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 Algoritma AES-256 untuk Pengamanan Data Transaksi pada Sistem Informasi UMKM Warung Aris

Implementation of the AES-256 Algorithm for Transaction Data Security in the Warung Aris MSME Information System

Sone Rahmadani1, Isnain Farras Syah[2], Fazri Iqbal Khoirinata[3], Rio Dwitra Anbagaswara[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]sonerahmadani@gmail.com , [2]farrasfarras01@gmail.com* , [3]iqbalkhoirinata@gmail.com* ,
[4]riodwitraanbagaswara1@gmail.com*

Abstract

Information System Development in Abstract. The purpose of this research is to create an encrypted transaction information system for the Warung Aris MSME. This will utilize the Advanced Encryption Standard (AES) 256-bit algorithm to enhance the security of customer transaction data. The Laravel 12 framework, which has a Model-View-Controller (MVC) architecture and a MySQL database, is used to build the system. The main security component utilizes AES-256-CBC encryption with a 16-byte random Initialization Vector (IV) for each transaction. This protects sensitive data from leaks and cryptanalysis attacks. Non-sensitive data is stored in plaintext to maintain system efficiency, but transaction descriptions and sensitive metadata are included in the encrypted data. The system provides a real-time dashboard to monitor encrypted transactions and CRUD features, including automatic encryption and decryption. Implementation results show that the system can improve data security and transaction management efficiency for MSMEs, with encryption and decryption speeds below 100 milliseconds per transaction. This research demonstrates that the implementation of enterprise-grade encryption technology can be implemented efficiently and cost-effectively at the MSME scale.

Keywords: *Cryptography, AES-256, Data Security, Information Systems, Micro and Small Businesses*

Abstrak

Perkembangan sistem informasi pada *Abstract*. Tujuan dari penelitian ini adalah untuk membuat sistem informasi transaksi terenkripsi untuk UMKM Warung Aris. Ini akan menggunakan algoritma *Advanced Encryption Standard* (AES) 256-bit untuk meningkatkan keamanan data transaksi pelanggan. *Framework* Laravel 12 digunakan untuk membangun sistem, yang memiliki arsitektur *Model-View-Controller* (MVC) dan database MySQL. Komponen keamanan utama menggunakan enkripsi AES-256-CBC dengan *Initialization Vector* (IV) random 16-byte pada setiap transaksi. Ini memungkinkan untuk melindungi data sensitif dari kebocoran dan serangan kriptanalisis. Data yang tidak sensitif disimpan dalam bentuk *plaintext* untuk menjaga efisiensi sistem, tetapi deskripsi transaksi dan metadata sensitif termasuk dalam data yang dienkripsi. *Dashboard real-time* diberikan oleh sistem untuk memantau transaksi terenkripsi dan fitur CRUD, termasuk enkripsi dan dekripsi otomatis. Hasil implementasi menunjukkan bahwa sistem dapat meningkatkan keamanan data dan efisiensi pengelolaan transaksi UMKM dengan kecepatan enkripsi dan dekripsi di bawah 100 milidetik per transaksi. Penelitian ini membuktikan bahwa penerapan teknologi enkripsi tingkat perusahaan dapat dilaksanakan secara efisien dan murah pada skala UMKM.

Kata kunci: Kriptografi, AES-256, Keamanan Data, Sistem Informasi, Bisnis Mikro dan Kecil

Pendahuluan

Digitalisasi di banyak industri, termasuk usaha mikro, kecil, dan menengah (UMKM), telah didorong oleh kemajuan teknologi informasi yang pesat [1]. Digitalisasi proses bisnis, khususnya pencatatan dan pengelolaan transaksi, memiliki banyak keuntungan, seperti meningkatkan efisiensi operasional, membuat pengelolaan data menjadi lebih mudah, dan membantu pengambilan keputusan berbasis data [2]. Sebagian

besar UMKM masih menggunakan pencatatan transaksi secara manual atau sistem digital sederhana tanpa mekanisme keamanan yang memadai, tetapi penggunaan sistem digital juga meningkatkan risiko keamanan data, terutama data transaksi pelanggan yang sensitif [3].

Kondisi seperti ini dapat menyebabkan berbagai masalah, seperti kebocoran data, manipulasi transaksi, dan penyalahgunaan data pelanggan [4]. Meskipun risiko yang dihadapi semakin meningkat seiring dengan penggunaan teknologi, UMKM seringkali tidak menerapkan sistem keamanan data yang kuat karena kurangnya pemahaman dan keterbatasan sumber daya [5]. Padahal, perlindungan data pelanggan merupakan aspek krusial dalam menjaga kepercayaan konsumen dan kepatuhan terhadap regulasi yang berlaku [6].

Salah satu metode yang efektif untuk melindungi data dari akses yang tidak sah adalah kriptografi [7]. Sistem keamanan tingkat perusahaan, seperti sektor perbankan dan pemerintahan, menggunakan algoritma enkripsi simetris *Advanced Encryption Standard* (AES) [8]. AES-256, versi dengan panjang kunci 256-bit, sangat aman dan tahan terhadap berbagai serangan kriptanalisis modern [9]. Studi oleh Sari dan Nugroho (2021) menunjukkan bahwa implementasi AES-256 pada sistem informasi UMKM mampu meningkatkan keamanan data transaksi secara signifikan [1]. Penelitian serupa oleh Putra dan Lestari (2022) juga mengonfirmasi efektivitas algoritma ini dalam sistem penjualan berbasis web [2].

Mode operasi *Cipher Block Chaining* (CBC) yang digunakan dalam AES-256 menambahkan lapisan keamanan ekstra dengan cara meng-XOR-kan blok plaintext sebelumnya dengan blok ciphertext sebelumnya sebelum proses enkripsi [10]. Hal ini membuat hasil enkripsi menjadi lebih acak dan sulit dianalisis oleh pihak yang tidak berwenang [11]. Diharapkan algoritma ini dapat digunakan pada sistem informasi transaksi UMKM untuk meningkatkan perlindungan data tanpa menambah kompleksitas yang berarti [3], [5].

Beberapa penelitian terdahulu telah membuktikan keunggulan AES-256 dalam berbagai konteks aplikasi. Rahmawati dan Saputra (2021) menerapkannya pada aplikasi e-commerce dan mendapatkan hasil pengujian keamanan yang memuaskan [3]. Hidayat dan Pratama (2020) mengimplementasikannya pada sistem penjualan berbasis web dengan tingkat enkripsi yang kuat [4]. Nugraha dan Setiawan (2023) bahkan mengintegrasikannya dalam sistem informasi UMKM terintegrasi [5]. Prasetyo dan Wibowo (2021) menekankan pentingnya implementasi yang tepat agar algoritma dapat bekerja optimal [6].

Fokus penelitian ini adalah membuat sistem informasi transaksi terenkripsi untuk UMKM Warung Aris yang menggunakan algoritma AES-256-CBC. Sistem ini dibangun menggunakan *framework* Laravel 12 dengan arsitektur *Model-View-Controller* (MVC), yang membuatnya terstruktur, mudah dikembangkan, dan memiliki tingkat keamanan yang tinggi [12]. Data transaksi sensitif dienkripsi sebelum disimpan ke dalam *database*, tetapi data non-sensitif tetap disimpan dalam bentuk biasa untuk memastikan sistem berjalan dengan baik [13]. Pendekatan ini sejalan dengan rekomendasi Kurniawan dan Hidayatullah (2022) yang menyarankan enkripsi selektif pada data sensitif untuk menjaga performa sistem [7].

Tujuan dari penelitian ini adalah untuk merancang dan menerapkan sistem informasi transaksi yang aman, efisien, dan mudah digunakan untuk UMKM. Diharapkan bahwa sistem ini akan meningkatkan efisiensi pengelolaan transaksi dan meningkatkan keamanan data transaksi pelanggan [8], [9]. Sistem ini juga akan menjadi fondasi untuk pengembangan sistem yang lebih kompleks di masa mendatang, seperti integrasi *payment gateway*, aplikasi *mobile*, dan analitik bisnis berbasis data [10]. Dengan demikian, kontribusi penelitian ini tidak hanya pada aspek keamanan, tetapi juga pada kesiapan UMKM dalam menghadapi era digital yang semakin kompetitif [14], [15].

Metode Penelitian

Untuk membangun sistem informasi transaksi terenkripsi ini, metode *System Development Life Cycle* (SDLC) dengan model *Waterfall* digunakan. Model ini dipilih karena memiliki tahapan yang sistematis dan terstruktur serta cocok untuk pengembangan sistem dengan kebutuhan yang jelas dan terdefinisi sejak awal. Tahapan

yang dilakukan meliputi analisis persyaratan, perancangan sistem, implementasi sistem, pengujian sistem, dan evaluasi.

Pada tahap analisis persyaratan, dilakukan identifikasi permasalahan yang dihadapi UMKM Warung Aris dalam pengelolaan transaksi. Hasil analisis menunjukkan bahwa pencatatan transaksi belum memiliki mekanisme keamanan yang memadai sehingga berisiko menyebabkan kebocoran atau penyalahgunaan data. Oleh karena itu, sistem yang dikembangkan harus mudah digunakan, efektif, serta mampu melindungi data pelanggan yang sensitif. Kebutuhan fungsional sistem meliputi pengelolaan data transaksi, data pelanggan, serta tampilan *dashboard*. Adapun kebutuhan non-fungsional mencakup aspek keamanan, kinerja, dan kemudahan penggunaan.

Perancangan sistem dilakukan dengan membangun arsitektur berbasis *Model–View–Controller* (MVC) menggunakan *framework* Laravel 12. Perancangan mencakup mekanisme keamanan data, struktur *database*, dan desain alur sistem. Algoritma AES-256-CBC diterapkan untuk mengenkripsi data transaksi sensitif sebelum disimpan ke dalam *database* MySQL. Setiap proses enkripsi menggunakan *Initialization Vector* (IV) acak sepanjang 16-byte untuk meningkatkan tingkat keamanan. Selain itu, logika bisnis, layanan enkripsi, dan penyimpanan data dipisahkan guna mendukung arsitektur keamanan berlapis.

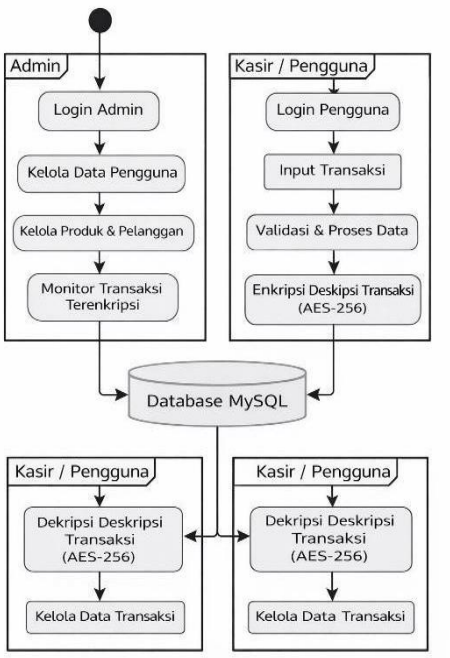
Tahap implementasi sistem dilakukan dengan mengembangkan sistem sesuai dengan rancangan yang telah dibuat. *Library* OpenSSL digunakan dalam proses enkripsi dan dekripsi data, sementara kunci enkripsi diperoleh dari APP_KEY Laravel melalui proses *hashing* SHA-256. Sistem dilengkapi dengan fitur CRUD transaksi yang secara otomatis melakukan enkripsi saat data disimpan dan dekripsi saat data ditampilkan.

Pengujian sistem dilakukan untuk memastikan seluruh fungsi berjalan sesuai dengan kebutuhan yang telah ditetapkan. Pengujian mencakup verifikasi proses enkripsi dan dekripsi data, pengujian performa untuk mengukur waktu yang diperlukan dalam setiap proses transaksi, serta pengujian terhadap kinerja sistem secara keseluruhan. Hasil pengujian menunjukkan bahwa data sensitif tidak dapat dibaca tanpa melalui proses dekripsi, dan sistem tetap berjalan secara efisien.

Tahap evaluasi dilaksanakan untuk menilai peningkatan keamanan dan efisiensi dalam pengelolaan transaksi UMKM. Evaluasi mencakup analisis terhadap tingkat keamanan data, kemudahan penggunaan sistem, serta dampak implementasi sistem terhadap proses operasional UMKM. Hasil evaluasi digunakan sebagai dasar untuk menarik kesimpulan dan menyusun rekomendasi bagi pengembangan sistem di masa mendatang.

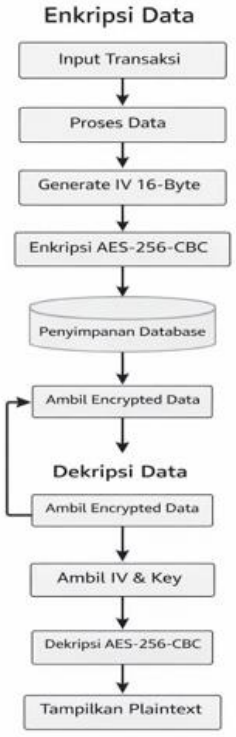
Hasil dan Pembahasan

Hasil dari penggunaan algoritma AES-256 pada sistem informasi UMKM Warung Aris menunjukkan bahwa sistem memiliki dua jenis pengguna: admin dan kasir/pengguna. Input dan pengelolaan data transaksi dilakukan oleh pengguna, sedangkan admin mengelola sistem dan mengawas data. Untuk menjaga keamanan data, sistem ini secara otomatis menggunakan mekanisme untuk enkripsi dan dekripsi data transaksi. Alur kerja sistem pengamanan data transaksi UMKM Warung Aris digambarkan dalam diagram *flowchart* berikut.



Gambar 1. *Flowchat* alur kerja sistem Informasi UMKM Warung

Pada Gambar 1 menggambarkan flowchat menjelaskan alur sistem transaksi yang aman menggunakan enkripsi AES-256. Admin melakukan login untuk mengelola data pengguna, produk, pelanggan, serta memantau transaksi dalam bentuk terenkripsi. Kasir atau pengguna *login* ke sistem, melakukan input transaksi, lalu data divalidasi dan dienkripsi sebelum disimpan ke database MySQL Data yang tersimpan bersifat terenkripsi untuk menjaga keamanan. Saat data diperlukan kembali, sistem melakukan dekripsi agar transaksi dapat dibaca dan dikelola.Tujuan utama sistem ini adalah menjaga keamanan dan kerahasiaan data transaksi.



Gambar 2. Flowchat Enkripsi dan Dekripsi

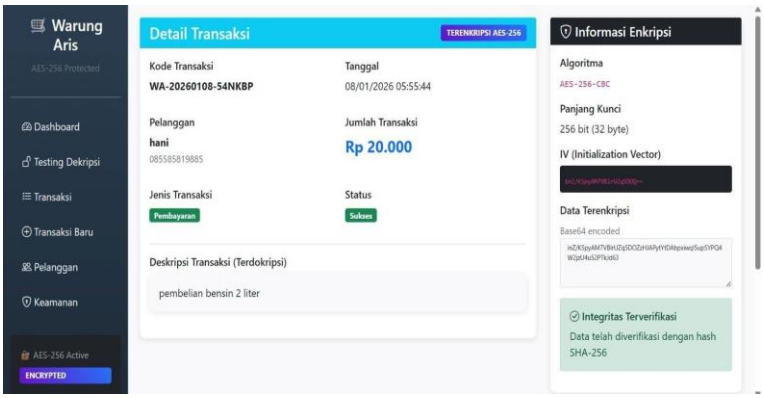
Gambar 2 Diagram ini menjelaskan alur keamanan data transaksi pada Sistem UMKM Warung Aris menggunakan enkripsi dan dekripsi AES-256-CBC. Pada proses enkripsi, data transaksi dimasukkan dan diproses oleh sistem, kemudian dibuat IV 16- byte sebagai nilai acak untuk meningkatkan keamanan. Setelah itu data dienkripsi menggunakan AES-256-CBC sehingga berubah menjadi data terenkripsi, lalu disimpan ke dalam database. Pada proses dekripsi, sistem mengambil data terenkripsi dari *database*, kemudian mengambil IV dan key yang sesuai. Data tersebut didekripsi menggunakan AES-256-CBC sehingga kembali ke bentuk aslinya (*plaintext*) dan dapat ditampilkan kepada pengguna. Dengan proses ini, data transaksi tersimpan dengan aman dan terlindungi dari akses yang tidak berwenang.

Spesifikasi pada Tabel 1 merupakan komponen algoritma dan teknologi yang digunakan pada sistem informasi UMKM Warung Aris. Setiap komponen dalam sistem berfungsi untuk mendukung pengelolaan transaksi, menjaga keamanan data, serta meningkatkan efisiensi operasional melalui penerapan mekanisme kriptografi.

Tabel 1. Spesifikasi Komponen Algoritma Sistem Informasi UMKM Warung Aris

No	Algoritma Teknologi	Fungsi Sistem	Keterangan
1	**SHA-256**	Generasi dan pengamanan kunci enkripsi	Digunakan untuk menghasilkan kunci enkripsi dari APP_KEY Laravel melalui proses hashing satu arah.
2	**AES-256-CBC**	Enkripsi dan dekripsi data transaksi	Menjaga kerahasiaan data transaksi sensitif seperti deskripsi transaksi.
3	**MySQL**	Penyimpanan data sistem	Menyimpan data transaksi, data pelanggan, serta data hasil enkripsi dalam database.
4	**Laravel 12**	Pengembangan sistem informasi UMKM	Mengelola alur sistem, logika bisnis, dan integrasi enkripsi menggunakan arsitektur MVC.
5	**Tabel Transaksi Terenkripsi**	Pengamanan data transaksi	Menyimpan data transaksi dalam bentuk terenkripsi sehingga tidak dapat dibaca secara klangsung tanpa proses dekripsi.

Tabel di atas menunjukkan spesifikasi komponen algoritma dan teknologi yang digunakan untuk sistem informasi UMKM Warung Aris. Menghasilkan dan melindungi kunci enkripsi melalui proses hashing satu arah dari APP_KEY Laravel dilakukan oleh algoritma SHA-256. Selain itu, algoritma AES-256-CBC enkripsi dan dekripsi data transaksi sensitif untuk menjaga kerahasiaan informasi. MySQL menyimpan data transaksi, data pelanggan, dan hasil enkripsi *database*. Selain mengelola alur sistem, logika bisnis, dan integrasi proses enkripsi melalui arsitektur MVC, *Framework* Laravel 12 juga menggunakan tabel transaksi terenkripsi untuk memastikan bahwa data transaksi disimpan dalam bentuk terenkripsi sehingga tidak dapat dibaca secara langsung tanpa menggunakan proses dekripsi yang sah.

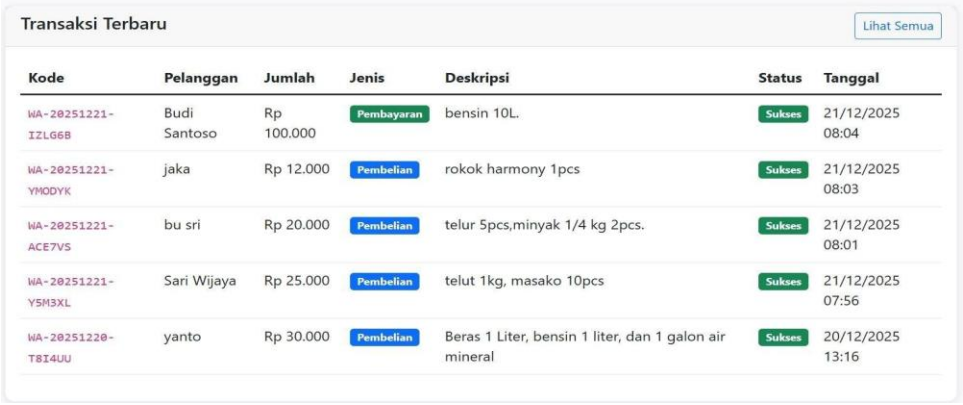


Gambar 3. satu data hasil enkripsi

Gambar 3 tersebut menunjukkan contoh data transaksi yang telah dienkripsi pada sistem informasi UMKM Warung Aris. Pada halaman Detail Transaksi, sistem menampilkan informasi umum tentang transaksi, seperti kode transaksi, tanggal, nama pelanggan, jumlah transaksi, jenis transaksi, dan status transaksi. Karena fakta bahwa informasi ini dianggap sebagai data non-sensitif, informasi ini disimpan dan ditampilkan secara plaintext untuk memastikan sistem tetap beroperasi dengan baik.

Bagian Deskripsi Transaksi menunjukkan bahwa data awal, yang berisi "pembelian bensin 2 liter," telah dienkripsi menggunakan algoritme AES-256-CBC sebelum disimpan ke dalam database. Ini memastikan bahwa pengguna tetap dapat membaca isi transaksi tanpa mengetahui proses kriptografi yang terjadi di belakang sistem.Di sisi kanan, panel Informasi Enkripsi menampilkan detail teknis keamanan yang digunakan. Algoritma AES-256-CBC memiliki panjang kunci 256 bit (32 byte) dan Initialization Vector (IV) yang dibuat secara acak untuk setiap transaksi untuk memastikan bahwa hasil enkripsi selalu berbeda meskipun data transaksi yang dimasukkan sama. Selain itu, data ditunjukkan dalam format Base64, yang merupakan hasil dari proses enkripsi sebelum disimpan ke database.

Data tidak dapat dibaca secara langsung tanpa melakukan proses dekripsi dengan kunci dan IV yang tepat. Selain itu, sistem menggunakan hash SHA-256 untuk verifikasi integritas data, yang ditunjukkan dengan status "Integritas Terverifikasi". Hal ini memastikan bahwa data transaksi tidak akan berubah selama proses pengambilan atau penyimpanan data.Tampilan tersebut menunjukkan bahwa sistem berhasil melindungi data transaksi. Data sensitif dilindungi dengan enkripsi AES-256, integritas data dijamin dengan hashing SHA-256, dan sistem memastikan bahwa aplikasi dapat digunakan dengan mudah.



Gambar 4. hasil keseluruhan enkripsi

Gambar 4 tersebut menunjukkan data transaksi keseluruhan dari sistem informasi UMKM Warung Aris, yang dienkripsi dengan algoritma AES-256. Pada halaman Transaksi Terbaru, sistem menampilkan daftar transaksi yang termasuk kode transaksi, nama pelanggan, jumlah transaksi, jenis transaksi, deskripsi, status, dan tanggal. Informasi umum seperti kode transaksi, nama pelanggan, jumlah transaksi, jenis transaksi, status, dan tanggal disimpan dalam bentuk plaintext karena tidak sensitif dan diperlukan untuk kemudahan pengawasan dan efisiensi proses pengelolaan data. Selain itu, data deskripsi transaksi sistem telah dienkripsi sebelum disimpan ke dalam database menggunakan algoritma AES-256-CBC. Ketika data ditampilkan pada antarmuka pengguna, data tersebut secara otomatis didekripsi, sehingga pengguna tetap dapat membaca isi transaksi tanpa mengetahui proses enkripsi dan dekripsi yang terjadi di belakang sistem. Ini menunjukkan bahwa sistem keamanan tidak mengganggu kenyamanan pengguna saat menjalankan transaksi.

Tampilan tersebut menunjukkan bahwa sistem berhasil mengenkripsi data transaksi secara menyeluruh. Sistem tetap memberikan tampilan data yang informatif, real-time, dan mudah dipahami, sementara semua data sensitif dilindungi di tingkat penyimpanan. Implementasi ini menunjukkan bahwa algoritma enkripsi AES-256 dapat digunakan pada skala UMKM untuk meningkatkan keamanan data transaksi tanpa mengurangi fungsionalitas dan efisiensi sistem.

Kesimpulan

Kesimpulan b Hasil penelitian dan implementasi menunjukkan bahwa algoritma AES-256 berhasil meningkatkan keamanan data transaksi di sistem informasi UMKM Warung Aris. Data sensitif, terutama deskripsi transaksi, telah dienkripsi sebelum disimpan dalam database sehingga pihak yang tidak berwenang tidak dapat membacanya. Proses pembangkitan kunci enkripsi yang menggunakan SHA-256 meningkatkan keamanan sistem, dan penggabungan dengan framework Laravel 12 memungkinkan proses enkripsi dan dekripsi berjalan secara otomatis tanpa mengganggu kenyamanan pengguna. Hasil pengujian menunjukkan bahwa sistem dapat menampilkan data transaksi secara real-time melalui mekanisme dekripsi yang aman. Ini memungkinkan sistem untuk mencapai efisiensi operasional dan keamanan data pada saat yang sama.

Dengan demikian, sistem ini membuktikan bahwa teknologi enkripsi tingkat tinggi dapat diterapkan secara efektif pada skala UMKM untuk melindungi data transaksi dan mendukung digitalisasi usaha.

Ucapan Terima Kasih

Terima kasih banyak kepada Bapak Muhammad Najamuddin Dwi Miharja, S.Kom., M.Kom. atas bimbingaan, dukungan serta memantau selama proses penelitian ini dari awal hingga akhir. Atas dukungannya penelitian ini dapat selesai tepat waktu, sehingga penelitian dapat berjalan dengan lancar

Daftar Rujukan

[1] D. P. Sari and A. Nugroho, "Implementasi Algoritma Advanced Encryption Standard (AES-256) untuk Pengamanan Data Transaksi pada Sistem Informasi UMKM," *Jurnal Sistem Informasi dan Informatika*, vol. 8, no. 2, pp. 115–124, 2021.

[2] R. A. Putra and T. Lestari, "Analisis Keamanan Data Transaksi Menggunakan Algoritma AES-256 pada Sistem Informasi Penjualan Berbasis Web," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 4, no. 1, pp. 45–54, 2022.

[3] N. Rahmawati and M. Y. Saputra, "Penerapan Algoritma AES-256 untuk Keamanan Data Transaksi Digital pada Aplikasi E-Commerce," *Jurnal Teknologi Informasi dan Komputer*, vol. 9, no. 3, pp. 201–210, 2021.

[4] R. Hidayat and A. Pratama, "Pengamanan Data Transaksi Penjualan Menggunakan Algoritma AES-256 Berbasis Web," *Jurnal Ilmiah Teknologi dan Sistem Informasi*, vol. 6, no. 2, pp. 89–97, 2020.

[5] A. Nugraha and D. Setiawan, "Implementasi Algoritma AES-256 untuk Perlindungan Data Transaksi UMKM pada Sistem Informasi Terintegrasi," *Jurnal Sistem Informasi Bisnis*, vol. 13, no. 1, pp. 33–41, 2023.

[6] B. Prasetyo and A. Wibowo, "Implementasi Keamanan Data Menggunakan Algoritma AES-256 pada Sistem Informasi Berbasis Web," *Jurnal Informatika Terapan*, vol. 5, no. 2, pp. 78–87, 2021.

[7] D. Kurniawan and F. Hidayatullah, "Analisis Enkripsi AES-256 untuk Perlindungan Data Transaksi pada Sistem Informasi UMKM," *Jurnal Teknologi Informasi dan Sistem Komputer*, vol. 10, no. 1, pp. 55–64, 2022.

[8] R. Firmansyah and F. Ramadhan, "Penerapan Algoritma Kriptografi AES-256-CBC pada Sistem Informasi Penjualan UMKM," *Jurnal Sistem Informasi dan Aplikasi*, vol. 7, no. 1, pp. 21–30, 2023.

[9] I. Maulana and D. Setiawan, "Pengamanan Basis Data Transaksi Menggunakan Algoritma AES-256 dan SHA-256," *Jurnal Rekayasa Perangkat Lunak*, vol. 3, no. 2, pp. 92–101, 2021.

[10] A. N. Putri and H. Saputro, "Implementasi Keamanan Data Transaksi Digital Menggunakan Algoritma AES-256 pada Aplikasi Web," *Jurnal Teknologi dan Keamanan Informasi*, vol. 4, no. 1, pp. 44–53, 2022.

[11] A. Nugrahantoro, A. Fadlil, and I. Riadi, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)," *Jurnal Ilmiah FIFO*, vol. 12, no. 1, p. 12, 2020. doi: 10.22441/fifo.2020.v12i1.002.

[12] Fathansyah, *Basis Data*. Bandung: Informatika, 2018.

[13] A. Kadir, *Konsep dan Tuntunan Praktis Basis Data*. Yogyakarta: Andi Offset, 2018.

[14] D. Widyaningsih, E. Zusrony, and H. Utomo, "Peran digital entrepreneurship mindset: keputusan adopsi platform

digital bagi pelaku bisnis," *Jurnal Sistem Informasi Bisnis*, vol. 13, no. 2, pp. 162-171, 2023. doi: 10.21456/vol13iss2pp162-171.

[15] M. Hutauruk, "Pendampingan dan Pelatihan Digitalisasi Akuntansi Manufaktur Usaha Kecil dan Menengah di Wonosari, Gunung Kidul, Yogyakarta," *Warta LPM*, pp. 346-355, 2022. doi: 10.23917/warta.v25i3.1030.