

IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK PENGAMANAN DATA *PURCHASE ORDER* PADA PT ANTILOPE MADJU PURI INDAH

Hadi Sutarjo¹, Sejati Waluyo^{2*}

^{1,2} Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: ¹2011510258@student.budiluhur.ac.id, ^{2*}sejati.waluyo@budiluhur.ac.id

(* : corresponding author)

Abstrak- PT. Antilope Madju Puri Indah menghadapi tantangan terkait keamanan data *purchase order* yang rentan terhadap pencurian dan penyalahgunaan oleh pihak yang tidak sah. Untuk mengatasi hal ini, perusahaan mengimplementasikan algoritma AES-128 pada aplikasi web mereka guna mengamankan data *purchase order*. Metode ini dipilih karena kemampuannya dalam mengolah enkripsi dan mendekripsi data dengan cepat dan aman. Proses enkripsi dilakukan dengan mengubah data *purchase order* menjadi *ciphertext* yang hanya dapat dibaca kembali setelah melalui proses dekripsi oleh pengguna yang berwenang. Hasil pengujian menunjukkan bahwa algoritma AES-128 efektif dalam melindungi data sensitif, dengan aplikasi yang mudah digunakan oleh admin perusahaan. Penelitian ini menyimpulkan bahwa penggunaan algoritma AES-128 berhasil meningkatkan keamanan informasi dalam *database* PT. Antilope Madju Puri Indah, memberikan perlindungan yang signifikan terhadap ancaman keamanan. Aplikasi ini tidak hanya meningkatkan keamanan tetapi juga mudah dioperasikan, memudahkan admin dalam mengelola data *purchase order*. Hasil pengujian mengindikasikan bahwa sistem pengamanan ini dapat diterapkan secara efektif mengurangi risiko keamanan dalam lingkungan perusahaan, serta membuka peluang pengembangan lebih lanjut dalam bidang keamanan data menggunakan teknik kriptografi.

Kata Kunci: Kriptografi, Algoritma (AES-128), Aplikasi Berbasis Web

IMPLEMENTATION OF AES-128 CRYPTOGRAPHY FOR SECURING *PURCHASE ORDER* DATA AT PT ANTILOPE MADJU PURI INDAH

Abstract- PT. Antilope Madju Puri Indah faces challenges related to the security of *purchase order* data which is vulnerable to theft and misuse by unauthorized parties. To overcome this, the company implemented the AES-128 algorithm in their web application to secure *purchase order* data. This method was chosen because of its ability to process encryption and decrypt data quickly and safely. The encryption process is carried out by changing the *purchase order* data into *ciphertext* which can only be read again after going through the decryption process by an authorized user. Test results show that the AES-128 algorithm is effective in protecting sensitive data, with an application that is easy to use by company admins. This research concludes that the use of the AES-128 algorithm has succeeded in increasing information security in the PT *database*. Antilope Madju Puri Indah, provides significant protection against security threats. This application not only increases security but is also easy to operate, making it easier for admins to manage *purchase order* data. The test results indicate that this security system can be implemented to effectively reduce security risks in the company environment, as well as open opportunities for further development in the field of data security using cryptographic techniques.

Keywords: Cryptography, Algorithms (AES-128), Web Based Application

1. PENDAHULUAN

Perkembangan digital menghasilkan sistem canggih yang memudahkan pekerjaan tanpa batasan jarak dan waktu, berdampak pada berbagai lembaga pemerintah dan swasta. Kemajuan ini meningkatkan kebutuhan akan aplikasi keamanan data yang mampu mencegah ancaman atau kebocoran informasi. Bidang keamanan data, termasuk kriptografi, menjadi semakin penting untuk melindungi informasi sensitif yang dipertukarkan [1].

PT Antilope Madju Puri Indah menyimpan banyak data penting yang rentan terhadap kerusakan, perubahan, atau pencurian. Oleh karena itu, perlindungan *database* sangat diperlukan untuk menghindari kerugian. Salah satu metode perlindungan data adalah kriptografi, yaitu mengubah data menjadi kode yang hanya bisa dibaca oleh pihak berwenang. Proses ini disebut enkripsi (mengubah *plaintext* menjadi *ciphertext*) dan dekripsi (mengembalikan *ciphertext* ke *plaintext*) [2]

Untuk melindungi komunikasi data digital antara pengirim dan penerima, berbagai aplikasi kriptografi telah digunakan, seperti enkripsi dan dekripsi data. Aplikasi ini termasuk membuat tanda tangan digital (tanda tangan digital), melakukan otentikasi terhadap pengirim data (otentikasi), dan memeriksa integritas data (pemeriksaan integritas data) [3].

Dalam penelitian sebelumnya kriptografi asimetris digunakan karena lebih aman dan cocok untuk komunikasi jarak jauh serta tanda tangan digital, sedangkan kriptografi simetris seperti AES dan DES menggunakan kunci yang sama untuk enkripsi dan dekripsi. Pemilihan jenis kriptografi harus disesuaikan dengan kebutuhan sistem informasi, dengan kunci privat dalam algoritma asimetris dijaga kerahasiaannya, sementara kunci publik dapat dibagikan secara terbuka [4].

Algoritma kriptografi yang akan digunakan oleh PT Antilope Madju Puri Indah adalah AES128, sebuah *cipher block* simetris. AES128 mengenkripsi data menjadi *ciphertext* dan mendekripsinya kembali menjadi *plaintext* menggunakan kunci kriptografi sepanjang 128, 192, atau 256 bit untuk blok data 128 bit [5].

Tujuan penelitian ini adalah untuk mengenkripsi dan deskripsi data penting menggunakan algoritma AES 128 dan menciptakan aplikasi pengamanan yang mudah digunakan, yang hanya dapat diakses oleh administrator yang bertanggung jawab.

2. METODE PENELITIAN

2.1 Algoritma Advanced Encryption Standard (AES128)

Algoritma (AES-128) menggantikan (DES) karena masalah keamanan terkait kecepatan komputer yang meningkat. Pada 2 Maret 2001, algoritma Rijndael dipilih sebagai standar AES berdasarkan tiga kriteria utama: keamanan, biaya, dan karakteristik serta implementasi algoritma. AES harus setidaknya seaman triple DES, bebas royalti, murah untuk diimplementasikan pada perangkat dengan memori terbatas, serta efisien dan cepat pada berbagai mesin dan perangkat lunak [6].

AES menggunakan struktur Substitution Permutation Network (SPN) yang lebih cepat dibandingkan struktur Feistel DES, karena tingkat paralelismenya lebih tinggi. AES memproses data dalam blok 128 bit (*plaintext*) dan mengenkripsi menjadi *ciphertext*, dengan kunci sepanjang 128 bit, 192 bit, atau 256 bit, yang mempengaruhi jumlah putaran dalam algoritma seperti pada tabel 1.

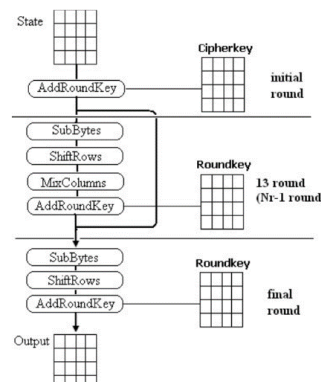
Tabel 1. Tabel Perbandingan Jumlah Putaran Dan Kunci

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Dalam enkripsi dan dekripsi, data dan kunci diolah menggunakan struktur array yang disebut "state". Proses ini terdiri dari empat tahap utama: *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*, dengan *MixColumns* tidak diterapkan pada tahap terakhir. Dekripsi adalah kebalikan dari enkripsi, menggunakan *subkey* yang relevan. Jumlah total *subkey* yang dibutuhkan adalah $Nb(Nr+1)$, di mana Nb adalah ukuran blok data dalam *word* dan Nr adalah jumlah tahapan dalam *word* [7].

2.2 Penerapan Metode Enkripsi Dan Deskripsi (AES)

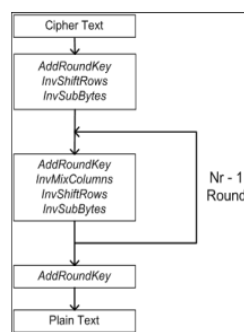
AES dikenal sebagai AES-128, AES-192, dan AES-256 karena memiliki panjang kunci 128, 192, dan 256. Meskipun panjang kunci paling sedikit AES adalah 128 bits, AES masih tahan terhadap serangan pencarian kunci menyeluruh dengan teknologi saat ini. Dengan panjang kunci 128 bits, $2^{128} = 3,4 \times 10^{38}$ kemungkinan kunci. Rijndael dan AES menggunakan permutasi dan substitusi serta sejumlah *cipher* atau putaran berulang berikut gambar 1 menunjukkan proses enkripsi AES-128. Tidak ada kunci internal yang sama untuk setiap putaran. Berikut adalah empat operasi utama algoritma AES:



Gambar 1. Proses Enkripsi (AES)

- Addroundkey* adalah proses di mana kunci putaran dihasilkan dari kunci *cipher* dan di-XOR-kan dengan setiap *byte* dari matriks *state*. Kunci baru dihasilkan untuk setiap putaran melalui operasi pada kunci *cipher* sebelumnya.
- SubBytes*, atau substitusi *byte*, adalah langkah pertama dalam setiap putaran algoritma, di mana setiap *byte* dalam matriks *state* direorganisasi menggunakan Rijndael S-box, yang menambah sifat non-linier pada *cipher* dan dirancang untuk menghindari serangan aljabar.
- Shiftrows* menggeser *byte* dalam matriks *state*: baris pertama tetap, baris kedua digeser satu posisi ke kiri, baris ketiga dua posisi, dan baris keempat tiga posisi. Pola ini berlaku untuk ukuran 128-bit dan 192-bit.
- MixColumns* menggabungkan empat *byte* dari setiap kolom matriks *state* menggunakan transformasi linear dengan matriks polinomial 4x4, yang digunakan juga dalam proses dekripsi [8].

Dalam gambar 2 proses dekripsi AES, terdapat empat transformasi yang diterapkan, di mana tiga di antaranya adalah kebalikan dari transformasi yang digunakan dalam proses enkripsi AES. Berikut ini adalah alur proses Dekripsi dari AES [9]:



Gambar 2. Proses Deskripsi (AES)

- Transformasi *Addroundkey* dalam dekripsi menggabungkan kunci ronde dengan *state* (16 *byte ciphertext*) menggunakan operasi XOR, yang merupakan kebalikan dari proses enkripsi.
- InverseShiftrows* menggeser *byte* pada baris 2, 3, dan 4 ke kanan, membalik transformasi *Shiftrows* yang diterapkan selama enkripsi.
- Inversesubbytes*, dilakukan setelah *Addroundkey* dan *InverseShiftrows*, menggantikan *byte* dalam *state* yang dihasilkan dari transformasi sebelumnya.
- Inversemixcolumns* mengalikan *state* hasil *Addroundkey* dengan matriks polinomial, menerapkan modulus jika hasilnya melebihi 0xFF. Transformasi ini berulang dari ronde pertama hingga kesepuluh, tetapi pada putaran terakhir, hanya *Addroundkey* yang digunakan untuk menghasilkan *plaintext* [10].

2.3 Metode Penelitian

Pada saat ini, studi riset kasus dilakukan untuk mendapatkan data *purchase order* PT. Antilope Madju Puri Indah dan untuk mengidentifikasi berbagai masalah yang ada. Hasil studi ini akan digunakan untuk membuat solusi untuk masalah yang ada:

- Pengumpulan Data, Fase ini melibatkan pengumpulan data yang telah disebutkan sebelumnya, yang dilakukan melalui wawancara dan observasi.
 - Wawancara (*Interview*): Orang-orang yang terlibat dalam pengembangan dan pengembangan aplikasi diwawancarai untuk mengetahui tentang sistem keamanan dan aplikasi.
 - Observasi (*Observation*): Pengamatan langsung proses dan pelaksanaan sistem adalah metode pengumpulan data untuk riset yang efektif mempelajari sistem.
- Identifikasi Permasalahan, yang harus diperbaiki untuk memenuhi batasan saat ini. Proses identifikasi masalah ini melibatkan beberapa tahap analisis yang diperlukan untuk menyelesaikan masalah penelitian:
 - Analisis Data: Tahap penting dalam penyelesaian masalah keamanan adalah analisis data. Pada saat ini, hal-hal berikut dilakukan adalah Pengumpulan data untuk merancang program dan pengelompokannya berdasarkan jenis dan fungsinya; dan Pendeskripsian data dengan antarmuka yang jelas dan mudah dipahami untuk menetapkan tahapan pembangunan aplikasi.
 - Analisis Penerapan Algoritma: Analisis ini dilakukan setelah data dikumpulkan dan proses sistem diamati. Pada titik ini, data pesanan aman dengan menggunakan metode kriptografi (AES128). Proses ini termasuk Proses menentukan *key* yang akan di gunakan untuk proses enkripsi dimana pada kasus ini hanya admin dari PT Antilope saja yang menentukan untuk diberikan kepada user yang di izinkan; Menerapkan

Algoritma (AES128) sebagai enkripsi *database purchase order* PT Antilope Madju Puri Indah dan mengubahnya menjadi *chiphertext*; dan Dengan menggunakan *key* yang diberikan oleh admin maka user bisa merubah *database* pada aplikasi *purchase order* yang sudah dienkripsi dapat dikembalikan menjadi *plaintext*.

2.4 Perancangan Aplikasi

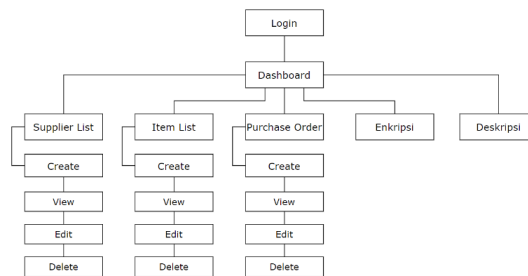
Saat ini, proses perancangan aplikasi berfokus pada hasil analisis sistem yang telah dilakukan. Ini mencakup pembuatan desain untuk modul enkripsi dan dekripsi, serta modul pendukung lainnya, yang akan diintegrasikan ke dalam aplikasi. Desain antarmuka pengguna akan dikembangkan sebagai bagian dari perancangan ini. Metode pengembangan perangkat lunak yang digunakan adalah model *Waterfall*, yang mengharuskan setiap tahap mulai dari analisis, desain, implementasi, hingga pengujian diselesaikan sepenuhnya sebelum melanjutkan ke tahap berikutnya. Setiap tahap dalam proses ini akan didokumentasikan dengan lengkap oleh penulis.

3. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sebuah web service yang menggunakan proses enkripsi dan dekripsi menggunakan algoritma AES-128 setelah melakukan perancangan dan analisis sistem yang akan dibangun. Penjelasan ini disertai dengan gambar, tabel dan elemen relevan lainnya untuk memperjelas hasil dan temuan dari penelitian ini.

3.1 Desain Struktur Tampilan (Menu)

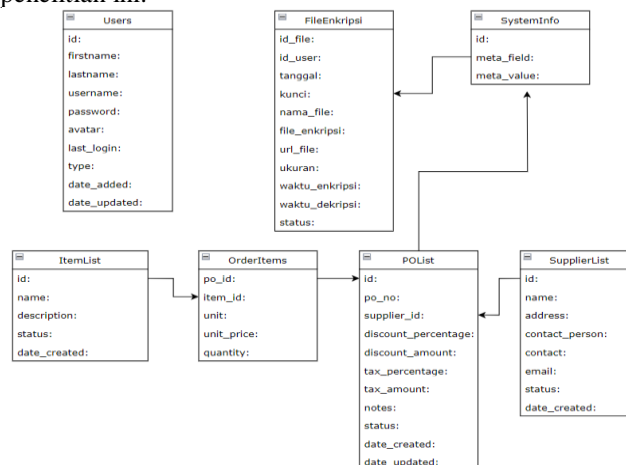
Tahapan ini menggambarkan antarmuka atau menu yang terlihat pada gambar 3 yang digunakan untuk menerapkan aplikasi *purchase order* (AES-128) dalam perlindungan basis data untuk *purchase order* di PT. Antilope Madju Puri Indah.



Gambar 3. Rancangan Menu

3.2 Struktur Rekaman Logis (LRS)

LRS menggambarkan bagaimana data diatur secara logis di dalam basis data, yang membuat pengaksesan, pemeliharaan, dan pengolahan data lebih mudah. Dengan menggunakan LRS, pengembang dapat memahami bagaimana setiap bagian data berhubungan satu sama lain dan bagaimana aplikasinya dapat digunakan. Gambar 4 menunjukkan LRS dalam penelitian ini:



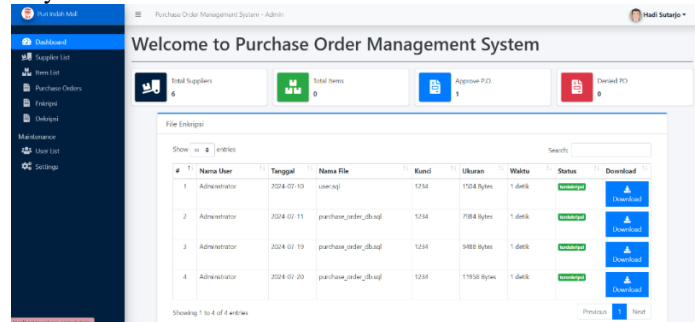
Gambar 4. Struktur Rekaman Logis (LRS)

3.3 Tampilan Aplikasi *Purchase Order*

Bagian ini menjelaskan hasil dari penelitian ini, berikut tampilan antarmuka aplikasi yang menerapkan algoritma AES-128, dari awal hingga akhir, sesuai dengan desain aplikasi *purchase order* PT Antilope Madju Puri Indah. Penjelasan mencakup deskripsi dan gambar berbagai tampilan antarmuka yang telah dikembangkan.

3.3.1 Tampilan *Screenshot Dashboard*

Berikut adalah tampilan *dashboard* yang muncul setelah pengguna berhasil masuk ke aplikasi. Tampilan ini, yang dapat dilihat untuk lebih jelasnya pada gambar 5 memungkinkan pengguna untuk melihat hasil enkripsi dan deskripsi lalu mengundahnya.



Gambar 5. Tampilan *Screenshot Dashboard*

3.3.2 Tampilan *Screenshot Supplier List*

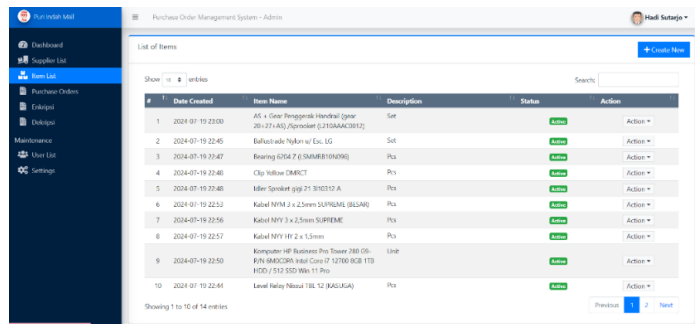
Gambar 6 berikut menunjukkan daftar *Supplier List* beserta kontak dan alamatnya. Daftar ini dapat diperbarui dengan menambahkan entri baru menggunakan tombol "Create New". Selain itu, tombol "Action" memungkinkan admin untuk mengubah atau menghapus data *Supplier* yang ada.



Gambar 6. Tampilan *Screenshot Supplier List*

3.3.3 Tampilan *Screenshot Item List*

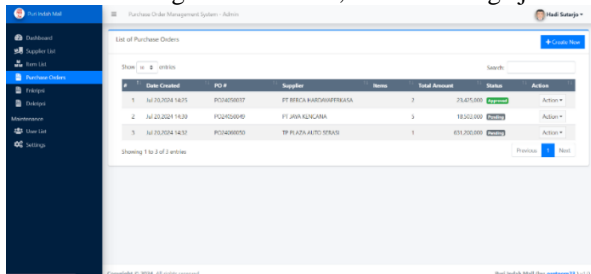
Gambar 7 menampilkan daftar antrian barang yang akan dipesan, mencakup tanggal pembuatan dan jumlah barang. Pengguna juga dapat mengubah atau menghapus data yang ada dalam formulir dengan menekan tombol "Action".



Gambar 7. Tampilan *Screenshot Item List*

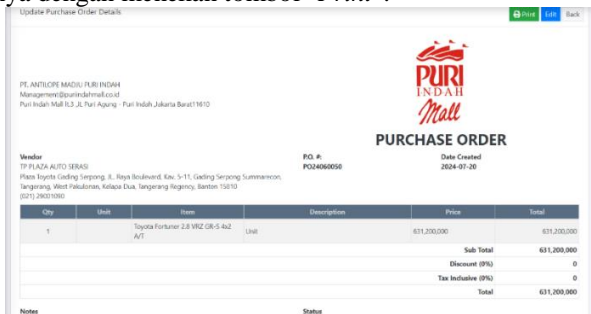
3.3.4 Tampilan Screenshot Purchase Order

Tampilan Layar pada gambar 8 menunjukkan formulir *Purchase Order*, di mana pengguna dapat memasukkan jumlah barang, harga, dan pemasok. Jika barang sudah dipesan, pengguna harus mengubah status menjadi "Approve" untuk menunjukkan bahwa barang telah diterima, atau "Pending" jika barang belum diterima.



Gambar 8. Tampilan Screenshot Purchase Order

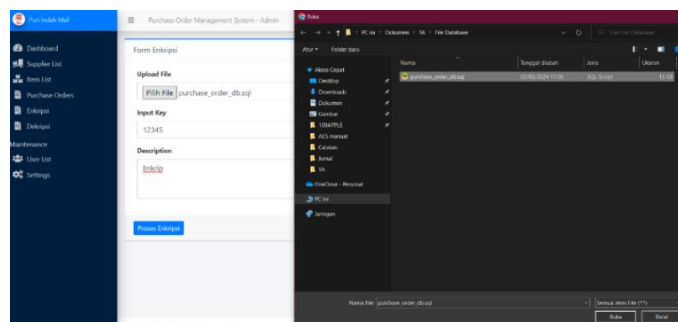
Pada gambar 9 tombol "Action" terdapat tombol "View" yang memungkinkan pengguna melihat detail barang yang dipesan dan mencetaknya dengan menekan tombol "Print".



Gambar 9. Tampilan Screenshot View Purchase Order

3.3.5 Tampilan Proses Enkripsi

Gambar 10 menunjukkan *screenshot* dari desain layar formulir Enkripsi, di mana pengguna harus mengunggah file master *database* dengan format *purchase_order_db.sql* yang diperoleh dari *database* phpMyAdmin untuk dienkripsi.



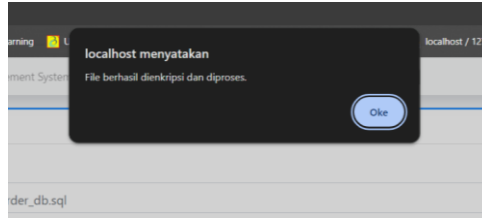
Gambar 10. Tampilan Screenshot Enkripsi

Pada saat sebelum data terenkripsi, data berisikan informasi data *purchase order* dan masih bisa terbaca seperti pada Gambar 11.



Gambar 11. Tampilan Screenshot Data Purchase Order

Jika data sudah di-*upload* dan sudah memasukan *key* dan juga *description* maka langkah selanjutnya klik tombol proses enkripsi dan akan muncul pop up “*file* berhasil di enkripsi dan diproses” enkripsi telah berhasil seperti pada gambar 12.



Gambar 12. Tampilan Screenshot Proses Berhasil

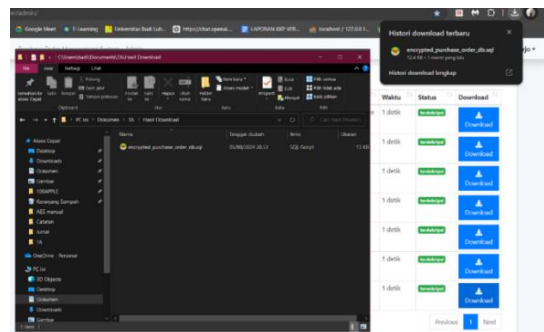
Setelah proses enkripsi telah selesai dan berhasil dan otomatis *file* tersebut akan bisa di *download* pada halaman *dashboard*, seperti yang di tunjukan pada gambar 13.



#	Nama User	Tanggal	Nama File	Kunci	Ukuran	Waktu	Status	Download
1	Administrator	2024-07-10	user.sql	1234	1504 Bytes	1 detik	berhasil	Download
2	Administrator	2024-07-11	purchase_order_db.sql	1234	12122 Bytes	1 detik	berhasil	Download
3	Administrator	2024-07-15	purchase_order_db.sql	1234	12122 Bytes	1 detik	berhasil	Download
4	Administrator	2024-07-20	purchase_order_db.sql	1234	12144 Bytes	1 detik	berhasil	Download
5	Administrator	2024-07-25	purchase_order_db.sql	1234	12144 Bytes	1 detik	berhasil	Download
6	Administrator	2024-07-25	decrypted_encrypted_purchase_order_db.sql	asdghijklmnopqrstu	12144 Bytes	1 detik	berhasil	Download
7	Administrator	2024-08-05	purchase_order_db.sql	12345	12000 Bytes	1 detik	berhasil	Download

Gambar 13. Tampilan Screenshot Dashboard Hasil Enkripsi

Jika pada saat di klik *Download* maka *file* hasil enkripsi akan tersimpan pada *file* lokal yang terlihat pada gambar 14.



Gambar 14. Tampilan Screenshot Download Hasil Enkripsi

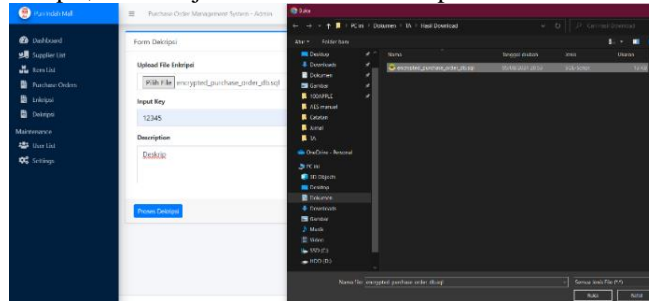
Setelah hasil enkripsi telah di *download* dan tersimpan maka jika di buka hasilnya seperti yang terlihat pada gambar 15.



Gambar 15. Tampilan Screenshot Hasil Enkripsi

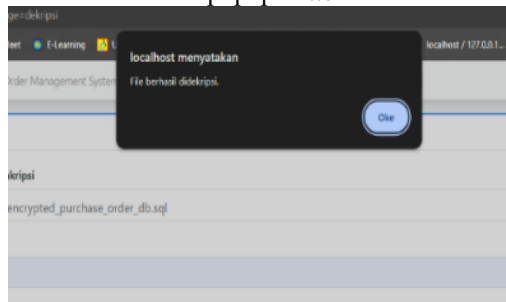
3.3.6 Tampilan Proses Deskripsi

Gambar 16. menampilkan *screenshot* dari desain layar formulir Deskripsi. Jika pengguna ingin mendekripsi atau mengembalikan *file* master data ke kondisi sebelum dienkripsi, pengguna harus mengunggah kembali *file* data yang sebelumnya telah dienkripsi, lalu menjalankan Proses Deskripsi.



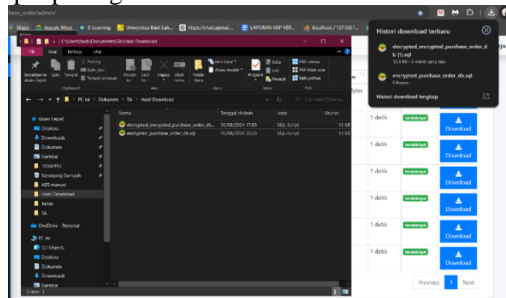
Gambar 16. Tampilan *Screenshot* Deskripsi

Jika admin sudah mengupload kembali *file* dengan memasukan *key* yang sebelumnya di gunakan untuk enkripsi maka proses deskripsi akan memunculkan popup ”File berhasil dienkripsi” seperti pada gambar 17.



Gambar 17. Tampilan *Screenshot* Berhasil Deskripsi

Langkah selanjutnya yang sebelumnya melakukan deskripsi berhasil maka pergi ke halaman *dashboard* dan *download* hasil dari proses deskripsi pada gambar 18.



Gambar 18. Tampilan *Screenshot* Download Deskripsi

Pada penyimpanan lokal hasil dari *download* deskripsi, jika di buka maka hasil dari deskripsi terlihat seperti pada gambar 19.



Gambar 19. Tampilan *Screenshot* Hasil Deskripsi

3.4 Pengujian Aplikasi *Purchase Order*

Pada tabel 2 pengujian telah dilakukan oleh administrator terhadap aplikasi yang dibuat yang menggunakan Algoritma (AES-128) untuk memastikan dan mengetahui bahwa aplikasi tersebut berjalan dengan baik. Untuk menjamin bahwa hasil yang dihasilkan sesuai dengan tujuan yang diharapkan, pengujian model dilakukan melalui pengujian Blackbox yang berfokus pada aplikasi *purchase order* spesifikasi dan fungsional.

Tabel 2. Pengujian Aplikasi *Purchase Order*

Data Entri	Diharapkan	Output	Hasil
Pengguna menekan tombol <i>Supplier List</i> .	Pengguna akan di arahkan ke halaman <i>Supplier List</i> .	Pengguna di arahkan ke halaman <i>Supplier List</i> .	Sesuai dan valid
Pengguna menambah form data <i>Supplier List</i> pada tombol <i>Create New</i> .	Jika data input benar dan berhasil melewati validasi oleh sistem, data tersebut akan diproses dan kemudian disimpan dalam <i>database</i> .	Pengguna mendapatkan notifikasi data sudah tersimpan.	Sesuai dan valid
Pengguna menekan tombol <i>Item List</i> .	Pengguna akan di arahkan ke halaman <i>Item List</i> .	Pengguna di arahkan ke halaman <i>Item List</i> .	Sesuai dan valid
Pengguna menambah form data <i>Item List</i> pada tombol <i>Create New</i> .	Jika data input benar dan berhasil melewati validasi oleh sistem, data tersebut akan diproses dan kemudian disimpan dalam <i>database</i> .	Pengguna mendapatkan notifikasi data sudah tersimpan.	Sesuai dan valid
Pengguna menekan tombol <i>Purchase Order</i> .	Pengguna akan di arahkan ke halaman <i>Purchase Order</i> .	Pengguna di arahkan ke halaman <i>Purchase Order</i> .	Sesuai dan valid
Pengguna menambah form data <i>Purchase Order</i> pada tombol <i>Create New</i> .	Jika data input benar dan berhasil melewati validasi oleh sistem, data tersebut akan diproses dan kemudian disimpan dalam <i>database</i> .	Pengguna mendapatkan notifikasi data sudah tersimpan.	Sesuai dan valid
<i>View Data</i>	Data yang tersimpan pada <i>database</i> akan muncul di sistem.	<i>Database</i> akan menampilkan informasi yang tersimpan dalam sistem.	Sesuai dan valid
<i>Create New</i>	<i>Database</i> dapat diakses oleh sistem.	<i>Database</i> dapat menyimpan informasi yang dibuat oleh pengguna oleh sistem.	Sesuai dan valid
<i>Delete</i>	Data dari basis data dapat dihapus oleh sistem sesuai dengan informasi yang ingin dihapus.	Pengguna dapat memilih untuk menghapus data dari basis data oleh sistem.	Sesuai dan valid
Fungsi <i>Action</i>	Proses sistem fungsi <i>Action</i> akan menampilkan opsi menu <i>View, Edit, Delete</i>	Pengguna dapat memilih tombol <i>View, Edit, Delete</i>	Sesuai dan valid
Fungsi <i>Upload</i>	Proses sistem fungsi <i>Upload</i> sistem diminta untuk chose <i>file database</i> format <i>sql.db</i>	Pengguna dapat mengupload <i>file</i> dan enkripsi/deskripsi berjalan.	Sesuai dan valid
Fungsi <i>Download</i>	Proses sistem <i>Download</i> sistem diminta untuk menyimpan hasil proses enkripsi/deskripsi <i>database</i>	Pengguna dapat menyimpan kedalam lokal <i>file</i> dan melihat hasil enkripsi/deskripsi	Sesuai dan valid

3.5 Analisis Pengujian Enkripsi Dan Deskripsi

Setelah menerapkan Algoritma AES-128 aplikasi dapat dilakukan pengujian untuk mengukur keberhasilan dan kecepatan enkripsi serta dekripsi pada 7 file, dengan ukuran di bawah 1MB, semuanya berupa file SQL. Hasil pengujian menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan baik, dengan waktu enkripsi rata-rata 1 detik, menunjukkan kinerja yang sangat cepat. Data hasil pengujian ditampilkan pada gambar 20.

#	Nama User	Tanggal	Nama File	Kunci	Ukuran	Waktu	Status
1	Adminstrator	2024-07-10	user.sql	1234	1504 Bytes	1 detik	terdekripsi
2	Adminstrator	2024-07-11	purchase_order_db.sql	1234	12122 Bytes	1 detik	terdekripsi
3	Adminstrator	2024-07-19	purchase_order_db.sql	1234	12122 Bytes	1 detik	terdekripsi
4	Adminstrator	2024-07-20	purchase_order_db.sql	1234	12144 Bytes	1 detik	terdekripsi
5	Adminstrator	2024-07-29	purchase_order_db.sql	1234	12144 Bytes	1 detik	terdekripsi
6	Adminstrator	2024-07-29	decrypted_encrypted_purchase_order_db.sql	asdfghdskajhtgankhgt	12144 Bytes	1 detik	terdekripsi
7	Adminstrator	2024-08-05	purchase_order_db.sql	12345	12704 Bytes	1 detik	terdekripsi

Gambar 20. Analisis Enkripsi Dan Deskripsi

4. KESIMPULAN

Berdasarkan hasil dan analisis yang telah dilakukan, dapat disimpulkan bahwa implementasi algoritma kriptografi *Advanced Encryption Standard* 128 (AES-128) berhasil memenuhi kebutuhan pengamanan data *purchase order* di PT. Antilope Madju Puri Indah. Pengujian dilakukan 7 kali dengan *file* berukuran di bawah 1MB, menunjukkan bahwa rata-rata waktu untuk enkripsi dan dekripsi adalah 1 detik dengan tingkat keberhasilan 100%. Disarankan bagi penulis selanjutnya untuk mempertimbangkan algoritma kriptografi lain untuk meningkatkan keamanan dan efisiensi. Penelitian lebih lanjut diperlukan untuk mengoptimalkan performa enkripsi, dekripsi, dan antarmuka pengguna. Fitur tambahan seperti notifikasi keamanan dan log aktivitas juga dianjurkan untuk mendeteksi ancaman lebih dini.

DAFTAR PUSTAKA

- [1] Hulu, Delisman, Nadeak, Berto, Aripin, Soeb. "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan *File* Hasil Radiologi di RSUD Imelda Medan." *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 4, no. 1, pp. 1-10, 2020. DOI: 10.30865/komik.v4i1.2590.
- [2] Mahfud, I., & Utomo, P. H. "Implementasi Sistem Kriptografi RSA Signature dengan SHA-256 pada Mekanisme Autentikasi REST API". *Seminar Nasional Teknoka*, Vol 6, 27 November 2021.
- [3] Fauzi, Rizky Restu, and Wellem, Theophilus. "Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice." *AITI: Jurnal Teknologi Informasi*, vol. 18, no. 1, 2021, pp. 158-172, 2021.
- [4] Arif, Z., & Nurokhman, A. "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi". *Jurnal Teknologi dan Sistem Informasi*, vol. 4, no. 2, pp. 394-405, 2023.
- [5] Adi Kannatasik, and Moh. Ali Romli. "Aplikasi Pengamanan Data Karyawan Menggunakan Algoritma Advanced Encryption Standard dan Cloud Computing Berbasis Mobile." *Edumatic: Jurnal Pendidikan Informatika*, vol. 7, no. 2, Dec. 2023, pp. 485-494. Doi: 10.29408/edumatic.v7i2.23948.
- [6] S. Saripa. "Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi." *PISCES*, vol. 01, no. 02, pp. 138-148, 2023.
- [7] U. Wahyuningsih, et al, "Analisis Proses Enkripsi Algoritma Kriptografi Modern Advanced Encryption Standard (AES)", *Jurnal Matematika dan Informatika*, vol. 1, no. 2, pp. 380-387, 2023.
- [8] Y. Wiharto, and M. Mufti. "Implementasi Advanced Encryption Standard 128 Sebagai Pengamanan Basis Data Obat-obatan Apotek". *JUTISI: Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 2, pp. 335-350, 2022.
- [9] Andriyanto, Muhammad Riyan, and Pristi 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, Nov. 2022, pp. 179-187. Doi: 10.47065/josyc.v4i1.2451.
- [10] A. Kannatasik, and Moh. A. Romli. "Aplikasi Pengamanan Data Karyawan Menggunakan Algoritma Advanced Encryption Standard dan Cloud Computing Berbasis Mobile." *Edumatic: Jurnal Pendidikan Informatika*, vol. 7, no. 2, 2023, pp. 485-494. Doi: 10.29408/edumatic.v7i2.23948.