

ABSTRAK

SISTEM PEMBAYARAN DIGITAL TERENKRIPSI UNTUK PENCEGAHAN KEBOCORAN DATA TRANSAKSI PADA WEBSITE *E-COMMERCE*

(2025:xiii + 67 halaman + 30 gambar + 8 tabel + lampiran)

LUTHFIA AFIFAH

062140352376

JURUSAN TEKNIK ELEKTRO

**PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUNIKASI
POLITEKNIK NEGERI SRIWIJAYA**

Digitalisasi Usaha Mikro, Kecil, dan Menengah (UMKM) dalam *e-commerce* membawa tantangan krusial dalam melindungi data pelanggan. Meskipun penggunaan protokol komunikasi terenkripsi seperti HTTPS dan TLS sudah meluas untuk transmisi data yang aman, banyak UMKM masih gagal mengimplementasikan enkripsi pada tingkat penyimpanan data. Ini berarti, setelah data sampai di server, data tersebut seringkali disimpan dalam bentuk tidak terenkripsi di dalam *database*. Penelitian ini mengimplementasikan enkripsi AES-128 pada tingkat (field-level) dalam sistem *e-commerce* berbasis Laravel untuk melindungi data pelanggan UMKM. Enkripsi diterapkan pada data sensitif dan diuji melalui pengujian *black-box* dan analisis *benchmark*. Sebanyak 10.000 catatan data digunakan untuk membandingkan kinerja antara operasi plaintext (data tidak terenkripsi) dan terenkripsi. Hasil penelitian menunjukkan overhead enkripsi rata-rata 0,0409 detik, menandakan dampak minimal terhadap kinerja. Proses enkripsi-dekripsi secara konsisten menghasilkan output yang benar di semua percobaan. Solusi ini menawarkan model enkripsi yang terjangkau dan terukur untuk UMKM, meningkatkan keamanan data pelanggan tanpa bergantung pada alat atau infrastruktur eksternal.

Kata Kunci : Enkripsi, AES-128, *E-Commerce*, Keamanan Data.

ABSTRACT

ENCRYPTED DIGITAL PAYMENT IN LARAVEL-BASED E-COMMERCE FOR MSME DATA PROTECTION

(2025:xiii + 67 pages + 30 pictures + 8 tabel + appendixes)

LUTHFIA AFIFAH

062140352376

ELECTRICAL ENGINEERING DEPARTMENT

PROGRAM OF STUDY IN APPLIED GRADUATION OF THE

TELECOMMUNICATION ENGINEERING

STATE POLYTECHNIC OF SRIWIJAYA

The increasing digitization of micro, small, and medium enterprises (MSMEs) in e-commerce brings critical challenges in protecting customer data. Despite the widespread use of encrypted communication protocols such as HTTPS and TLS for secure data transmission, many MSMEs still fail to implement encryption at the data storage level. This means that once the data reaches the server, it is often stored in unencrypted form within the database. This study implemented AES-128 encryption at the field-level in a Laravel-based e-commerce system to protect MSME customer data. The encryption was applied to sensitive data fields and tested through black-box testing and benchmark analysis. A dataset of 10,000 records was used to compare performance between plaintext and encrypted operations. Results showed an average encryption overhead of 0.0409 seconds, indicating minimal impact on performance. The encryption-decryption process consistently returned correct outputs across all trials. This solution offers an affordable and scalable encryption model for MSMEs, enhancing customer data security without relying on external tools or infrastructure.

Keywords : Encryption, AES-128, E-Commerce, Data Security