ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Implementasi Kriptografi untuk Pengamanan Data Transaksi Theking Coffee House, Cikarang utara, Bekasi Menggunakan Algoritma AES-256

Implementation of AES-256 Cryptographic Algorithm for Securing Transaction Data at Theking Coffee House, North Cikarang, Bekasi

Endang Sirait[1], Muhammad Fiqri Firmansyah[2], Theresia A.K Nababan[3]

[1]Informatika, Teknik, Universitas Pelita Bangsa
[2]Informatika, Teknik, Universitas Pelita Bangsa
[3]Informatika, Teknik, Universitas Pelita Bangsa
[1]endangsirait2005@gmail.com, **[2]mfiqrifirmansyah.92@gmail.com***,
[3]nababantheresia84@gmail.com*

Abstract

The rapid development of digital transaction systems in small and medium-sized enterprises, such as coffee shops, increases the risk of unauthorized access and data breaches, particularly concerning transaction data stored in databases. Many transaction systems still store data in plaintext, making them vulnerable to security threats. This study addresses the issue of transaction data security through the application of cryptographic techniques in a web-based transaction management system. The proposed solution is the implementation of the Advanced Encryption Standard (AES) algorithm to encrypt transaction data before storage and decrypt it when accessed by authorized users. The contribution of this research lies in the real-world implementation of the AES algorithm in a transaction system that enhances data security while transparently displaying the encryption and decryption processes through an administrative dashboard. The research method involves system development using Node.js and Express, the application of AES-256 cryptography for data security, and JSON-based data storage. Transaction data such as customer names, order details, quantities, and total prices are encrypted on the server side before being stored. In addition, a dedicated dashboard is provided to display ciphertext, perform decryption based on transaction IDs, and present plaintext results to administrators. The research results show that the developed system successfully implements the AES algorithm to secure transaction data before storage, ensuring that all transaction information is stored in encrypted form. The testing results demonstrate that encrypted data can be accurately decrypted using a valid secret key and effectively prevent direct readability of data in the database without affecting system integrity, accuracy, or functionality. In conclusion, the implementation of the AES algorithm is proven to be effective in enhancing transaction data security and is suitable for application in information systems of small and medium-sized enterprises.

Keywords— *Cryptography, Advanced Encryption Standard (AES), Transaction Security, WebBased Information System, Data Encryption*

Abstrak

Pesatnya perkembangan sistem transaksi digital pada usaha kecil dan menengah, seperti kedai kopi, meningkatkan risiko akses tidak sah dan kebocoran data, khususnya terhadap informasi transaksi yang tersimpan dalam basis data. Banyak sistem transaksi masih menyimpan data dalam bentuk plaintext, sehingga rentan terhadap pelanggaran keamanan. Penelitian ini membahas permasalahan pengamanan data transaksi melalui penerapan teknik kriptografi pada sistem manajemen transaksi berbasis web. Solusi yang diusulkan adalah penerapan algoritma Advanced Encryption Standard (AES) untuk mengenkripsi data transaksi sebelum disimpan dan mendekripsinya kembali saat diakses oleh pengguna yang berwenang. Kontribusi penelitian ini adalah implementasi nyata algoritma AES pada sistem transaksi, yang meningkatkan keamanan data serta menampilkan proses enkripsi dan dekripsi melalui dashboard administrasi. Metode penelitian dilakukan melalui pengembangan sistem menggunakan Node.js dan Express, penerapan kriptografi AES-256 untuk keamanan data, serta penyimpanan data berbasis JSON.

Data transaksi seperti nama pelanggan, detail pesanan, jumlah, dan total harga dienkripsi di sisi server sebelum disimpan. Selain itu, disediakan dashboard khusus untuk menampilkan ciphertext, melakukan dekripsi berdasarkan ID transaksi, serta menampilkan hasil plaintext kepada admin. Hasil penelitian menunjukkan bahwa sistem yang dikembangkan berhasil mengimplementasikan algoritma Advanced Encryption Standard (AES) untuk mengamankan data transaksi sebelum disimpan, sehingga seluruh informasi transaksi tersimpan dalam bentuk terenkripsi. Dari hasil pengujian membuktikan bahwa data terenkripsi dapat didekripsi kembali secara akurat menggunakan kunci rahasia yang valid serta mampu mencegah keterbacaan langsung data pada basis data tanpa memengaruhi integritas, akurasi, dan fungsionalitas sistem. Kesimpulannya, penerapan algoritma AES terbukti efektif dalam meningkatkan keamanan data transaksi dan layak diterapkan pada sistem informasi usaha skala kecil dan menengah.

Kata kunci— Kriptografi, Advanced Encryption Standard (AES), Keamanan Transaksi, Sistem Informasi Berbasis Web, Enkripsi Data

Pendahuluan

Perkembangan teknologi informasi telah mendorong pelaku usaha, termasuk sektor kuliner, untuk mengadopsi sistem informasi berbasis web dalam mendukung aktivitas operasional. Penggunaan sistem digital pada coffee shop memungkinkan proses pencatatan transaksi menjadi lebih cepat, akurat, dan efisien. Namun, di sisi lain, hal tersebut juga meningkatkan risiko terhadap keamanan data, terutama data transaksi yang bersifat sensitif dan bernilai strategis bagi keberlangsungan usaha[1].

Theking Coffee House sebagai salah satu coffee shop di wilayah Cikarang Utara, Bekasi, telah memanfaatkan sistem berbasis web untuk mengelola data menu, harga, dan transaksi penjualan. Sistem ini menyimpan data transaksi pada basis data terpusat yang berpotensi menjadi target serangan seperti pencurian data, penyadapan, maupun manipulasi informasi[2]. Tanpa mekanisme pengamanan yang memadai, kerahasiaan dan integritas data transaksi tidak dapat dijamin.

Kriptografi merupakan salah satu pendekatan yang umum digunakan untuk melindungi data dengan cara mengubah data asli (plaintext) menjadi bentuk tidak terbaca (ciphertext)[3]. Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris modern yang telah banyak digunakan karena tingkat keamanannya yang tinggi dan efisiensi dalam implementasi. AES dengan panjang kunci 256-bit (AES-256) dikenal memiliki ketahanan yang sangat kuat terhadap serangan brute force. Keamanan data transaksi menjadi isu yang sangat penting bagi usaha kecil dan menengah, termasuk coffee shop yang telah memanfaatkan sistem digital dalam pengelolaan penjualan dan data pelanggan. Theking Coffee House yang berlokasi di Cikarang Utara, Bekasi, menghadapi potensi risiko kebocoran, manipulasi, serta akses tidak sah terhadap data transaksi seiring meningkatnya penggunaan sistem berbasis web[4].

Beberapa penelitian sebelumnya menunjukkan bahwa AES efektif dalam mengamankan data pada berbagai sistem informasi, namun implementasi spesifik pada sistem transaksi coffee shop masih relatif terbatas. Oleh karena itu, penelitian ini dilakukan untuk mengisi celah tersebut dengan menerapkan AES-256 pada sistem transaksi Theking Coffee House[5]. Tujuan dari penelitian ini adalah merancang dan mengimplementasikan mekanisme enkripsi dan dekripsi data transaksi menggunakan algoritma AES-256, serta menganalisis efektivitasnya dalam meningkatkan keamanan data pada sistem informasi Theking Coffee House[6].

Beberapa penelitian terdahulu menunjukkan bahwa algoritma AES efektif dalam mengamankan data transaksi dan data sensitif pada sistem berbasis web maupun aplikasi, serta dapat dikombinasikan dengan metode lain seperti hashing untuk meningkatkan keamanan, sehingga menjadi dasar dan pembanding dalam penelitian ini. Hasil penelitian menunjukkan bahwa penerapan AES-256 mampu melindungi data transaksi sensitif yang tersimpan di basis data tanpa memberikan dampak signifikan terhadap kinerja sistem[7].

Metode Penelitian

Penelitian ini menggunakan pendekatan penelitian terapan (applied research) dengan tujuan mengimplementasikan algoritma kriptografi modern Advanced Encryption Standard (AES) pada sistem transaksi berbasis web. Pendekatan ini dipilih karena penelitian berfokus pada penyelesaian masalah keamanan data transaksi yang tersimpan dalam sistem informasi, khususnya pada lingkungan coffee shop[8].

Objek penelitian adalah data transaksi pada TheKing Coffee House yang meliputi nama pembeli, daftar menu pesanan, jumlah pembelian, harga total, serta identitas transaksi. Penelitian dilakukan melalui simulasi sistem digital yang merepresentasikan kondisi operasional nyata, tanpa menggunakan data pelanggan sebenarnya sehingga tetap menjaga aspek etika dan privasi[9].

Pengumpulan data dilakukan melalui observasi terhadap alur transaksi penjualan, studi literatur dari jurnal ilmiah dan buku yang membahas kriptografi serta keamanan sistem informasi, serta eksperimen sistem dengan cara menguji proses enkripsi dan dekripsi data transaksi. Metode ini digunakan untuk memastikan bahwa sistem yang dikembangkan mampu mengamankan data transaksi secara efektif dan sesuai dengan tujuan penelitian [10].

Pengembangan sistem dilakukan menggunakan metode **Waterfall** yang mencakup tahapan analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan pemeliharaan [11]. Pada tahap analisis kebutuhan ditentukan fitur utama sistem, seperti autentikasi pengguna, input data transaksi, enkripsi otomatis data sebelum penyimpanan, serta tampilan hasil dekripsi pada dashboard admin. Tahap perancangan meliputi pembuatan flowchart proses enkripsi dan dekripsi, perancangan struktur penyimpanan data, serta alur pengamanan data transaksi.

Pada tahap implementasi, sistem dikembangkan menggunakan bahasa pemrograman **JavaScript** dengan **Node.js** dan **Express.js** sebagai backend. Algoritma kriptografi yang digunakan adalah **Advanced Encryption Standard (AES) dengan panjang kunci 256-bit (AES-256)** untuk mengamankan data transaksi. Secara matematis, proses enkripsi AES dapat direpresentasikan dengan persamaan berikut:

$$C = EK(P)$$

di mana CCC adalah ciphertext, PPP adalah plaintext, dan EKE_KEK merupakan fungsi enkripsi menggunakan kunci rahasia KKK. Proses dekripsi dilakukan dengan persamaan:

$$P = DK(C)$$

di mana DKD_KDK adalah fungsi dekripsi menggunakan kunci yang sama.

Algoritma AES bekerja dengan memproses data dalam bentuk blok 128-bit melalui beberapa putaran (round) transformasi. Untuk AES-256, proses enkripsi terdiri dari **14 putaran**, yang masing-masing melibatkan operasi **SubBytes**, **ShiftRows**, **MixColumns**, dan **AddRoundKey**. Data transaksi yang telah dienkripsi kemudian disimpan dalam basis data dalam bentuk ciphertext. Proses dekripsi dilakukan dengan menerapkan operasi kebalikan dari setiap tahapan enkripsi sehingga data dapat dikembalikan ke bentuk plaintext saat diakses oleh pengguna yang berwenang.

Pengujian sistem dilakukan untuk memastikan bahwa seluruh data transaksi berhasil dienkripsi sebelum penyimpanan dan dapat didekripsi kembali secara akurat tanpa memengaruhi integritas, akurasi, dan fungsionalitas sistem.

Pada tahap analisis kebutuhan ditentukan fitur utama sistem, seperti autentikasi pengguna, input data transaksi, enkripsi otomatis data, serta tampilan dekripsi pada dashboard admin. Tahap perancangan meliputi pembuatan flowchart proses enkripsi dan dekripsi serta perancangan struktur penyimpanan data. Implementasi sistem dilakukan menggunakan bahasa pemrograman JavaScript dengan Node.js dan

Express.js sebagai backend, serta algoritma AES-256 sebagai metode kriptografi untuk mengamankan data transaksi[10].

Proses enkripsi dilakukan dengan cara memvalidasi data transaksi terlebih dahulu, kemudian mengenkripsi data dalam bentuk plaintext menggunakan secret key AES-256 sehingga menghasilkan ciphertext[12]. Ciphertext tersebut selanjutnya dikodekan dalam format Base64 atau Hex sebelum disimpan ke dalam database. Proses ini bertujuan untuk memastikan bahwa data yang tersimpan tidak dapat dibaca secara langsung tanpa melalui proses dekripsi[13].

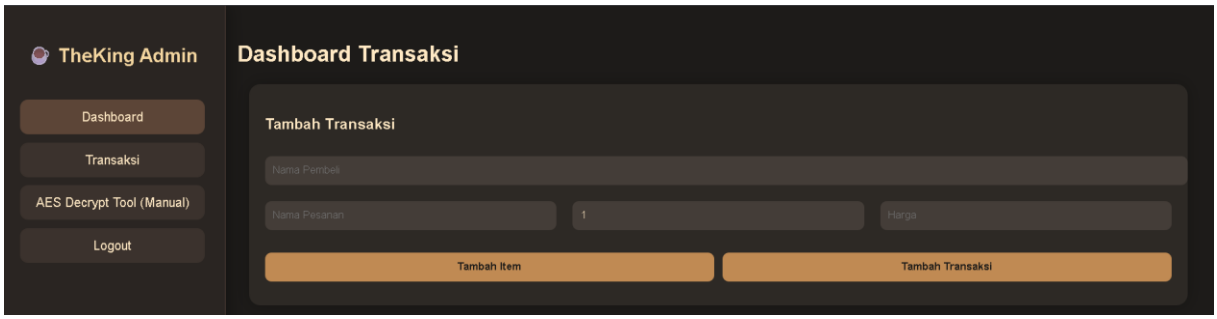
Proses dekripsi dilakukan dengan mengambil data ciphertext dari database, kemudian melakukan decoding dari format Base64 atau Hex ke bentuk biner. Selanjutnya sistem menggunakan secret key AES yang sama untuk mendekripsi ciphertext menjadi plaintext[14]. Hasil dekripsi dikonversi ke format UTF-8 agar dapat ditampilkan kembali sebagai teks asli pada dashboard admin. Proses ini hanya dapat dilakukan oleh pengguna yang telah berhasil melakukan autentikasi.

Analisis data dilakukan dengan membandingkan data transaksi sebelum dienkripsi, data yang telah dienkripsi, serta hasil dekripsi yang dikembalikan ke bentuk plaintext. Analisis ini bertujuan untuk memastikan bahwa algoritma AES mampu menjaga kerahasiaan data tanpa mengubah isi informasi asli[15]. Hasil dari penelitian ini diharapkan dapat menunjukkan bahwa penerapan algoritma AES-256 efektif dalam meningkatkan keamanan data transaksi pada sistem informasi berbasis web.

Hasil dan Pembahasan

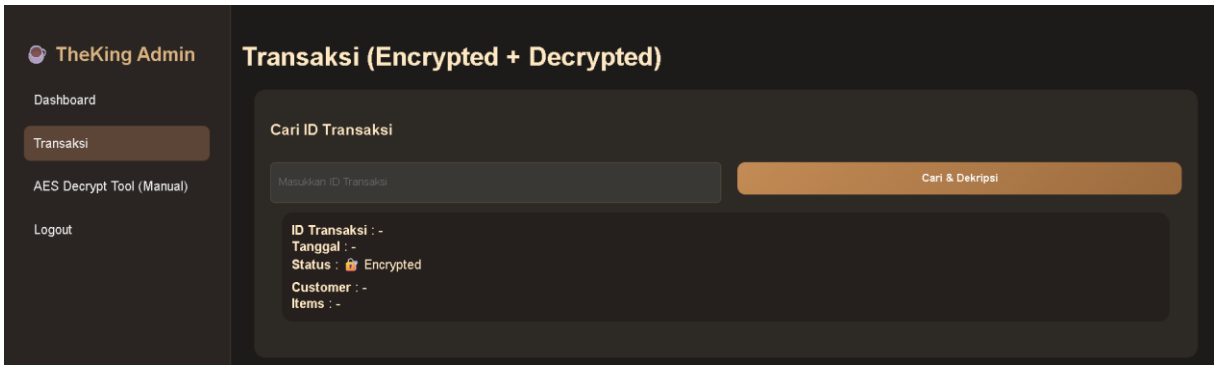
Hasil penelitian ini diperoleh melalui implementasi dan pengujian sistem transaksi berbasis web pada TheKing Coffee House dengan menerapkan algoritma kriptografi Advanced Encryption Standard (AES-256) untuk mengamankan data transaksi. Sistem dikembangkan menggunakan Node.js dan Express.js sebagai backend, serta HTML, CSS, dan JavaScript sebagai frontend. Autentikasi pengguna diterapkan untuk memastikan bahwa hanya admin yang berwenang dapat mengakses data transaksi dan melakukan proses dekripsi.

Pada tahap implementasi, sistem menyediakan dashboard utama yang memungkinkan admin memasukkan data transaksi berupa nama pembeli, daftar menu pesanan yang dapat lebih dari satu item, jumlah pembelian (quantity), serta harga total transaksi. Setiap transaksi secara otomatis diberikan ID transaksi sebagai identitas unik. Data transaksi yang dimasukkan akan langsung diproses oleh sistem dan dienkripsi menggunakan algoritma AES-256 sebelum disimpan ke dalam database berbasis file JSON.



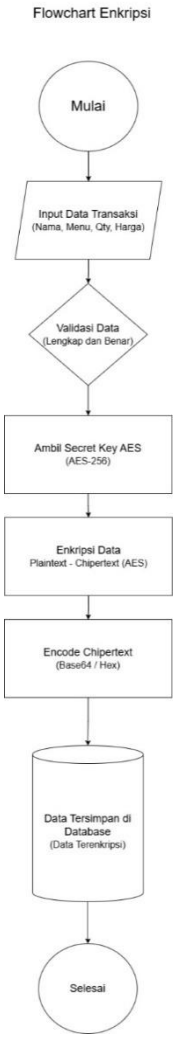
Gambar 1.Tampilan Dashboard Utama

Selain dashboard utama, sistem juga menyediakan dashboard khusus enkripsi dan dekripsi. Pada dashboard ini, admin dapat melihat data transaksi dalam bentuk ciphertext, serta melakukan proses dekripsi secara manual dengan memasukkan ID transaksi atau ciphertext tertentu. Sistem menampilkan tahapan dekripsi mulai dari decode Base64, proses dekripsi AES, hingga konversi hasil ke format UTF-8 sehingga plaintext asli dapat ditampilkan.

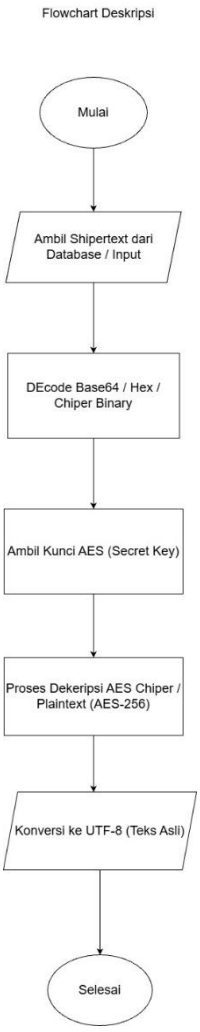


Gambar 2. Tampilan Dashboard Mencari ID Transaksi

Flowchart enkripsi dan dekripsi yang telah dirancang pada bab sebelumnya diimplementasikan secara langsung dalam sistem. Flowchart enkripsi menggambarkan proses mulai dari validasi data hingga penyimpanan ciphertext ke database, sedangkan flowchart dekripsi menggambarkan proses pengambilan ciphertext hingga penampilan plaintext pada dashboard admin.



Gambar 3. Flowchart Proses Enkripsi Data Transaksi



Gambar 4. Flowchart Proses Dekripsi Data Transaksi

Berdasarkan hasil implementasi dan pengujian sistem, diperoleh bahwa sistem mampu mengenkripsi seluruh data transaksi secara otomatis menggunakan algoritma AES-256. Data transaksi yang disimpan di dalam database tidak lagi berbentuk teks asli (plaintext), melainkan dalam bentuk ciphertext yang tidak dapat dibaca secara langsung. Hal ini menunjukkan bahwa sistem berhasil meningkatkan keamanan data transaksi dari risiko akses tidak sah.

Pengujian dilakukan dengan memasukkan beberapa data transaksi yang berbeda. Hasil pengujian menunjukkan bahwa setiap transaksi menghasilkan ciphertext yang berbeda meskipun memiliki struktur data yang sama, karena adanya proses enkripsi dan encoding. Ketika ciphertext tersebut dimasukkan kembali ke sistem untuk dilakukan dekripsi, hasil plaintext yang diperoleh sama persis dengan data transaksi awal sebelum dienkripsi. Hal ini membuktikan bahwa proses enkripsi dan dekripsi berjalan dengan benar dan konsisten.

Gambar 5. Hasil Pengujian Enkripsi Data Transaksi

Gambar 6. Hasil Pengujian Dekripsi pada Data Transaksi

Pada dashboard enkripsi dan dekripsi, sistem juga mampu menampilkan tahapan proses dekripsi secara jelas, dimulai dari decode Base64, proses dekripsi menggunakan secret key AES yang sama, hingga konversi hasil ke format UTF-8. Fitur ini memberikan pemahaman yang lebih baik mengenai cara kerja kriptografi AES secara praktis dan transparan, khususnya untuk keperluan pembelajaran dan demonstrasi akademik.

Dari hasil pengujian juga diketahui bahwa penerapan autentikasi pengguna berperan penting dalam menjaga keamanan sistem. Proses dekripsi hanya dapat dilakukan oleh admin yang telah berhasil login, sehingga akses terhadap data sensitif dapat dikontrol dengan baik. Dengan demikian, sistem tidak hanya mengamankan data melalui kriptografi, tetapi juga melalui mekanisme kontrol akses.

Penerapan algoritma AES-256 pada sistem transaksi TheKing Coffee House terbukti efektif dalam menjaga kerahasiaan data transaksi. Penggunaan kriptografi modern ini memastikan bahwa data yang tersimpan di database tidak dapat dimanfaatkan oleh pihak yang tidak berwenang meskipun berhasil mengakses penyimpanan data. Selain itu, integrasi proses enkripsi dan dekripsi secara langsung ke dalam alur sistem transaksi membuat keamanan data tidak mengganggu kenyamanan pengguna.

Pada penelitian ini, proses pengamanan data customer dilakukan menggunakan algoritma Advanced Encryption Standard (AES-256). Data customer yang digunakan sebagai contoh pengujian adalah plaintext berupa nama customer "Endang". Pada tahap awal, plaintext tersebut dikonversi ke dalam bentuk blok data berukuran 128 bit sesuai dengan spesifikasi algoritma AES. Selanjutnya, data diproses menggunakan secret key dengan panjang 256 bit yang telah ditentukan sebelumnya. Proses enkripsi dilakukan melalui beberapa tahapan utama, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*, yang dieksekusi secara berulang sebanyak 14 ronde sesuai dengan standar AES-256.

Hasil dari proses enkripsi tersebut berupa ciphertext yang telah mengalami transformasi secara menyeluruh sehingga tidak dapat dikenali bentuk aslinya. Ciphertext yang dihasilkan kemudian dikodekan ke dalam format Base64 untuk memudahkan penyimpanan dan pengelolaan data pada basis data. Dari hasil pengujian, plaintext "Endang" setelah melalui proses enkripsi menggunakan algoritma AES-256 menghasilkan ciphertext *U2FsdGVkX18WGfSMLUOau6XFII3V7xl4J0IPBEF+CbE=*.

Pada tahap selanjutnya dilakukan proses dekripsi untuk memastikan keakuratan dan keandalan sistem. Ciphertext yang tersimpan terlebih dahulu dilakukan proses decoding Base64, kemudian diproses menggunakan algoritma AES-256 dengan secret key yang sama seperti pada proses enkripsi. Tahapan dekripsi dilakukan dengan urutan kebalikan dari proses enkripsi, yaitu *AddRoundKey*, *Inverse MixColumns*, *Inverse ShiftRows*, dan *Inverse SubBytes*. Hasil dari proses dekripsi menunjukkan bahwa ciphertext berhasil dikembalikan ke bentuk plaintext awal, yaitu "Endang", tanpa adanya perubahan data.

Berdasarkan hasil pengujian tersebut, dapat disimpulkan bahwa algoritma AES-256 mampu mengamankan data customer dengan baik melalui proses enkripsi yang kuat serta memastikan integritas data melalui proses dekripsi yang akurat. Hal ini menunjukkan bahwa penerapan algoritma AES-256 layak digunakan untuk melindungi data sensitif pada sistem transaksi.

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma kriptografi Advanced Encryption Standard (AES-256) pada sistem transaksi berbasis web TheKing Coffee House berhasil meningkatkan keamanan data transaksi. Data yang disimpan dalam sistem tidak lagi berada dalam bentuk plaintext, melainkan telah dienkripsi menjadi ciphertext sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang.

Hasil pengujian menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan baik dan konsisten. Data transaksi yang telah dienkripsi dapat dikembalikan ke bentuk plaintext tanpa mengalami perubahan isi informasi, sehingga integritas data tetap terjaga. Selain itu, penggunaan mekanisme autentikasi admin memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat melakukan proses dekripsi dan melihat data transaksi secara lengkap.

Dengan demikian, penelitian ini membuktikan bahwa algoritma AES-256 dapat diimplementasikan secara efektif dan efisien pada sistem informasi berbasis web untuk melindungi data transaksi. Penerapan kriptografi modern ini tidak hanya meningkatkan aspek keamanan sistem, tetapi juga dapat dijadikan sebagai solusi praktis dalam pengelolaan dan perlindungan data pada lingkungan usaha seperti coffee shop.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Bapak **Muhammad Najamuddin Dwi Miharja, S.Kom, M.Kom.,** selaku dosen pengampu mata kuliah Kriptografi yang telah memberikan bimbingan, arahan, serta masukan selama proses penelitian ini. Ucapan terima kasih juga disampaikan kepada semua pihak yang telah membantu dan mendukung penyelesaian penelitian ini, baik secara langsung maupun tidak langsung, sehingga penelitian ini dapat diselesaikan dengan baik.

Daftar Rujukan

[1] M. L. Assidiq, F. Mahardika, and D. Santika, "Implementasi Algoritma Kriptografi AES dan SHA-3 Dalam Mengamankan Data Sensitif Pengguna Pada Website Transaksi," 2024. [Online]. Available: http://jurnal.bsi.ac.id/index.php/simpatik

[2] L. Sidabutar, M. Ramadhan, Z. Panjaitan, S. Informasi, and S. Triguna Dharma, "Implementasi Kriptografi Pengamanan Data Pemesanan Produk Menggunakan Meotode AES", [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jsi

[3] A. Rahayu, G. Abdillah, and H. Ashaury, "PENGAMANAN MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN BCRYPT (BLOWFISH CRYPT) PADA FILE DOKUMEN," 2024.

[4] M. Hanindia Prami Swari, H. Maulana, I. Putu Susila Handika, and I. Kadek Susila Satwika, "Implementasi AES 256 untuk Pengamanan Data pada Supply Chain Management Bumdes Sarining Winangun Kukuh", [Online]. Available: https://s.id/jurnalresistor

[5] S. Amini, "SKANIKA VOLUME 1 NO. 1 MARET 2018 217 Implementasi AES-256 Untuk Mengamankan Database E-Commerce."

[6] "Pengembangan Aplikasi Mobile Kriptografi untuk Enkripsi dan Dekripsi Teks AHMAD YUSUF AL-HAFIZ 1 , ANGGI FERITA OKTAVIANI 2 , AYU AMELIA PERTIWI 3 , AZHARA AMELIA H 4 , DESNI PARAMITHA PURBA 5 , LENI KARMILA DAULAY 6 , SABRINA AKVA 7 , SARAH PUTRI SYAIFULLAH 8 , YOHANA LORINEZ S 9".

[7] A. Handayani, N. Budi Nugroho, and R. I. Ginting, "Implementasi Kriptografi Dengan Metode AES(Advance Encryption Standard) Untuk Mengamankan Data Penjualan Di Toko Sweet Amirah," *Jurnal CyberTech*, vol. 2, no. 2, pp. 297–311, 2019, [Online]. Available: https://ojs.trigunadharma.ac.id/

[8] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *Journal of Computer System and Informatics (JoSYC)*, vol. 4, no. 1, pp. 179–187, Dec. 2022, doi: 10.47065/josyc.v4i1.2451.

[9] D. Pandya Pangestu, D. Virgian, and S. Y. Sakti, "6 th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)," 2025.

[10] "3_124_Naskah_PUB_Irawan_91-96".

[11] A. Puji Nugroho, H. Bayu Suseno, and U. Islam Negeri Syarif Hidaytullah Jakarta, "QUERY: Jurnal Sistem Informasi Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES," 2020.

[12] A. Permana, U. Tatang Suryadi, A. Zezen Zaenal Abidin, Y. Murdianingsih, and M. Faizal, "Optimalisasi Sistem Pemilu Melalui Implementasi E-Voting Berbasis Blockchain Dengan Keamanan Kriptografi AES-128."

[13] F. A. Jebadu and S. Waluyo, "6 th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)," 2025.

[14] R. Pradipa Purba, B. Angga Wijaya, L. Wati Nazara, and S. Suryati Utami, "Desain Protokol Keamanan Data Berbasis Blockchain pada Pengolahan Data Pengguna Aplikasi E-commerce," vol. 9, p. 2025, doi: 10.47002/metik.v9i2.1104.

[15] "Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi".