JURNAL ILMIAH FIFO **P-ISSN 2085-4315 / E-ISSN 2502-8332**
DOI: http://dx.doi.org/10.22441/fifo.2024.v16i2.001

Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan *Systematic Literature Review*

Hastin Atas Asih[1*], Indrayadi[2], Soraya[3], Khairunnisa[4]

Sarjana Terapan Manajemen Informasi Kesehatan, Politeknik Kesdam VI Banjarmasin[1,3]
Diploma III Keperawatan, Politeknik Kesdam VI Banjarmasin[2]
Diploma III Perekam dan Informasi Kesehatan, Stikes Husada Borneo[4]
hastinatasasih87@gmail.com[1*], ketikindrayadi@gmail.com[2], aryamik@gmail.com[3], khairunnisa@gmail.com[4]

*) Corresponding Author

(***received*****:** 07-05-24, ***revised*****:** 19-06-24, ***accepted*****:** 17-07-24)

Abstract

This research aims to evaluate security threats and patient data vulnerabilities, proposing effective solutions to enhance system security and patient data integrity in Electronic Medical Record (EMR) systems through a Systematic Literature Review. Literature sources are from reputable indexes such as DOAJ, Scopus, and Google Scholar with publication years from 2013 to 2024. The findings indicate that security issues in EMR are critical, affecting the integrity and confidentiality of patient data in modern healthcare. The review identifies key factors influencing EMR security, including regulatory compliance, technological infrastructure, and human factors. Proposed solutions include the use of authentication, encryption, temporal signatures, and proactive measures to raise awareness of patient data privacy. Thus, this research provides important insights for understanding and addressing security challenges in patient data management through EMR systems.

.

Keywords*: Electronic Medical Record Systems, Security Threats, Patient Data Vulnerabilities*

Abstrak

Penelitian ini bertujuan untuk melakukan evaluasi terhadap ancaman keamanan dan kerentanan data pasien, serta mengusulkan solusi-solusi yang efektif untuk meningkatkan keamanan sistem dan integritas data pasien dalam sistem rekam medis elektronik (RME) melalui *Systematic Literature Review*. Sumber literatur berasal dari pengindeks terpercaya seperti DOAJ, Scopus, dan Google Scholar dengan interval tahun terbit antara tahun 2013 hingga tahun 2024. Hasil penelitian menunjukkan bahwa masalah keamanan dalam RME menjadi isu krusial yang memengaruhi integritas dan kerahasiaan data pasien dalam layanan kesehatan modern. Tinjauan literatur mengidentifikasi berbagai faktor kunci yang memengaruhi keamanan RME, termasuk kepatuhan terhadap peraturan, infrastruktur teknologi, dan faktor manusia. Solusi yang telah diajukan antara lain penggunaan autentikasi, enkripsi, tanda tangan temporal, dan langkah-langkah proaktif untuk meningkatkan kesadaran akan privasi data pasien. Dengan demikian, penelitian ini menyajikan wawasan yang penting untuk memahami dan mengatasi tantangan keamanan dalam pengelolaan data pasien melalui sistem RME.

Kata Kunci: Sistem Rekam Medis Elektronik, Ancaman Keamanan, Kerentanan Data Pasien

I. Pendahuluan

Rekam Medis Elektronik (RME) merupakan sebuah konsep pengelolaan informasi kesehatan pasien dalam bentuk digital [1], yang memainkan peran penting dalam perkembangan industri kesehatan modern. Peran RME yang krusial terletak pada efisiensi, akurasi, dan aksesibilitas informasi pasien. Dalam era kesehatan yang semakin kompleks dan terhubung secara digital, RME memungkinkan penyedia layanan kesehatan untuk dengan mudah mengakses rekam medis pasien dari berbagai tempat, memfasilitasi koordinasi perawatan yang lebih baik, dan memastikan bahwa informasi pasien tersedia secara tepat waktu ketika dibutuhkan. RME juga membawa perubahan signifikan dalam cara informasi pasien disimpan dan dikelola [2]. Menggantikan sistem tradisional berbasis kertas, RME memperkenalkan model pengelolaan data yang terstruktur dan terorganisir

secara digital. Ini mengurangi ketergantungan pada penyimpanan fisik berbasis kertas yang memakan banyak ruang dan membutuhkan biaya penyimpanan yang signifikan. Dengan RME informasi pasien dapat disimpan secara elektronik dan diakses dengan cepat melalui komputer atau perangkat lainnya [3], menghilangkan kebutuhan akan pencarian manual yang memakan waktu dan meminimalkan risiko kehilangan atau kerusakan dokumen.

Pentingnya menjaga keamanan data pasien dalam sistem RME menjadi fokus utama dalam era digitalisasi kesehatan saat ini [4]. Keamanan data pasien adalah fondasi dari integritas sistem kesehatan modern, karena informasi medis yang sensitif dapat menjadi target utama bagi pihak yang tidak bertanggung jawab. Penjagaan keamanan data pasien dalam RME mencakup langkah-langkah seperti enkripsi data, akses terbatas dengan izin yang sesuai, serta pemantauan dan deteksi kegiatan yang mencurigakan. Hal ini penting untuk melindungi privasi dan kerahasiaan informasi pasien, serta memastikan bahwa data medis hanya diakses oleh pihak yang berwenang. Pelanggaran keamanan data pasien dalam sistem RME dapat memiliki konsekuensi negatif yang serius [5]. Salah satu risiko utama adalah potensi pencurian identitas, di mana informasi pribadi dan medis pasien dapat digunakan untuk tujuan penipuan atau kejahatan identitas lainnya. Penyalahgunaan informasi medis juga dapat terjadi, di mana data medis pasien disalahgunakan untuk keuntungan finansial [6], atau untuk merugikan individu yang bersangkutan secara pribadi atau profesional. Dampaknya bisa sangat merugikan, baik bagi pasien secara langsung maupun bagi kepercayaan publik terhadap sistem kesehatan secara keseluruhan.

Sistem RME menghadapi berbagai jenis ancaman keamanan yang dapat membahayakan integritas dan kerahasiaan informasi pasien. Salah satu ancaman utama adalah serangan siber, di mana peretas menggunakan teknologi untuk mengakses, merusak, atau mencuri data pasien [7]. Serangan siber dapat mencakup aktivitas seperti peretasan sistem, malware, ransomware, atau serangan phishing yang bertujuan untuk memperoleh informasi login dan sandi [8]. Pencurian fisik juga merupakan ancaman yang signifikan, di mana perangkat keras atau perangkat penyimpanan data RME dapat dicuri atau diakses secara fisik oleh pihak yang tidak berwenang. Ancaman lainnya adalah kesalahan pengguna baik disengaja maupun tidak disengaja seperti pengguna yang tidak sengaja mengungkapkan informasi sensitif atau melakukan tindakan yang dapat merusak keamanan sistem. Kerentanan dalam infrastruktur RME juga dapat dieksploitasi oleh pihak yang tidak bermoral untuk mengakses data pasien secara tidak sah [9]. Kerentanan tersebut dapat berasal dari kelemahan dalam perangkat lunak atau sistem operasi yang digunakan, ketidakmampuan untuk melakukan pembaruan perangkat lunak secara teratur, atau kelemahan dalam konfigurasi sistem yang memungkinkan akses yang tidak sah. Penggunaan perangkat yang tidak aman atau koneksi internet yang tidak terenkripsi juga dapat meningkatkan risiko kerentanan yang dieksploitasi oleh pihak yang tidak bermoral.

Perkembangan terbaru dalam teknologi keamanan telah memperkuat sistem RME. Perkembangan ini termasuk enkripsi data, otentikasi ganda, dan deteksi intrusi [10] [11]. Teknologi ini bertujuan untuk melindungi informasi digital dan melindungi dari entitas jahat dan serangan siber. Selain itu, teknologi baru seperti *Artificial Intelligence* (AI) dan *Machine Learning* (ML) memainkan peran penting dalam mendeteksi dan mencegah ancaman keamanan dalam sistem RME [12]. Algoritma pembelajaran mesin telah ditemukan bekerja lebih baik daripada metode tradisional dalam meningkatkan keamanan [13]. Teknologi AI dan ML digunakan untuk memverifikasi catatan, mendeteksi aktivitas berbahaya, dan menjaga kerahasiaan, integritas, dan ketersediaan RME [14]. Kemajuan dalam teknologi keamanan dan integrasi AI dan ML berkontribusi untuk menciptakan lingkungan yang aman untuk RME dan meningkatkan perawatan pasien di industri perawatan kesehatan.

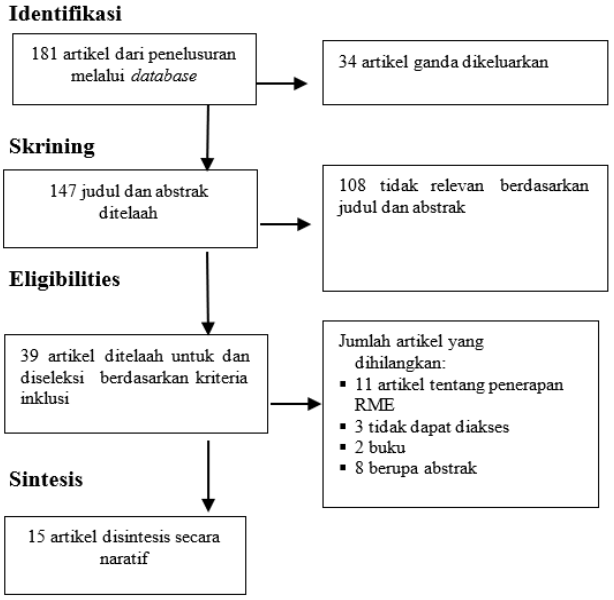
Organisasi kesehatan telah mengakui meningkatnya ancaman kejahatan dunia maya dan kerentanan dalam infrastruktur keamanan mereka, terutama dalam konteks RME [15]. Pandemi COVID-19 semakin menyoroti perlunya peningkatan langkah-langkah keamanan siber dalam sistem perawatan kesehatan [16]. Untuk mengurangi risiko ini, organisasi harus menerapkan berbagai tindakan keamanan, termasuk penilaian keamanan reguler untuk mengidentifikasi kerentanan [17]. Selain itu, memantau aktivitas jaringan dan memperbarui alat keamanan secara teratur dapat membantu mendeteksi dan menanggapi potensi insiden keamanan [18]. Ketergantungan industri perawatan kesehatan pada perangkat yang saling berhubungan, seperti *Internet of Medical Things* (IoMT), telah memperluas permukaan ancaman untuk serangan siber [19].

Mengatasi tantangan keamanan dalam sistem RME dapat dijawab melalui penelitian ini, diharapkan akan tercipta lingkungan yang lebih aman untuk pengelolaan data pasien, yang pada akhirnya akan meningkatkan kualitas layanan kesehatan. Penelitian ini tidak hanya penting bagi praktisi dan peneliti di bidang kesehatan tetapi juga memberikan manfaat langsung bagi pasien dengan memastikan data mereka aman dan privasi terjaga. Penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan melakukan tinjauan sistematis terhadap literatur yang ada, mengevaluasi celah dalam keamanan RME, dan mengusulkan solusi-solusi yang efektif untuk meningkatkan keamanan sistem dan integritas data pasien.

II. Metodologi Penelitian

Penelitian ini menggunakan metode *Systematic* Literature Review dengan mengacu pada panduan PRISMA [20] untuk mengisi celah pengetahuan terkait keamanan sistem rekam medis elektronik. Tahapan awal penelitian melibatkan identifikasi basis data yang relevan, di antaranya adalah Scopus, DOAJ, dan Google Scholar, dengan menggunakan kata kunci yang telah ditentukan, seperti "Sistem Rekam Medis Elektronik", "Ancaman Keamanan", dan "Kerentanan Data Pasien". Rentang tahun publikasi artikel yang dimasukkan dalam penelitian ini dibatasi antara tahun 2013 hingga 2024. Seluruh penulis melakukan identifikasi basis data kemudian dikumpulkan dan dilakukan proses identifikasi, dilanjutkan dengan proses seleksi artikel berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan sebelumnya. Hasil sintesis artikel ditampilkan pada Gambar 1.

Artikel-artikel yang memenuhi kriteria tersebut kemudian akan dikaji secara sistematis untuk mengevaluasi dan mengidentifikasi celah dalam keamanan sistem rekam medis elektronik serta kerentanan data pasien yang terkait. Pendekatan analitis digunakan untuk menganalisis hasil-hasil dari artikel-artikel yang terpilih, dan hasil analisis ini menjadi landasan dalam merumuskan solusi-solusi yang efektif guna meningkatkan keamanan sistem serta integritas data pasien dalam lingkungan rekam medis elektronik. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi penting dalam memperkuat pemahaman dan pengelolaan keamanan sistem rekam medis elektronik serta meningkatkan perlindungan data pasien secara keseluruhan.



Gambar 1. hasil sintesis artikel

III. Hasil dan Pembahasan

Berdasarkan penelusuran yang kami lakukan, kami menemukan empat artikel yang relevan dan memberikan informasi yang mendukung fokus dan tujuan penelitian ini. Informasi yang diperoleh dari penelitian-penelitian tersebut memberikan kontribusi yang berharga untuk pemahaman lebih lanjut tentang topik yang dibahas dalam penelitian. Hasil dari penelitian-penelitian tersebut seperti terangkum pada Tabel 1.

Tabel 1. Fokus dan hasil penelitian sesuai standar yang ditetapkan

No	Bidang atau Fokus	Penulis & Tahun Terbit	Variabel Riset yang Dibahas
1	Keamanan Siber dalam Sistem RME	Herrera et al. (2023), Vilakazi & Adebesin (2023)	a. Pentingnya keamanan siber dalam sektor perawatan kesehatan. b. Meningkatnya kejadian serangan siber pada institusi perawatan kesehatan.

No	Bidang atau Fokus	Penulis & Tahun Terbit	Variabel Riset yang Dibahas
2	Kerentanan Data Pasien dalam Sistem RME	Nyakina & Taher (2023), Sofia et al. (2022), Basil et al. (2022), Vilakazi & Adebesin (2023)	a. Rentannya RME terhadap masalah keamanan yang mempengaruhi kerahasiaan dan privasi data pasien. b. Tren peningkatan pencurian data dan serangan siber pada institusi perawatan kesehatan.
3	Faktor yang Mempengaruhi Tingkat Keamanan Sistem RME	Basil et al. (2022), Yeo & Banfield (2022), Yeng et al. (2022), Park (2022), Lewiset al. (2022)	a. Kepatuhan terhadap peraturan seperti HIPAA. b. Infrastruktur teknologi RME dan perlindungan teknis. c. Peran faktor manusia dalam insiden keamanan data.
4	Solusi untuk Meningkatkan Keamanan Sistem RME	Singh et al. (2023), Liea & Astuti (2023), Kumbhare & Warkar (2016), Charanya et al. (2022), Nyakina & Taher (2023)	a. Penggunaan otentikasi dan skema perjanjian kunci. b. Enkripsi dan integritas data. c. Penggunaan tanda tangan temporal untuk memverifikasi integritas dokumen pasien.

Tabel 1 menjelaskan masing-masing bidang atau fokus penelitian diidentifikasi bersama dengan nama-nama penulis yang relevan. Selain itu insight atau variabel riset yang dibahas dalam setiap penelitian juga disajikan dengan ringkas. Hasil pencarian menemukan beberapa hal penting terkait evaluasi terhadap ancaman keamanan dan kerentanan data pasien yaitu keamanan sistem rekam medis elektronik, evaluasi terhadap kerentanan data pasien, faktor kunci meningkatkan keamanan sistem rekam medis elektronik dan solusi mengatasi perlindungan terhadap kerentanan data pasien

1. Keamanan sistem rekam medis elektronik

Tinjauan literatur sistematis dilakukan untuk mengidentifikasi berbagai jenis ancaman keamanan yang dapat mempengaruhi integritas dan kerahasiaan data pasien dalam sistem rekam medis elektronik (RME). Tinjauan tersebut mencakup beberapa makalah yang menyoroti pentingnya keamanan siber di sektor perawatan kesehatan dan meningkatnya kejadian serangan siber pada institusi perawatan kesehatan [21] [22]. Pentingnya pendekatan holistik yang melibatkan orang, teknologi, dan kepatuhan terhadap peraturan sebagai upaya untuk mengurangi risiko keamanan siber. Pendekatan tersebut dapat memunculkan teknologi, seperti *Medical Internet of Things* (MIoT), berkontribusi pada kerentanan keamanan siber di sektor perawatan kesehatan [23].

Tinjauan ini juga menekankan perlunya pendekatan holistik yang menggabungkan orang, teknologi, dan kepatuhan terhadap peraturan untuk mengurangi ancaman keamanan siber di sektor perawatan kesehatan [24]. Selain itu, tinjauan mengidentifikasi tantangan keamanan tertentu, seperti *phishing*, serangan *ransomware*, pelanggaran data, serangan *Denial of Service Terdistribusi*, dan injeksi SQL, yang mengancam kerahasiaan, integritas, dan ketersediaan data pasien dalam sistem RME [25].

2.Evaluasi terhadap kerentanan data pasien

Evaluasi kerentanan data pasien dalam konteks sistem rekam medis elektronik telah dilakukan dalam beberapa penelitian. Studi-studi ini telah mengidentifikasi berbagai masalah keamanan dan privasi yang muncul ketika data pasien sensitif dibagikan di antara beberapa perangkat dan pengguna [29]. Tinjauan literatur mengungkapkan bahwa Rekam Medis Elektronik (RME) rentan terhadap masalah keamanan yang dapat mempengaruhi kerahasiaan dan privasi informasi pribadi pasien [24].

Kerentanan data pasien dalam sistem rekam medis elektronik merupakan masalah serius yang mempengaruhi keamanan dan privasi informasi perawatan kesehatan. Hal ini terjadi karena tren peningkatan pencurian data dan serangan cyber pada institusi perawatan kesehatan, menekankan perlunya strategi yang efektif untuk melindungi akses tidak sah ke data perawatan kesehatan [27]. Selain itu, penelitian menunjukkan bahwa fasilitas kesehatan telah menerapkan langkah-langkah keamanan data, tetapi masih ada kesenjangan dan area untuk perbaikan dalam hal aspek keamanan informasi [22]. Evaluasi terhadap kerentanan data pasien dalam konteks sistem rekam medis elektronik dilakukan dengan menganalisis berbagai aspek keamanan dan privasi informasi perawatan kesehatan. Secara keseluruhan, tinjauan literatur memberikan wawasan tentang kerentanan data

pasien dalam sistem rekam medis elektronik dan menyoroti pentingnya mengatasi masalah ini untuk memastikan keamanan dan privasi informasi perawatan kesehatan [28].

3.Faktor kunci meningkatkan keamanan sistem rekam medis elektronik

Faktor-faktor kunci yang mempengaruhi tingkat keamanan sistem rekam medis elektronik (RME) termasuk kepatuhan terhadap peraturan, infrastruktur teknologi, dan faktor manusia. Kepatuhan terhadap peraturan seperti Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) sangat penting untuk menjaga informasi pasien dan memastikan privasi dan kerahasiaan [27]. Selain itu dengan memenuhi infrastruktur teknologi sistem RME, termasuk perlindungan teknis, harus dikombinasikan dengan intervensi perilaku manusia untuk mempromosikan keamanan siber yang kuat [29].

infrastruktur teknologi yang telah ditingkatkan akan bermasalah apabila tidak dilakukan intervensi perilaku terhadap manusia. Faktor manusia memainkan peran penting dalam insiden keamanan data, dengan pelanggaran sering disebabkan oleh praktik keamanan manusia yang buruk, seperti jatuh pada penipuan phishing dan berbagi kata sandi [33], [31]. Penting untuk mengatasi aspek perilaku manusia ini dan memberikan pelatihan dan program kesadaran untuk meningkatkan keamanan sistem RME [32]. Selain itu, adopsi teknik kriptografi canggih dapat meningkatkan keamanan data, tetapi hambatan yang terkait dengan regulator, penyedia layanan kesehatan, dan vendor perlu diatasi agar implementasi berhasil.

4.Solusi mengatasi perlindungan terhadap kerentanan data pasien

Mengelola keamanan sistem RME rumit karena faktor-faktor seperti volume data yang besar, akses pengguna yang beragam, kepatuhan terhadap peraturan, dan kebutuhan untuk mengintegrasikan sistem keamanan yang efektif tanpa mengganggu akses dan produktivitas pengguna [33]. Memastikan keamanan sumber daya informasi perawatan kesehatan melibatkan langkah-langkah teknis dan organisasi, persyaratan hukum, dan perlindungan data pribadi, keamanan siber, dan rahasia profesional dalam perawatan Kesehatan [34]. Metode tradisional dari perawatan kesehatan. perlindungan keamanan informasi, seperti fisik batasan dan teknologi firewall, tidak memadai dalam menghadapi meningkatnya ketergantungan pada Rekam Medis Elektronik (RME) dan risiko serangan cyber [35]. Para peneliti telah mengusulkan berbagai teknik, termasuk otentikasi biometrik, enkripsi data, dan kontrol akses berbasis peran, untuk mengatasi tantangan keamanan RME [36].

Solusi yang diusulkan untuk mengatasi berbagai ancaman keamanan dan meningkatkan perlindungan terhadap kerentanan data pasien dalam sistem rekam medis elektronik telah dirumuskan dalam berbagai penelitian. diantaranya adalah penggunaan otentikasi dan skema perjanjian kunci [36], yang memperkuat pengamanan akses ke sistem dengan memvalidasi identitas pengguna dan mengatur pertukaran kunci untuk enkripsi data. Langkah-langkah keamanan yang kuat seperti enkripsi dan integritas juga menjadi solusi yang efektif untuk melindungi data pasien dari akses yang tidak sah [37] dan modifikasi yang tidak diizinkan. Penelitian juga menyarankan skema otentikasi yang ditingkatkan dengan manajemen enkripsi yang kuat [38], menghadirkan lapisan keamanan tambahan dengan mengintegrasikan manajemen enkripsi yang cermat dalam proses otentikasi. Penggunaan tanda tangan temporal untuk memverifikasi integritas dokumen pasien [40] telah diusulkan sebagai metode tambahan untuk memastikan keabsahan dan tidak terubahnya data dalam rekam medis elektronik. Lebih lanjut, mekanisme pencegahan dan rekomendasi untuk peningkatan keamanan dan privasi di lingkungan perawatan kesehatan elektronik telah dijelaskan dalam penelitian lain [29], mencakup langkah-langkah proaktif untuk mencegah serangan dan meningkatkan kesadaran akan pentingnya privasi data pasien dalam praktik klinis. Dengan demikian, implementasi solusi-solusi ini dapat memberikan kontribusi signifikan dalam meningkatkan keamanan dan integritas data pasien dalam sistem rekam medis elektronik.

Tinjauan ini memberikan wawasan yang berharga tentang ancaman keamanan yang dihadapi oleh sistem rekam medis elektronik. Dengan mencakup berbagai sumber literatur, penelitian ini memberikan landasan yang kuat untuk pemahaman tentang kompleksitas masalah keamanan siber di sektor perawatan kesehatan. Namun tinjauan ini mungkin memiliki keterbatasan dalam cakupan literatur yang digunakan atau dalam metode pencarian dan analisis yang digunakan.

IV. Kesimpulan

Berdasarkan hasil evaluasi literatur tentang keamanan sistem rekam medis elektronik (RME), dapat disimpulkan bahwa masalah keamanan ini adalah isu kritis yang mempengaruhi integritas dan kerahasiaan data pasien dalam konteks perawatan kesehatan modern. Tinjauan literatur telah mengidentifikasi beberapa faktor kunci yang mempengaruhi keamanan RME, termasuk kepatuhan terhadap peraturan, infrastruktur teknologi, dan faktor manusia. Selain itu solusi-solusi telah diusulkan, seperti penggunaan otentikasi, enkripsi, dan tanda tangan

temporal, serta langkah-langkah proaktif untuk meningkatkan kesadaran akan privasi data pasien. Meskipun demikian, masih terdapat kesenjangan dalam literatur, terutama dalam evaluasi efektivitas implementasi solusi-solusi yang diusulkan dan dalam pemahaman terhadap faktor-faktor manusia yang mempengaruhi keamanan RME. Oleh karena itu topik riset yang mendesak untuk diteliti di masa mendatang adalah evaluasi implementasi solusi keamanan yang diusulkan dalam konteks sistem RME, serta pemahaman lebih lanjut tentang faktor-faktor manusia yang berkontribusi terhadap kerentanan data pasien dalam sistem RME. Penelitian ini akan memberikan wawasan yang lebih dalam dan solusi yang lebih efektif dalam meningkatkan keamanan dan integritas data pasien dalam sistem rekam medis elektronik.

Daftar Pustaka

[1] L. Masyfufah, M. Sriwati, A. Ali, and B. Nudji, 'Readiness of Application of Electronic Medical Records in Health Services (Literature Study)', Proceeding Int. Conf. Med. Rec., vol. 2, no. 1, pp. 1–12, 2022.
[2] R. Mahdani, T. Yaumi, Y. Syahidin, and Y. Yunengsih, 'Tata Kelola Rekam Medis Berbasis Elektronik Dalam Pembuatan Laporan Poliklinik Pasien Rawat Jalan Menggunakan Metode Agile', J. Indones. Manaj. Inform. dan Komun., 2023.
[3] R. Priambodo, 'Rekam Medis Elektronik Menggunakan Sistem Penyimpanan Foto Intraoral Gigi untuk Aplikasi Teledentistry berbasis Internet of Things', INOVTEK Polbeng - Seri Inform., vol. 4, no. 2, p. 121, 2019.
[4] M. A. Hapsari and K. Mubarokah, 'Analisis Kesiapan Pelaksanaan Rekam Medis Elektronik (RME) Dengan Metode Doctor's Office Quality-Information Technology (DOQ-IT) di Klinik Pratama Polkesmar', J-REMI J. Rekam Med. dan Inf. Kesehat., 2023.
[5] A. H. Seh et al., 'Healthcare data breaches: Insights and implications', Healthc., vol. 8, no. 2, 2020.
[6] F. Hukum Universitas Sriwijaya and A. Yudha Ramadianto, 'Hak Milik Pasien Atas Isi Rekam Medis (Suatu Pendekatan Filosofis dan Hukum Perdata)', Simbur Cahaya, 2020.
[7] L. V. Tata Sutabri, Danisa Enjelika, Septi Mujiranda, 'Transformasi Digital di Puskesmas Menuju Pelayanan Kesehatan yang Lebih Efisien dan Berkualitas', IJM Indones. J. Multidiscip., vol. 1, no. 5, pp. 1705–1716, 2023.
[8] Z. F. Hapsah and M. I. P. Nasution, 'Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen', J. Manaj. Dan Akunt., vol. 1, no. 2, pp. 338–343, 2023.
[9] T. Sujithra, N. M. Masoodhu Banu, N. Poornima, and S. Durai, 'Swift and Secure Medical Data Transaction', in Lecture Notes in Networks and Systems, 2022.
[10] Z. Diao and F. Sun, 'A Deep-Learning Neural Network Approach for Secure Wireless Communication in the Surveillance of Electronic Health Records', Processes, 2023.
[11] B. Tarajit Singh, B. Sundara Kumar, T. Rama Reddy, and B. S. Kiruthika Devi, 'Artificial Intelligence Based System for Securing Computer Networks: A Survey', in Advances in Transdisciplinary Engineering, 2023.
[12] A. Momand, S. U. Jan, and N. Ramzan, 'A Systematic and Comprehensive Survey of Recent Advances in Intrusion Detection Systems Using Machine Learning: Deep Learning, Datasets, and Attack Taxonomy', Journal of Sensors. 2023.
[13] H. J. Singh, S. Gupta, and S. Vyas, 'A Prevention Technique-Based Framework for Securing Healthcare Data', in Lecture Notes in Networks and Systems, 2023.
[14] A. Singh, A. Kumar, Z. Akhtar, and M. K. Khan, 'Guest Editorial: Cybersecurity Intelligence in the Healthcare System', IEEE Transactions on Industrial Informatics. 2023.
[15] N. Shingari, S. Verma, B. Mago, and M. S. Javeid, 'A review of cybersecurity challenges and recommendations in the healthcare sector', in 2nd International Conference on Business Analytics for Technology and Security, ICBATS 2023, 2023.
[16] V. Radhakrishnan, 'Review Analysis of Cyber Security in Healthcare System: A Systematic Approach of Modern Development', Int. J. Innov. Res. Comput. Sci. Technol., 2023.
[17] R. Sendelj and I. Ognjanovic, 'Cybersecurity Challenges in Healthcare', in Studies in Health Technology and Informatics, 2022.
[18] N. Thapliyal and M. S. Gaur, 'Security Threats in Healthcare Big Data: A Comparative Study', in Proceedings of International Conference on Computational Intelligence and Sustainable Engineering Solution, CISES 2023, 2023.
[19] A. J. Cartwright, 'The elephant in the room: cybersecurity in healthcare', Journal of Clinical Monitoring and Computing. 2023.

[20] H. J. Pielken, D. Urbanitz, P. Koch, and J. van de Loo, 'PRISMA-S: an extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews', Haematol. Blood Transfus., vol. 30, pp. 385–386, 2021.
[21] C. V. P. Herrera, J. S. M. Valcarcel, M. Díaz, J. L. H. Salazar, and L. Andrade-Arenas, 'Cybersecurity in health sector: a systematic review of the literature', Indones. J. Electr. Eng. Comput. Sci., 2023.
[22] K. Vilakazi and F. Adebesin, 'A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies', in EPiC Series in Computing, 2023.
[23] A. Gunawan, Richard, G. A. Susanto, A. Saputra, and A. C. Rizal, 'Understanding the Use of Blockchain in Medical Data Security: A Systematic Literature Review', in ACM International Conference Proceeding Series, 2022.
[24] S. Sofia, E. T. Ardianto, N. Muna, and S. Sabran, 'Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan', J. Rekam Med. Manaj. Inf. Kesehat., 2022.
[25] A. Alhammad, M. M. Yusof, and D. I. Jambari, 'A Review of Cyber Threats to Medical Devices Integration with Electronic Medical Records', in International Conference on Cyber Resilience, ICCR 2022, 2022.
[26] Judith Nyakanga Nyakina and Bahaa Hussein Taher, 'A survey of healthcare sector digitization strategies: Vulnerabilities, countermeasures and opportunities', World J. Adv. Eng. Technol. Sci., 2023.
[27] N. N. Basil, S. Ambe, C. Ekhator, and E. Fonkem, 'Health Records Database and Inherent Security Concerns: A Review of the Literature', Cureus, 2022.
[28] S. Mukhopadhyay, R. Basak, and B. J. Reithel, 'Security/Privacy Perceptions in Patient Use of Online Medical Records', Int. J. Healthc. Inf. Syst. Informatics, 2022.
[29] L. H. Yeo and J. Banfield, 'Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis', Perspect. Heal. Inf. Manag., 2022.
[30] P. Kandabongee Yeng, B. Yang, and M. Stolt Pedersen, 'Assessing cyber-security compliance level in paperless hospitals: An ethnographic approach', in 2022 9th International Conference on Internet of Things, Systems, Management and Security, IOTSMS 2022, 2022.
[31] H. A. Park, 'Security and privacy model of an electronic medical record system', Int. J. Healthc. Technol. Manag., 2022.
[32] N. Lewis, Y. Connelly, G. Henkin, M. Leibovich, and A. Akavia, 'Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records', Healthc. Inform. Res., 2022.
[33] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, 'Managing Security of Healthcare Data for a Modern Healthcare System', Sensors, 2023.
[34] K. Switala, 'Medical Data in the Digital Era - Legal Challenges Related to Providing Information Security, Applying GDPR and Respecting the Professional Secrecy', in 2023 46th ICT and Electronics Convention, MIPRO 2023 - Proceedings, 2023.
[35] M. Shamim, 'Information Security : The Landscape of Management In Electronic Record', Proc. Int. Semin. Business, Educ. Sci., 2022.
[36] N. K. Rout, D. Dansana, N. Parida, and R. K. Rout, 'Improving Performance of Electronic Healthcare Record Management Systems (EHRMS) using Low Complexity Blockchain', in 2022 2nd International Conference on Computer Science, Engineering and Applications, ICCSEA 2022, 2022.
[37] D. Singh, M. Wazid, D. P. Singh, A. K. Das, and R. P. C. Joel, 'Embattle The Security of E-Health System Through A Secure Authentication and Key Agreement Protocol', in 2023 International Wireless Communications and Mobile Computing, IWCMC 2023, 2023.
[38] G. M. Liea and L. G. Astuti, 'Pengenkripsian File Data Pasien untuk Menjamin Kerahasian Informasi Medis', J. Nas. Teknol. Inf. dan Apl., vol. 2, no. 1, pp. 255–260, 2023.
[39] K. K. Kumbhare and K. V. Warkar, 'A Review on Noisy Password, Voiceprint Biometric and One-Time-Password', in Physics Procedia, 2016.
[40] R. Charanya, R. K. Saravanaguru, and M. Aramudhan, 'Design of secure ehealth system through temporal shadow using Blockchain', Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 6, pp. 1584–1588, 2019.