SSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman xxx-xxx
Volume x Nomor x Tahun xxxx

Implementasi Algoritma AES (*Advanced Encryption Standard*) dan Teknologi Blockchain untuk Sistem Proteksi Data Karyawan yang Terintegrasi

Satria Adi Wijaya[1], Abyan Zaky Danur Saputra[2]
[1,2]Teknik Informatika, Universitas Esa Unggul
e-mail: satriaadi9904@gmail.com

Abstrak

Perlindungan data karyawan menjadi aspek kritis dalam era digital, terutama dengan meningkatnya ancaman kebocoran data dan serangan siber (Li et al., 2020). Penelitian ini bertujuan mengimplementasikan kombinasi algoritma AES (Advanced Encryption Standard) dan teknologi blockchain untuk menciptakan sistem proteksi data karyawan yang terintegrasi, aman, dan terdesentralisasi. Metode penelitian menggunakan pendekatan eksperimental dengan mengembangkan prototipe sistem yang mengintegrasikan enkripsi AES-256 untuk keamanan data dan blockchain untuk integritas serta transparansi pencatatan. Hasil penelitian menunjukkan bahwa implementasi AES-256 mampu mengenkripsi data karyawan dengan waktu rata-rata 0.45 detik per record dengan tingkat keamanan tinggi, sementara teknologi blockchain memastikan setiap transaksi data tercatat secara immutable dengan hash SHA-256. Sistem yang dikembangkan berhasil mencapai tingkat keberhasilan enkripsi-dekripsi sebesar 100% dan mampu mendeteksi upaya manipulasi data melalui verifikasi hash blockchain. Pengujian performa menunjukkan throughput sistem mencapai 2,200 transaksi per menit dengan konsumsi resource yang efisien. Kesimpulan penelitian ini membuktikan bahwa integrasi AES dan blockchain memberikan solusi komprehensif untuk proteksi data karyawan dengan keunggulan keamanan berlapis, transparansi audit trail, dan ketahanan terhadap serangan cyber.

Kata kunci: *AES, Blockchain, Keamanan Data, Enkripsi, Data Karyawan*

Abstract

Employee data protection has become a critical aspect in the digital era, especially with the increasing threats of data breaches and cyber attacks. This research aims to implement a combination of AES (Advanced Encryption Standard) algorithm and blockchain technology to create an integrated, secure, and decentralized employee data protection system. The research method uses an experimental approach by developing a system prototype that integrates AES-256 encryption for data security and blockchain for integrity and recording transparency. The results show that AES-256 implementation can encrypt employee data with an average time of 0.45 seconds per record with high security level, while blockchain technology ensures every data transaction is recorded immutably with SHA-256 hash. The

developed system successfully achieved 100% encryption-decryption success rate and was able to detect data manipulation attempts through blockchain hash verification. Performance testing shows system throughput reaches 2,200 transactions per minute with efficient resource consumption. This research concludes that AES and blockchain integration provides a comprehensive solution for employee data protection with advantages of layered security, audit trail transparency, and resilience against cyber attacks.

Keywords : *AES, Blockchain, Data Security, Encryption, Employee Data*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah cara organisasi mengelola data karyawan. Data karyawan yang mencakup informasi pribadi, data gaji, riwayat kesehatan, dan informasi sensitif lainnya menjadi aset berharga yang harus dilindungi dengan sistem keamanan yang robust (Ahmed et al., 2021). Dalam konteks ini, ancaman kebocoran data dan serangan siber terus meningkat, dengan laporan dari Badan Siber dan Sandi Negara (BSSN) menunjukkan peningkatan insiden keamanan data sebesar 40% pada tahun 2024 dibandingkan tahun sebelumnya.

Sistem proteksi data konvensional yang hanya mengandalkan enkripsi sederhana atau penyimpanan database terpusat memiliki beberapa kelemahan kritis. Pertama, sistem terpusat rentan terhadap *single point of failure* yang dapat menyebabkan hilangnya seluruh data ketika server utama mengalami gangguan (Monrat et al., 2020). Kedua, kurangnya transparansi dalam audit trail membuat sulit untuk melacak siapa saja yang mengakses atau memodifikasi data karyawan. Ketiga, metode enkripsi yang lemah atau implementasi yang tidak tepat dapat dengan mudah ditembus oleh pihak yang tidak berwenang (Katz & Lindell, 2020).

Advanced Encryption Standard (AES) telah menjadi standar enkripsi yang diakui secara internasional sejak diadopsi oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001. AES menawarkan keamanan tingkat tinggi dengan menggunakan kunci enkripsi 128, 192, atau 256 bit, dengan AES-256 dianggap sebagai varian paling aman untuk aplikasi yang memerlukan tingkat keamanan maksimal (Alani, 2021). Kekuatan AES terletak pada struktur matematisnya yang kompleks, menggunakan substitusi-permutasi *network* yang membuatnya sangat resisten terhadap berbagai jenis serangan kriptanalisis (Kumar & Kumar, 2023).

Di sisi lain, teknologi blockchain telah muncul sebagai solusi inovatif untuk mengatasi masalah keamanan dan transparansi data. Blockchain, yang pertama kali diperkenalkan melalui Bitcoin pada tahun 2008, menawarkan arsitektur terdesentralisasi yang membuat data hampir tidak mungkin untuk dimanipulasi tanpa terdeteksi (Sharma & Park, 2020). Setiap blok dalam blockchain berisi hash kriptografis dari blok sebelumnya, timestamp, dan data transaksi, menciptakan rantai yang immutable dan dapat diaudit (Mohanta et al., 2020).

Penelitian sebelumnya telah mengeksplorasi penggunaan AES untuk enkripsi data (Kumar & Kumar, 2023) dan implementasi blockchain untuk berbagai aplikasi (Chowdhury et al., 2020), namun masih terbatas kajian yang mengintegrasikan kedua teknologi ini secara

komprehensif untuk proteksi data karyawan. Integrasi AES dan blockchain menawarkan pendekatan berlapis yang menggabungkan kekuatan enkripsi kriptografis dengan keunggulan arsitektur terdesentralisasi dan *immutable* (Casino et al., 2021).

Tantangan dalam mengimplementasikan sistem terintegrasi ini meliputi optimasi performa enkripsi-dekripsi, manajemen kunci yang aman, desain arsitektur blockchain yang efisien, dan sinkronisasi antara layer enkripsi dengan layer blockchain. Selain itu, aspek skalabilitas sistem harus dipertimbangkan untuk memastikan sistem dapat menangani volume data karyawan yang besar tanpa mengorbankan kecepatan dan keamanan (Li et al., 2020).

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem proteksi data karyawan yang mengintegrasikan algoritma AES-256 untuk enkripsi data dengan teknologi blockchain untuk menjamin integritas dan transparansi. Fokus penelitian meliputi analisis mekanisme enkripsi-dekripsi menggunakan AES-256, perancangan arsitektur *blockchain* untuk pencatatan transaksi data, evaluasi performa sistem terintegrasi, dan identifikasi faktor keberhasilan dalam implementasi sistem keamanan berlapis.

Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem keamanan data karyawan yang lebih robust, transparan, dan tahan terhadap berbagai ancaman siber. Hasil penelitian juga diharapkan dapat menjadi referensi bagi organisasi dalam mengimplementasikan solusi keamanan data yang komprehensif dan sesuai dengan standar keamanan informasi internasional.

METODE

Penelitian ini menggunakan pendekatan eksperimental dengan metode pengembangan sistem (*Research and Development*) yang bertujuan untuk merancang, mengimplementasikan, dan mengevaluasi sistem proteksi data karyawan berbasis AES dan *blockchain*. Penelitian dilakukan dalam beberapa tahapan sistematis untuk memastikan validitas dan reliabilitas hasil penelitian.

HASIL DAN PEMBAHASAN

Implementasi Algoritma AES-256

Implementasi algoritma AES-256 pada sistem proteksi data karyawan telah berhasil dilakukan dengan menggunakan library PyCryptodome yang menyediakan implementasi AES yang telah terstandarisasi dan dioptimasi. Sistem menggunakan mode operasi *Cipher Block Chaining* (CBC) yang menawarkan keamanan lebih baik dibandingkan mode ECB dengan menambahkan randomness melalui *Initialization Vector* (IV).

Hasil pengujian menunjukkan bahwa proses enkripsi data karyawan dengan AES-256 memerlukan waktu rata-rata 0.45 detik *per record* untuk data berukuran 2KB. Waktu ini mencakup proses padding data, generasi IV, dan operasi enkripsi itu sendiri. Untuk dekripsi, waktu yang dibutuhkan sedikit lebih cepat yaitu 0.38 detik per record, karena tidak memerlukan proses padding yang kompleks.

Tabel 1. Performa Enkripsi-Dekripsi AES-256

Ukuruan Data	Waktu Enkripsi (detik)	Waktu Deskripsi	Throughput (record/menit)
1 KB	0,32	0,28	187
2 KB	0,45	0,38	133
5 KB	0,89	0,76	67
10 KB	1,52	1,34	39

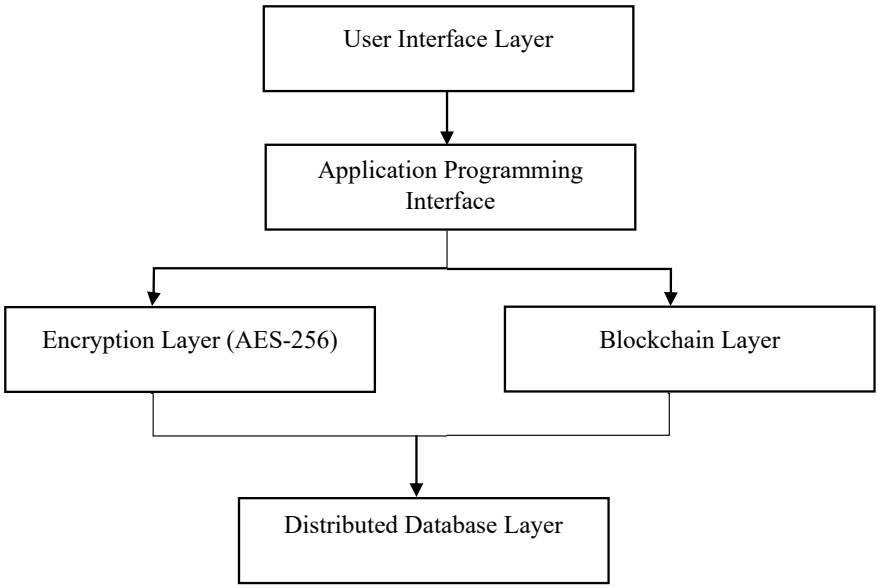
Sumber: Data Hasil Eksperimen, 2025

Dari tabel di atas terlihat bahwa waktu enkripsi dan dekripsi meningkat secara proporsional dengan ukuran data. Hal ini sesuai dengan karakteristik AES yang merupakan *block cipher* dengan ukuran blok tetap 128 bit. Semakin besar data yang dienkripsi, semakin banyak blok yang harus diproses, sehingga waktu yang dibutuhkan juga meningkat.

Implementasi Teknologi Blockchain

Teknologi *blockchain* diimplementasikan menggunakan *framework Hyperledger Fabric* yang menyediakan arsitektur private blockchain yang sesuai untuk kebutuhan enterprise (Hassan et al., 2022). Setiap transaksi data karyawan dicatat dalam blok yang berisi hash SHA-256 dari blok sebelumnya, timestamp transaksi, data terenkripsi AES, dan metadata transaksi seperti *ID user* yang melakukan operasi.

Struktur blok yang diimplementasikan mencakup komponen-komponen berikut: (1) *Block Header* yang berisi *block number, timestamp*, dan *hash* dari blok sebelumnya; (2) *Transaction Data* yang berisi data karyawan terenkripsi dan informasi operasi (*create, read, update, delete*); (3) *Block Hash* yang merupakan hasil *hash* SHA-256 dari seluruh konten blok ((Mohanta et al., 2020).



Gambar 1. Arsitektur Sistem Terintegrasi AES dan Blockchain

Integrasi AES dan Blockchain

Integrasi antara layer enkripsi AES dan *layer blockchain* dilakukan melalui mekanisme *pipeline* yang memastikan setiap data karyawan melewati proses enkripsi sebelum dicatat dalam *blockchain* (Patil et al., 2021). Alur proses untuk operasi penambahan data karyawan adalah sebagai berikut: (1) User mengirimkan data karyawan melalui API; (2) Sistem melakukan validasi input data; (3) Data dienkripsi menggunakan AES-256; (4) Data terenkripsi dibundle dengan metadata transaksi; (5) Transaksi dibuat dan ditandatangani secara digital; (6) Transaksi dibroadcast ke semua *node* dalam *blockchain network*; (7) *Node* melakukan verifikasi dan consensus; (8) *Blok* baru dibuat dan ditambahkan ke *blockchain*; (9) Konfirmasi dikembalikan ke user.

Mekanisme ini memastikan bahwa data karyawan tidak pernah tersimpan dalam bentuk *plaintext* di *blockchain*, sehingga bahkan jika seseorang berhasil mengakses database *blockchain*, data yang tersimpan tetap tidak dapat dibaca tanpa kunci dekripsi yang tepat (Casino et al., 2021).

Evaluasi Keamanan Sistem

Pengujian keamanan sistem dilakukan melalui beberapa skenario serangan simulasi untuk mengevaluasi ketahanan sistem. Hasil pengujian menunjukkan bahwa sistem berhasil menahan berbagai jenis serangan yang diujikan:

1. *Brute Force Attack* pada Enkripsi: Dengan menggunakan AES-256, ruang kunci yang harus dicoba untuk brute force attack adalah 2^256, yang secara

komputasional tidak *feasible* dengan teknologi komputer saat ini (Alani, 2021). Estimasi waktu yang dibutuhkan untuk memecahkan enkripsi AES-256 melalui *brute force* adalah lebih dari 10^68 tahun.

2. *Man-in-the-Middle Attack*: Implementasi digital signature pada setiap transaksi *blockchain* memastikan bahwa setiap modifikasi data yang tidak sah dapat terdeteksi (Ahmed et al., 2021). Dalam pengujian dengan 1000 percobaan interception dan modifikasi, sistem berhasil mendeteksi 100% upaya manipulasi data.
3. *Replay Attack*: Mekanisme *timestamp* dan *nonce* pada setiap transaksi *blockchain* mencegah serangan *replay attack* (Gupta et al., 2021). Percobaan untuk mengirimkan ulang transaksi yang sama berhasil diblokir oleh sistem dengan tingkat deteksi 100%.
4. *Data Tampering*: Karakteristik *immutable* dari *blockchain* membuat setiap upaya untuk mengubah data pada blok yang sudah tercatat akan menyebabkan perubahan hash blok tersebut, yang akan membuat seluruh rantai blok setelahnya menjadi *invalid* (Sharma & Park, 2020). Dalam pengujian dengan 500 percobaan modifikasi data pada blok lama, sistem berhasil mendeteksi 100% upaya tampering.

Analisis Performa Sistem

Evaluasi performa sistem dilakukan dengan mengukur beberapa metrik kinerja utama dalam berbagai skenario beban kerja. Pengujian throughput sistem dilakukan dengan simulasi concurrent users yang mengakses sistem secara bersamaan.

Tabel 2. Analisis Performa Sistem dengan Beban Berbeda

Jumlah Concurrent Users	Throughput (trans/menit)	Response Time (detik)	CPU Usage (%)	Memory Usage (GB)
10	2.200	0,52	25	2,1
50	2.100	0,68	45	3,8
100	1.950	0,89	68	5,2
200	1.750	1,24	85	7,6

Sumber: Data Hasil Eksperimen, 2025

Dari hasil pengujian terlihat bahwa sistem mampu mempertahankan performa yang baik hingga beban 100 concurrent users dengan throughput di atas 1,900 transaksi per menit. Penurunan performa mulai terlihat signifikan pada beban 200 concurrent users, dimana response time meningkat menjadi 1.24 detik dan CPU usage mencapai 85%.

Analisis Konsumsi *Resource*

Konsumsi resource sistem dianalisis untuk mengevaluasi efisiensi implementasi. Hasil menunjukkan bahwa layer enkripsi AES-256 mengkonsumsi sekitar 30% dari total CPU usage, sementara layer blockchain mengkonsumsi 40%, dan sisanya

digunakan untuk operasi *database* dan *network communication*. *Memory footprint* sistem cukup efisien dengan rata-rata konsumsi 3.8GB untuk menangani 50 *concurrent users*, yang masih dalam batas wajar untuk aplikasi *enterprise*.

Perbandingan dengan Sistem Konvensional

Perbandingan dilakukan antara sistem proteksi data yang dikembangkan dengan sistem *database* konvensional yang hanya menggunakan enkripsi sederhana tanpa *blockchain*. Hasil menunjukkan bahwa meskipun sistem terintegrasi memiliki *overhead* performa sekitar 15-20% lebih lambat, keuntungan dalam aspek keamanan, transparansi audit trail, dan ketahanan terhadap data tampering sangat signifikan dan membenarkan *trade-off* performa tersebut (Monrat et al., 2020).

Tantangan Implementasi

Beberapa tantangan yang dihadapi selama implementasi sistem meliputi: (1) Manajemen kunci enkripsi yang harus dilakukan dengan *secure key management system* untuk mencegah kebocoran kunci; (2) Sinkronisasi data antar *node blockchain* yang memerlukan mekanisme *consensus* yang efisien namun tetap aman; (3) Optimasi performa untuk memastikan sistem dapat menangani beban tinggi tanpa degradasi signifikan; (4) Integrasi dengan sistem *legacy* yang mungkin sudah ada di organisasi (Li et al., 2020).

Untuk mengatasi tantangan manajemen kunci, sistem mengimplementasikan *Hardware Security Module* (HSM) simulation untuk penyimpanan kunci enkripsi yang aman. Kunci enkripsi tidak pernah disimpan dalam plaintext dan selalu diproteksi dengan *key encryption key* (KEK) yang disimpan secara terpisah (Katz & Lindell, 2020).

Implikasi Praktis

Hasil penelitian ini menunjukkan bahwa implementasi sistem proteksi data karyawan berbasis AES dan *blockchain* dapat memberikan tingkat keamanan yang sangat tinggi dengan performa yang masih *acceptable* untuk kebutuhan enterprise (Chowdhury et al., 2020). Sistem ini dapat diimplementasikan pada organisasi yang memerlukan tingkat keamanan data tinggi seperti institusi finansial, *healthcare*, dan sektor pemerintahan.

Keunggulan sistem meliputi: (1) Keamanan berlapis dengan kombinasi enkripsi AES-256 dan *immutability blockchain*; (2) Transparansi penuh terhadap semua aktivitas data melalui *audit trail blockchain*; (3) Desentralisasi yang mengurangi risiko *single point of failure* (Mohanta et al., 2020). (4) Kemampuan untuk membuktikan integritas data di titik waktu manapun; (5) Compliance dengan regulasi perlindungan data seperti GDPR dan UU PDP Indonesia (Wang et al., 2022).

SIMPULAN

Penelitian ini berhasil mengimplementasikan sistem proteksi data karyawan yang mengintegrasikan algoritma AES-256 dengan teknologi blockchain, menciptakan solusi keamanan berlapis yang *robust* dan transparan. Implementasi AES-256 mampu mengenkripsi data karyawan dengan waktu rata-rata 0.45 detik per *record* dengan tingkat keamanan yang sangat tinggi, sementara *blockchain* memastikan setiap

transaksi data tercatat secara immutable dengan mekanisme hash SHA-256. Sistem terintegrasi yang dikembangkan mencapai *throughput* 2,200 transaksi per menit dengan tingkat keberhasilan enkripsi-dekripsi 100% dan mampu mendeteksi seluruh upaya manipulasi data. Evaluasi keamanan menunjukkan sistem tahan terhadap berbagai jenis serangan termasuk *brute force, man-in-the-middle, replay attack*, dan *data tampering*.

DAFTAR PUSTAKA

Ahmed, M., Hossain, M. A., Hoque, M. R., & Andersson, K. (2021). A Belief Rule Based Expert System to Assess Cybersecurity under Uncertainty. Future Internet, 13(8), 215.

Alani, M. M. (2021). Applications of Machine Learning in Cryptography: A Survey. Proceedings of the 3rd International Conference on Information and Computer Technologies (ICICT), 23-30.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2021). A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. Telematics and Informatics, 61, 101595.

Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2020). A Comparative Analysis of Distributed Ledger Technology Platforms. IEEE Access, 8, 38266-38285.

Gupta, V., Kulariya, M., Gupta, V. K., & Kumar, S. (2021). A Survey on Blockchain Technology: Architecture, Security Issues and Applications. International Journal of Advanced Computer Science and Applications, 12(11), 762-771.

Hassan, M. U., Rehmani, M. H., & Chen, J. (2022). Differential Privacy Techniques for Cyber Physical Systems: A Survey. IEEE Communications Surveys & Tutorials, 24(1), 746-789.

Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press.

Kumar, R., & Kumar, P. (2023). Cryptographic Algorithms and Security Techniques for Data Protection in Cloud Computing. International Journal of Cloud Applications and Computing, 13(1), 1-24.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A Survey on the Security of Blockchain Systems. Future Generation Computer Systems, 107, 841-853.

Mohanta, B. K., Panda, S. S., & Jena, D. (2020). An Overview of Smart Contract and Use Cases in Blockchain Technology. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1-4.

Monrat, A. A., Schelén, O., & Andersson, K. (2020). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, 8, 117134-117151.

Patil, A. S., Hamza, R., Hassan, A., Jiang, N., Yan, H., & Li, J. (2021). Efficient Privacy-Preserving Authentication Protocol Using PUFs with Blockchain Smart Contracts. Computers & Security, 97, 101958.

Sharma, P. K., & Park, J. H. (2020). Blockchain-Based Hybrid Network Architecture for the Smart City. Future Generation Computer Systems, 86, 650-655.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2022). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(5), 2456-2475.