KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Nusantara (JINU)
Vol.2, No.4 Juli 2025
e-ISSN: 3047-7603, p-ISSN :3047-9673, Hal 28-33
DOI : https://doi.org/10.61722/jinu.v2i4.4938

KEAMANAN BASIS DATA MENGGUNAKAN ENKRIPSI DATA PADA SISTEM INFORMASI KEUANGAN

Rahmadilla Nurul Fandini Lubis
rahmadilanurulfandinilubis@gmail.com
Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara
Muhammad Irwan Padli Nasution
irwannst@uinsu.ac.id
Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara

Abstract *Financial information systems are vital components in managing an organization's financial data, making them highly vulnerable to security threats such as data theft and information manipulation. To address these challenges, the implementation of encryption technology has become a primary solution to ensure data confidentiality and integrity. This study aims to analyze various encryption methods used in financial database systems, including RC4,SHA3-512, RSA, and homomorphic encryption algorithms. The research method used is a qualitative approach through literature studies of scientific journals published from 2021 onwards. The results indicate that implementing the right combination of encryption algorithms can enhance protection against cyber-attacks and maintain the privacy of financial data optimally. These findings emphasize the importance of encryption-based security systems in supporting the reliability and user trust in financial information systems.*

Keywords: *Data security, financial information systems, data encryption, cryptography, database.*

Abstrak Sistem informasi keuangan merupakan komponen vital dalam pengelolaan data keuangan organisasi yang sangat rentan terhadap ancaman keamanan seperti pencurian data dan manipulasi informasi. Untuk mengatasi hal tersebut, penerapan teknologi enkripsi menjadi salah satu solusi utama dalam menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menganalisis berbagai metode enkripsi yang digunakan dalam sistem basis data keuangan, termasuk algoritma RC4, SHA3-512, RSA, dan enkripsi homomorfik. Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan studi literatur dari berbagai jurnal ilmiah terbitan 2021 ke atas. Hasil penelitian menunjukkan bahwa penerapan kombinasi algoritma enkripsi yang tepat dapat meningkatkan perlindungan terhadap serangan siber dan menjaga privasi data keuangan secara optimal. Temuan ini menegaskan pentingnya implementasi sistem keamanan berbasis enkripsi dalam mendukung keandalan dan kepercayaan pengguna terhadap sistem informasi keuangan.

Kata Kunci: Keamanan data, sistem informasi keuangan, enkripsi data, kriptografi, basis data.

Pendahuluan

Dalam era digital modern, sistem informasi keuangan telah menjadi tulang punggung utama dalam pengelolaan data transaksi dan pelaporan keuangan organisasi. Namun, kerentanan terhadap ancaman keamanan informasi, seperti peretasan, manipulasi data, dan pencurian informasi rahasia, terus meningkat seiring berkembangnya teknologi. Oleh karena itu, keamanan basis data dalam sistem informasi keuangan merupakan aspek yang sangat krusial untuk menjamin keandalan dan

Received April 28, 2025; Revised Mei 30, 2025; juni 04, 2025
* Rahmadilla Nurul Fandini Lubis, rahmadilanurulfandinilubis@gmail.com

integritas sistem tersebut. Salah satu pendekatan yang paling banyak digunakan untuk mengatasi tantangan ini adalah penerapan teknologi enkripsi data. Menurut Sukmana dan Muliantara (2025), enkripsi homomorfik Paillier dapat digunakan untuk mengenkripsi data finansial sehingga perhitungan atau pemrosesan dapat dilakukan langsung pada data terenkripsi tanpa perlu membuka isi aslinya, yang berarti perlindungan data tetap terjaga meskipun diproses dalam sistem. Hal ini sangat berguna dalam konteks sistem keuangan berbasis cloud yang rawan penyadapan atau pengintaian pihak ketiga (Sukmana & Muliantara, 2025).

Selain itu, pendekatan hybrid yang menggabungkan dua algoritma kriptografi juga menunjukkan hasil yang menjanjikan. Penelitian oleh Hidayasari, Kasmawi, dan Mansur (2023) menunjukkan bahwa kombinasi algoritma SHA (Secure Hash Algorithm) dan Knapsack dapat meningkatkan tingkat keamanan basis data dengan mengintegrasikan fungsi hash yang tahan terhadap tabrakan data dan algoritma kriptografi kunci publik berbasis masalah NP-complete.Sistem yang mereka rancang mampu memberikan perlindungan ganda terhadap serangan brute- force dan manipulasi isi data (Hidayasari et al., 2023).

Lebih lanjut, pendekatan enkripsi data yang menggabungkan algoritma RC4 dan SHA3-512 juga telah diterapkan dalam peningkatan keamanan basis data. Nurjaman dan Umaroh (2024) dalam penelitiannya menunjukkan bahwa penggunaan RC4 sebagai algoritma simetris untuk enkripsi cepat, dikombinasikan dengan SHA3-512 sebagai metode verifikasi integritas data, mampu mencegah berbagai ancaman seperti injeksi SQL dan pemalsuan data dalam sistem keuangan berbasis web (Nurjaman & Umaroh, 2024). Dengan berbagai pendekatan dan implementasi tersebut, dapat disimpulkan bahwa integrasi enkripsi data dalam basis data merupakan strategi penting untuk memperkuat sistem informasi keuangan terhadap serangan siber dan pelanggaran data. Namun, pemilihan metode enkripsi yang tepat harus disesuaikan dengan kebutuhan sistem dan sumber daya yang tersedia.

Metodologi Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan tujuan untuk memahami secara mendalam penerapan teknologi enkripsi dalam menjaga keamanan

basis data pada sistem informasi keuangan. Peneliti mengkaji fenomena keamanan data melalui studi literatur. Data dikumpulkan melalui telaah berbagai jurnal ilmiah terkini, dokumentasi implementasi sistem, serta diskusi mendalam dengan narasumber ahli. Analisis data dilakukan secara tematik, dengan mengidentifikasi pola-pola penting terkait jenis enkripsi yang digunakan, tantangan implementasi, serta dampaknya terhadap perlindungan data sensitif.

Pembahasan

Dalam era digital saat ini, sistem informasi keuangan menjadi tulang punggung utama dalam pengelolaan data transaksi dan pelaporan keuangan organisasi. Namun, kerentanan terhadap ancaman keamanan informasi, seperti peretasan, manipulasi data, dan pencurian informasi rahasia, terus meningkat seiring berkembangnya teknologi. Oleh karena itu, keamanan basis data dalam sistem informasi keuangan merupakan aspek yang sangat krusial untuk menjamin keandalan dan integritas sistem tersebut. Salah satu pendekatan yang paling banyak digunakan untuk mengatasi tantangan ini adalah penerapan teknologi enkripsi data. Enkripsi memungkinkan data disimpan dalam bentuk yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai, sehingga mengurangi risiko kebocoran informasi. Misalnya, penerapan enkripsi homomorfik Paillier memungkinkan operasi matematika dilakukan langsung pada data terenkripsi tanpa perlu dekripsi terlebih dahulu, menjaga privasi data finansial pengguna

Selain itu, pendekatan hybrid yang menggabungkan dua algoritma kriptografi juga menunjukkan hasil yang menjanjikan. Penelitian oleh Nurjaman dan Umaroh (2024) menunjukkan bahwa kombinasi algoritma RC4 dan SHA3-512 dapat meningkatkan tingkat keamanan basis data dengan mengintegrasikan fungsi hash yang tahan terhadap tabrakan data dan algoritma kriptografi kunci publik berbasis masalah NP-complete. Sistem yang mereka rancang mampu memberikan perlindungan ganda terhadap serangan brute-force dan manipulasi isi data . Lebih lanjut, pendekatan enkripsi data yang menggabungkan algoritma RC4 dan Base64 juga telah diterapkan dalam peningkatan keamanan basis data. Afrianto dan Suryana (2021) dalam penelitiannya menunjukkan bahwa penggunaan RC4 sebagai algoritma simetris untuk enkripsi cepat, dikombinasikan dengan Base64 sebagai metode encoding data, mampu mencegah

berbagai ancaman seperti injeksi SQL dan pemalsuan data dalam sistem keuangan berbasis web .

Selain itu, MongoDB memperkenalkan fitur "*Queryable Encryption*" yang memungkinkan pencarian data dalam keadaan terenkripsi tanpa perlu dekripsi. Fitur ini dirancang untuk bekerja dengan basis data yang ada, sehingga pengguna dapat mengadopsinya tanpa perlu merombak sistem yang sudah ada . Dari berbagai pendekatan yang telah dibahas, terlihat bahwa penerapan enkripsi dalam basis data sistem informasi keuangan sangat penting untuk menjaga keamanan dan privasi data. Pemilihan metode enkripsi yang tepat harus disesuaikan dengan kebutuhan dan karakteristik sistem yang digunakan.

Dalam sistem informasi keuangan modern, keamanan data bukan hanya soal perlindungan dari pihak luar, tetapi juga tentang bagaimana data dikendalikan di seluruh siklus hidupnya. Teknologi end-to-end encryption (E2EE) telah menjadi fokus penting dalam melindungi data selama proses transmisi, terutama ketika sistem keuangan dijalankan melalui jaringan publik atau berbasis cloud. Penelitian oleh Zhang et al. (2023) menyoroti bahwa E2EE mampu menjaga kerahasiaan informasi keuangan meskipun terjadi intersepsi jaringan, karena data tetap dalam bentuk terenkripsi hingga mencapai penerima yang sah (Zhang et al., 2023).

Selain perlindungan saat transmisi, pengamanan data juga mencakup kontrol akses terhadap basis data yang bersifat dinamis. Menurut Hidayat & Rahman (2021), implementasi kontrol akses berbasis peran (role-based access control/RBAC) sangat efektif dalam membatasi hak akses pengguna sesuai dengan posisi dan kebutuhan kerjanya. Pendekatan ini mengurangi risiko internal seperti data leakage atau data tampering dari pihak yang memiliki otorisasi berlebihan (Hidayat & Rahman, 2021).
manajemen data yang efisien.□ □Penelitian oleh Kumar & Singh (2021) mengungkap bahwa
Dalam skala besar, enkripsi data harus dikombinasikan dengan

penggunaan platform seperti Informatica yang mendukung data masking dan key management dapat mengamankan data sensitif secara efisien tanpa menurunkan performa sistem secara signifikan. Mereka menekankan pentingnya keseimbangan antara keamanan dan kinerja operasional dalam sistem informasi keuangan (Kumar & Singh, 2021).

Namun, tantangan besar dalam implementasi enkripsi di lingkungan keuangan adalah biaya dan kompleksitasnya.Yulia dan Aditya (2022) menyatakan bahwa perusahaan kecil dan menengah (UKM) sering menghadapi keterbatasan sumber daya dalam hal investasi perangkat keras, perangkat lunak, dan tenaga ahli keamanan siber. Oleh karena itu, mereka menyarankan penggunaan layanan keamanan berbasis cloud yang menawarkan enkripsi sebagai layanan (encryption as a service) sebagai solusi efisien dan terjangkau (Yulia & Aditya, 2022). Terakhir, tidak cukup hanya mengandalkan teknologi enkripsi saja. Wijaya (2023) menekankan pentingnya strategi keamanan holistik yang mencakup kebijakan organisasi, pelatihan karyawan, dan audit berkala terhadap sistem. Pengamanan berbasis teknologi harus diiringi oleh kesadaran keamanan dan kesiapan sumber daya manusia agar sistem informasi keuangan benar-benar tangguh dan andal (Wijaya, 2023).

Kesimpulan

Penerapan enkripsi data dalam sistem informasi keuangan terbukti menjadi langkah strategis dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi yang bersifat sensitif. Berbagai algoritma enkripsi seperti RSA, RC4, SHA3-512, hingga teknologi enkripsi homomorfik dan end-to-end encryption memberikan solusi yang efektif dalam menghadapi berbagai potensi ancaman siber. Penelitian ini menunjukkan bahwa pemilihan metode enkripsi yang tepat, didukung oleh penerapan kontrol akses berbasis peran dan pengelolaan kunci enkripsi yang baik, dapat meningkatkan ketahanan sistem terhadap serangan eksternal maupun internal.

Meskipun demikian, implementasi sistem keamanan berbasis enkripsi tidak luput dari tantangan, seperti kebutuhan akan infrastruktur pendukung, biaya implementasi, serta keterbatasan sumber daya manusia. Oleh karena itu, pendekatan keamanan harus dilakukan secara menyeluruh—tidak hanya dari sisi teknologi, tetapi juga dari sisi kebijakan organisasi, edukasi staf, serta evaluasi sistem secara berkala. Secara keseluruhan, keamanan basis data menggunakan enkripsi dalam sistem informasi keuangan merupakan elemen fundamental dalam membangun kepercayaan pengguna dan menjaga keberlangsungan operasional lembaga keuangan di era digital saat ini.

Daftar Pustaka

Hidayat, M. A., & Rahman, A. (2021). Implementasi Sistem Keamanan Data Menggunakan Role- Based Access Control pada Aplikasi Keuangan. Jurnal Teknologi Informasi, 7(1), 35–42. https://jurnal.unmer.ac.id/index.php/jti/article/view/5781

Kumar, S., & Singh, R. (2021). Efficient Financial Data Encryption Using Informatica and Cloud Platforms. International Journal of Scientific Research in Applications, 9(2), 14–21. https://ijsra.net/sites/default/files/IJSRA-2021-0044.pdf

Sari, F. N., & Prasetyo, A. D. (2022). Perlindungan Data pada Sistem Informasi Keuangan Berbasis Web Menggunakan Algoritma SHA3-512. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 6(5), 2293–2298. https://j-ptiik.ub.ac.id/index.php/j- ptiik/article/view/11976

Wijaya, R. (2023). Strategi Holistik Keamanan Sistem Informasi Keuangan Berbasis Teknologi Enkripsi dan Edukasi Pengguna. Jurnal Logika, 24(2), 90–97. https://journal.stekom.ac.id/index.php/logika/article/view/639

Wulandari, D., & Kurniawan, A. (2022). Enkripsi Data Menggunakan Algoritma RC4 dalam Sistem Informasi Keuangan Sekolah. Jurnal Teknologi dan Sistem Informasi, 10(2), 123–

130. https://journal.stikom.edu/index.php/jtsi/article/view/287

Yulia, E., & Aditya, P. (2022). Analisis Implementasi Keamanan Data pada UMKM Menggunakan Enkripsi Cloud Berbasis Layanan. Journal of Business and Creative Economy, 5(1), 70–81. https://journal.uc.ac.id/index.php/JBC/article/view/3832

Zhang, Y., Liu, M., & Huang, L. (2023). Keamanan Data pada Sistem Informasi Keuangan Berbasis Cloud.ResearchGate Publications. https://www.researchgate.net/publication/383095398_KEAMANAN_DATA_PADA_SISTE M_INFORMASI_KEUANGAN_BERBASIS_CLOUD