

Penerapan Algoritma Caesar Chiper Untuk Keamanan Data Pelanggan Pada Mardhatillah Muslim Store

Implementation Of Caesar Cipher Algorithm For Customer Data Security
At Mardhatillah Muslim Store

Habib Burrahman^{a,1}, Rika Rosnelly^{b,2}

^{a,b}Universitas Potensi Utama, Medan 20241, Sumatera Utara, Indonesia
e-mail : bonjohabib@gmail.com¹, e-mail : rikarosnelly@gmail.com²

ABSTRAK

Keamanan data pelanggan merupakan hal yang sangat penting dalam pengelolaan informasi, terutama bagi toko yang telah berbasis digital. Mardhatillah Muslim Store sebagai toko yang bergerak di bidang penjualan produk-produk muslim, membutuhkan sistem yang mampu menjaga kerahasiaan data pelanggan agar tidak mudah disalahgunakan. Penelitian ini bertujuan untuk merancang dan membangun sebuah aplikasi desktop yang berfungsi mengenkripsi data pelanggan, khususnya pada bagian kontak dan total belanja, dengan menggunakan metode Caesar Cipher. Data pelanggan diinput melalui file Excel, kemudian diproses oleh sistem berdasarkan pilihan kunci enkripsi, yaitu 3, 6, atau 9. Aplikasi ini juga dilengkapi fitur login yang membedakan hak akses antara owner dan staff. Berdasarkan hasil pengujian, aplikasi dapat berjalan dengan baik dan mampu mengenkripsi data sesuai dengan ketentuan yang diterapkan. Antarmuka aplikasi dirancang sederhana agar mudah digunakan. Dengan adanya sistem ini, diharapkan pengelolaan data pelanggan di Mardhatillah Muslim Store menjadi lebih aman dan efisien.

Kata Kunci: Keamanan data, enkripsi, Caesar Cipher, Excel, aplikasi web

ABSTRACT

Customer data security is a crucial aspect of information management, especially for stores that operate digitally. Mardhatillah Muslim Store, which specializes in selling Muslim products, requires a system capable of protecting customer data confidentiality to prevent misuse. This study aims to design and develop a desktop application that functions to encrypt customer data, specifically in the contact and total purchase sections, using the Caesar Cipher method. Customer data is inputted via an Excel file and then processed by the system based on the selected encryption key, which can be 3, 6, or 9. The application also includes a login feature that differentiates access rights between the owner and staff. Based on the test results, the application runs properly and is able to encrypt data according to the specified rules. The interface is designed to be simple and easy to use. With this system, it is expected that customer data management at Mardhatillah Muslim Store will become more secure and efficient.

Keywords: Data security, encryption, Caesar Cipher, Excel, web application

Disubmit:

Info Artikel :
Direview:

Diterima :

Copyright © 2025 – senadimu. All rights reserved.

1. PENDAHULUAN

Informasi menjadi tidak bernilai apabila disalahgunakan oleh kelompok yang tidak bertanggung jawab. Dengan meningkatnya tuntutan keamanan atas kerahasiaan informasi yang dipertukarkan, maka tuntutan akan ketersediaan data dan sistem keamanan informasi yang lebih baik untuk melindungi data dari ancaman pencurian data [1]. Kondisi tersebut jelas dapat merugikan pihak terkait, terutama apabila informasi yang dipublikasikan mencakup data bersifat pribadi. Secara umum, data pribadi merupakan data yang dapat memberikan informasi mengenai

ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, serta dapat mengidentifikasi seseorang, yang tentunya bersifat rahasia [2]. Oleh karena itu, dibutuhkan sesuatu untuk mengamankan data yang disimpan. Kriptografi merupakan salah satu metode yang digunakan untuk mengamankan informasi sehingga hanya pengguna yang disebutkan yang dapat membaca melalui penggunaan kode rahasia. Tujuan utama dari kriptografi adalah untuk menjaga keutuhan, kerahasiaan, dan autentikasi dari seluruh sumber daya informasi [3]. Bruce Schneier dalam bukunya yang berjudul *Applied Cryptography* mendefinisikan kriptografi sebagai ilmu pengetahuan dan seni dalam menjaga keamanan pesan-pesan. Meskipun masih sederhana, konsep kriptografi telah digunakan sejak lama oleh manusia di berbagai peradaban seperti Mesir dan Romawi [4]. Dalam kriptografi terdapat dua tahapan, yaitu enkripsi dan dekripsi. Proses enkripsi melibatkan perubahan teks asli menjadi sebuah susunan karakter atau simbol yang tidak dapat dipahami oleh manusia. Proses ini dapat menghasilkan sebuah pesan yang susunan karakternya jauh berbeda dari teks aslinya [5]. Penerapan enkripsi ini akan difokuskan bagaimana enkripsi dapat mengamankan data sampai pada level baris (row) dan kolom (field) dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data [6]. Algoritma caesar cipher merupakan metode enkripsi yang sangat sederhana dan sangat populer. Dimana di dalamnya terdapat sebuah kode dan kode ini terdiri dari semua huruf dari teks asli (plaintext), yang kemudian diganti dengan kode lainnya dan kemudian diubah dengan huruf lain dengan perbedaan posisi tertentu dalam alfabet. Enkripsi caesar ini dapat melindungi dan memulihkan data tanpa mengubah bentuk aslinya (plaintext) [7]. Database merupakan salah satu aset penting dalam sebuah Perusahaan, yang mana dapat berisi informasi yang ditampilkan halaman web kepada pengguna, atau tujuan database untuk menyimpan informasi yang disediakan oleh pengguna. Dalam beberapa aplikasi, database menyediakan informasi yang tersedia dan menyimpan informasi baru [8]. Keberadaan database memiliki peran dan fungsi yang penting dalam mendukung proses yang lebih efektif dan efisien [9]. Ada beberapa tipe data yang dimiliki oleh sebuah Perusahaan dan setiap data memiliki kegunaan masing-masing. Salah satunya adalah database pelanggan, database pelanggan ini berguna untuk mencatat dan menyimpan informasi yang diperlukan oleh Perusahaan, baik dari nama pelanggan, nomor telepon, maupun lokasi.

Kasus pencurian data pribadi seperti dokumen elektronik, dimana pada tahun 2014 jumlah pelanggaran 1225 di tingkat penyidikan adalah 790, jadi 2 persentasenya 64%, tahun 2015 jumlah pelanggaran di tingkat penyidikan adalah 1569 dengan sebesar 851 dari 54% kasus, dan pada tahun 2016, jumlah total kejahatan adalah 1207, sedangkan investigasi kriminal adalah 699, dan persentasenya 57%, sehingga kasus kejahatan di dunia digital Keamanan data sangat penting di masa perkembangan teknologi [10]. Dalam hal ini, Mardhatillah Muslim Store merupakan salah satu supplier yang bergerak di bidang penjualan berbagai produk muslim, seperti madu, pakaian, aksesoris, dan perlengkapan ibadah. Seiring dengan perkembangan bisnis dan meningkatnya jumlah pelanggan, kebutuhan akan pengelolaan data pelanggan yang aman, terstruktur, dan efisien menjadi semakin penting. Namun, hingga saat ini pencatatan dan penyimpanan data pelanggan masih dilakukan secara manual, menggunakan file berformat Excel yang dapat diakses oleh seluruh pihak internal tanpa pembatasan hak akses. Hal ini menimbulkan berbagai risiko, seperti kebocoran informasi, penyalahgunaan data oleh pihak yang tidak berwenang, hingga hilangnya data akibat kesalahan manusia (human error).

Kondisi ini terbukti menimbulkan permasalahan serius karena pernah terjadi insiden kebocoran data pelanggan, di mana informasi tersebut dimanfaatkan oleh pihak yang tidak bertanggungjawab untuk kepentingan pribadi. Akibat dari kejadian ini, Mardhatillah Muslim Store mengalami penurunan omzet sebesar 40 hingga 50 persen dari biasanya. Penurunan ini berdampak langsung pada ketidakstabilan keuangan perusahaan dan menurunkan kepercayaan pelanggan. Mengelola data pelanggan secara aman merupakan aspek penting dalam menjaga kepercayaan pelanggan sekaligus mendukung pertumbuhan bisnis. Oleh karena itu, dibutuhkan solusi yang mampu meningkatkan keamanan data pelanggan melalui penerapan sistem informasi berbasis web, yang dilengkapi dengan sistem enkripsi pada kolom data sensitif. Sistem ini akan membatasi akses sesuai peran masing-masing pengguna. Hanya pemilik usaha yang memiliki hak untuk mengakses data asli secara utuh, sementara staf hanya akan melihat data dalam bentuk terenkripsi. Berdasarkan uraian tersebut, penelitian ini bertujuan untuk merancang sebuah aplikasi enkripsi

untuk mengamankan data pelanggan ini. Aplikasi ini diharapkan mampu mengamankan database pelanggan agar tidak dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Berdasarkan penjelasan di atas, penulis berinisiatif mengambil judul "PENERAPAN ALGORITMA CAESAR CIPHER UNTUK KEAMANAN DATA PELANGGAN PADA MARDHATILLAH MUSLIM STORE". Dengan pendekatan ini, diharapkan tidak hanya keamanan data pelanggan dapat terjaga, tetapi juga stabilitas bisnis dapat dipulihkan dan ditingkatkan.

Ada beberapa penelitian terdahulu yang menjadi acuan peneliti sebagai bahan referensi, yaitu penelitian yang dilakukan oleh Vara Maulidiah Hidayah dkk pada tahun 2023 berjudul "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks" membahas pentingnya kriptografi sebagai ilmu yang mempelajari cara untuk menjaga keamanan informasi dan mencegah pihak yang tidak berwenang mengetahui isi data. Penelitian ini membandingkan dua algoritma kriptografi, yaitu Caesar Cipher dan Vigenere Cipher, dalam proses enkripsi dan dekripsi pesan teks. Pada metode Caesar Cipher, enkripsi dilakukan dengan menggunakan operasi shift, yaitu pergeseran posisi huruf dalam teks sesuai dengan nilai kunci tertentu. Hasil pengujian dalam aplikasi kriptografi ini menunjukkan bahwa keamanan penginputan teks sangat diperlukan untuk menjaga kerahasiaan pesan. Selain itu, penggunaan kunci acak dalam enkripsi dan dekripsi dengan algoritma Caesar Cipher dan Vigenere Cipher menghasilkan ciphertext dan plaintext yang berbeda meskipun teks yang sama digunakan, sehingga meningkatkan keamanan data dan menjadikannya lebih sulit untuk dibaca tanpa kunci yang sesuai [11].

Selanjutnya penelitian yang dilakukan oleh Roman Gusmana dkk pada tahun 2022 berjudul "Implementasi Algoritma Affine Cipher dan Caesar Cipher dalam Mengamankan Data Teks" membahas peningkatan keamanan data dalam menghadapi maraknya pencurian data di era digital saat ini. Penelitian ini menggabungkan dua algoritma kriptografi, yaitu Affine Cipher dan Caesar Cipher, untuk meningkatkan tingkat keamanan data yang dienkripsi. Proses enkripsi pertama dilakukan dengan menggunakan algoritma Affine Cipher, yang kemudian dienkripsi kembali menggunakan algoritma Caesar Cipher. Kombinasi kedua algoritma ini bertujuan untuk memperkuat perlindungan terhadap data. Meskipun masing-masing algoritma memiliki kelemahan, yaitu tingkat keamanan yang relatif rendah apabila diterapkan secara terpisah, kombinasi keduanya dapat memberikan perlindungan yang lebih baik. Kedua algoritma tersebut termasuk dalam jenis cipher substitusi, di mana setiap huruf pada plaintext digantikan dengan huruf lain yang sesuai dengan posisi tertentu dalam alfabet. Namun, metode ini masih rentan terhadap serangan brute force attack, di mana pihak yang tidak berwenang mencoba berbagai kemungkinan untuk menemukan kunci enkripsi [12].

Penelitian yang dilakukan oleh Meriska Hamni dkk pada tahun 2022 berjudul "Penerapan Keamanan Data Dengan Menggunakan Metode Caesar Cipher Untuk Mengamankan Database MySQL" membahas pentingnya perlindungan data dari pencurian dan penyalahgunaan yang dilakukan oleh pihak yang tidak berwenang. Metode penelitian yang digunakan adalah kualitatif, yang berfokus pada analisis makna dari fenomena yang terjadi di lapangan. Peneliti menggunakan teknik kriptografi dengan metode Caesar Cipher untuk menyandikan data yang tersimpan dalam database MySQL. Proses enkripsi dilakukan dengan menggantikan karakter dalam database menggunakan pergeseran tertentu dalam alfabet yang ditentukan oleh kunci enkripsi. Hasil penelitian ini menunjukkan bahwa penggunaan metode Caesar Cipher dalam menyandikan data di database MySQL dapat meningkatkan keamanan data secara signifikan. Data yang disimpan menjadi lebih terlindungi dari akses yang tidak sah, meskipun database tetap dapat diakses oleh pengguna yang memiliki kunci untuk mendekripsi data tersebut [13].

Penelitian yang dilakukan oleh Maulid Hidayat dkk pada tahun 2023 berjudul "Penerapan Kriptografi Caesar Cipher Dalam Pengamanan Data" membahas pentingnya keamanan informasi untuk melindungi data dari kelompok yang tidak terotorisasi. Dalam penelitian ini, digunakan algoritma Caesar Cipher, sebuah metode enkripsi yang sederhana namun populer, di mana setiap huruf pada teks asli (plaintext) digantikan dengan huruf lain yang memiliki perbedaan posisi tertentu dalam alfabet. Proses ini memungkinkan data untuk dienkripsi tanpa mengubah bentuk aslinya, sehingga informasi dapat disembunyikan dan dipulihkan kembali dengan mudah. Algoritma Caesar Cipher dapat memproses karakter dari A hingga Z dan akan menghapus karakter yang bukan huruf alfabet, karena hanya angka 26 yang digunakan dalam perhitungan. Hasil

penelitian ini menunjukkan bahwa metode Caesar Cipher berhasil dalam melindungi dan memulihkan pesan, memberikan cara sederhana namun efektif untuk 18 mengamankan data [14].

Penelitian yang dilakukan oleh Desi Fitriani Ningrum dkk berjudul “Implementasi Keamanan Data menggunakan Kriptografi Caesar Cipher” mengangkat topik penting mengenai keamanan data dan kerahasiaan informasi dalam pertukaran data. Dalam penelitian ini, penulis menggunakan metode kriptografi Caesar Cipher, sebuah teknik enkripsi klasik yang menggunakan kunci simetris, di mana kunci yang sama digunakan untuk proses enkripsi dan dekripsi data. Proses enkripsi dan dekripsi dilakukan dengan metode substitusi atau perpindahan, yaitu menggeser posisi karakter dalam pesan sesuai dengan nilai kunci yang ditentukan. Hasil dari penelitian ini menunjukkan bahwa penggunaan Caesar Cipher mampu menjaga keamanan dan kerahasiaan data, meskipun merupakan algoritma kriptografi klasik, karena orang yang tidak memiliki kunci tidak dapat mengakses informasi yang terenkripsi. Penelitian ini juga menunjukkan bahwa meskipun algoritma ini sederhana, ia masih relevan dan efektif dalam mengamankan data pada tingkat dasar [15].

Penelitian yang di lakukan oleh S. D. Nasution yang berjudul “Pengamanan Perintah Koneksi ke Database MySQL dengan Caesar Cipher dan Stout Codes” pada tahun 2024. Tujuan penelitian adalah menambah lapisan keamanan pada perintah koneksi (connection strings) ke MySQL dengan melakukan enkripsi; metode pengembangan dan pengujian prototipe enkripsi pada string koneksi, lalu mengukur keterbacaan dan kemampuan dekripsi saat runtime; hasilnya menyatakan bahwa mengenkripsi perintah koneksi membuat isi string sulit dibaca oleh pihak tak berwenang dan bisa meningkatkan keamanan sistem, walau perlu manajemen kunci yang baik [16].

Penelitian yang di lakukan oleh F. D. Ardiansyah yang berjudul “ Implementasi Kriptografi Caesar Chiper Pada Aplikasi Enkripsi dan Dekripsi ” pada tahun 2023. Tujuan penelitian ini adalah mengimplementasikan Caesar Cipher pada aplikasi enkripsi/dekripsi sederhana berbasis HTML; metode meliputi perancangan antarmuka, pengkodean algoritma, dan pengujian efisiensi serta efektivitas pada teks contoh; hasil menyatakan bahwa implementasi mudah dilakukan dan efektif untuk skenario dasar, namun peneliti menegaskan keterbatasan keamanan untuk penggunaan yang membutuhkan proteksi kuat [17].

Penelitian yang di lakukan oleh S. V. Wahdini — “Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi ” pada tahun 2021. Tujuan penelitian ini adalah mengamankan file Excel yang berisi data pelanggan dan penjualan saat dikirim ke kantor pusat; metode yang dipakai adalah merancang aplikasi enkripsi (kombinasi teknik kriptografi sederhana) untuk file Excel dan melakukan pengujian enkripsi/dekripsi pada dataset nyata; hasil uji menunjukkan file Excel berhasil dienkripsi/dekripsi dan alur pengiriman data menjadi lebih aman sehingga risiko kebocoran berkurang pada skenario yang diuji [18].

Penelitian yang di lakukan oleh Y. Dwi Putri, R. Rosihan, S. Lutfi yang berjudul “Penerapan Kriptografi Caesar Cipher pada Fitur Chatting Sistem Informasi Freelance” pada tahun 2019. Penelitian ini bertujuan menerapkan Caesar Cipher untuk mengamankan pesan pada fitur chatting sistem freelance; peneliti membangun dan menguji modul enkripsi/dekripsi pada aplikasi (implementasi praktis) menggunakan studi kasus sistem informasi freelance, lalu mengevaluasi fungsionalitasnya melalui uji coba fungsional; hasilnya menunjukkan Caesar Cipher dapat melindungi pesan pada tingkat dasar dan dapat diintegrasikan ke sistem chatting, meskipun penulis mencatat keterbatasan keamanan jika dihadapkan pada serangan kriptanalisis modern [19].

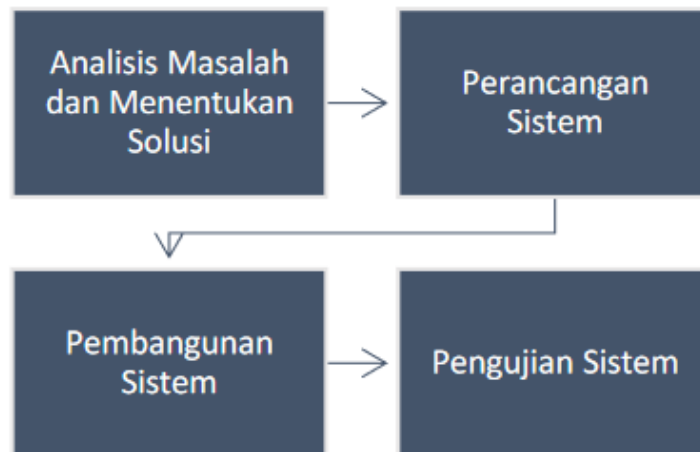
Penelitian yang di lakukan oleh I. Wibowo dan M. C. Wibowo yang berjudul “Implementation of Base64 and Caesar Cipher in securing video files” pada tahun 2020. Penelitian ini bertujuan mengamankan file video sederhana dengan kombinasi encoding (Base64) dan Caesar Cipher; metode implementasi teknik pada file multimedia dan pengujian pemulihan file setelah dekripsi; hasil menunjukkan kombinasi tersebut dapat mempersulit pembacaan langsung konten video oleh pihak tidak berwenang pada skenario terbatas, namun efektivitasnya masih jauh dari standar kriptografi modern untuk konten sensitive [20].

Penelitian yang di lakukan oleh Alfaruq Marsalsani Supriyatno & Eka Ardianto dengan judul “Peningkatan Keamanan Pesan Teks Menggunakan Super Enkripsi Algoritma Caesar Cipher Standard Dan Vigenere Autokey” pada tahun 2024. Tujuan penelitian ini adalah meningkatkan keamanan pesan teks dengan menerapkan konsep super enkripsi yang menggabungkan algoritma Caesar Cipher standar dan Vigenère Autokey Cipher. Metode penelitian meliputi implementasi kedua algoritma, pengujian performa dengan metrik entropi, Character Error Rate (CER), dan Bit

Error Rate (BER). Hasil penelitian menunjukkan bahwa nilai entropi meningkat secara signifikan dari 59,3 % menjadi 63,2 %, yang berarti kombinasi kedua algoritma tersebut memberikan peningkatan keamanan terhadap pesan teks [21].

2. METODE

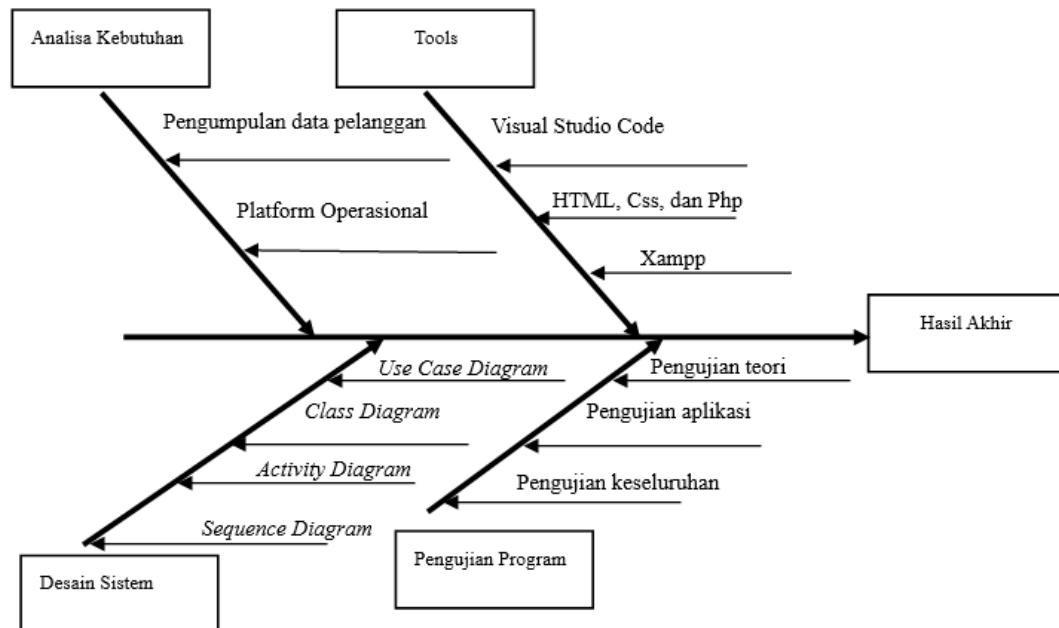
Penelitian ini dilakukan dengan beberapa tahapan. Adapun tahapan tersebut ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

2.1 Kerangka Penelitian

Kerangka kerja penelitian merupakan Rangkaian Kebutuhan yang harus dilakukan dalam mendukung proses penelitian. Adapun kerangka penelitian yang digunakan pada penelitian ini dapat dilihat pada gambar berikut.



Gambar 2. Penerapan Algoritma Caesar Chiper Untuk keamanan Data Pelanggan Pada Mardhatillah Muslim Store Menggunakan Kerangka Penelitian Fishbone Diagram

3. HASIL DAN PEMBAHASAN

3.1. Halaman Login

Gambar 3 merupakan implementasi dari perancangan halaman login. Pada halaman ini pengguna harus mengisi email dan password yang tersedia.

Gambar 3. Halaman Login

3.2. Halaman Data Pelanggan

Gambar 4 merupakan tampilan data pelanggan merupakan komponen penting dalam sistem yang berfungsi sebagai wadah penyimpanan data pelanggan yang telah diunggah sebelumnya. Melalui halaman ini, pengguna (dalam hal ini owner) dapat memantau keberadaan data pelanggan secara langsung, baik untuk memastikan data telah tersimpan dengan benar

Gambar 4. Halaman Data Pelanggan

3.3. Halaman Upload Data Pelanggan

Gambar 5 merupakan tampilan *upload* data pelanggan merupakan halaman untuk *input* data pelanggan yang sudah di simpan di dalam perangkat dalam berbentuk file excel. Di dalam halaman *upload* juga di tampilkan menu enkripsi dan kunci yang bisa di tentukan oleh *user*.

Mardhatillah Owner

DATA UPLOAD USER LOGOUT

Upload Data Excel

Pilih File Excel:

Choose File No file chosen

Pilih Kunci Enkripsi:

3 3 6 9

Upload & Enkripsi

Gambar 5. Halaman Upload Data Pelanggan

3.4. Halaman Database User

Gambar 6 merupakan *Database User* berfungsi untuk menampilkan data user pada aplikasi.

Mardhatillah Owner

DATA UPLOAD USER LOGOUT

Manajemen User

ID	Username	Password	Role	Aksi
1	owner1	password123	Owner	Tidak bisa hapus
5	habib	1h1	Staff	 
21	dasa	1e1	Staff	 
22	salma	1e3	Staff	 

Gambar 6. Halaman Database User

3.5. Halaman Edit Data User

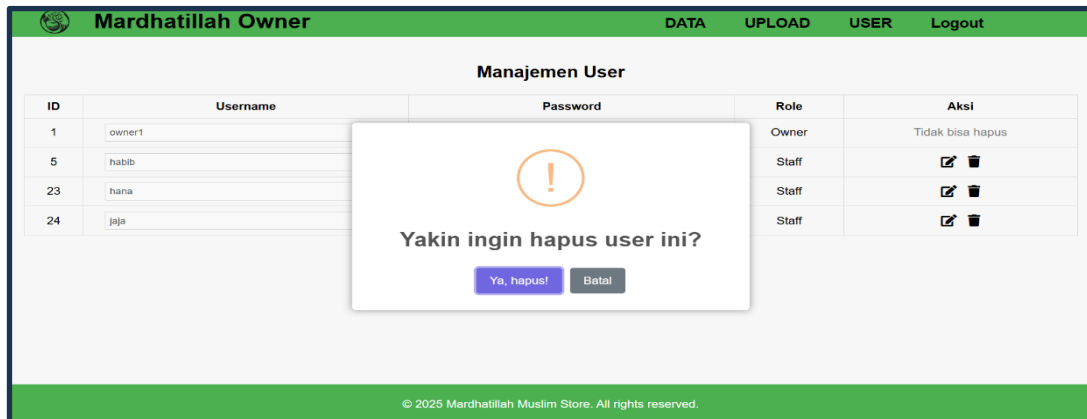
Gambar 7 merupakan *Form edit user* berfungsi untuk mengedit data user.

Username	Password	Role	Aksi
owner1	password123	Owner	Tidak bisa hapus
habib	1h1	Staff	 

Gambar 7. Halaman Edit Data User

3.6. Halaman Delete Data User

Gambar 8 merupakan *Delete Data User* berfungsi untuk menghapus data user.



Gambar 8. Halaman Delete Data User

3.7. Halaman Deskripsi Data

Gambar 9 merupakan implementasi dari perancangan popuphapus barang. Popup ini akan muncul sebagai peringatan sebelum pengguna menghapus barang.

Mardhatillah Owner					
DATA UPLOAD USER LOGOUT					
Manajemen User					
ID	Username	Password	Role	Aksi	
1	owner1		Owner	Tidak bisa hapus	
5	habib		Staff	 	
23	hana		Staff	 	
24	jaja		Staff	 	

Gambar 9. Halaman Deskripsi Data

3.8. Halaman Menu Dashboard Staff

Gambar 10 merupakan dashboard staff berfungsi untuk membantu operasional harian, tapi dengan akses yang lebih terbatas dibanding owner.

Mardhatillah Owner					
DATA UPLOAD USER LOGOUT					
Data Pelanggan					
rizki Cari					
Hapus Semua Data					
No	Nama	Kontak	Lokasi	Total Belanja	Aksi
256	Apotik Rizki Farma	3,55:7479839	Medan Marelان	#Us#7/96/38;133#	Dekripsi
678	Apotik Rizki Farma 2	081315631509	Tembung Jl Simpang Jodoh	Rp 3,060,911.00	Dekripsi
680	Apotik Rizki Farma	3,55:9786;86	Tembung Jl Simpang Jodoh	#Us#5/483/3:133#	Dekripsi
Page 1 of 1					

Gambar 10. Halaman Menu Dashboard Staff

3.9. Halaman Data Pelanggan

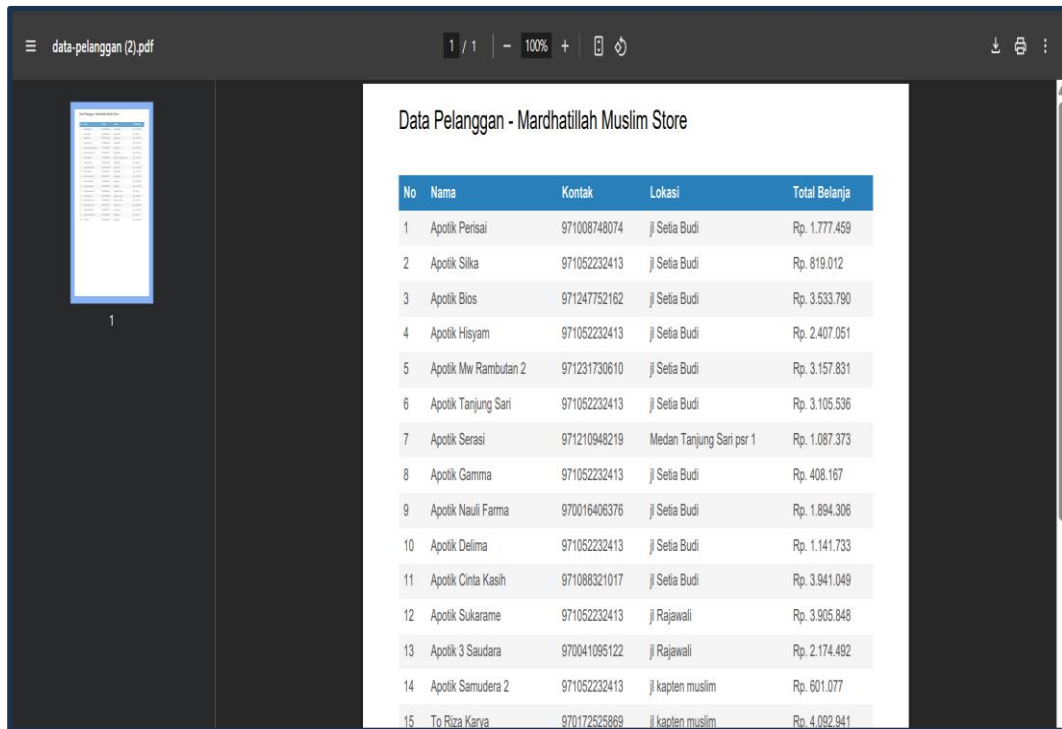
Gambar 11 merupakan tampilan data pelanggan merupakan komponen penting dalam sistem yang berfungsi sebagai wadah penyimpanan data pelanggan yang telah diunggah sebelumnya. Melalui halaman ini, pengguna (dalam hal ini staff) dapat memantau informasi umum secara langsung.

Mardhatillah Owner					
DATA UPLOAD USER Logout					
Data Pelanggan					
Cari nama apotik... Cari					
Hapus Semua Data					
No	Nama	Kontak	Lokasi	Total Belanja	Aksi
1	Apotik Perisai	315442182418	jl Setia Budi	Rp. 5.111.893	Dekripsi
2	Apotik Silka	315496676857	jl Setia Budi	Rp. 4.253.456	Dekripsi
3	Apotik Bios	315681196506	jl Setia Budi	Rp. 7.977.134	Dekripsi
4	Apotik Hisyam	315496676857	jl Setia Budi	Rp. 6.841.495	Dekripsi
5	Apotik Mw Rambutan 2	315675174054	jl Setia Budi	Rp. 7.591.275	Dekripsi

Gambar 11. Halaman Data Pelanggan

3.10. Halaman Cetak Data Pelanggan

Gambar 12 merupakan tampilan cetak data pelanggan merupakan hasil dari proses ketika pengguna menekan tombol Cetak pada halaman dashboard. Sistem secara otomatis menghasilkan file dalam format PDF yang berisi daftar data pelanggan, yang kemudian langsung diunduh dan dibuka di peramban atau aplikasi pembaca PDF.



data-pelanggan (2).pdf

1 / 1 | - 100% +

Data Pelanggan - Mardhatillah Muslim Store

No	Nama	Kontak	Lokasi	Total Belanja
1	Apotik Perisai	971008748074	j Setia Budi	Rp. 1.777.459
2	Apotik Silka	971052232413	j Setia Budi	Rp. 819.012
3	Apotik Bios	971247752162	j Setia Budi	Rp. 3.533.790
4	Apotik Hisyam	971052232413	j Setia Budi	Rp. 2.407.051
5	Apotik Mw Rambutun 2	971231730610	j Setia Budi	Rp. 3.157.831
6	Apotik Tanjung Sari	971052232413	j Setia Budi	Rp. 3.105.536
7	Apotik Serasi	971210948219	Medan Tanjung Sari psr 1	Rp. 1.087.373
8	Apotik Gamma	971052232413	j Setia Budi	Rp. 408.167
9	Apotik Nauli Farma	970016406376	j Setia Budi	Rp. 1.894.306
10	Apotik Delima	971052232413	j Setia Budi	Rp. 1.141.733
11	Apotik Cinta Kasih	971088321017	j Setia Budi	Rp. 3.941.049
12	Apotik Sukrame	971052232413	j Rajawali	Rp. 3.905.848
13	Apotik 3 Saudara	970041095122	j Rajawali	Rp. 2.174.492
14	Apotik Samudera 2	971052232413	j kapten muslim	Rp. 601.077
15	To Riza Karva	970172525889	j kapten muslim	Rp. 4.082.941

Gambar 12. Halaman Cetak Data Pelanggan

4. KESIMPULAN

Dari serangkaian kegiatan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Sistem berhasil meningkatkan keamanan data pelanggan, khususnya pada data sensitive seperti nomor telepon sehingga mengurangi kecurangan yang akan dilakukan oleh pihak yang tidak bertanggung jawab.
2. Dengan menerapkan algoritma Caesar Cipher, sistem ini mampu menyembunyikan informasi sensitif pelanggan sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian penelitian ini.

REFERENSI

- [1] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, 2(1), 163–171.
- [2] Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia*, 2(3), 654-666.
- [3] Alasi, T. S. (2019). Implementasi Kriptografi Dengan Algoritma Ceasar Cipher Untuk Keamanan Data Microsoft Office Word Dan Excel. *Jurnal Informasi Komputer Logika*, 1(2).
- [4] Azis, N. (2018). Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chipper dan operasi xor. *IKRA-ITH Informatika: Jurnal Komputer dan Informatika*, 2(1), 72-80.
- [5] Ridho, A., Mutia, C., & Sinaga, A. P. (2022). Analisis Enkripsi dan Dekripsi Cipher Teks

- Menggunakan Kombinasi Gronsfield Cipher dengan Reverse Cipher. *JTIK (Jurnal Teknik Informatika Kaputama)*, 6(1), 87-94.
- [6] Hermawan, A., & Ujianto, E. I. H. (2021). Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA. *Jurnal Nasional Informatika dan Teknologi Jaringan*, 5(2), 326-330.
- [7] Hidayat, M., Tahir, M., Sukriyadi, A., & Sulton, A. (2023). Penerapan kriptografi Caesar cipher dalam pengamanan data. *Jurnal Ilmiah Multidisiplin*, 2(3), 35-41.
- [8] Silalahi, F. D. (2022). Manajemen Database MySQL (Structured Query Language). *Penerbit Yayasan Prima Agus Teknik*, 1-158.
- [9] Shidqi, S., Sulisty, D. A., & Ahda, F. A. I. (2022). Pembuatan Infrastruktur Database Menggunakan Metode Replikasi Untuk Pelanggan Jagoan Hosting. *Jurnal Ilmiah Teknologi Informasi Asia*, 16(1), 65-74.
- [10] Imron, M., & Pratama, A. (2022). Pengamanan e-dokumen berbasis steganografi dengan kombinasi Advanced Encryption Standard (AES) 128 bit. *InfoTekJar*, 2, 6-10.
- [11] Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar cipher atau Vigenere cipher pada pengenkripsian pesan teks. *Journal on Education*, 5(3), 8563-8573.
- [12] Gusmana, R., Haryansyah, H., & Fitria, F. (2022). Implementasi algoritma Affine cipher dan Caesar cipher dalam mengamankan data teks. *Sebatik*, 26(2), 517-524.
- [13] Hamni, M., Amri, M. K., Rezeki, S., & Nasution, A. B. (2022). Penerapan keamanan data dengan menggunakan metode Caesar cipher untuk mengamankan database MySQL. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, 4(4), 472-477.
- [14] Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar cipher atau Vigenere cipher pada pengenkripsian pesan teks. *Journal on Education*, 5(3), 8563-8573.
- [15] Ningrum, D. F., Tahir, M., Puspitasari, W. D. A., Permatasari, E., Rofiq, F. R., Hidayati, M., ... & Setiawan, A. (2023). Implementasi keamanan data menggunakan kriptografi Caesar cipher. *Jurnal Adijaya Multidisiplin*, 1(2), 388-396.
- [16] Nasution, S. D. (2024). Pengamanan Perintah Koneksi ke Database MySQL Menggunakan Algoritma Caesar Cipher dan Algoritma Stout Codes. *Bulletin of Information Technology (BIT)*, 5(1), 9-16.
- [17] Ardiansyah, F. D., Damayanti, A., Putri, C. A. M., Rany, A. F. D., Biroso, S. J., & Tahir, M. (2023). Implementasi Kriptografi Caesar Chiper Pada Aplikasi Enkripsi dan Dekripsi. *Jurnal ilmiah Sistem Informasi dan Ilmu Komputer*, 3(1), 105-112.
- [18] Wahdini, S. V., Hartama, D., & Kirana, I. O. (2021). Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi. *Journal of Informatics Management and Information Technology*, 1(3), 101-107.
- [19] Metro, J. J. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance.
- [20] Wibowo, M. C., Nguyen, P. T., Armay, E. F., & Rahim, R. (2020). Implementation of Base64 and

caesar cipher in securing video files. *Journal of Advanced Research in Dynamical and Control Systems*, 12(2), 761-765.

- [21] Supriyatno, A. M., & Ardhianto, E. (2024). Peningkatan Keamanan Pesan Teks Menggunakan Super Enkripsi Algoritma Caesar Cipher Standard Dan Vigenere Autokey. *Jurnal Ilmiah KOMPUTASI*, 23(2), 167-172.