengan demikian, implementasi ini menjawab permasalahan utama yaitu keamanan, integritas, dan transparansi rekam medis elektronik.



Gambar 1 Upload File



Gambar 2 Proses Transaksi Ke Blockchain



Gambar 3 Hash Di Simpan Ke Dalam Blockchain

Pembahasan

Hasil implementasi menunjukkan bahwa integrasi teknologi blockchain dengan skema enkripsi AES-256 mampu menghasilkan mekanisme penyimpanan rekam medis elektronik yang jauh lebih aman dan andal dibandingkan pendekatan konvensional yang masih terpusat. Dalam sistem yang dikembangkan, data rekam medis tidak disimpan secara langsung pada blockchain, mengingat keterbatasan kapasitas block serta biaya gas yang tinggi jika data berukuran besar dicatat secara on-

chain. Sebagai gantinya, data rekam medis disimpan pada media penyimpanan *off-chain* dalam bentuk terenkripsi menggunakan AES-256, sementara hash SHA-256 dari data terenkripsi tersebut dicatat secara permanen dan tidak dapat diubah pada blockchain Ethereum Sepolia. Pendekatan *hybrid storage* ini terbukti memberikan keseimbangan antara keamanan, efisiensi, dan skalabilitas.

1. Peningkatan Keamanan dan Kerahasiaan Data

Penggunaan enkripsi AES-256 memastikan bahwa seluruh data medis yang disimpan tetap bersifat privat meskipun penyimpanan *off-chain* mengalami kebocoran atau diakses oleh pihak yang tidak berwenang. AES-256 merupakan algoritma enkripsi simetris yang dikenal sangat kuat karena panjang kuncinya yang besar, sehingga tidak dapat dipecahkan dengan teknik *brute force* dalam kondisi komputasi saat ini. Implementasi menunjukkan bahwa file yang telah terenkripsi tidak dapat didekripsi tanpa key yang valid, sehingga melindungi informasi sensitif pasien dari risiko kebocoran data.

Hasil ini konsisten dengan berbagai penelitian sebelumnya yang menyimpulkan bahwa kombinasi blockchain dan enkripsi simetris merupakan metode paling efektif untuk menjaga kerahasiaan data medis, terutama pada sistem yang membutuhkan kontrol akses ketat dan perlindungan privasi pasien. Dengan kata lain, walaupun data disimpan di luar blockchain, lapisan keamanan tetap terjaga melalui pengamanan kriptografi tingkat tinggi.

2. Integritas Data Terjamin Melalui Hash yang Tersimpan Permanen

Blockchain berfungsi sebagai lapisan verifikasi integritas data. Hash SHA-256 yang dicatat pada smart contract bertindak sebagai *fingerprint* unik dari dokumen rekam medis. Setiap kali dokumen diverifikasi, sistem menghitung ulang hash dari file terenkripsi dan membandingkannya dengan hash yang tersimpan di blockchain. Jika hasilnya identik, maka dipastikan data belum dimodifikasi. Jika berbeda, maka dapat disimpulkan ada perubahan, baik disengaja maupun akibat kerusakan data.

Pengujian yang dilakukan menunjukkan bahwa:

- Hash akan langsung berbeda meskipun hanya ada perubahan satu karakter pada data.
- Data yang rusak atau sengaja diubah selalu terdeteksi melalui mismatched hash.
- Hash yang tersimpan di blockchain tidak dapat dihapus atau dimodifikasi karena sifat *immutability* blockchain.

Bukti transaksi di Etherscan mendukung hasil ini, menampilkan dengan jelas setiap proses pencatatan hash sebagai transaksi blockchain yang publik dan tidak dapat diubah setelah dikonfirmasi. Hal ini menciptakan jejak audit (*audit trail*) yang transparan dan dapat diverifikasi oleh pihak berwenang kapan saja.

3. Validasi Alur Sistem Melalui Implementasi dan Pengujian

Rangkaian proses yang dimulai dari *upload* file, enkripsi data, penyimpanan *off-chain*, generasi hash SHA-256, hingga pencatatan hash ke blockchain berjalan sesuai dengan alur yang telah dirancang pada bagian metode. Tampilan antarmuka sistem memperlihatkan bahwa pengguna dapat mengunggah dokumen dengan mudah dan menerima notifikasi ketika proses penyimpanan berhasil.

Fitur verifikasi juga menunjukkan fungsionalitas yang stabil, di mana pengguna dapat memeriksa integritas data hanya dengan mengunggah file untuk dibandingkan hash-nya dengan hash yang telah disimpan sebelumnya. Bukti transaksi blockchain memberikan tambahan konfirmasi bahwa data telah tercatat secara resmi di jaringan Ethereum.

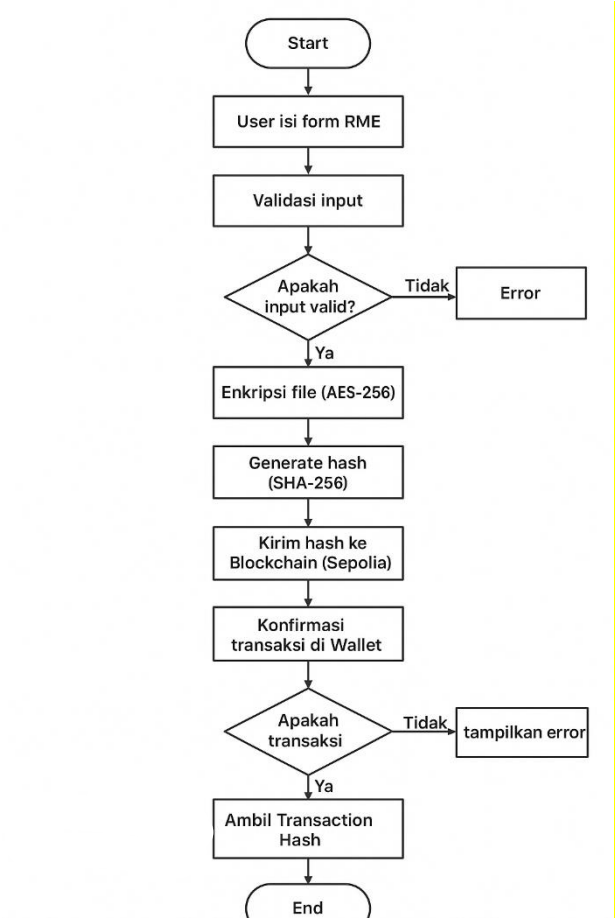
Secara keseluruhan, hasil implementasi ini membuktikan bahwa sistem yang dibangun mampu menjawab tiga permasalahan utama dalam penyimpanan rekam medis elektronik:

- **Keamanan data**, melalui penggunaan enkripsi AES-256.
- **Integritas informasi**, melalui pencatatan hash SHA-256 yang tidak dapat dimodifikasi.
- **Transparansi proses**, melalui jejak transaksi di blockchain yang terbuka dan dapat diverifikasi.

Dengan demikian, model ini dapat dipertimbangkan sebagai solusi alternatif dalam pengembangan sistem rekam medis elektronik yang lebih aman, terpercaya, dan sesuai dengan kebutuhan transformasi digital di sektor kesehatan. Implementasi berbasis blockchain dan enkripsi memungkinkan setiap proses penyimpanan data memiliki jejak audit yang transparan sekaligus menjaga kerahasiaan informasi medis. Karakteristik ini menjadikan model yang dikembangkan tidak hanya relevan untuk lingkup penelitian akademik, tetapi juga potensial untuk diadaptasi oleh fasilitas kesehatan yang membutuhkan mekanisme perlindungan data tanpa harus melakukan investasi infrastruktur yang besar. Pendekatan hybrid—di mana data medis disimpan dalam bentuk terenkripsi secara off-chain, sementara hash integritas disimpan secara permanen di blockchain—memberikan fleksibilitas serta efisiensi yang sulit dicapai oleh sistem penyimpanan konvensional.

Selain itu, sistem ini membuka peluang untuk pengembangan lebih lanjut sehingga dapat mendukung ekosistem kesehatan digital yang lebih luas. Dengan menambahkan fitur seperti manajemen akses berbasis peran, otentikasi terdesentralisasi, interoperabilitas dengan sistem informasi kesehatan yang sudah ada, serta pengelolaan kunci enkripsi yang lebih komprehensif, model ini berpotensi dikembangkan menjadi solusi yang memenuhi standar industri kesehatan modern. Kemampuan teknologi blockchain dalam melindungi integritas data, dikombinasikan dengan enkripsi AES-256 yang menjaga kerahasiaan dokumen, menjadikan model ini layak untuk dijadikan landasan dalam membangun sistem rekam medis elektronik generasi berikutnya. Dengan demikian, penelitian ini memberikan kontribusi penting dalam memperkuat literatur mengenai keamanan data kesehatan serta memberikan contoh implementasi nyata yang dapat dikembangkan lebih jauh oleh peneliti maupun praktisi di bidang teknologi kesehatan.

Di bawah ini merupakan Flowchart dari sistem yang di kembangkan



Figur 2 Flowchart Sistem

KESIMPULAN

Penelitian ini membuktikan bahwa proses penyimpanan dokumen rekam medis elektronik dapat dilakukan secara lebih aman, transparan, dan terdistribusi melalui integrasi teknologi blockchain dan enkripsi AES-256. Meskipun sistem yang dikembangkan masih bersifat sederhana—hanya berupa formulir unggah file yang kemudian dienkripsi dan dikirim ke jaringan blockchain Sepolia—hasil implementasi menunjukkan bahwa mekanisme dasar pencatatan medis berbasis blockchain dapat berfungsi dengan baik tanpa memerlukan infrastruktur besar seperti yang digunakan dalam sistem informasi rumah sakit modern. Hal ini mengindikasikan bahwa adopsi awal teknologi blockchain pada sektor kesehatan dapat dilakukan secara bertahap melalui prototipe kecil yang fungsional.

Pengujian menunjukkan bahwa blockchain mampu memberikan jaminan integritas data yang kuat. Setiap dokumen yang diunggah dikonversi menjadi hash SHA-256 dan dicatat secara permanen dalam blok sehingga tidak dapat diubah, dihapus, maupun dimanipulasi. Dengan demikian, setiap rekam medis yang disimpan memperoleh identitas digital unik yang dapat diverifikasi kapan saja. Di sisi lain, penerapan enkripsi AES-256 memastikan bahwa meskipun data asli tidak disimpan di blockchain dan tetap berada pada penyimpanan *off-chain*, kerahasiaannya tetap terjaga sepenuhnya. Tanpa kunci dekripsi yang benar, isi dokumen medis tetap tidak dapat diakses, bahkan jika penyimpanan off-chain mengalami kebocoran data.

Temuan ini menegaskan bahwa kombinasi blockchain dan enkripsi simetris modern dapat menciptakan model perlindungan berlapis untuk data medis, bahkan pada implementasi berskala kecil dan sederhana. Dengan kemampuan mencatat bukti data secara *immutable* serta melindungi isi dokumen melalui enkripsi kuat, sistem yang dikembangkan dalam penelitian ini memberikan fondasi awal bagi model Rekam Medis Elektronik (RME) yang lebih aman, efisien, dan terverifikasi secara terbuka.

Walaupun sistem ini belum mencakup fitur kompleks seperti manajemen peran pengguna, interoperabilitas antar sistem kesehatan, otorisasi berbasis identitas, maupun mekanisme dekripsi berbasis izin, penelitian ini berhasil menunjukkan kelayakan teknis (technical feasibility) dari pendekatan hybrid: data terenkripsi disimpan off-chain, sedangkan hash dan metadata transaksi dicatat on-chain. Keberhasilan implementasi alur *upload → enkripsi → hashing → penyimpanan off-chain → pencatatan hash di blockchain* menunjukkan bahwa pendekatan ini dapat direplikasi, diperluas, dan diadaptasi untuk kebutuhan lingkungan kesehatan berskala lebih besar.

Saran penelitian ditujukan kepada pengembang, institusi pendidikan, dan penyedia layanan kesehatan. Bagi pengembang, model ini dapat menjadi dasar untuk mengembangkan fitur lanjutan seperti kontrol hak akses berbasis smart contract, audit log lengkap, proses dekripsi aman, serta pengelolaan kunci enkripsi yang lebih terstruktur. Bagi institusi pendidikan, hasil penelitian ini dapat digunakan sebagai bahan ajar praktis untuk mengenalkan teknologi blockchain dalam konteks kesehatan dan keamanan data. Sementara bagi fasilitas kesehatan berskala kecil, prototipe ini dapat menjadi inspirasi implementasi awal sistem keamanan dokumen medis yang lebih terjangkau namun tetap kuat, sebelum beralih ke sistem rekam medis elektronik yang lebih besar dan terintegrasi. Dengan demikian, penelitian ini tidak hanya menghasilkan bukti implementatif, tetapi juga membuka ruang bagi inovasi berkelanjutan dalam pengamanan data kesehatan berbasis teknologi modern.

DAFTAR PUSTAKA

Guo, Z. (2025). Blockchain-enhanced smart contracts for formal verification of IoT access control mechanisms. *Alexandria Engineering Journal*, *118*(January), 315–324. https://doi.org/10.1016/j.aej.2024.12.109

Hakim, A. R., & Margolang, K. F. (2025). *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD Analisis Keamanan Data Rekam Medis Digital Menggunakan Algoritma Kriptografi AES Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*. *8*, 108–114.

Lax, G., Nardone, R., & Russo, A. (2024). *Enabling secure health information sharing among healthcare organizations by public blockchain*. 64795–64811. https://doi.org/10.1007/s11042-024-18181-4

Pangidoan, A. M., Buana, P. W., & Purnama, F. (2025). *Prototype of Implementation of Smart Contract for Blockchain-Based Document Storage*. *9*(4), 1242–1253.

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). *Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System*.

Sha-, A., Sitorus, N., Sharon, J., Sinaga, G., & Samosir, S. L. (2024). *Analisis Kinerja Algoritma Hash pada Keamanan Data : Perbandingan*. *2*(2).

View of Penerapan Blockchain Untuk Keamanan Data Rekam Medis Elektronik _ Literatur Review.pdf. (n.d.).