

Analisis dan Perancangan Sistem Informasi Pelayanan Rawat Jalan Terintegrasi (Poli Umum, Gigi, dan Imunisasi) pada Puskesmas Rahayu Taman Kopo Indah

Surya Cahyadi^{a,1,*},

^aPIKSI Ganesha Jalan Gatot Subroto No. 301, Kota Bandung dan Kode Pos 40274, Indonesia
¹sierraamri28@gmail.com

* Penulis Korespondensi

Dikirim 3 Mei 2026; Direvisi 6 Mei 2026; Diterima 10 Mei 2026

ABSTRAK

Puskesmas Rahayu memberlakukan sistem filtrasi klinis (screening) guna mengelompokkan pasien berdasarkan derajat risiko penularan, yang terbagi menjadi IGD, TB, ISPA, dan Non-ISPA. Unit pelayanan rawat jalan seperti Poli Umum, Gigi, serta Imunisasi (KIA) dikategorikan ke dalam kelompok Non-ISPA. Kelompok ini memiliki rangkaian birokrasi operasional yang relatif cukup panjang meliputi : pengambilan nomor urut, validasi data di loket pendaftaran internal, dan penyelesaian administrasi di kasir sebelum pasien dapat diperiksa. Panjangnya tahapan ini berisiko dapat menimbulkan penumpukan antrean, kerancuan dalam pemisahan dokumen rekam medis fisik, serta keterlambatan distribusi data resep menuju instalasi farmasi. Studi ini berorientasi untuk mengkaji serta menyusun rancangan Sistem Informasi Pelayanan Rawat Jalan Terpadu yang mampu mendigitalisasi alur kerja kluster Non- ZISPA secara nirkertas (paperless). Metodologi rekayasa sistem yang diterapkan mengacu pada System Development Life Cycle (SDLC) dengan model Waterfall yang ruang lingkupnya dibatasi sampai fase System Design. Proses analisis dikembangkan lewat metode berorientasi objek (Object-Oriented Analysis and Design) menggunakan notasi Unified Modeling Language (UML). Output dari riset ini berupa dokumen cetak biru (blueprint) fungsionalitas sistem yang menyinkronkan data pendaftaran internal, pencatatan rekam medis elektronik terstandarisasi di Poli Umum, visualisasi grafik pada Poli Gigi, serta kalkulator otomatisasi jadwal imunisasi, yang semuanya terhubung secara instan ke modul Kasir dan Farmasi. Melalui pengujian skenario berbasis logika, pemodelan sistem ini terbukti valid untuk memotong rantai birokrasi layanan fisik dan siap diteruskan ke tahap pengkodean (programming).

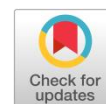


KATA KUNCI

Rekam Medis Elektronik;
Telemedicine;
Blockchain;
Smart Contract;
Keamanan Data Kesehatan.

ABSTRACT

Puskesmas Rahayu implements a clinical screening system to classify patients based on transmission risk levels, segregating them into Emergency Room (ER), Tuberculosis (TB), Acute Respiratory Infection (ARI), and Non-ARI clusters. Outpatient service units, including the General, Dental, and Immunization (MCH) clinics, are designated under the Non-ARI cluster. This specific group undergoes a relatively lengthy administrative workflow, which involves obtaining queue numbers, verifying data at the internal registration desk, and settling administrative clearances at the cashier before receiving clinical examinations. This multi layered process poses significant operational risks, such as bottleneck queues, mismanaged physical medical records, and delayed prescription transmissions to the pharmacy unit. This study aims to analyze and construct a blueprint for an Integrated Outpatient Information System capable of digitalizing the Non-ARI cluster workflow into a paperless ecosystem. The system engineering methodology relies on the System Development Life Cycle (SDLC) Waterfall model, with the scope structurally confined to the System Design phase. The analytical approach is developed through Object-Oriented Analysis and Design (OOAD) utilizing Unified Modeling Language (UML) notations. The output of this research delivers a functional system blueprint that synchronizes internal registration data, standardized electronic medical records in the General Clinic, digital visualizations in the Dental Clinic, and an automated immunization schedule calculator, all of which are instantly cross-linked to the Cashier and Pharmacy modules. Based on logical scenario testing, this system modeling is proven valid in eliminating physical bureaucratic bottlenecks and is fully prepared for the programming stage.



KEYWORD

Electronic Medical Records;
Telemedicine;
Blockchain;
Smart Contracts;
Health Data Security.



This is an open-access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam sistem pelayanan kesehatan, salah satunya melalui penerapan telemedicine. Telemedicine merupakan layanan kesehatan jarak jauh yang memanfaatkan teknologi digital untuk mendukung konsultasi, diagnosis, pengobatan, hingga monitoring pasien tanpa harus melakukan tatap muka secara langsung. Implementasi telemedicine semakin berkembang sejak meningkatnya kebutuhan pelayanan kesehatan yang cepat, efisien, dan mudah diakses oleh masyarakat. Dalam praktiknya, telemedicine sangat berkaitan dengan penggunaan Rekam Medis Elektronik (RME) sebagai media penyimpanan dan pertukaran informasi kesehatan pasien secara digital.

Rekam Medis Elektronik memiliki peran penting dalam mendukung kontinuitas pelayanan kesehatan karena mampu menyediakan data pasien secara cepat, akurat, dan terintegrasi. Namun, penggunaan RME pada layanan telemedicine juga menimbulkan berbagai tantangan, terutama terkait keamanan dan kerahasiaan data pasien. Data kesehatan merupakan informasi yang bersifat sensitif sehingga rentan terhadap ancaman seperti kebocoran data, manipulasi informasi, akses tidak sah, hingga serangan siber. Permasalahan keamanan data kesehatan menjadi perhatian penting karena dapat memengaruhi kepercayaan pasien terhadap layanan telemedicine serta berdampak pada aspek hukum dan etika pelayanan kesehatan.

Di Indonesia, perlindungan data kesehatan telah diatur dalam berbagai regulasi, seperti Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan [1], Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [2], serta Peraturan Menteri Kesehatan terkait penyelenggaraan rekam medis elektronik. Regulasi tersebut menegaskan bahwa fasilitas pelayanan kesehatan wajib menjaga keamanan, kerahasiaan, integritas, dan ketersediaan data pasien. Oleh karena itu, diperlukan sistem keamanan yang mampu memberikan perlindungan optimal terhadap data rekam medis elektronik, khususnya pada layanan telemedicine.

Salah satu teknologi yang dinilai mampu meningkatkan keamanan data rekam medis elektronik adalah blockchain. Blockchain merupakan teknologi penyimpanan data terdesentralisasi yang memiliki karakteristik transparansi, immutability, dan keamanan tinggi melalui mekanisme kriptografi. Pada sistem blockchain, setiap transaksi atau perubahan data tercatat secara permanen dan sulit dimanipulasi, sehingga dapat meningkatkan integritas data rekam medis elektronik. Selain itu, penggunaan smart contract memungkinkan proses autentikasi, validasi, dan pengaturan hak akses data dilakukan secara otomatis sesuai aturan yang telah diprogram sebelumnya. Kombinasi blockchain dan smart contract dinilai dapat meminimalkan risiko kebocoran maupun penyalahgunaan data pasien pada layanan telemedicine.

Klinik Pratama Medika sebagai salah satu fasilitas pelayanan kesehatan yang mulai memanfaatkan teknologi digital dalam pelayanan kesehatan perlu memperhatikan aspek keamanan rekam medis elektronik pada sistem telemedicine yang digunakan. Pengelolaan data pasien secara elektronik membutuhkan mekanisme perlindungan yang memadai agar keamanan informasi kesehatan tetap terjaga. Evaluasi terhadap penerapan keamanan data pada layanan telemedicine menjadi penting untuk mengetahui efektivitas sistem yang digunakan serta mengidentifikasi potensi risiko keamanan informasi.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis keamanan rekam medis elektronik pada layanan telemedicine menggunakan teknologi blockchain dan smart contract di Klinik Pratama Medika. Penelitian ini diharapkan dapat memberikan gambaran mengenai penerapan teknologi keamanan data kesehatan modern dalam mendukung pelayanan telemedicine yang aman, efektif, dan sesuai dengan regulasi yang berlaku. Selain itu, hasil penelitian diharapkan dapat menjadi bahan pertimbangan bagi fasilitas pelayanan kesehatan dalam meningkatkan sistem keamanan rekam medis elektronik di era transformasi digital kesehatan.

2. Tinjauan Pustaka

2.1 Penelitian Terdahulu yang Relevan

Penelitian Azaria dkk. [3] menyimpulkan bahwa teknologi *blockchain* mampu meningkatkan keamanan data rekam medis melalui sistem desentralisasi dan kriptografi serta menjelaskan bahwa *blockchain* dapat menjaga integritas, autentikasi, serta kerahasiaan data pasien pada sistem rekam medis elektronik.

Sedangkan pada Ekblaw dkk. [4] menemukan bahwa penerapan *blockchain* dan *smart contract* pada rekam medis elektronik mampu meningkatkan kontrol akses data pasien dan interoperabilitas antar fasilitas pelayanan Kesehatan dan menunjukkan bahwa pasien dapat memiliki kendali lebih besar terhadap data kesehatannya melalui mekanisme *smart contract* yang otomatis dan transparan. Berdasarkan beberapa penelitian terdahulu

tersebut, dapat diketahui bahwa *blockchain* dan *smart contract* memiliki potensi besar dalam meningkatkan keamanan rekam medis elektronik pada layanan *telemedicine*. Namun, sebagian besar penelitian masih berfokus pada pengembangan sistem dan simulasi teknologi, sehingga penelitian terkait implementasi keamanan rekam medis elektronik berbasis *blockchain* dan *smart contract* pada fasilitas pelayanan kesehatan tingkat klinik masih terbatas. Oleh karena itu, penelitian ini dilakukan untuk menganalisis keamanan Rekam Medis Elektronik pada *telemedicine* di Klinik Pratama Medika di era integrasi global, di mana faktor keamanan data dan kepercayaan pengguna diprediksi memiliki pola pengaruh yang berbeda terhadap kualitas pelayanan kesehatan digital.

2.2 Kajian Teori dan Konsep

2.2.1 Keamanan Informasi pada Rekam Medis Elektronik (Keamanan RME – X1)

Rekam Medis Elektronik (RME) merupakan sistem pencatatan data kesehatan pasien yang dibuat dan disimpan dalam bentuk digital. RME berfungsi untuk mendokumentasikan identitas pasien, hasil pemeriksaan, diagnosis, tindakan medis, pengobatan, serta pelayanan kesehatan lainnya yang diberikan oleh tenaga kesehatan. Penggunaan RME bertujuan meningkatkan efisiensi pelayanan, mempercepat akses informasi kesehatan, serta mendukung integrasi data antar fasilitas pelayanan kesehatan. Menurut World Health Organization (WHO) [5], rekam medis elektronik memiliki peranan penting dalam meningkatkan mutu pelayanan kesehatan karena mampu menyediakan informasi pasien secara cepat, akurat, dan berkesinambungan. Selain itu, penerapan RME juga mendukung transformasi digital kesehatan dalam pelayanan modern.

Di Indonesia, penyelenggaraan rekam medis elektronik diatur dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis [6]. Dalam regulasi tersebut dijelaskan bahwa setiap fasilitas pelayanan kesehatan wajib menjaga keamanan, kerahasiaan, integritas, dan ketersediaan data rekam medis pasien. Keunggulan RME antara lain yaitu mempermudah akses informasi pasien, mengurangi penggunaan kertas, meningkatkan efisiensi pelayanan, mendukung interoperabilitas data kesehatan, serta mempermudah penyimpanan dan pencarian data.

Keamanan informasi merupakan upaya melindungi data dan sistem informasi dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Pada sistem rekam medis elektronik, keamanan informasi menjadi aspek penting karena data kesehatan bersifat rahasia dan sensitif. Konsep keamanan informasi dikenal dengan istilah CIA Triad [7], yaitu:

1. Confidentiality (Kerahasiaan), menjamin bahwa data pasien hanya dapat diakses oleh pihak yang berwenang.
2. Integrity (Integritas), menjamin bahwa data tidak berubah atau dimanipulasi tanpa izin.
3. Availability (Ketersediaan), menjamin bahwa data dapat diakses ketika dibutuhkan dalam pelayanan kesehatan.

Kontrol hak akses pengguna (access control) merupakan mekanisme keamanan informasi yang digunakan untuk mengatur dan membatasi akses pengguna terhadap sistem maupun data tertentu sesuai dengan kewenangan yang dimiliki. Pada sistem Rekam Medis Elektronik (RME), kontrol hak akses sangat penting untuk menjaga kerahasiaan, integritas, dan keamanan data pasien agar tidak diakses oleh pihak yang tidak berwenang.

Menurut National Institute of Standards and Technology (NIST) [8], access control adalah proses pemberian otorisasi kepada pengguna, program, atau sistem untuk mengakses sumber daya tertentu berdasarkan kebijakan keamanan yang telah ditetapkan. Kontrol akses bertujuan untuk memastikan bahwa hanya pengguna yang memiliki hak tertentu yang dapat melihat, mengubah, atau mengelola data kesehatan pasien.

Dalam sistem pelayanan kesehatan digital dan *telemedicine*, kontrol hak akses dilakukan melalui proses autentikasi dan otorisasi pengguna. Autentikasi merupakan proses verifikasi identitas pengguna, seperti penggunaan username dan password, sedangkan otorisasi merupakan proses pemberian hak akses sesuai peran atau tugas pengguna dalam sistem.

1) Telemedicine (Telemedicine – X2)

Telemedicine merupakan pelayanan kesehatan jarak jauh yang memanfaatkan teknologi informasi dan komunikasi untuk pertukaran informasi medis guna diagnosis, pengobatan, pencegahan penyakit, penelitian,

dan pendidikan kesehatan. Telemedicine memungkinkan pasien memperoleh pelayanan kesehatan tanpa harus datang langsung ke fasilitas pelayanan kesehatan. Menurut WHO, telemedicine adalah penggunaan teknologi komunikasi untuk memberikan layanan kesehatan ketika jarak menjadi faktor utama. Implementasi telemedicine berkembang pesat seiring meningkatnya kebutuhan pelayanan kesehatan digital. Manfaat Telemedicine yaitu mempermudah akses pelayanan kesehatan, menghemat waktu dan biaya pasien, meningkatkan efisiensi pelayanan, mendukung pelayanan kesehatan di daerah terpencil, dan mengurangi kontak langsung pada kondisi tertentu.

2) Blockchain dan Smart Contract (Y)

Blockchain merupakan teknologi penyimpanan data digital berbentuk rantai blok yang terhubung menggunakan kriptografi. Teknologi ini bersifat desentralisasi sehingga data tidak tersimpan pada satu server pusat, melainkan tersebar pada beberapa node dalam jaringan. Konsep blockchain pertama kali diperkenalkan oleh Satoshi Nakamoto [9] melalui pengembangan cryptocurrency Bitcoin. Saat ini, blockchain telah banyak digunakan dalam berbagai bidang, termasuk kesehatan.

Smart contract merupakan program digital otomatis yang berjalan pada jaringan blockchain untuk menjalankan aturan atau perjanjian tertentu tanpa pihak ketiga. Smart contract bekerja berdasarkan kondisi yang telah diprogram sebelumnya. Dalam bidang kesehatan, smart contract digunakan untuk mengatur akses data rekam medis elektronik secara otomatis sesuai hak akses pengguna. Menurut Budiyanto [8] Smart contract adalah program komputer otomatis yang berjalan di jaringan blockchain untuk mengotomatisasi pelaksanaan kontrak sesuai aturan yang telah ditentukan.

2.3 Kerangka Berpikir

Penelitian ini membahas pengaruh keamanan Rekam Medis Elektronik (RME) dan pelaksanaan telemedicine terhadap penerapan blockchain dan smart contract dalam sistem pelayanan kesehatan digital. RME merupakan bagian penting dalam pelayanan kesehatan modern karena berfungsi sebagai media penyimpanan dan pengelolaan data pasien secara digital. Dalam implementasinya, keamanan RME menjadi faktor utama untuk menjaga kerahasiaan, integritas, dan ketersediaan data pasien.

Selain itu, telemedicine sebagai layanan kesehatan berbasis teknologi informasi memerlukan sistem keamanan yang kuat karena proses pertukaran data kesehatan dilakukan melalui jaringan digital. Risiko seperti kebocoran data, akses ilegal, manipulasi informasi, dan serangan siber menjadi tantangan dalam penggunaan telemedicine. Blockchain hadir sebagai teknologi keamanan data berbasis desentralisasi yang mampu menjaga integritas dan transparansi data rekam medis elektronik. Sementara itu, smart contract berfungsi untuk mengatur autentikasi, validasi, dan hak akses pengguna secara otomatis sesuai aturan yang telah diprogram. Penerapan blockchain dan smart contract diperkirakan dapat meningkatkan keamanan sistem telemedicine dan perlindungan data pasien.

Berdasarkan uraian tersebut, penelitian ini menganalisis pengaruh Keamanan Rekam Medis Elektronik (X1) dan Telemedicine (X2) terhadap Blockchain dan Smart Contract (Y) pada sistem pelayanan kesehatan digital di Klinik Pratama Medika.

2.4 Hipotesis Penelitian

Penelitian ini merumuskan hipotesis untuk mengetahui apakah terdapat pengaruh antara variabel independen terhadap variabel dependen sebagai berikut:

- H1: Terdapat pengaruh Keamanan Rekam Medis Elektronik (X1) terhadap penerapan *Blockchain* dan *Smart Contract* (Y).
- H2: Terdapat pengaruh *Telemedicine* (X2) terhadap penerapan *Blockchain* dan *Smart Contract* (Y).
- H3: Terdapat pengaruh Keamanan Rekam Medis Elektronik (X1) dan *Telemedicine* (X2) secara simultan terhadap *Blockchain* dan *Smart Contract* (Y).

3. Metodologi Penelitian

3.1 Jenis Penelitian

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan deskriptif. Metode kualitatif deskriptif digunakan untuk menggambarkan secara mendalam mengenai keamanan RME pada telemedicine menggunakan blockchain dan smart contract di Klinik Pratama Medika. Pendekatan ini dipilih karena penelitian berfokus pada pemahaman fenomena, proses, serta kondisi nyata terkait penerapan keamanan data kesehatan dalam pelayanan telemedicine.

Penelitian deskriptif bertujuan untuk memperoleh informasi secara sistematis, faktual, dan akurat mengenai implementasi keamanan rekam medis elektronik, hambatan yang dihadapi, serta upaya peningkatan keamanan data pada sistem telemedicine.

3.2 Populasi, Sampel, dan Teknik Penarikan Sampel

1) Populasi

Populasi dalam penelitian ini adalah seluruh tenaga kesehatan dan petugas yang terlibat dalam penggunaan RME dan pelaksanaan layanan telemedicine di Klinik Pratama Medika. Populasi penelitian dipilih karena memiliki keterkaitan langsung dengan pengelolaan keamanan data RME dan penggunaan sistem telemedicine di fasilitas pelayanan kesehatan. Populasi tersebut dijabarkan pada Tabel 1.

Table 1. Jumlah Populasi

Populasi	Banyak (orang)
Kepala Rekam Medis	1
Perekam Medis	7
Dokter	18
Perawat	10
Apoteker	2
Staf Teknologi Informasi (IT)	4
Operator Sistem <i>Telemedicine</i>	2
Total Populasi	44

2) Sampel

Sampel dalam penelitian ini merupakan sebagian dari populasi yang dipilih sebagai informan penelitian untuk memberikan informasi terkait keamanan RME pada telemedicine menggunakan blockchain dan smart contract. Jumlah sampel dalam penelitian kualitatif tidak ditentukan berdasarkan perhitungan statistik, tetapi berdasarkan kecukupan informasi. Oleh karena itu, penelitian ini menggunakan teknik purposive sampling, yaitu pemilihan informan berdasarkan keterlibatan langsung dalam penggunaan RME, telemedicine, serta sistem keamanan data kesehatan.

Menurut pendapat Sugiyono [10] penelitian kualitatif umumnya menggunakan jumlah informan antara 5–25 orang tergantung kebutuhan data dan tingkat kejenuhan informasi. Dalam penelitian ini, peneliti memfokuskan informan pada pihak yang paling relevan terhadap keamanan RME dan telemedicine. Adapun sampel atau informan penelitian pada Tabel 2 sebagai berikut:

Table 2. Sampel Penelitian

Kode Informan	Informan	Banyak (orang)
Informan Utama 1	Kepala Rekam Medis	1
Informan Utama 2, 3	Perekam Medis	2
Informan Pendukung 1	Dokter	1
Informan Pendukung 2	Perawat	1

Informan Pendukung 3	Apoteker	1
Informan Kunci 1	Staf Teknologi Informasi (IT)	1
Informan Kunci 2	Operator Sistem Telemedicine	1
Total Sampel		8

Peneliti menetapkan jumlah awal sebanyak 8 informan karena dianggap telah mewakili seluruh unit yang berkaitan langsung dengan pengelolaan Rekam Medis Elektronik dan telemedicine. Apabila dalam proses wawancara masih ditemukan informasi baru, maka jumlah informan dapat ditambah sampai mencapai titik kejenuhan data (data saturation).

3) Teknik Penarikan Sampel

Teknik penarikan sampel yang digunakan dalam penelitian ini yaitu *purposive sampling*. *Purposive sampling* merupakan teknik pemilihan sampel berdasarkan pertimbangan tertentu yang disesuaikan dengan tujuan penelitian. Kriteria informan dalam penelitian ini meliputi:

1. Terlibat langsung dalam penggunaan Rekam Medis Elektronik (RME),
2. Memahami pelaksanaan *telemedicine* di klinik,
3. Memiliki pengetahuan mengenai sistem keamanan data kesehatan,
4. Bersedia menjadi informan penelitian.

3.2 Fokus Penelitian

Fokus penelitian dalam penelitian kualitatif ini diarahkan pada analisis keamanan Rekam Medis Elektronik (RME) pada telemedicine menggunakan blockchain dan smart contract di Klinik Pratama Medika. Adapun aspek yang dikaji dalam penelitian meliputi:

Table 3. Fokus Penelitian

No	Topik Wawancara
1	Keamanan Rekam Medis Elektronik (RME)
	a. Kerahasiaan Data Pasien (<i>Confidentiality</i>)
	b. Integritas Data (<i>Integrity</i>)
	c. Ketersediaan Data (<i>Availability</i>)
	d. Kontrol Hak Akses Pengguna (<i>Access Control</i>)
2	Pelaksanaan <i>Telemedicine</i>
3	Penerapan Blockchain
4	Penerapan Smart Contract

3.3 Metode Pengumpulan Data

1) Metode pengumpulan data

Metode pengumpulan data pada penelitian ini meliputi:

- a. Wawancara mendalam, dilakukan secara langsung kepada informan penelitian untuk memperoleh informasi terkait pelaksanaan keamanan RME, penggunaan telemedicine, penerapan blockchain dan smart contract, serta kendala yang dihadapi dalam pengelolaan data kesehatan digital.
- b. Observasi, dilakukan dengan mengamati secara langsung proses penggunaan rekam medis elektronik dan sistem telemedicine di Klinik Pratama Medika, khususnya terkait keamanan akses data dan pengelolaan informasi pasien.
- c. Dokumentasi, dilakukan dengan mengumpulkan dokumen pendukung seperti kebijakan keamanan data, prosedur operasional standar (SOP), laporan penggunaan sistem, serta regulasi terkait rekam medis elektronik dan telemedicine.

2) Instrumen Penelitian

Instrumen utama dalam penelitian kualitatif adalah peneliti sendiri. Selain itu, penelitian ini menggunakan pedoman wawancara, lembar observasi, alat perekam suara, dan dokumentasi sebagai instrumen pendukung dalam proses pengumpulan data.

3) Teknik Analisis Data

Analisis data dalam penelitian ini menggunakan model analisis interaktif Miles dan Huberman [11] yang meliputi:

- Reduksi Data, dimana data yang diperoleh dari hasil wawancara, observasi, dan dokumentasi diseleksi, disederhanakan, dan difokuskan sesuai tujuan penelitian.
- Penyajian Data, dimana data yang telah direduksi kemudian disajikan dalam bentuk uraian naratif, tabel, maupun bagan agar mudah dipahami.
- Penarikan Kesimpulan, yaitu tahap akhir dilakukan dengan menarik kesimpulan berdasarkan hasil analisis data mengenai keamanan RME pada *telemedicine* menggunakan *blockchain* dan *smart contract*.

4) Uji Keabsahan Data

Keabsahan data dalam penelitian ini dilakukan menggunakan teknik triangulasi, yaitu triangulasi sumber, triangulasi teknik, dan triangulasi waktu. Teknik tersebut digunakan untuk memastikan bahwa data yang diperoleh valid, akurat, dan dapat dipercaya.

5) Etika Penelitian

Penelitian ini memperhatikan prinsip etika penelitian, antara lain:

- Menjaga kerahasiaan identitas informan
- Meminta persetujuan informan sebelum wawancara
- Menjamin kerahasiaan data penelitian
- Menggunakan data hanya untuk kepentingan penelitian

4. Hasil dan Pembahasan

4.1 Hasil

Penelitian ini dilaksanakan di Klinik Pratama Medika dengan tujuan menganalisis keamanan Rekam Medis Elektronik (RME) pada *telemedicine* menggunakan *blockchain* dan *smart contract*. Data penelitian diperoleh melalui wawancara mendalam, observasi, dan dokumentasi terhadap informan yang terdiri dari kepala klinik, perekam medis, dokter, perawat, staf teknologi informasi (IT), serta operator sistem *telemedicine*.

Berdasarkan hasil analisis data, keamanan Rekam Medis Elektronik pada *telemedicine* dianalisis melalui empat aspek utama, yaitu kerahasiaan data pasien, integritas data, ketersediaan data, dan kontrol hak akses pengguna menggunakan *blockchain* dan *smart contract* pada Tabel 4 berikut ini:

Table 4. Kesimpulan Analisis Data

No	Aspek yang dianalisis	Hasil Wawancara, Observasi, dan Dokumentasi
1	Kerahasiaan Data Pasien (<i>Confidentiality</i>)	Menggunakan <i>username</i> dan <i>password</i> untuk setiap pengguna. Akses data pasien dibatasi sesuai kewenangan pengguna. Terdapat SOP kerahasiaan data dan autentikasi pengguna pada sistem <i>telemedicine</i> . Namun, <i>password</i> masih sederhana dan belum dilakukan pergantian secara berkala. Sistem belum menggunakan <i>blockchain</i> dalam penyimpanan data.
2	Integritas Data (<i>Integrity</i>)	Sistem mencatat histori aktivitas pengguna, waktu akses, dan perubahan data. Data tidak dapat dihapus oleh pengguna umum dan hanya dapat diperbaiki oleh administrator yang bertujuan menjaga keaslian dan integritas data pasien. Audit trail telah tersedia, namun belum menggunakan validasi berbasis <i>blockchain</i> .
3	Ketersediaan Data (<i>Availability</i>)	Data rekam medis dapat diakses dengan cepat

		selama jaringan dan server berfungsi dengan baik. Klinik melakukan <i>backup data</i> secara berkala. Namun masih terdapat gangguan jaringan dan belum tersedia <i>backup server</i> untuk pemulihan sistem secara menyeluruh. <i>Telemedicine</i> cukup membantu pelayanan pasien karena data kesehatan dapat diakses secara digital tanpa penggunaan rekam medis konvensional.
4	Kontrol Hak Akses Pengguna (<i>Access Control</i>) menggunakan <i>Blockchain</i> dan <i>Smart Contract</i>	Sesuai tugas dan tanggung jawabnya. Sistem telah menerapkan autentikasi login, tetapi masih menggunakan username dan password tanpa autentikasi dua faktor. Informan menilai <i>blockchain</i> dan <i>smart contract</i> dapat meningkatkan pengelolaan hak akses terutama dalam pengaturan hak akses otomatis dan pencatatan aktivitas pengguna secara transparan.

4.2 Pembahasan

Berdasarkan hasil penelitian, Klinik Pratama Medika telah menerapkan upaya perlindungan kerahasiaan data pasien melalui sistem login dan pembatasan hak akses pengguna. Hal ini sejalan dengan prinsip confidentiality dalam keamanan informasi yang bertujuan menjaga data pasien agar hanya dapat diakses oleh pihak yang berwenang. Meskipun demikian, penelitian menemukan bahwa sistem keamanan masih menggunakan password sederhana dan belum menerapkan teknologi *blockchain* maupun autentikasi berlapis. Kondisi tersebut dapat meningkatkan risiko kebocoran data dan akses ilegal pada layanan *telemedicine*.

Integritas data merupakan kemampuan sistem menjaga keaslian dan konsistensi data pasien. Hasil penelitian menunjukkan bahwa sistem RME telah memiliki audit trail untuk mencatat aktivitas pengguna. Hal ini membantu memantau perubahan data pasien serta mengurangi risiko manipulasi data. Namun, sistem yang digunakan masih bersifat terpusat sehingga data tetap memiliki potensi untuk diubah oleh administrator tertentu. Penggunaan *blockchain* dapat menjadi solusi dalam meningkatkan integritas data karena teknologi tersebut memiliki sifat immutability, yaitu data sulit dimodifikasi setelah tersimpan dalam jaringan *blockchain*.

Ketersediaan data menjadi aspek penting dalam pelayanan *telemedicine* karena data pasien harus dapat diakses dengan cepat saat dibutuhkan. Hasil penelitian menunjukkan bahwa sistem *telemedicine* cukup membantu pelayanan kesehatan karena memungkinkan akses data pasien secara digital dan efisien. Namun, gangguan jaringan internet masih menjadi hambatan utama dalam akses data *telemedicine*. Selain itu, belum tersedianya *backup server* dapat meningkatkan risiko kehilangan data apabila terjadi gangguan sistem. Availability bertujuan memastikan bahwa data tetap tersedia dan dapat digunakan saat diperlukan. Oleh karena itu, diperlukan penguatan infrastruktur teknologi informasi serta sistem pemulihan data yang lebih baik.

Hasil penelitian menunjukkan bahwa kontrol hak akses pengguna telah diterapkan berdasarkan tugas masing-masing pengguna sistem. Akan tetapi, mekanisme autentikasi masih bersifat konvensional sehingga memiliki risiko penyalahgunaan akun pengguna. Penerapan *blockchain* dan *smart contract* dinilai berpotensi meningkatkan keamanan sistem melalui autentikasi otomatis, validasi akses pengguna, serta pencatatan aktivitas pengguna secara transparan. *Smart contract* dapat digunakan untuk mengatur hak akses data pasien secara otomatis sesuai kewenangan tenaga kesehatan. Teknologi *blockchain* juga memungkinkan pencatatan data secara permanen dan transparan sehingga dapat meningkatkan kepercayaan pengguna terhadap keamanan sistem *telemedicine*. Secara keseluruhan, hasil penelitian menunjukkan bahwa keamanan RME pada *telemedicine* di Klinik Pratama Medika sudah cukup baik, namun masih memerlukan pengembangan teknologi keamanan berbasis *blockchain* dan *smart contract* untuk meningkatkan perlindungan data pasien, integritas data, serta keamanan akses pengguna pada sistem pelayanan kesehatan digital.

5. Penutup

5.1 Kesimpulan

Keamanan Rekam Medis Elektronik (RME) pada *telemedicine* di Klinik Pratama Medika telah menerapkan sistem keamanan dasar berupa penggunaan *username* dan *password*, pembatasan hak akses pengguna, serta pencatatan aktivitas pengguna dalam sistem. Hal tersebut menunjukkan bahwa klinik telah berupaya menjaga kerahasiaan dan keamanan data pasien.

Aspek kerahasiaan data pasien telah diterapkan melalui pembatasan akses sesuai kewenangan pengguna. Namun, sistem keamanan masih memiliki kelemahan karena belum menggunakan autentikasi berlapis dan teknologi keamanan berbasis blockchain sehingga masih berpotensi mengalami risiko akses ilegal maupun kebocoran data.

Integritas data Rekam Medis Elektronik sudah didukung dengan adanya *audit trail* dan pembatasan perubahan data oleh pengguna tertentu. Akan tetapi, sistem yang digunakan masih bersifat terpusat sehingga belum sepenuhnya mampu mencegah manipulasi data secara permanen.

Ketersediaan data pada layanan *telemedicine* dinilai cukup baik karena data pasien dapat diakses secara digital dengan cepat saat dibutuhkan. Namun, kendala jaringan internet dan belum tersedianya *backup server* masih menjadi hambatan dalam menjaga stabilitas pelayanan *telemedicine*.

Kontrol hak akses pengguna telah diterapkan sesuai tugas dan tanggung jawab masing-masing tenaga kesehatan. Penerapan *blockchain* dan *smart contract* dinilai memiliki potensi dalam meningkatkan keamanan sistem melalui autentikasi otomatis, validasi akses pengguna, transparansi data, dan perlindungan data pasien secara lebih optimal.

Secara keseluruhan, keamanan Rekam Medis Elektronik pada *telemedicine* di Klinik Pratama Medika sudah berjalan cukup baik, namun masih memerlukan pengembangan teknologi keamanan informasi berbasis *blockchain* dan *smart contract* untuk meningkatkan perlindungan data kesehatan pasien pada pelayanan kesehatan digital.

5.2 Saran

Klinik diharapkan dapat meningkatkan sistem keamanan Rekam Medis Elektronik dengan menerapkan autentikasi berlapis, memperkuat pengelolaan password pengguna, serta mengembangkan sistem keamanan berbasis blockchain dan smart contract untuk meningkatkan perlindungan data pasien pada layanan *telemedicine*. Petugas kesehatan dan pengguna sistem diharapkan dapat meningkatkan kesadaran terhadap pentingnya keamanan data pasien dengan menjaga kerahasiaan akun pengguna, mematuhi prosedur keamanan sistem, dan menggunakan akses data sesuai kewenangan masing-masing. Pengembang sistem diharapkan dapat mengembangkan sistem *telemedicine* yang lebih aman melalui penerapan blockchain, smart contract, audit trail yang lebih optimal, serta sistem autentikasi otomatis guna meminimalkan risiko kebocoran dan manipulasi data pasien. Peneliti selanjutnya diharapkan dapat melakukan penelitian lebih mendalam terkait implementasi blockchain dan smart contract pada Rekam Medis Elektronik dengan metode penelitian yang berbeda, cakupan fasilitas pelayanan kesehatan yang lebih luas, serta pengukuran efektivitas teknologi keamanan informasi kesehatan secara lebih komprehensif.

Daftar Pustaka

- [1] Republik Indonesia. "Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang Kesehatan," Jakarta: Pemerintah Republik Indonesia; 2023.
- [2] Republik Indonesia. "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi," Jakarta: Pemerintah Republik Indonesia; 2022.
- [3] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. 2016. "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, pp. 25–30. IEEE; 2016. <https://doi.org/10.1109/OBD.2016.11>
- [4] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. "A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data," MIT Media Lab White Paper, Massachusetts Institute of Technology; 2016.
- [5] World Health Organization. "Consolidated Telemedicine Implementation Guide," Geneva: World Health Organization; 2022. Available at: WHO Consolidated Telemedicine Implementation Guide.
- [6] Kementerian Kesehatan Republik Indonesia. "Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis," Jakarta: Kementerian Kesehatan Republik Indonesia; 2022. Available at: JDIH Kementerian Kesehatan RI.

- [9] Whitman, M. E., & Mattord, H. J. "Principles of Information Security", 7th Edition. Boston: Cengage Learning; 2022.
- [10] National Institute of Standards and Technology (NIST). "Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)," Gaithersburg: U.S. Department of Commerce; 2020.
- [11] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. Available at: <https://bitcoin.org/bitcoin.pdf>.
- [12] Sugiyono. "Metode Penelitian Kualitatif, Kuantitatif dan R&D," Bandung: Alfabeta; 2023.
- [13] Miles, M. B., Huberman, A. M., & Saldaña, J. "Qualitative Data Analysis: A Methods Sourcebook," 3rd Edition. Thousand Oaks, California: Sage Publications; 2014.