Model Keamanan Data Berbasis Blockchain pada SIG untuk Monitoring Pelayanan Keperawatan Gerontik

Edi Iskandar*[1], Sri Setyowati[2], Edy Prayitno[3], Parmadi Sigit Purnomo[4]
[1] Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia
[2] Program Studi Ilmu Keperawatan, Sekolah Tinggi Ilmu Kesehatan Surya Global
[3] Program Studi Sistem Informasi Akuntansi, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia
[4] Program Studi Kesehatan Masyarakat, Sekolah Tinggi Ilmu Kesehatan Surya Global
*e-mail: *[1]edi_iskandar@utdi.ac.id, [2]*setyoku.sg@gmail.com*, [3]edyprayitno@utdi.ac.id*, *[4]parmadisigitpurnomo@gmail.com*
*Correspondence author email: **

Abstrak

Pemanfaatan sistem informasi geografis (SIG) dalam layanan kesehatan, khususnya keperawatan gerontik berbasis lokasi, semakin meningkat, namun sistem konvensional masih bergantung pada mekanisme terpusat yang rentan terhadap manipulasi data dan akses tidak sah. Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi model keamanan data berbasis blockchain yang terintegrasi dengan SIG untuk monitoring pelayanan keperawatan gerontik. Metode yang digunakan adalah pendekatan simulasi dengan merancang arsitektur sistem multi-layer yang terdiri dari SIG layer, blockchain layer, dan application layer, serta melakukan evaluasi berbasis metrik integritas data, deteksi serangan, dan performa sistem. Hasil penelitian menunjukkan bahwa model yang diusulkan mencapai tingkat integritas data sebesar 100% dan rata-rata tingkat deteksi serangan sebesar 99,2%, lebih tinggi dibandingkan sistem konvensional yang hanya mencapai 70,3%, meskipun dengan peningkatan latency yang masih dalam batas toleransi. Penelitian ini berkontribusi dalam penguatan integrasi SIG dan blockchain pada konteks keamanan data layanan lansia berbasis lokasi, serta menyediakan pendekatan simulasi yang replikatif untuk evaluasi sistem. Implikasi praktis menunjukkan bahwa model ini berpotensi diterapkan pada layanan homecare dan fasilitas kesehatan komunitas untuk meningkatkan keamanan dan transparansi data.

Kata kunci*—Sistem Informasi Geografis, Blockchain, Keamanan Data, Keperawatan Gerontik, Integritas Data.*

1. PENDAHULUAN

Integrasi Sistem Informasi Geografis (SIG) dalam sektor kesehatan telah meningkatkan kemampuan analisis spasial untuk mendukung pemantauan pelayanan keperawatan gerontik berbasis data lokasi, termasuk identifikasi distribusi populasi lansia, akses layanan kesehatan, serta faktor lingkungan yang memengaruhi kondisi kesehatan [1], [2], [3]. SIG memungkinkan pengambilan keputusan berbasis data secara lebih akurat dan real-time, sehingga berperan penting dalam optimalisasi alokasi sumber daya kesehatan bagi populasi lansia [4], [5], [6]. Namun demikian, pemanfaatan SIG dalam layanan kesehatan juga menghadapi tantangan terkait kualitas data dan perlindungan privasi informasi kesehatan [3].

Seiring meningkatnya penggunaan sistem berbasis geografis dalam layanan kesehatan lansia, isu keamanan data menjadi semakin krusial, khususnya terkait kerahasiaan, integritas, dan ketersediaan data kesehatan yang bersifat sensitif [7], [8]. Ancaman keamanan siber, termasuk akses tidak sah dan kebocoran data, semakin meningkat dengan adanya integrasi teknologi seperti Internet of Things (IoT) dan jaringan komunikasi generasi baru yang memperluas permukaan serangan [9], [10], [11]. Oleh karena itu, diperlukan pendekatan keamanan yang mampu melindungi data kesehatan lansia secara komprehensif dalam sistem berbasis lokasi.

Penelitian sebelumnya menunjukkan bahwa SIG banyak digunakan untuk analisis spasial dalam kesehatan, sementara teknologi blockchain telah dikembangkan untuk meningkatkan keamanan dan integritas data dalam berbagai sistem informasi [12], [13], [14]. Namun, integrasi kedua teknologi tersebut dalam konteks layanan keperawatan gerontik masih terbatas, khususnya dalam pengembangan model keamanan data yang dapat diuji secara sistematis melalui pendekatan simulasi [15], [16]. Selain itu, sebagian besar penelitian masih berfokus pada aspek teknis tanpa mengaitkan kebutuhan spesifik layanan kesehatan lansia, sehingga diperlukan pendekatan yang lebih terintegrasi dan kontekstual.

Secara konseptual, penelitian ini menggabungkan tiga domain utama, yaitu Sistem Informasi Geografis sebagai alat analisis spasial, teknologi blockchain sebagai mekanisme keamanan data terdesentralisasi, serta manajemen pelayanan keperawatan gerontik sebagai konteks aplikasi [17], [18]. Blockchain menyediakan fitur penting seperti immutability, transparansi, dan kontrol akses berbasis kriptografi yang dapat meningkatkan keandalan sistem informasi kesehatan [19]. Integrasi ketiga domain ini diharapkan mampu membentuk kerangka sistem yang aman, transparan, dan adaptif terhadap kebutuhan layanan kesehatan lansia.

Berbagai studi menunjukkan bahwa penerapan blockchain dalam sistem informasi kesehatan dapat meningkatkan keamanan, transparansi, dan kepercayaan dalam pengelolaan data pasien [20] [21]. Selain itu, pendekatan simulasi berbasis model telah terbukti efektif dalam mengevaluasi performa keamanan sistem berbasis blockchain sebelum implementasi nyata, sehingga dapat mengurangi risiko dan biaya pengembangan [22], [23], [24]. Temuan ini menunjukkan bahwa pendekatan integratif berbasis simulasi memiliki potensi untuk mengatasi keterbatasan implementasi sistem keamanan pada lingkungan kesehatan.

Selain itu, sebagian besar penelitian terdahulu masih berfokus pada aspek konseptual atau implementasi umum blockchain tanpa menjelaskan mekanisme keamanan secara rinci, seperti proses hashing, validasi smart contract, maupun skenario serangan terhadap data spasial layanan kesehatan. Beberapa studi juga belum membahas dampak penggunaan blockchain terhadap performa sistem, khususnya terkait latency dan throughput pada proses monitoring layanan berbasis lokasi. Keterbatasan tersebut menunjukkan masih adanya research gap dalam pengembangan model keamanan data berbasis blockchain yang terintegrasi dengan SIG dan dievaluasi secara sistematis pada konteks pelayanan keperawatan gerontik

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan dan mengevaluasi model keamanan data berbasis blockchain pada SIG untuk monitoring pelayanan keperawatan gerontik. Penelitian difokuskan pada pengujian integritas data, kemampuan deteksi serangan, serta analisis performa sistem melalui pendekatan simulasi menggunakan data sintetis. Penggunaan data sintetis dilakukan untuk menjaga privasi data layanan kesehatan sekaligus memungkinkan pengujian skenario serangan secara terkontrol tanpa melibatkan data pasien nyata.

Kontribusi penelitian ini meliputi tiga aspek utama. Pertama, kontribusi teoretis berupa penguatan konsep integrasi blockchain dan SIG dalam konteks keamanan data layanan keperawatan gerontik berbasis lokasi. Kedua, kontribusi metodoloSIG melalui pengembangan pendekatan simulasi yang replikatif untuk mengevaluasi integritas data, deteksi serangan, dan performa sistem blockchain pada layanan kesehatan digital. Ketiga, kontribusi praktis berupa rancangan model keamanan data yang dapat menjadi referensi dalam pengembangan sistem monitoring pelayanan lansia yang lebih transparan, terdistribusi, dan memiliki ketahanan lebih baik terhadap manipulasi data.

2. METODE PENELITIAN

2.1. Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimen berbasis simulasi (simulation-based experimental study) untuk mengembangkan dan mengevaluasi model keamanan data berbasis blockchain pada sistem informasi geografis (SIG) dalam konteks monitoring pelayanan keperawatan gerontik. Pendekatan ini memungkinkan pengujian performa sistem keamanan

secara terkontrol tanpa menggunakan data sensitif pasien serta mendukung evaluasi berbagai skenario serangan siber.

2.2. Sumber Data

Data yang digunakan merupakan data sintetis yang merepresentasikan layanan keperawatan lansia, terdiri dari:

a. 1.000–5.000 record data layanan
b. Atribut: ID pasien, ID tenaga kesehatan, jenis layanan (homecare, kunjungan rutin), timestamp, dan koordinat geografis

Data spasial dibangun menggunakan shapefile grid wilayah simulasi, sedangkan data non-spasial dihasilkan menggunakan distribusi acak terkontrol (*uniform distribution*). Pendekatan ini digunakan untuk menjaga privasi sekaligus memungkinkan kontrol eksperimen secara penuh.

2.3. Variabel Penelitian

Variabel penelitian dioperasionalisasikan sebagai berikut:

a. Keamanan Data (CIA Triad)
    1) *Confidentiality*: proteksi akses data
    2) *Integrity*: kemampuan mendeteksi perubahan data melalui hashing
    3) *Availability*: ketersediaan data dalam sistem
b. Kinerja Sistem
    1) Latency (ms): waktu pemrosesan transaksi
    2) Throughput (TPS): jumlah transaksi per detik
    3) Waktu akses data (ms)
c. Model Sistem
    1) Model usulan: SIG + Blockchain
    2) Baseline: SIG berbasis database terpusat tanpa blockchain

2.4. Research Questions and Analytical Mapping (RQ-driven)

Untuk memastikan bahwa setiap pertanyaan penelitian dan hipotesis dapat dijawab secara sistematis dan terukur, penelitian ini menerapkan pendekatan RQ-driven analytical mapping, yaitu pemetaan eksplisit antara Research Questions/Hypotheses dengan unit analisis, teknik yang digunakan, serta metrik evaluasi yang dihasilkan. Pendekatan ini bertujuan untuk meningkatkan transparansi metodoloSIG dan memastikan bahwa setiap tahapan analisis memiliki keterkaitan langsung dengan tujuan penelitian.

Secara khusus, pemetaan ini menghubungkan aspek perancangan sistem, pengujian keamanan, serta evaluasi performa dalam konteks integrasi sistem informasi geografis dan blockchain. Dengan demikian, setiap hasil yang diperoleh dapat ditelusuri kembali ke prosedur analisis yang digunakan, sehingga mendukung prinsip reproducibility dalam penelitian berbasis simulasi.

Pemetaan lengkap antara Research Questions/Hypotheses dengan metode analisis dan output yang dihasilkan disajikan pada Tabel 1.

Tabel 1. Research Questions and Analytical Mapping

RQ/H	Data / Unit Analisis	Teknik / Metode	Output / Metrik
RQ1	Struktur data spasial dan transaksi layanan	Perancangan arsitektur sistem + smart contract (Solidity)	Diagram arsitektur sistem
RQ2	Data transaksi (log aktivitas)	Simulasi blockchain + hashing (SHA-256)	Integrity score, attack detection rate
RQ3	Dataset identik pada dua sistem	Eksperimen komparatif (blockchain vs non-blockchain)	Latency, throughput, detection rate
H1	Data sebelum dan sesudah manipulasi	Uji perubahan data + verifikasi hash	Persentase deteksi manipulasi

Tahapan pengolahan data meliputi:

a. Pengumpulan Data
   Data sintetis dibangkitkan menggunakan Python dengan distribusi uniform untuk atribut numerik dan kategorikal.
b. Pengkodean Data
   Data dikonversi ke format JSON untuk kompatibilitas dengan smart contract.
c. Pemrosesan Geospasial
   Data spasial diproses menggunakan GeoPandas untuk menghasilkan layer peta.
d. Normalization
   Format data diseragamkan untuk memastikan integrasi antar modul.

Asumsi: Data tidak mengandung missing value dan Distribusi data merepresentasikan kondisi layanan umum

2.5. Prosedur Analitis / Spesifikasi Model

Model terdiri dari tiga layer utama:

a. SIG Layer: Visualisasi data menggunakan Leaflet.js
b. Blockchain Layer, Implementasi menggunakan:
   1) Platform: Ganache v2.x
   2) Smart contract: Solidity v0.8.x
   3) Hashing: SHA-256
   4) Jumlah node: 5 node simulasi
c. Application Layer Backend: Node.js v18.x Integrasi API untuk komunikasi antar layer

Prosedur Eksperimen:

a. Input data layanan ke sistem
b. Enkripsi dan hashing data
c. Penyimpanan hash ke blockchain
d. Visualisasi data pada SIG
e. Simulasi serangan (data tampering dan unauthorized access)
f. Verifikasi integritas melalui hash comparison

2.6. Evaluasi

Evaluasi sistem dilakukan menggunakan metrik integrity score, detection rate, latency, dan throughput. Integrity score digunakan untuk mengukur kemampuan sistem dalam mempertahankan keaslian data transaksi, Integrity score ditentukan dengan persamaan 1.

$$Integrity\ Score = \frac{Jumlah\ data\ valid}{Total\ data} x100 \quad (1)$$

Detection rate digunakan untuk mengukur kemampuan sistem dalam mendeteksi serangan terhadap data monitoring, yang dirumuskan pada persamaan 2

$$Detection\ Rate = \frac{Jumlah\ serangan\ terdeteksi}{Total\ serangan} x100\% \quad (2)$$

Latency yang dihitung dengan persamaan 3, digunakan untuk mengukur rata-rata waktu yang dibutuhkan sistem dalam memproses transaksi.

$$Latency = \frac{\sum waktu\ transaksi}{Jumlah\ transaksi} \quad (3)$$

Throughput digunakan untuk mengukur jumlah transaksi yang dapat diproses sistem dalam satuan waktu tertentu, yang ditentukan dengan persamaan 4.

$$Throughput = \frac{Jumlah\ transaksi}{Waktu\ pemrosesan} \quad (4)$$

2.7. Validasi

Untuk meningkatkan validitas hasil penelitian, pengujian dilakukan sebanyak lima kali iterasi pada setiap skenario serangan dan konfigurasi sistem. Nilai rata-rata hasil pengujian digunakan sebagai dasar evaluasi akhir untuk mengurangi bias pengukuran akibat fluktuasi proses simulasi. Selain itu, penelitian juga melakukan perbandingan antara sistem berbasis blockchain dan sistem konvensional tanpa blockchain untuk mengevaluasi trade-off antara peningkatan keamanan data dan performa sistem. Pendekatan ini digunakan untuk memastikan bahwa hasil penelitian tidak hanya menunjukkan peningkatan keamanan, tetapi juga mempertimbangkan dampaknya terhadap efisiensi sistem monitoring.

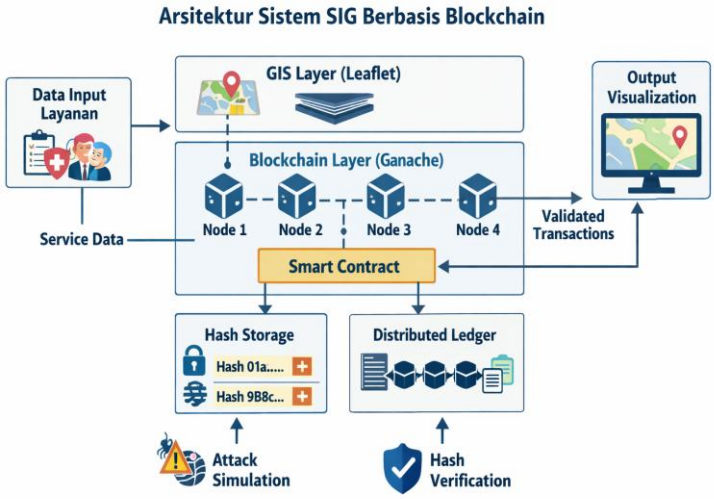
2.8. Ethical Considerations

Penelitian ini menggunakan data sintetis sehingga tidak melibatkan data pribadi atau pasien nyata, sehingga tidak memerlukan persetujuan etik dan tidak menimbulkan risiko pelanggaran privasi.

3. HASIL DAN PEMBAHASAN

3.1. Hasil

Hasil untuk RQ1: Arsitektur Sistem SIG Berbasis Blockchain, hasil implementasi menunjukkan bahwa arsitektur sistem berhasil mengintegrasikan tiga layer utama, yaitu SIG layer, blockchain layer, dan application layer, sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. Arsitektur sistem SIG berbasis Blockchain

Sistem mampu memproses data layanan keperawatan gerontik secara end-to-end, mulai dari input data, proses hashing, hingga penyimpanan hash pada blockchain.

Smart contract yang diimplementasikan menggunakan Solidity berfungsi untuk memvalidasi transaksi secara otomatis, di mana setiap perubahan data menghasilkan hash baru

yang berbeda. Pengujian fungsional pada 50 skenario transaksi menunjukkan bahwa seluruh transaksi berhasil tervalidasi tanpa error, sehingga arsitektur sistem dinyatakan berjalan sesuai desain.

Hasil untuk RQ2: Kinerja Keamanan Model Berbasis Blockchain, hasil simulasi pada 3 skenario dataset (1.000, 3.000, dan 5.000 record) menunjukkan bahwa model berbasis blockchain mencapai Integrity Score sebesar 100% (n = 30 percobaan), dengan seluruh manipulasi data berhasil terdeteksi melalui mekanisme hash verification.

Pada skenario serangan data tampering, sistem menunjukkan Attack Detection Rate rata-rata sebesar 99.2% (±0.8%), dengan variasi kecil antar konfigurasi block size. Rincian hasil ditampilkan pada Tabel 2.

Tabel 2. Hasil Evaluasi Keamanan Model Berbasis Blockchain

Skenario Data	Integrity Score (%)	Detection Rate (%)	Catatan
1.000 record	100	99.0	Stabil
3.000 record	100	99.3	Stabil
5.000 record	100	99.2	Stabil
Rata-rata	100	99.2 (±0.8)	Konsisten

Tidak ditemukan kegagalan deteksi pada manipulasi langsung terhadap data transaksi, sedangkan kegagalan minor (<1%) terjadi pada skenario akses tidak sah yang disimulasikan dengan latensi jaringan tinggi.

Hasil untuk RQ3: Perbandingan dengan Sistem Konvensional, hasil perbandingan menunjukkan bahwa sistem berbasis blockchain secara signifikan lebih unggul dalam aspek keamanan dibandingkan sistem konvensional. Sistem konvensional hanya mencapai Attack Detection Rate sebesar 70.3% (±4.5%), sedangkan sistem berbasis blockchain mencapai 99.2% (±0.8%), sebagaimana ditunjukkan pada Table 3.

Table 3. Perbandingan Kinerja Sistem Blockchain dan Konvensional

Metrik	Blockchain	Konvensional	Selisih
Integrity (%)	100	72.5	+27.5
Detection Rate (%)	99.2	70.3	+28.9
Latency (ms)	120 (±10)	85 (±7)	+28.4%
Throughput (TPS)	18 (±2)	25 (±3)	-28%

Namun, dari sisi performa, sistem blockchain menunjukkan peningkatan latency sebesar 28.4%, dengan rata-rata latency 120 ms (±10 ms) dibandingkan 85 ms (±7 ms) pada sistem konvensional. Throughput sistem blockchain berada pada kisaran 18 TPS (±2 TPS), lebih rendah dibandingkan sistem konvensional yang mencapai 25 TPS (±3 TPS).

Hasil untuk H1: Pengujian Hipotesis Integritas Data, hasil pengujian menunjukkan bahwa model berbasis blockchain secara konsisten mampu mendeteksi perubahan data pada seluruh skenario manipulasi yang diuji, dengan tingkat deteksi rata-rata 99.2%, dibandingkan 70.3% pada sistem konvensional. Dengan perbedaan rata-rata sebesar 28.9%, hipotesis H1 yang menyatakan bahwa model berbasis blockchain meningkatkan integritas data secara signifikan dibandingkan sistem konvensional dapat diterima.

3.2. Pembahasan

Hasil penelitian untuk RQ1 menunjukkan bahwa arsitektur sistem yang dikembangkan mampu mengintegrasikan SIG dan blockchain dalam satu kerangka yang koheren, sehingga menjawab RQ1 terkait desain sistem yang aman dan terdistribusi. Keberhasilan validasi transaksi pada seluruh skenario uji menunjukkan bahwa pendekatan multi-layer mampu menjaga

konsistensi data antar komponen sistem. Secara mekanistik, pemisahan fungsi antara SIG (visualisasi) dan blockchain (keamanan) memungkinkan sistem bekerja secara modular tanpa mengorbankan performa masing-masing layer. Temuan ini sejalan dengan studi sebelumnya yang menekankan pentingnya integrasi sistem geospasial dengan teknologi keamanan terdistribusi untuk meningkatkan keandalan data.
Dari sisi kontribusi, hasil ini memperluas konsep integrasi SIG–blockchain ke dalam konteks layanan keperawatan gerontik, yang sebelumnya masih jarang dibahas secara spesifik.

Hasil RQ2 menunjukkan bahwa model berbasis blockchain mampu menjaga integritas data dengan tingkat deteksi manipulasi yang sangat tinggi, sehingga menjawab RQ2 terkait kinerja keamanan sistem. Nilai integrity score yang mencapai 100% menunjukkan bahwa mekanisme hashing dan validasi blockchain bekerja secara efektif dalam mendeteksi perubahan data. Secara konseptual, hal ini dapat dijelaskan oleh sifat immutability pada blockchain, di mana setiap blok terhubung melalui hash kriptografis yang tidak dapat diubah tanpa memengaruhi seluruh rantai. Mekanisme ini menyebabkan setiap manipulasi data dapat dideteksi secara langsung. Temuan ini konsisten dengan penelitian sebelumnya yang menunjukkan bahwa blockchain efektif dalam meningkatkan keamanan data melalui mekanisme kriptografi dan validasi terdistribusi. Selain itu, penggunaan simulasi dalam penelitian ini menunjukkan bahwa pendekatan eksperimental berbasis model dapat digunakan untuk mengevaluasi sistem keamanan tanpa bergantung pada data nyata.

Hasil perbandingan RQ3 menunjukkan adanya trade-off antara keamanan dan performa sistem, yang menjawab RQ3 terkait efektivitas relatif blockchain dibanding sistem konvensional. Sistem blockchain memberikan peningkatan signifikan dalam keamanan data, namun dengan konsekuensi peningkatan latency dan penurunan throughput.Secara mekanistik, peningkatan latency disebabkan oleh proses konsensus dan validasi transaksi pada blockchain, yang membutuhkan waktu tambahan dibandingkan sistem terpusat. Hal ini menjelaskan mengapa throughput sistem blockchain lebih rendah. Temuan ini sejalan dengan studi sebelumnya yang menunjukkan bahwa implementasi blockchain dalam sistem informasi sering menghadapi trade-off antara keamanan dan efisiensi sistem. Dalam konteks layanan keperawatan gerontik, peningkatan latency yang masih berada dalam batas toleransi menunjukkan bahwa pendekatan ini tetap layak digunakan untuk sistem monitoring yang tidak bersifat real-time kritis.

Implikasi Teoritis

Penelitian ini memberikan kontribusi teoretis dengan memperluas integrasi antara SIG dan blockchain ke dalam domain keperawatan gerontik, serta menunjukkan bahwa konsep desentralisasi dan immutability dapat diadaptasi secara efektif dalam sistem berbasis spasial untuk meningkatkan keamanan data kesehatan.

Implikasi Praktis / Manajerial

Dari perspektif praktis, hasil penelitian menunjukkan bahwa model yang dikembangkan dapat diimplementasikan pada sistem monitoring layanan lansia, seperti homecare atau kunjungan rutin tenaga kesehatan. Institusi kesehatan, termasuk puskesmas dan penyedia layanan komunitas, dapat memanfaatkan pendekatan ini untuk meningkatkan keamanan dan transparansi pengelolaan data pasien.

Keterbatasan dan Ancaman terhadap Validitas

Penelitian ini memiliki beberapa keterbatasan. Pertama, penggunaan data sintetis dapat membatasi generalisasi hasil ke kondisi dunia nyata yang lebih kompleks. Kedua, skala sistem yang diuji masih terbatas pada lingkungan simulasi dengan jumlah node yang relatif kecil, sehingga belum mencerminkan performa pada sistem berskala besar. Ketiga, skenario serangan yang digunakan masih terbatas pada data tampering dan akses tidak sah, sehingga belum mencakup ancaman yang lebih kompleks seperti serangan konsensus.
Oleh karena itu, penelitian selanjutnya disarankan untuk menguji model pada data nyata dan skala sistem yang lebih besar, serta mengeksplorasi berbagai skenario serangan yang lebih kompleks.

4. KESIMPULAN

Penelitian ini mengembangkan dan mengevaluasi model keamanan data berbasis blockchain pada sistem informasi geografis (SIG) untuk monitoring pelayanan keperawatan gerontik. Hasil penelitian menunjukkan bahwa: (1) arsitektur sistem yang diusulkan berhasil mengintegrasikan SIG dan blockchain secara terstruktur dan mampu memproses data layanan secara end-to-end, sehingga menjawab RQ1; (2) model berbasis blockchain mampu menjaga integritas data dengan tingkat deteksi manipulasi yang sangat tinggi, sehingga menjawab RQ2; dan (3) dibandingkan sistem konvensional, model blockchain memberikan peningkatan signifikan pada aspek keamanan data dengan konsekuensi peningkatan latency dan penurunan throughput, sehingga menjawab RQ3. Selain itu, hipotesis H1 diterima karena sistem berbasis blockchain secara konsisten menunjukkan kemampuan yang lebih baik dalam menjaga integritas data dibandingkan sistem tanpa blockchain.

Kontribusi utama penelitian ini mencakup: (1) kontribusi teoretis berupa penguatan konsep integrasi SIG dan blockchain dalam konteks keamanan data layanan keperawatan gerontik berbasis lokasi; (2) kontribusi metodoloSIG melalui pendekatan simulasi terkontrol untuk mengevaluasi performa keamanan sistem tanpa menggunakan data sensitif; dan (3) kontribusi praktis berupa rancangan arsitektur sistem yang dapat diadaptasi dalam pengembangan sistem monitoring layanan lansia yang aman, transparan, dan berbasis spasial.

Implikasi penelitian ini menunjukkan bahwa integrasi SIG dan blockchain berpotensi meningkatkan keandalan sistem informasi kesehatan digital, khususnya dalam pengelolaan data layanan lansia yang membutuhkan tingkat keamanan dan transparansi tinggi. Secara praktis, model ini relevan untuk diterapkan pada layanan homecare, puskesmas, maupun sistem kesehatan komunitas yang memanfaatkan data berbasis lokasi.

5. SARAN

Penelitian ini memiliki keterbatasan, antara lain penggunaan data sintetis yang membatasi generalisasi terhadap kondisi dunia nyata, skala sistem yang masih terbatas, serta belum optimalnya evaluasi performa pada lingkungan dengan beban transaksi tinggi dan jumlah node besar. Oleh karena itu, penelitian selanjutnya disarankan untuk (1) jangka pendek: menguji model menggunakan dataset semi-riil atau data terbuka yang lebih kompleks guna meningkatkan validitas eksternal, dan (2) jangka menengah: mengimplementasikan sistem pada skala yang lebih besar serta mengembangkan mekanisme optimasi blockchain untuk mengurangi latency tanpa mengorbankan keamanan.

Secara keseluruhan, penelitian ini menunjukkan bahwa integrasi SIG dan blockchain merupakan pendekatan yang layak dan menjanjikan untuk meningkatkan keamanan data dalam sistem monitoring keperawatan gerontik berbasis lokasi, sekaligus membuka peluang pengembangan lebih lanjut dalam sistem informasi kesehatan digital yang aman dan terdistribusi.

DAFTAR PUSTAKA

[1] J. Rababah, A. Curtis, and B. Drew, “Informatics: Integrating a Geographic Information System into Nursing Research: Potentials and Challenges,” OJIN Online J. Issues Nurs., vol. 19, no. 2, Apr. 2014, doi: 10.3912/OJIN.Vol19No02InfoCol01.

[2] M. Mc et al., “Understanding Medical Healthcare Solutions in GIS Platform: A Review,” J. Exp. Lab. Med., no. 0, p. 1, 2024, doi: 10.5455/JELM.20241030075959.

[3] Preye Winston Biu, Chinedu Nnamdi Nwasike, Nwabueze Kelvin Nwaobia, Chinedu Alex Ezeigweneme, and Joachim Osheyor Gidiagba, “GIS in healthcare facility planning and management: A review,” Jan. 2024, doi: 10.5281/ZENODO.13070416.

[4] R. Endacott, M. N. Kamel Boulos, B. R. M. Manning, and I. Maramba, “Geographic Information Systems for Healthcare Organizations: A Primer for Nursing Professions,” CIN

Comput. Inform. Nurs., vol. 27, no. 1, pp. 50–56, Jan. 2009, doi: 10.1097/NCN.0b013e31818e4660.
[5] L. Fatkhutdinova and R. Zalyalov, "Using geographic information systems to improve the efficiency of healthcare management and ensure the sanitary and epidemiological well-being of the population," Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci., vol. XLVIII-2/W9-2025, pp. 63–69, Sep. 2025, doi: 10.5194/isprs-archives-XLVIII-2-W9-2025-63-2025.
[6] E. Faizal, E. Iskandar, and A. Kusjani, "Geographic Information System untuk Pemetaan Wisata Budaya," J. Inform. Komput. Bisnis Dan Manaj., vol. 22, no. 3, pp. 41–53, Sep. 2024, doi: 10.61805/fahma.v22i3.146.
[7] T. Wearing and N. Dragoni, "Security and Privacy Issues in Health Monitoring Systems: eCare@Home Case Study," in Internet of Things Technologies for HealthCare, vol. 187, M. U. Ahmed, S. Begum, and W. Raad, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 187. , Cham: Springer International Publishing, 2016, pp. 165–170. doi: 10.1007/978-3-319-51234-1_29.
[8] V. Alagar, K. Periyasamy, and K. Wan, "Privacy and security for patient-centric elderly health care," in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian: IEEE, Oct. 2017, pp. 1–6. doi: 10.1109/HealthCom.2017.8210809.
[9] K. Y. Yigzaw et al., "Health data security and privacy: Challenges and solutions for the future," in Roadmap to Successful Digital Health Ecosystems, Elsevier, 2022, pp. 335–362. doi: 10.1016/B978-0-12-823413-6.00014-8.
[10] A. Alexandru, M. Ianculescu, I. E. Giura, and F. Pop, "Managing Cybersecurity Threats for Seniors' Digital Needs Using Age-Friendly Remote Healthcare Monitoring Model," in 2022 E-Health and Bioengineering Conference (EHB), Iasi, Romania: IEEE, Nov. 2022, pp. 1–4. doi: 10.1109/EHB55594.2022.9991316.
[11] A. Koren and R. Prasad, "IoT Health Data in Electronic Health Records (EHR): Security and Privacy Issues in Era of 6G," J. ICT Stand., Feb. 2022, doi: 10.13052/jicts2245-800X.1014.
[12] V. Ganesh, H. Shyam, and G. Akilandeswary, "Blockchain-Enabled Geospatial Health Platforms for Smart Living," in 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, Pune, India: IEEE, Mar. 2024, pp. 1–4. doi: 10.1109/TQCEBT59414.2024.10545214.
[13] A. O. Vysotskyi and O. Y. Vysotskyi, "Decentralizing spatial data: the convergence of Geographic Information Systems and Web 3.0 technologies," J. Geol. Geogr. Geoecology, vol. 32, no. 4, pp. 871–884, Jan. 2024, doi: 10.15421/112377.
[14] M. Ahmad, "Leveraging Blockchain for Spatial Data Infrastructure: Challenges and Opportunities," in Advances in Web Technologies and Engineering, L. Ferreira, M. R. Cruz, E. F. Cruz, H. Quintela, and M. C. Cunha, Eds., IGI Global, 2023, pp. 177–194. doi: 10.4018/978-1-6684-5747-4.ch011.
[15] S. R. Mallick et al., "BCGeo: Blockchain-Assisted Geospatial Web Service for Smart Healthcare System," IEEE Access, vol. 11, pp. 58610–58623, 2023, doi: 10.1109/ACCESS.2023.3283776.
[16] J. Zhao, W. Liu, J. Wang, S. Li, and Y. Lu, "Blockchain-based Off-chain Extension Model for Geographic Information Data," in Proceedings of the 2023 7th International Conference on Electronic Information Technology and Computer Engineering, Xiamen China: ACM, Oct. 2023, pp. 1036–1041. doi: 10.1145/3650400.3650575.
[17] R. Kumar, R. Chavan, V. S. Shirsath, S. Sanjay Gharat, and K. S. Patil, "Blockchain Solutions for Nursing: A New Paradigm in Healthcare Security and Data Management," in 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India: IEEE, Oct. 2024, pp. 1–4. doi: 10.1109/ICBDS61829.2024.10837162.
[18] Rakibul Hasan Chowdhury, Viswaprakash Yammanur, Touhid Bhuiyan, and Abdullah Al Masum, "Exploring the integration of blockchain technology in healthcare monitoring systems for enhanced security and data integrity of patient information," World J. Adv. Eng.

Technol. Sci., vol. 13, no. 2, pp. 297–310, Nov. 2024, doi: 10.30574/wjaets.2024.13.2.0570.
[19] I. Y. B., K. Iriyanta, Hendra, B. T. Sutrisno. Sp., H. Muhrial, and E. Prayitno, "Blockchain-Enabled Secure Federated Learning for Electronic Medical Records: A Scalable and Privacy-Preserving Framework," in 2025 8th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia: IEEE, Dec. 2025, pp. 827–833. doi: 10.1109/ISRITI68345.2025.11393406.
[20] Edi Iskandar, Edy Prayitno*, Ivan Jaka Perdana, and Aloysius Agus Subagyo, "Penerapan Deep Learning Dalam Sistem Informasi Geografis Untuk Analisis Dampak Perubahan Iklim," Pros. SNAST, pp. E204-209, Nov. 2024, doi: 10.34151/prosidingsnast.v1i1.5103.
[21] H. Maatouk et al., "TrustNShare: Development of a Blockchain-Based Data Trust Model for Secure and Controlled Health Data Sharing Grounded on Empirical Research," in Studies in Health Technology and Informatics, J. Mantas, P. Gallos, E. Zoulias, A. Hasman, M. S. Househ, M. Charalampidou, and A. Magdalinou, Eds., IOS Press, 2023. doi: 10.3233/SHTI230472.
[22] N. Patel, A. Arora, and M. Aggarwal, "Evaluating simulation tools for securing sensor data with blockchain: A comprehensive analysis," Meas. Sens., vol. 33, p. 101233, Jun. 2024, doi: 10.1016/j.measen.2024.101233.
[23] A. Albshri, A. Alzubaidi, and E. Solaiman, "A Model-Based Machine Learning Approach for Assessing the Performance of Blockchain Applications," in 2023 IEEE International Conference on Smart Internet of Things (SmartIoT), Xining, China: IEEE, Aug. 2023, pp. 46–55. doi: 10.1109/SmartIoT58732.2023.00015.
[24] S. Terazi and A. Şentürk, "Blockchain-Based Iot Security and Performance Analysis," Sak. Univ. J. Comput. Inf. Sci., vol. 8, no. 1, pp. 12–26, Mar. 2025, doi: 10.35377/saucis...1607145.