

SISTEM KEAMANAN DATA BAGI HASIL KONSINYASI PADA UMKM WARUNG JAJANAN TRADISIONAL MENGUNAKAN ALGORITMA AES-256

DATA SECURITY SYSTEM FOR CONSIGNMENT RESULTS IN TRADITIONAL SNACK STALL SMALL AND MEDIUM ENTERPRISES USING THE AES-256

Faisal Fajar¹, Raul Putra Widodo²

^{1,2}Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

¹faisalfajar1305@gmail.com, ²ultrawdd@gmail.com*

Abstract

The need for digitisation with strong information security in traditional snack stall MSMEs to face significant challenges in managing profit-sharing consignment data. This study developed a web-based management system using AES-256 encryption to encrypt sensitive data such as capital costs, selling prices, and total revenue to maintain data confidentiality. The methodology included field observations at Warung Budeh Faisal, system requirements analysis, database design, and implementation with Node.js before the data was successfully stored. The implementation results show that the system successfully replaces manual recording with a login interface, goods input, recording, monitoring, sales recording and income statistics, where plaintext data such as the selling price of Rp.1500 is converted into random ciphertext such as '2u7OJZgFYG1ZTw7KQoBXvWaBYx9U7' in the database. Testing proved high security against illegal access, increased operational efficiency, and trust among related parties. The conclusion of this study confirms that AES-256 effectively protects the financial data of consignment MSMEs, supporting sustainable digital transformation.

Keywords: AES-256, Consignment, MSMEs, Encryption, Data Security.

Abstrak

Perlunya digitalisasi dengan keamanan informasi yang kuat pada UMKM warung jajanan tradisional untuk menghadapi tantangan signifikan dalam pengelolaan data konsinyasi bagi hasil. Penelitian ini mengembangkan sistem manajemen berbasis web menggunakan enkripsi dengan algoritma AES-256 untuk mengenkripsi data sensitif seperti harga modal, harga jual, dan total pendapatan, guna menjaga kerahasiaan data. Metodologi mencakup observasi lapangan di Warung Budeh Faisal, analisis kebutuhan sistem, perancangan database, serta di implementasikan dengan nodejs, sebelum data berhasil di simpan. Hasil implementasi menunjukkan sistem berhasil menggantikan pencatatan manual dengan antarmuka login, input barang, pencatatan, pemantauan, pencatatan penjualan serta statistik pendapatan, dimana data plaintext seperti harga jual Rp.1500 berubah menjadi chipertext acak seperti "2u7OJZgFYG1ZTw7KQoBXvWaBYx9U7" dalam database. Pengujian membuktikan keamanan tinggi pada akses ilegal, meningkatkan efisiensi operasional dan kepercayaan pihak terkait. Kesimpulan penelitian ini menegaskan bahwa AES-256 efektif melindungi data finansial UMKM konsinyasi, mendukung transformasi digital berkelanjutan.

Kata kunci: AES-256, Konsinyasi, UMKM, Enkripsi, Keamanan Data.

Pendahuluan

Dalam pemaparan mengenai Sektor Usaha Mikro, Kecil, dan Menengah (UMKM), khususnya dalam konteks sistem konsinyasi di UMKM Jajanan Tradisional, penting untuk menyoroti tantangan signifikan yang dihadapi oleh UMKM dalam aspek pengelolaan data dan keamanan informasi. Prosedur pencatatan

transaksi yang masih dilakukan secara manual berpotensi memunculkan risiko keamanan, seperti kehilangan catatan atau kesalahan perhitungan [1]. Sebagaimana diungkapkan oleh Hutauruk, digitalisasi akuntansi menjadi krusial dalam adaptasi UMKM terhadap situasi yang berubah, terutama di era kerja *online* pasca-pandemi Covid-19 [2]. Selain itu, Firdaus et al. menegaskan bahwa pemasaran yang konvensional di UMKM dapat dibarengi dengan digitalisasi untuk meningkatkan daya saing, demi mengatasi tantangan yang ada [3]. Digitalisasi merupakan alternatif yang dapat meningkatkan efisiensi operasional dan mengurangi risiko-risiko tersebut [4]. Banyak penelitian yang mendiskusikan transformasi digital pada UMKM, tetapi masih ada celah yang berkaitan dengan aspek keamanan data finansial yang spesifik [5].

Salah satu penelitian penting yang relevan dengan fokus ini adalah oleh M.D.C. Permana dkk. yang mengembangkan aplikasi *Financial Reporting* untuk UMKM. Meskipun memberikan kontribusi pada kecepatan transaksi, aplikasi tersebut tidak memadukan aspek kriptografi untuk melindungi data sensitif [5]. Dalam konteks ini, perlindungan terhadap data seperti harga modal dan profitabilitas harus diperkuat dengan menggunakan algoritma kriptografi yang ada. Penerapan algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit dapat menjadi solusi yang efektif, mengingat AES merupakan standar internasional yang telah terbukti aman dan tangguh terhadap serangan *brute-force* [6]. Penelitian oleh Rayapati et al. [6] menegaskan keunggulan AES dalam keamanan cloud, sementara Setiani et al. [7] dan Nugrahantoro et al. [8] mendemonstrasikan implementasi efektif AES dalam berbagai konteks. Lebih lanjut, studi oleh Kusyanti et al. [9] dan Utama et al. [10] memperkuat argumen bahwa kombinasi algoritma kriptografi dapat meningkatkan integritas dan kerahasiaan data secara signifikan.

Penelitian terbaru oleh Setiani et al. [7] bahkan menegaskan bahwa AES, bersama dengan SHA-256, adalah algoritma yang kuat dan mapan untuk enkripsi data dengan kecepatan yang hampir sama, sehingga sangat aplikatif untuk diimplementasikan. Implementasi AES-256 dalam berbagai studi menunjukkan ketahanannya terhadap ancaman keamanan siber modern [8], [10]. Abdul-Jabbar et al. [11] juga mengonfirmasi efisiensi metode enkripsi berbasis AES dalam pengamanan data.

Alih-alih hanya memfokuskan pada peningkatan kecepatan dan efisiensi transaksi, pendekatan penelitian ini akan mencakup penanganan yang lebih dalam terhadap keamanan informasi, dengan menerapkan mekanisme enkripsi yang kuat. Kebaruan dari penelitian ini terletak pada penggunaan AES-256 untuk melindungi data finansial sensitif dalam ekosistem konsinyasi [11] antara *consignor* (seterusnya akan disebut penitip) dan *consignee* (seterusnya akan disebut penjual) [12], [13]. Implementasi ini tidak hanya akan menggantikan cara pencatatan manual, tetapi juga memastikan kerahasiaan data antara pemilik usaha dan penitip barang, yang merupakan bagian penting dari model bisnis konsinyasi [1]. Model bisnis ini menuntut transparansi dan akurasi data yang hanya dapat dijamin dengan sistem terkomputerisasi [14]. Dengan mengadopsi sistem manajemen berbasis web yang memanfaatkan kriptografi, diharapkan pencatatan UMKM Toko Jajan Pasar dapat meningkat, bukan saja efisiensi operasional, tetapi juga tingkat keamanan data yang diperlukan untuk menjaga kepercayaan antara semua pihak dalam ekosistem konsinyasi [4], [14]. Upaya ini sejalan dengan tren dalam digitalisasi UMKM yang semakin matang di Indonesia, di mana fokus terhadap perlindungan data menjadi semakin kritis [5], [15].

Metode Penelitian

Penelitian ini menggunakan beberapa teknik pengumpulan data untuk memastikan sistem yang di bangun sesuai dengan kebutuhan operasional. Penulis melakukan observasi lapangan secara langsung di warung Bude Faisal untuk memahami alur penerimaan barang titipan, proses pencatatan manual pada buku, hingga prosedur rekapitulasi dan pembayaran kepada penitip. Selain observasi dilakukan juga studi literatur dengan mengkaji berbagai referensi ilmiah yang berkaitan dengan sistem konsinyasi serta penerapan teknik enkripsi Advance Encryption Standar (AES-256) guna meningkatkan data finansial.

Hasil dan Pembahasan

Implementasi sistem keamanan pada aplikasi konsinyasi ini dibangun menggunakan menggunakan menggunakan Node.js dengan framework React.js untuk sisi frontend dan express.js untuk backend dengan database menggunakan postgresQL. Sistem ini dirancang untuk memfasilitasi dua pengguna utama, yaitu penjual dan penitip, sistem menyediakan halaman login yang dilengkapi dengan verifikasi email dan katasandi yang telah di amankan dengan menggunakan hasing untuk password. Setelah berhasil masuk, pengguna akan diarahkan ke dasbor utama yang menyajikan informasi pendapatan serta menu navigasi untuk menuju halaman lain.

Proses pengelolaan barang seperti form input banrang konsnyasi dimana penitip memasukan nama dagangan, deskripsi produk, jumlah dan harga jual. Seperti Gambar 1.

Gambar 1 Input barang titipan.

Setelah pengguna menekan tombol simpan di tekan maka kolom yang bersifat rahasia hasil input penitip tersebut akan masuk dalam database dengan dengan data yang terenkripsi. Penerapan algoritma AES-256 ini di fokuskan pada kolom yang memuat data sensitif, seperti nominal uang, dan jumlah barang. Untuk mencegah terjadinya kebocoran informasi margin keuntungan toko apabila basis data diakses secara ilegal. Dalam proses nya algoritma AES-256 beroperasi dengan mode chiper block chaning(CBC) [9], yang mengubah angka nominal menjadi teks acak sebelum di simpan. Visualisasi hasil enkripsi data tersebut di lihat pada tabel 1 di bawah ini.

Tabel 1 visualisasi hasil enkripsi

No	Atribut Data	Kolom B	Kolom C
1	Harga jual	1500	2u7OJZgFYG1ZTw7KQoBXv WaBYx9U7/HWxLQ...
2	Harga Netto (pendapatan penjual)	500	+ZiEiJctd3DpDd0ptxZ4oXx1R 5RKsj+pHu...
3	Total Pendapatan (pendapatan penitip)	1000	ObCXUBHFqj+bMG+1ltX7H/ SsbEeeZpUDLDy...

Tabel 1. menunjukkan bahwa data nominal uang yang tersipan tidak dapat di baca makna nya jika diakses secara ilegal.

Kesimpulan

Berdasarkan hasil implementasi yang telah dilakukan dapat disimpulkan bahwa pengembangan sistem keamanan data bagi hasil sistem konsinyasi pada UMKM warung jajanan pasar tradisional berhasil memberikan solusi untuk pencatatan dan keamanan. Penerapan algoritma AES-256 pada sistem ini terbukti dalam menjaga kerahasiaan data pencatatan. Selain itu sistem ini tidak hanya memberikan kemudahan pencatatan dan keamanan saja tetapi juga memberikan solusi untuk *histori* pembukuan yang baik didukung dengan teknologi penyimpanan dari postgresSQL menjadikan solusi terbaik untuk aplikasi. Untuk pengembangan aplikasi selanjutnya disarankan agar aplikasi ini dikembangkan dengan notifikasi real-time dan pengembangan aplikasi *mobile* agar aksesibilitas bagi mitra penitip barang menjadi efektif.

Daftar Rujukan

- [1] Cahyadi and N. Pradnyani, "Digitalisasi umkm dengan menggunakan pendekatan toe model", *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, p. 1132, 2022. <https://doi.org/10.24843/ceb.2022.v11.i09.p10>
- [2] M. Hutauruk, "Pendampingan dan Pelatihan Digitalisasi Akuntansi Manufaktur Usaha Kecil dan Menengah di Wonosari, Gunung Kidul, Yogyakarta", *Warta LPM*, p. 346-355, 2022. <https://doi.org/10.23917/warta.v25i3.1030>
- [3] M. Firdaus, P. Azizah, & R. Sa'adah, "PENTINGNYA DIGITAL MARKETING SEBAGAI STRATEGI PEMASARAN UMKM DI ERA 4.0", *Jurnal Graha Pengabdian*, vol. 4, no. 2, p. 154, 2022. <https://doi.org/10.17977/um078v4i22022p154-162>
- [4] D. Widyaningsih, E. Zusrony, & H. Utomo, "Peran digital entrepreneurship mindset: keputusan adopsi platform digital bagi pelaku bisnis", *Jurnal Sistem Informasi Bisnis*, vol. 13, no. 2, p. 162-171, 2023. <https://doi.org/10.21456/vol13iss2pp162-171>
- [5] M. Permana, M. Iqbāl, S. Dewi, & A. Firmansyah, "Labaku: aplikasi pelaporan keuangan umkm terintegrasi", *Akuntansiku*, vol. 2, no. 4, p. 165-192, 2023. <https://doi.org/10.54957/akuntansiku.v2i4.555>
- [6] S. Rayapati, S. Muttavarapu, N. Nagasuri, & S. Singhal, "Security in cloud technologies: a brief overview", *Advances in Science and Technology*, 2023. <https://doi.org/10.4028/p-4pq758>
- [7] R. Setiani, E. Imananda, W. Wicaksono, M. Baihaqi, & J. Kuswanto, "Perbandingan Algoritma AES128 dengan SHA256 dalam Kecepatan Enkripsi Pengiriman Data", *Joins (Journal of Information System)*, vol. 9, no. 1, p. 13-22, 2024. <https://doi.org/10.33633/joins.v9i1.8800>
- [8] A. Nugrahantoro, A. Fadlil, & 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. <https://doi.org/10.22441/fifo.2020.v12i1.002>
- [9] A. Kusyanti, I. Wiguna, & F. Bakhtiar, "Implementasi Algoritme Spongnet sebagai Algoritme Hashing untuk Integritas pada Modul Komunikasi Lora", *Jurnal Teknologi Informasi Dan Ilmu Komputer*, vol. 10, no. 6, p. 1311-1318, 2023. <https://doi.org/10.25126/jtiik.1067119>
- [10] F. Utama, R. Faurina, & A. Vatesria, "Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256 dalam Pengamanan dan Validasi Data Ujian Online", *Jurnal Teknologi Informasi Dan Ilmu Komputer*, vol. 10, no. 5, p. 945-954, 2023. <https://doi.org/10.25126/jtiik.20231056558>
- [11] S. Abdul-Jabbar, A. Abed, S. Mohammed, & F. Mohammed, "Fast 128-bit multi-pass stream ciphering method", *Iraqi Journal of Science*, p. 2589-2600, 2023. <https://doi.org/10.24996/ijs.2023.64.5.40>
- [12] R. Hastuti, "Pendampingan penyusunan laporan penjualan konsinyasi pada gallery seni selasar 10", *Jurnal Serina Abdimas*, vol. 3, no. 1, p. 136-140, 2025. <https://doi.org/10.24912/jsa.v3i1.33951>
- [13] R. Hastuti, "Pendampingan penyusunan laporan penjualan konsinyasi pada gallery seni selasar 10", *Jurnal Serina Abdimas*, vol. 3, no. 1, p. 136-140, 2025. doi: 10.24912/jsa.v3i1.33951

- [14] B. Irianto, "PENERAPAN STANDAR AKUNTANSI EMKM", *Jurnal Pengabdian Bisnis Dan Akuntansi*, 2022. <https://doi.org/10.32424/1.jpba.2022.1.1.6722>
- [15] R. Setiani, E. T. Imananda, W. E. Wicaksono, M. A. Baihaqi, and J. Kuswanto, "Perbandingan Algoritma AES128 dengan SHA256 dalam Kecepatan Enkripsi Pengiriman Data", *Journal of Information System*, vol. 9, no. 1, pp. 13–22, Jul. 2024. doi: 10.33633/joins.v9i1.8800