Prosiding Seminar Nasional Akademik
Universitas Abdurachman Saleh Situbondo
akademikbirol.official@gmail.com https://unars.ac.id/ojs/index.php/SENADIKA

Manajemen Big Data dan Keamanan Data Informasi Kesehatan Ibu dan Anak di Rumah Sakit

Ananda Fadila Nisa[1)]

Magister of Midwifery, Universitas 'Aisyiyah Yogyakarta[1)]
nisa.anandaf@gmail.com[1]

ABSTRAK

Perkembangan internet mendorong era big data, mengintegrasikan teknologi medis dan informasi. Dalam kesehatan ibu-anak di rumah sakit, big data meningkatkan pemantauan, pencegahan, dan pengelolaan, sementara *registry digital* dan teknologi informasi kesehatan memperbaiki kualitas perawatan untuk ibu dan anak. Adanya artikel ini untuk mengeksplorasi Manajemen Big Data dan Keamanan Data Informasi Kesehatan Ibu dan Anak di Rumah Sakit. Penulisan artikel ini menggunakan metode *literatur review*. Pencarian artikel menggunakan *data base* elektronik berupa artikel ilmiah pada jurnal yang diterbitkan dalam lima tahun terakhir (2019-2024). Dari analisa yang dilakukan didapat kesimpulan bahwa Manajemen Big Data dalam kesehatan ibu-anak memerlukan keamanan data melalui autentikasi, enkripsi, pengelolaan hak akses, dan pemantauan aktivitas. Integritas data dijaga dengan aturan konsistensi, sementara backup cloud memastikan pemulihan data. Regulasi GDPR, HIPAA, dan PDPA mendukung perlindungan privasi.

Kata Kunci
Big Data; Keamanan; Manajemen; Rumah Sakit

The development of the internet has driven the era of big data, integrating medical and information technology. In maternal and child health in hospitals, big data enhances monitoring, prevention, and management, while digital registries and health information technology improve care quality for mothers and children. This article aims to explore Big Data Management and Data Security in Maternal and Child Health Information in Hospitals. The article employs a literature review method, with articles retrieved from electronic databases, focusing on scientific journals published in the last five years (2019–2024). The analysis concludes that Big Data Management in maternal and child health requires data security through authentication, encryption, access rights management, and activity monitoring. Data integrity is maintained with consistency rules, while cloud backup ensures data recovery. GDPR, HIPAA, and PDPA regulations support privacy protection.

Keywords
Big Data; Security; Management; Hospital

PENDAHULUAN

Industri kesehatan merupakan salah satu sektor terbesar dan paling berkembang di dunia. Dalam beberapa tahun terakhir, manajemen kesehatan global telah mengalami perubahan dari model yang berfokus pada penyakit ke model yang berorientasi pada pasien (Senthilkumar, 2018). Dengan pesatnya perkembangan industri internet, berbagai sektor telah memasuki era big data. Integrasi dan perkembangan berkelanjutan antara teknologi medis dan teknologi informasi telah memberikan dorongan konstan untuk pembentukan big data medis dan mendirikan dasar yang kokoh untuk aplikasi dan pengembangan teknologi big data di bidang medis (Guo ZJ, Luo YC, Cai ZP, 2021). Big data dimanfaatkan untuk memprediksi penyakit sebelum muncul berdasarkan catatan medis. Sistem kesehatan masyarakat di banyak negara kini menyediakan catatan pasien elektronik yang dilengkapi dengan media pencitraan medis yang canggih (Senthilkumar, 2018).

Big data dalam sektor kesehatan memiliki nilai yang besar. Penggunaan big data kesehatan yang terstandarisasi dan sesuai dapat memungkinkan pemerintah untuk mendorong aplikasi big data dalam penelitian klinis dan ilmiah serta kesehatan masyarakat, membentuk industri baru dalam aplikasi big data kesehatan (Li HQ, Yin CQ, 2019). Dengan mengakses data medis melalui sistem informasi medis rumah sakit, dokter dapat dengan cepat mengakses riwayat medis pasien dan memberikan rencana perawatan yang lebih tepat (Jiang, 2023). Dalam konteks informasi kesehatan ibu dan anak di rumah sakit, pemanfaatan big data dapat berdampak signifikan pada pemantauan, pencegahan, dan pengelolaan berbagai aspek terkait kesehatan ibu dan anak. Penggunaan registry digital dan teknologi informasi kesehatan dapat meningkatkan kualitas perawatan yang diberikan kepada wanita hamil dan anak-anak (Frøen, *et., al.,* 2021).

Sebagai contoh, penggunaan data kesehatan ibu dan anak di rumah sakit yaitu SIMRS. Sistem Informasi Rumah Sakit adalah suatu susunan yang menangani pengumpulan data, pengelolaan data, penyajian informasi, analisis dan inferensi informasi, serta penyimpanan informasi yang diperlukan untuk kegiatan rumah sakit (Dharma, *et., al.,* 2022). Dalam era globalisasi saat ini, rumah sakit diharuskan untuk meningkatkan kinerja dan daya saing sebagai entitas bisnis tanpa mengurangi misi sosial yang dibawanya. Rumah sakit harus merumuskan kebijakan strategis, termasuk efisiensi internal (organisasi, manajemen, dan sumber daya manusia), dan harus mampu membuat keputusan dengan cepat dan akurat untuk meningkatkan pelayanan kepada masyarakat agar menjadi organisasi yang responsif, inovatif, efektif, efisien, dan menguntungkan (Takain & Katmini, 2021). Sistem informasi kesehatan (SIK) telah mendapatkan pengakuan besar dalam arena kesehatan dan ruang global selama beberapa dekade terakhir. Hal ini dapat dikaitkan dengan

kemajuan implementasi teknologi, prioritas kesehatan global, dan cakupan kesehatan universal (Epizitone, *et., al.,* 2022).

Pelanggaran data dalam skala besar dilaporkan pada Desember 2020 oleh penyerang jahat yang berhasil mengakses 15 juta catatan (Qiu, *et., al.,* 2020). Memastikan keamanan data dalam menangani informasi kesehatan ibu dan anak sangat penting untuk menjaga privasi dan mencegah akses yang tidak sah. Penelitian menekankan pentingnya melindungi informasi pribadi di era big data (Bi, *et., al.,* 2023). Pertimbangan antara kualitas data dan keamanan data adalah faktor utama dalam menangani big data, yang menyoroti kebutuhan untuk menyeimbangkan akurasi informasi dengan perlindungan data sensitif (Talha, *et., al.,* 2019).

Diperlukan sistem terpusat yang lebih aman di rumah sakit, klinik swasta, laboratorium, dan lain-lain. Penyimpanan jutaan catatan kesehatan dapat menyebabkan hilangnya atau akses yang tidak semestinya ke catatan pasien akibat kebocoran privasi (Kumari, *et., al.,* 2024), oleh karena itu sangat penting untuk memprioritaskan langkah-langkah keamanan data guna melindungi informasi sensitif dan menjaga kerahasiaan pasien di lingkungan rumah sakit. Dalam tinjauan review ini, tujuannya adalah untuk mengeksplorasi Manajemen Big Data dan Keamanan Data Informasi Kesehatan Ibu dan Anak di Rumah Sakit

METODE PENELITIAN

Penelitian ini dilakukan dengan pendekatan *literature review* untuk menganalisis penerapan manajemen big data dan keamanan data informasi kesehatan ibu dan anak di rumah sakit. Artikel ilmiah yang menjadi sumber data diperoleh melalui pencarian sistematis pada tiga basis data utama, yaitu *Science Direct*, *PubMed*, dan *Google Scholar*. Pencarian dilakukan menggunakan kata kunci utama "*Big Data Management*", "*Data Security*", "*Maternal and Child Health*", "*Health Information System*", guna memastikan relevansi terhadap topik yang dikaji. Kriteria inklusi dalam seleksi literatur adalah artikel yang diterbitkan dalam kurun waktu lima tahun terakhir, yakni dari tahun 2019 hingga 2024. Artikel yang didapatkan kemudian diidentifikasi dan disajikan.

HASIL DAN PEMBAHASAN

Tabel 1. Penelitian Terdahulu

No	Nama Penulis	Judul Artikel	Hasil
1	(Gupta, *et., al.,* 2023a)	*Analysis of security and privacy issues of information management of*	Perlindungan privasi dan keamanan adalah pilar utama dalam manajemen big data kesehatan. Privasi dilindungi melalui regulasi (GDPR, HIPAA, PDPA), teknik de-identifikasi (*K-Anonymity, L-Diversity, T-*

No	Nama Penulis	Judul Artikel	Hasil
		big data in B2B based healthcare systems	*Closeness*), privasi diferensial, dan metode *HybrEx* (perturbasi, *walled garden*, *Jujutsu Security*). Keamanan data mencakup otentikasi (kata sandi, biometrik, kartu pintar, otentikasi anonim), kontrol akses (berdasarkan peran, atribut, audit), dan enkripsi (pencarian berbasis kata kunci, kunci publik yang dapat dicari, enkripsi berbasis atribut, enkripsi terselubung). Teknik-teknik ini memastikan data tetap aman dan privasi individu terjaga selama analisis dan transmisi.
2	(Perez, *et., al.,* 2022)	*Big Data Needs and Challenges to Advance Research on Racial and Ethnic Inequities in Maternal and Child Health*	Kekhawatiran tentang Privasi dan Keamanan Data, peneliti harus mengatasi kekhawatiran terkait privasi, etika, dan keamanan dalam pengumpulan data. Kolaborasi dengan mitra komunitas sangat penting untuk membangun kepercayaan dan memastikan komunikasi yang transparan.
3	(Chuma & Ngoepe, 2022)	*Security of electronic personal health information in a public hospital in South Africa*	Langkah-langkah keamanan seperti username-password, enkripsi, firewall, antivirus, dan log audit keamanan ada di rumah sakit untuk melindungi ePHI (*electronic personal health information*). Studi ini merekomendasikan perlunya mengimplementasikan sistem perlindungan intrusi dan terus memperbarui firewall serta antivirus. Disimpulkan bahwa tanpa protokol keamanan yang tepat, ePHI dapat terpapar ancaman dan serangan siber. Rumah sakit umum didesak untuk menggunakan teknologi blockchain untuk memperkuat keamanan ePHI.
4	(Vesoulis, *et., al.,* 2023)	*Improving child health through Big Data and data science*	Big Data dan metode ilmu data inovatif menyediakan alat untuk mengintegrasikan berbagai dimensi data guna menggambarkan praktik klinis, prediktif, dan preventif terbaik, mengurangi disparitas rasial dalam hasil kesehatan anak, memasukkan masukan pasien dan keluarga dalam penilaian medis,

No	Nama Penulis	Judul Artikel	Hasil
			serta mendefinisikan risiko penyakit individu, mekanisme, dan terapi. Namun, untuk memanfaatkan sumber daya ini, diperlukan strategi baru yang secara sengaja menangani hambatan institusional, etika, regulasi, budaya, teknis, dan sistemik, serta membangun kemitraan dengan anak-anak dan keluarga dari berbagai latar belakang yang mengakui sumber-sumber ketidakpercayaan historis
5	(Zaabar, *et., al.,* 2021)	*HealthBlock: A secure blockchain-based healthcare data management system*	Blockchain yang diusulkan dirancang untuk berkontribusi pada ketangguhan sistem manajemen kesehatan dan menghindari keterbatasan keamanan yang tercatat dalam sistem yang biasa digunakan untuk layanan kesehatan cerdas. Hasil evaluasi kinerja dari *Hyperledger Caliper* dan analisis komparatif telah membuktikan ketangguhan dan keunggulan sistem yang diusulkan dalam hal persyaratan keamanan dan privasi, fitur-fitur utama dari sistem kesehatan berbasis blockchain, serta metrik kinerja yang mencakup berbagai *throughput* dan *latency*.
6	(Takain & Katmini, 2021)	*Privacy in the Age of Medical Big Data*	Pentingnya menyeimbangkan perlindungan privasi dengan inovasi berbasis data. Meskipun perlindungan privasi diperlukan, akses yang terlalu ketat terhadap data dapat menghambat kemajuan. Menemukan keseimbangan yang tepat sangat penting untuk memastikan kepercayaan, transparansi, dan manfaat yang adil dari data kesehatan. Studi ini menyarankan bahwa kurangnya perlindungan privasi dan perlindungan yang berlebihan masing-masing memiliki dampak negatif, dan pendekatan yang bijaksana diperlukan untuk menavigasi lanskap yang kompleks ini.
7	(Ganiga, *et., al.,* 2020)	*Security framework for cloud based electronic health*	Keamanan EHR (*Electronic Health Record)* berbasis cloud membantu para profesional kesehatan dan penyedia layanan berbagi informasi pasien di semua tingkat sistem

No	Nama Penulis	Judul Artikel	Hasil
		record (ehr) system	kesehatan. *Cloud* bermanfaat bagi ekosistem kesehatan dengan menghubungkan pusat kesehatan dengan laboratorium, apotek, penagihan medis, dan secara efektif menangani kekhawatiran keamanan seperti pelanggaran informasi medis sensitif
8	(Panda, *et., al.,* 2021)	*A Blockchain-Based Distributed Authentication System for Healthcare*	Implementasi protokol keamanan dan sistem autentikasi dapat membantu mengurangi risiko yang terkait dengan berbagi data dan memastikan privasi informasi pasien

Manajemen big data mencakup proses pembersihan, analisis, dan pengamanan volume data besar dari berbagai sumber untuk memastikan keandalan dan privasi (Nda, R. and Tasmin, 2019). Di sisi lain, Sistem Manajemen Basis Data (DBMS) adalah perangkat lunak canggih yang dirancang untuk menghasilkan, menyimpan, mengambil, dan mengelola data dalam basis data secara efisien (Salim, *et., al.,* 2020).

1. Keamanan *big data healthcare* terutama Informasi Kesehatan Ibu dan Anak di Rumah Sakit

Keamanan *big data healthcare* mencakup otentikasi, kontrol akses, dan enkripsi. Untuk otentikasi, metode berbasis kata sandi, biometrik, kartu pintar, dan otentikasi anonim digunakan untuk memastikan hanya pengguna yang sah yang dapat mengakses data. Kontrol akses dapat dilakukan berdasarkan peran, atribut, dan audit untuk membatasi akses data sesuai dengan kebutuhan dan otorisasi. Enkripsi memastikan bahwa data yang disimpan dan ditransmisikan tetap aman, dengan teknik seperti pencarian berbasis kata kunci, kunci publik yang dapat dicari, enkripsi berbasis atribut, dan enkripsi yang dapat diotentikasi secara terselubung (Gupta, *et., al.,* 2023a). Menerapkan langkah-langkah keamanan yang kuat sangat penting untuk mengatasi masalah privasi dalam sistem informasi kesehatan. Teknologi seperti blockchain menyediakan mekanisme berbagi data yang aman, memastikan privasi pasien, dan pertukaran informasi yang aman (Panda, *et., al.,* 2021; Shen, *et., al.,* 2019). Namun, tantangan tetap ada dalam memastikan privasi data pasien, khususnya terkait perangkat IoT yang digunakan untuk memantau tanda-tanda vital pasien (Hussein, *et., al.,* 2022).

Mengintegrasikan fitur keamanan ke dalam sistem informasi kesehatan sangat penting untuk melindungi data pasien dari akses tidak sah dan pelanggaran. Penggunaan teknologi yang terdesentralisasi dan menjaga privasi dapat meningkatkan keamanan data sambil menjaga kerahasiaan pasien (Panda, *et., al.,*

2021). Selain itu, implementasi protokol keamanan dan sistem autentikasi dapat membantu mengurangi risiko yang terkait dengan berbagi data dan memastikan privasi informasi pasien (Panda, *et., al.,* 2021).

Rumah sakit dapat meningkatkan perlindungan data kesehatan ibu dan anak yang sensitif, memastikan kerahasiaan dan integritas sambil meningkatkan hasil perawatan pasien. Strategi ini meliputi berbagi data yang aman (Madhavi, *et., al.,* 2024). Berbagi catatan medis secara elektronik yang aman dan terlindungi sangat penting untuk manajemen perawatan yang efektif, kolaborasi kesehatan, serta peningkatan perawatan dan pengobatan pasien. Salah satu teknik yang dapat digunakan adalah quantum cryptography untuk mengamankan informasi kesehatan pribadi (Maheshwari & Mantry, 2022). Selain itu, watermarking digital juga digunakan dalam e-healthcare untuk menjaga kerahasiaan dan integritas informasi medis, yang pada gilirannya meningkatkan kesadaran kesehatan pasien. Untuk melindungi informasi medis, diusulkan sistem berbagi informasi medis pasien yang tangguh dan tanpa kehilangan menggunakan metode kripto-watermarking (Aparna & Kishore, 2020).

Keamanan EHR *(Electronic Health Record)* berbasis cloud membantu para profesional kesehatan dan penyedia layanan berbagi informasi pasien di semua tingkat sistem kesehatan. Cloud bermanfaat bagi ekosistem kesehatan dengan menghubungkan pusat kesehatan dengan laboratorium, apotek, penagihan medis, dan secara efektif menangani kekhawatiran keamanan seperti pelanggaran informasi medis sensitif (Ganiga, *et., al.,* 2020) Selain itu langkah-langkah keamanan informasi kesehatan elektronik, seperti username-password, enkripsi, firewall, antivirus, dan log audit keamanan, ada di rumah sakit diperlukan untuk melindungi ePHI (*electronic personal health information*). Perlunya mengimplementasikan sistem perlindungan intrusi dan terus memperbarui firewall serta antivirus dan menggunakan teknologi blockchain untuk memperkuat keamanan ePHI (Chuma & Ngoepe, 2022).

2. Perlindungan privasi pada *big data healthcare* terutama Informasi Kesehatan Ibu dan Anak di Rumah Sakit

Perlindungan privasi pada big data healthcare mencakup beberapa aspek penting: hukum, de-identifikasi, privasi diferensial, dan HybrEx. Regulasi seperti *General Data Protection Regulation* (GDPR), *Health Insurance Portability and Accountability Act* (HIPAA), serta *Personal Data Protection Act* (PDPA) memberikan dasar hukum untuk perlindungan data pribadi. (Gupta, *et., al.,* 2023b) Peraturan seperti HIPAA mengamanatkan langkah-langkah ketat untuk menjaga privasi, ketersediaan, dan integritas catatan kesehatan elektronik, yang menggarisbawahi pentingnya keamanan data di lingkungan pelayanan kesehatan (Khan, *et., al.,* 2022). Teknik de-identifikasi seperti K-Anonymity, L-Diversity, dan T-Closeness digunakan

untuk memastikan bahwa data individu tidak dapat diidentifikasi. Privasi diferensial dapat dilakukan melalui model interaktif dan non-interaktif untuk menambahkan noise pada data sehingga informasi sensitif tidak dapat diekspos. Metode HybrEx mencakup teknik perturbasi, walled garden method, dan Jujutsu Security untuk memastikan keamanan data selama analisis. (Gupta, *et., al.,* 2023a)

KESIMPULAN

Pentingnya manajemen Big Data dan keamanan data dalam informasi kesehatan ibu dan anak. Untuk melindungi data dari akses yang tidak sah, diperlukan fitur keamanan seperti pengelolaan hak akses pengguna, autentikasi, enkripsi data, dan pemantauan aktivitas pengguna. Selain itu, integritas data harus dijaga melalui penerapan aturan yang memastikan konsistensi dan akurasi data, termasuk integritas referensial dan keunikan data. *Backup* dan *recovery*, seperti yang disediakan oleh cloud, juga sangat penting untuk mencadangkan dan memulihkan data dalam kasus kegagalan sistem atau kehilangan data. Perlindungan privasi dalam big data healthcare mencakup aspek hukum, de-identifikasi, privasi diferensial, dan HybrEx. Regulasi seperti GDPR, HIPAA, dan PDPA memberikan dasar hukum yang kuat untuk perlindungan data pribadi.

REFERENSI

Aparna, P., & Kishore, P. V. V. (2019). A blind medical image watermarking for secure e-healthcare application using crypto-watermarking system. *Journal of Intelligent Systems*, *29*(1), 1558-1575.

Bi, J., Guo, Y., He, N., & Wang, S. Research on Key Technologies of Personal Information Security Protection in Big Data. *Academic Journal of Engineering and Technology Science*, *6*(4), 42-47.

Chuma, K. G., & Ngoepe, M. (2022). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, *31*(2), 179-195.

Dharma, I. G. N. A., Sukadarmika, G., & Pramaita, N. (2022). Application of DeLone and McLean methods to determine supporting factors for the successful implementation of electronic medical records at Bali Mandara Eye Hospital. *Journal of Applied Science, Engineering, Technology, and Education*, *4*(2), 146-156.

Epizitone, A., Moyane, S. P., & Agbehadji, I. E. (2022, November). Health information system and health care applications performance in the healthcare arena: a bibliometric analysis. In *Healthcare* (Vol. 10, No. 11, p. 2273). MDPI.

Frøen, J. F., Bianchi, A., Moller, A. B., Jacobsson, B., FIGO Working Group for Preterm Birth, Jacobsson, B., ... & Shennan, A. (2021). FIGO good practice recommendations on the importance of registry data for monitoring rates and

health systems performance in prevention and management of preterm birth. *International Journal of Gynecology & Obstetrics*, *155*(1), 5-7.

Ganiga, R., Pai, R. M., & Sinha, R. K. (2020). Security framework for cloud based electronic health record (EHR) system. *International Journal of Electrical and Computer Engineering*, *10*(1), 455.

Guo ZJ, Luo YC, Cai ZP, Z. T. (2021). Overview of privacy protection technology of big data in healthcare. *Comput Sci Explor*, *15(03):389*.

Gupta, B. B., Gaurav, A., & Panigrahi, P. K. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, *162*, 113859.

Gupta, B. B., Gaurav, A., & Panigrahi, P. K. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, *162*, 113859.

Hussein, S., Abed, I., & Hussien, Z. (2022, January). Lightweight Authentication Protocol For Smart Healthcare. In *Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey*.

Khan, S., Ahmed, F., Baig, M. S., Khan, Z. A., & Yousufzai, U. A. (2022). Securing Medical Datasets using Block Chain Technology. *JOURNAL OF NANOSCOPE (JN)*, *3*(2), 205-217.

Kumari, D., Parmar, A. S., Goyal, H. S., Mishra, K., & Panda, S. (2024). Healthrec-chain: patient-centric blockchain enabled ipfs for privacy preserving scalable health data. *Computer Networks*, *241*, 110223.

Li HQ, Yin CQ, F. J. (2019). National strategic development study on china's health care Big Data. *Lib*, *11*, 7–30.

Nda, R. M., & Tasmin, R. B. (2019). Big data management in education sector: an overview. *Traektoriâ Nauki= Path of Science*, *5*(6), 5009-5014.

Panda, S. S., Jena, D., & Das, P. (2021). A blockchain-based distributed authentication system for healthcare. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, *16*(4), 1-14.

Perez, L. G., Peet, E. D., Vegetabile, B., & Shih, R. A. (2022). Big Data needs and challenges to advance research on racial and ethnic inequities in maternal and child health. *Women's Health Issues*, *32*(2), 90-94.

Qiu, H., Qiu, M., Liu, M., & Memmi, G. (2020). Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE journal of biomedical and health informatics*, *24*(9), 2499-2505.

Senthilkumar, S. A., Rai, B. K., Meshram, A. A., Gunasekaran, A., & Chandrakumarmangalam, S. (2018). Big data in healthcare management: a

review of literature. *American Journal of Theoretical and Applied Business*, *4*(2), 57-69.

Mostafa, S. A., AbuSalim, S. W., & Saringat, M. Z. (2020). A Comparative Study of Data Management Systems. *Journal of Soft Computing and Data Mining*, *1*(1), 10-16.

Takain, I., & Katmini, K. (2021). The Implementation of Computer-Based administrative Information Systems to Improve the Performance of Services Quality in Hospitals. *Journal for Quality in Public Health*, *5*(1), 203-216.

Talha, M., Abou El Kalam, A., & Elmarzouqi, N. (2019). Big data: Trade-off between data quality and data security. *Procedia Computer Science*, *151*, 916-922.

Vesoulis, Z. A., Husain, A. N., & Cole, F. S. (2023). Improving child health through Big Data and data science. *Pediatric research*, *93*(2), 342-349.

Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, *200*, 108500.