Buletin Ilmiah
Ilmu Komputer dan Multimedia

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 516-520

Analisis Strategi dan Optimalisasi dalam Penanganan Kebocoran Data pada Pusat Data Nasional

Daffa Rifqi Al Faiz[1], Sevilla Makhay Agzia[2], Sella Pratiwi Permata Sari[3], Naufal Rifaldy[4], Annisa Elfina Augustia[5]

[1,2,3,4,5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta Timur, Indonesia
Email: [1]adaffaa28@gmail.com, [2]ziaaazii12@gmail.com, [3]sellapratiwipermatasari@gmail.com, [4]naufalrivaldy7@gmail.com, [5]annisa12elfina@gmail.com

Abstrak−Pentingnya penguatan keamanan data nasional di era digital, terutama dalam menghadapi ancaman kebocoran data yang semakin kompleks. Melalui pendekatan kualitatif berbasis studi literatur dan dokumentasi, penelitian ini mengidentifikasi berbagai strategi optimalisasi sistem keamanan data, termasuk pemanfaatan teknologi canggih seperti enkripsi, watermarking digital, AI, blockchain, dan Data Leakage Detection System (DLDS). Selain aspek teknis, penekanan juga diberikan pada pentingnya kebijakan yang fleksibel dan pelatihan sumber daya manusia untuk meningkatkan kesiapsiagaan organisasi dalam menangani insiden kebocoran data. Hasilnya menunjukkan bahwa pendekatan holistik yang mengintegrasikan teknologi, kebijakan, dan pelatihan merupakan kunci utama dalam meningkatkan ketahanan data nasional dan organisasi modern terhadap serangan siber di masa depan.

Kata Kunci: kebocoran data; enkripsi; sistem keamanan siber; keamanan data; perlindungan data

Abstract−*The importance of strengthening national data security in the digital age, especially in the face of increasingly complex data leakage threats. Through a qualitative approach based on literature studies and documentation, this research identifies various strategies for optimizing data security systems, including the use of advanced technologies such as encryption, digital watermarking, AI, blockchain, and Data Leakage Detection System (DLDS). In addition to technical aspects, emphasis is also placed on the importance of flexible policies and human resource training to improve organizational preparedness in handling data leakage incidents. The results show that a holistic approach that integrates technology, policy, and training is the key to improving the resilience of national data and modern organizations against future cyberattack.*

Keywords: *data breach; encryption; cybersecurity system; data security; data protection*

1. PENDAHULUAN

Kebocoran data di era digital menjadi ancaman serius terhadap keamanan informasi dan kepercayaan publik, terutama ketika melibatkan lembaga pemerintah yang mengelola data sensitif (Arquelau et al., 2023). Hal ini menacu pada transmisi atau paparan informasi sensitif yang tidak sah, menimbulkan risiko signifikan bagi individu, bisnis, dan institusi. Hal ini dapat terjadi karena niat jahat atau kesalahan yang tidak disengaja, yang menyebabkan kerusakan *finansial* dan reputasi yang parah. Meningkatnya volume data dan kompleksitas interaksi digital membuat perlindungan terhadap kebocoran data menjadi perhatian penting. Kasus kebocoran data di Pusat Data Nasional dan Statistik (PDNS) pada 26 Juni 2024 menjadi salah satu insiden paling serius dalam sejarah keamanan siber Indonesia. Peretasan yang melumpuhkan 282 instansi negara tersebut menimbulkan kekhawatiran besar terhadap keamanan data pribadi warga negara serta keandalan sistem pemerintahan digital. Masyarakat khawatir data mereka disalahgunakan oleh pihak tidak bertanggung jawab, yang dapat merugikan secara sosial dan ekonomi. Pemerintah dituntut untuk meningkatkan transparansi, memperkuat sistem keamanan siber, dan mengelola komunikasi publik secara efektif guna memulihkan serta mempertahankan kepercayaan masyarakat terhadap institusi negara.

Perkembangan teknologi informasi yang sangat pesat telah mendorong terjadinya digitalisasi di berbagai sektor kehidupan, seperti pemerintahan, pendidikan, kesehatan, dan industri. Digitalisasi ini memerlukan infrastruktur yang kuat dan andal, salah satunya adalah Pusat Data Nasional (PDN). PDN berperan penting sebagai pusat penyimpanan, pengelolaan, dan distribusi data strategis negara yang mendukung efisiensi dan efektivitas layanan publik berbasis teknologi. Namun, dengan meningkatnya volume dan kompleksitas data yang disimpan, tantangan terkait keamanan data menjadi semakin signifikan. Salah satu isu paling krusial yang dihadapi dalam pengelolaan pusat

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 516-520

data adalah kebocoran data, yang dapat mengancam kepercayaan publik dan stabilitas nasional (Priyambodo, 2021).

Kebocoran data merupakan ancaman serius yang dapat terjadi akibat serangan siber, kelalaian pengguna, atau bahkan penyalahgunaan akses dari pihak internal. Dampak dari kebocoran data tidak hanya bersifat finansial, tetapi juga dapat merusak reputasi lembaga serta menimbulkan risiko terhadap keamanan nasional. Berdasarkan laporan Ponemon Institute (2022), rata-rata kerugian akibat kebocoran data secara global mencapai sekitar USD 4,35 juta per insiden, menunjukkan betapa besar dampak yang ditimbulkan. Di Indonesia, sejumlah kasus kebocoran data yang melibatkan lembaga pemerintah maupun sektor swasta dalam beberapa tahun terakhir telah menimbulkan kekhawatiran masyarakat terhadap perlindungan data pribadi. Situasi ini menegaskan pentingnya penguatan sistem keamanan informasi dan penerapan kebijakan perlindungan data yang lebih ketat serta adaptif terhadap ancaman siber yang terus berkembang (Setiawan & Pratama, 2022). Selama ini, upaya penanganan kebocoran data lebih menitikberatkan pada aspek teknis seperti firewall, enkripsi, dan sistem deteksi intrusi. Meskipun penting, langkah tersebut belum sepenuhnya efektif untuk mengenali kebocoran data yang disebabkan oleh faktor non-teknis, seperti penyalahgunaan hak akses, manipulasi data, atau kelalaian pengguna internal. Dibutuhkan pendekatan yang lebih menyeluruh dan adaptif.

Hal dapat menjadi solusi inovatif dengan kemampuan mendeteksi anomali berdasarkan makna dan konteks data, sehingga memungkinkan identifikasi dini terhadap potensi kebocoran yang tidak terdeteksi oleh sistem keamanan konvensional (Zhou et al., 2021). Tantangan utama dalam penanganan kebocoran data di Pusat Data Nasional meliputi kompleksitas infrastruktur teknologi informasi, keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan siber, serta kurangnya implementasi strategi keamanan yang terintegrasi dan optimal. Selain itu, perkembangan teknologi seperti cloud computing, Internet of Things (IoT), dan artificial intelligence (AI) turut memperluas permukaan serangan (attack surface) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Di sisi lain, regulasi dan kebijakan terkait perlindungan data pribadi di Indonesia masih dalam tahap pengembangan dan penyesuaian dengan standar internasional, sehingga diperlukan upaya strategis untuk meningkatkan ketahanan dan keamanan data nasional (Rahardjo, 2020). Optimalisasi strategi penanganan kebocoran data menjadi sangat relevan dalam konteks industri saat ini, di mana transformasi digital berjalan sangat cepat dan data menjadi fondasi utama dalam pengambilan keputusan. Implementasi strategi yang efektif tidak hanya mencakup aspek teknis seperti penggunaan enkripsi, firewall, dan sistem deteksi intrusi, tetapi juga aspek non-teknis seperti pelatihan sumber daya manusia, penguatan kebijakan, serta peningkatan kesadaran akan pentingnya keamanan data.

Di era transformasi digital, kebutuhan akan keamanan data yang kuat semakin mendesak seiring meningkatnya volume dan kompleksitas data yang dikelola oleh Pusat Data Nasional (PDN). Regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) juga menuntut penerapan sistem pengelolaan data yang aman, transparan, dan akuntabel. Tantangan ini menegaskan pentingnya pengembangan metode deteksi kebocoran data yang lebih canggih dan adaptif. Oleh karena itu, penelitian mengenai optimalisasi strategi penanganan kebocoran data melalui pendekatan analisis menjadi sangat relevan untuk memastikan perlindungan data yang lebih efektif dan sesuai dengan prinsip keamanan informasi modern (Setiawan & Pratama, 2022).

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dalam mengoptimalkan strategi penanganan kebocoran data pada Pusat Data Nasional (PDN). Data diperoleh melalui dokumentasi dan studi literatur, kemudian dianalisis untuk mengidentifikasi pola makna dan konteks kebijakan yang mendukung peningkatan keamanan serta transparansi pengelolaan data.

3. ANALISA DAN PEMBAHASAN

3.1 Optimalisasi Sistem Keamanan Data

Mengoptimalkan sistem keamanan data merupakan langkah penting untuk memastikan perlindungan informasi tetap terjaga tanpa mengorbankan kinerja sistem. Optimalisasi ini

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 516-520

melibatkan peningkatan efisiensi dan efektivitas langkah-langkah keamanan melalui penerapan metode dan teknologi canggih di bidang komputasi awan, sistem informasi, serta keamanan jaringan. Berbagai penelitian menunjukkan bahwa pendekatan berbasis algoritma, klasifikasi keamanan, serta optimalisasi distribusi daya dapat memberikan hasil signifikan dalam memperkuat sistem keamanan data. Optimasi berbasis algoritma dalam komputasi awan, misalnya, mampu meningkatkan efisiensi pemanfaatan sumber daya. Penggunaan algoritma canggih memungkinkan peningkatan pemanfaatan CPU hingga 90% dan memori hingga 85%, sehingga mempercepat proses komputasi serta memperkuat sistem enkripsi. Penggunaan deteksi intrusi berbasis kecerdasan buatan (AI) dan enkripsi 256-bit terbukti mampu menurunkan jumlah pelanggaran data secara drastis (Pillai et al., 2024). Selain itu, pendekatan perilaku sistem keamanan menekankan pentingnya pemodelan dan pengujian untuk menentukan parameter yang paling efektif dalam menjaga keseimbangan antara keamanan dan kinerja system.

Dalam konteks big data, manajemen keamanan data jaringan menjadi aspek krusial yang memerlukan perhatian serius untuk memastikan integritas dan kerahasiaan informasi. Optimalisasi kecepatan transmisi dan respons sistem berperan penting dalam membantu organisasi memenuhi standar keamanan tinggi sekaligus mencegah akses tidak sah (Wang, 2021). Selain itu, algoritma keamanan berbasis klasifikasi (CBSA) berkontribusi signifikan dalam meningkatkan perlindungan data dengan cara mengelompokkan informasi berdasarkan tingkat kerahasiaannya serta menyesuaikan metode enkripsi secara dinamis. Pendekatan ini terbukti efektif dalam meningkatkan efisiensi sistem dan mengurangi waktu pemrosesan tanpa mengorbankan keamanan (Sudarsa et al., 2024). Lebih lanjut, optimalisasi distribusi daya dalam jaringan nirkabel juga berperan penting dalam meningkatkan throughput keamanan dan kualitas layanan bagi pengguna (Yuan et al., 2019). Namun, tantangan utama tetap terletak pada keseimbangan antara keamanan, biaya, dan performa sistem. Penelitian lanjutan perlu mengintegrasikan pendekatan ini dengan teknologi mutakhir seperti blockchain dan komputasi kuantum guna menciptakan sistem keamanan data yang lebih adaptif dan tangguh di masa depan.

3.2 Pemanfaatan Teknologi Keamanan dan Enkripsi

Pemanfaatan teknologi keamanan dan enkripsi merupakan langkah fundamental dalam melindungi data dari ancaman kebocoran, baik dalam penyimpanan berbasis cloud maupun selama proses transmisi antarjaringan. Di era digital yang semakin kompleks, data menjadi aset vital yang memiliki nilai strategis tinggi bagi organisasi maupun individu. Namun, peningkatan volume dan kompleksitas data turut memperluas potensi celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Oleh karena itu, penerapan algoritma enkripsi yang kuat serta integrasi teknik watermarking modern menjadi strategi utama untuk menjaga integritas, kerahasiaan, dan keaslian data dari berbagai bentuk ancaman siber.

Teknik enkripsi berperan sebagai lapisan pertama dalam sistem perlindungan data. Enkripsi simetris seperti Advanced Encryption Standard (AES) terus dikembangkan untuk meningkatkan efisiensi proses hingga 15%, sehingga dapat diterapkan secara efektif dalam sistem berskala besar yang membutuhkan perlindungan data secara real-time (Liu et al., 2025). Selain AES, penerapan enkripsi asimetris juga memiliki keunggulan dalam hal pengelolaan kunci dan verifikasi identitas antar pengguna, menjadikannya penting dalam sistem komunikasi yang melibatkan banyak entitas. Sementara itu, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) menghadirkan pendekatan yang lebih fleksibel melalui pengaturan kontrol akses dinamis dan pembaruan kebijakan keamanan secara otomatis. Metode ini memastikan bahwa hanya pengguna yang memiliki atribut tertentu yang dapat mengakses informasi, sehingga meningkatkan keamanan tanpa mengurangi efisiensi sistem (Husna & Dellia, 2021).

Teknik digital watermarking juga memainkan peran penting dalam melindungi data multimedia. Melalui penyisipan tanda air digital, watermarking dapat mendeteksi manipulasi atau pelanggaran hak cipta sekaligus melacak sumber kebocoran data. Kombinasi antara enkripsi dan watermarking menciptakan sistem perlindungan berlapis yang tidak hanya menjaga kerahasiaan data, tetapi juga menjamin autentikasi dan akuntabilitas. Dengan

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 516-520

demikian, integrasi teknologi enkripsi dan watermarking modern menjadi fondasi penting dalam membangun sistem keamanan data yang adaptif, efisien, dan tangguh terhadap ancaman siber di masa depan.Selain enkripsi, pendekatan watermarking digital juga memainkan peran penting dalam menjaga keamanan data, khususnya untuk konten multimedia. Teknik seperti Least Significant Bit (LSB) digunakan untuk menyisipkan tanda air digital ke dalam file, yang membantu mengautentikasi kepemilikan serta mencegah pelanggaran hak cipta. Lebih lanjut, model hibrida yang menggabungkan enkripsi dengan watermarking menawarkan perlindungan berlapis—tidak hanya mengamankan data dari akses ilegal, tetapi juga memungkinkan pelacakan sumber kebocoran data untuk tujuan akuntabilitas (Liu et al., 2025).

Namun, tantangan utama dalam penerapan teknologi keamanan modern terletak pada upaya menyeimbangkan antara tingkat perlindungan yang tinggi dan kemudahan akses bagi pengguna sah. Sistem keamanan yang terlalu ketat dapat menghambat produktivitas, sedangkan sistem yang terlalu longgar berisiko terhadap kebocoran data. Oleh karena itu, diperlukan strategi berkelanjutan untuk memastikan bahwa mekanisme enkripsi dan *watermarking* dapat berfungsi secara efisien, adaptif, dan responsif terhadap perubahan kebutuhan pengguna serta perkembangan ancaman siber. Proses optimalisasi ini mencakup evaluasi rutin terhadap performa sistem, pembaruan algoritma keamanan, serta penerapan kebijakan akses berbasis peran agar penggunaan data tetap terkendali. Selain itu, penting pula untuk mengintegrasikan teknologi ini dengan sistem *machine learning* guna mendeteksi anomali secara otomatis. Dengan demikian, organisasi dapat mempertahankan keseimbangan antara keamanan data, efisiensi operasional, dan kenyamanan pengguna dalam pengelolaan data yang semakin dinamis.

3.3 Penanganan dan Mitigasi Kebocoran Data

Penanganan dan mitigasi kebocoran data merupakan prioritas utama bagi setiap organisasi modern karena dampaknya dapat mencakup kerugian finansial, penurunan reputasi, serta hilangnya kepercayaan publik. Dalam ekosistem digital yang semakin kompleks, kebocoran data tidak hanya disebabkan oleh serangan eksternal, tetapi juga oleh kelalaian internal dan kesalahan sistemik. Oleh karena itu, diperlukan pendekatan holistik yang mengintegrasikan solusi teknologi, kebijakan tata kelola yang adaptif, serta peningkatan kompetensi sumber daya manusia. Tujuan utama dari strategi ini adalah untuk mencegah, mendeteksi, dan merespons kebocoran data baik yang disengaja maupun tidak disengaja secara cepat dan efektif.

Dari sisi teknologi, penerapan Data Leakage Detection System (DLDS) menjadi langkah krusial dalam mengidentifikasi potensi kebocoran sebelum berkembang menjadi insiden besar. Sistem ini berfungsi memberikan peringatan dini sehingga risiko dapat diminimalkan (Rathod et al., n.d.). Selain itu, penguatan infrastruktur keamanan melalui implementasi antivirus, firewall, sistem deteksi intrusi, serta pengendalian hak akses menjadi lapisan perlindungan penting terhadap ancaman eksternal maupun internal (Kiruthiga et al., 2021). Tidak kalah penting, penerapan prosedur pencadangan dan pemulihan data secara berkala menjamin kelangsungan operasional apabila terjadi pelanggaran atau kegagalan sistem. Proses backup yang terencana juga membantu meminimalkan kehilangan data penting yang dapat mengganggu aktivitas bisnis. Dengan demikian, kombinasi antara teknologi deteksi dini, perlindungan berlapis, dan manajemen risiko yang efektif menjadi fondasi utama dalam upaya mitigasi kebocoran data di organisasi modern.Pada aspek kebijakan dan tata kelola, organisasi perlu mengembangkan kebijakan keamanan yang fleksibel untuk merespons dinamika ancaman siber yang terus berkembang (Ginanjar, 2022). Selain itu, manajemen ancaman dari orang dalam menjadi faktor penting, mengingat karyawan dapat berperan ganda sebagai penyebab maupun pelindung kebocoran data. Oleh karena itu, pelatihan kesadaran keamanan perlu ditingkatkan agar budaya keamanan dapat tertanam dalam organisasi.

Langkah proaktif seperti penilaian risiko secara berkala membantu mengidentifikasi potensi kerentanan dan memperkuat kesiapsiagaan terhadap ancaman baru (Patil et al., 2023). Di samping itu, mengikuti perkembangan teknologi perlindungan data terbaru menjadi kunci dalam mempertahankan ketahanan siber organisasi (Sofyan et al., 2025). Meskipun tidak ada sistem yang sepenuhnya kebal terhadap kebocoran, kewaspadaan berkelanjutan dan adaptasi

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 516-520

strategi secara dinamis merupakan faktor utama dalam memastikan keamanan data jangka panjang.

4. KESIMPULAN

Perlindungan data nasional dan organisasi modern sangat penting di era digital. Strategi keamanan harus mengintegrasikan teknologi canggih seperti enkripsi, AI, blockchain, dan sistem deteksi kebocoran data, serta didukung oleh kebijakan yang fleksibel dan pelatihan sumber daya manusia. Pendekatan holistik ini bertujuan untuk meningkatkan ketahanan terhadap kebocoran dan serangan siber, dengan penekanan pada pentingnya adaptasi terhadap perkembangan teknologi dan penilaian risiko secara berkala. Meskipun tidak ada sistem yang sepenuhnya kebal, kewaspadaan dan inovasi berkelanjutan menjadi kunci utama dalam menjaga keamanan data jangka panjang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing atas bimbingan dan arahannya selama penelitian ini. Ucapan terima kasih juga disampaikan kepada rekan-rekan yang telah membantu dalam pengumpulan data serta keluarga atas dukungan dan doanya. Semoga kontribusi semua pihak menjadi amal kebaikan dan memberikan manfaat bagi pengembangan penelitian selanjutnya.

REFERENCES

Arquelau, G., Rodrigues, P., Luiz, A., Serrano, M., Nunes, A., Espiñeira, L., ... & Villalba, G. (2023). Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. In *International Conference on Data Technologies and Applications* (Vol. 9, No. 27, pp. 1-24).

Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. Dinamika Global: Jurnal Ilmu Hubungan Internasional, 7(02), 295-316.

Husna, M. U., & Dellia, P. (2021). Implementasi Blockchain Untuk Optimalisasi Sistem Keamanan Dokumen Transportasi Pada SIM dan STNK. *Jurnal Ilmiah Teknik Mesin, Elektro Dan Komputer*, *1*(3), 1-9.

Kiruthiga, T., Vaniprabha, A., & Sutharsan, M. (2021). *An improved intelligence approach to handling data leakagerisks in the corporate information security process*. 45–51. https://doi.org/10.54646/bijscit.2021.17

Liu, Y., Liu, K. J. R., Feng, L., & Guo, M. (2025). *Application Analysis of Data Leakage Prevention Technology in Power Enterprise Informatization Based on Encryption Algorithm*. 1431–1436. https://doi.org/10.1109/icipca65645.2025.11139015

Pillai, N. M., Jayarin, P. J., David, D. B., Jeeva, K., & Kumari, V. S. (2024). *Algorithm-Driven Optimization of Cloud Computing Architectures for Superior Data Security and Efficiency*. *10*, 1–4. https://doi.org/10.1109/tqcebt59414.2024.10545176

Priyambodo, T. K. (2021). Keamanan Data dan Informasi di Era Digital. Yogyakarta: Deepublish.

Rahardjo, B. (2020). Keamanan Informasi dan Perlindungan Data Pribadi. Jakarta: PT Elex Media Komputindo.

Setiawan, I., & Pratama, Y. (2022). Analisis Kebocoran Data pada Lembaga Pemerintah di Indonesia. Jurnal Keamanan Siber Indonesia, 4(2), 45-58.

Sofyan, R., Sriwidodo, J., & Hasibuan, E. S. (2025). Reformasi Tata Kelola Intelijen di Era Digital: Adaptasi Terhadap Ancaman Siber. *Jurnal Sosial dan Sains (SOSAINS)*, *5*(9).

Sudarsa, D., Rao, A. R., & Sivakumar, A. P. (2024). Data Security Optimization at Cloud Storage using Confidentiality-based Data Classification. *International Journal of Advanced Computer Science and Applications*, *15*(5). https://doi.org/10.14569/ijacsa.2024.0150570

Wu, Y., Ni, K., Wu, W., Qian, L., Lu, W., & Meng, L. (2019). *Downlink linear search type power distribution optimization method for non-orthogonal multiple access system based on data security*.

Zhou, Y., Han, J., & Li, X. (2021). Semantic Analysis for Data Leak Prevention: A Comprehensive Review. Journal of Information Security and Applications, 58, 102-112.