

Rancang Bangun Aplikasi Keamanan Data Penjualan Berbasis Web Menggunakan Metode Caesar Cipher Dan Base64 Pada Pabrik Tahu SS

Design-Based Sales Data Security Application Web Using Methods Caesar Cipher And Base64 At the Tofu Factory SS

Ahmad Latiep¹, Nita Syahputri²

¹Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama

²Program Studi Ilmu Komputer, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama
ahmadlatif763@gmail.com¹, nita20d@gmail.com²

ABSTRAK

Didalam bisnis teknologi memainkan sebuah peran yang sangat penting di era digitalisasi ini, dimulai dari pemasaran, produksi hingga manajemen operasional suatu perusahaan. Setiap kegiatan yang dilakukan didalam bisnis, akan lebih terasa efisien dan praktis jika diintegrasikan dengan sebuah teknologi. Keamanan data adalah suatu upaya perlindungan data di dalam sebuah sistem, yang berfungsi untuk melawan otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi. Keamanan data merupakan langkah yang paling penting dalam mengelola suatu data. Kumpulan data yang dikelola harus di amankan dari serangan penjahat cyber yang menargetkan data para pengguna maupun bisnis. Dalam melakukan pemesanan, pelaku pasar melakukan pemesanan dengan cara menghubungi perusahaan dalam hal ini petugas customer service (CS), lalu meminta jumlah produk yang diinginkan. Namun, dalam melakukan transaksi pemesanan, perusahaan memberikan harga yang lebih murah terhadap pelaku bisnis pasar yang memesan dalam jumlah yang banyak dibanding dengan harga rata-rata yang sudah ada dipasar, sehingga pelaku bisnis yang mengetahui perbedaan harga ini dan memesan jumlah yang tidak banyak melakukan protes terhadap perusahaan. Kendala yang ada dapat di minimalisir dengan teknologi berbasis web, yaitu suatu teknologi komputer yang mampu menyimpan data secara komputerisasi dan dengan didukung oleh metode Caesar Cipher dan Base64 yaitu merupakan algoritma kriptografi untuk melakukan encoding dan decoding suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 dan juga merupakan metode substitusi yang memiliki cara kerja menukarkan antara satu huruf dengan huruf lainnya sehingga data pemesanan dapat menjadi rahasia dan aman dari ancaman serangan cyber.

Kata Kunci : Keamanan Data, Caesar Cipher, Base64

ABSTRACT

In the technology business, it plays a very important role in this digitalization era, starting from marketing, production to the operational management of a company. Every activity carried out in business will be more efficient and practical if it is integrated with technology. Data security is an effort to protect data in a system, which functions to fight unauthorized authorization, modification, or destruction and protect computer systems against unauthorized use or modification. Data security is the most important step in managing data. Managed data sets must be secured from cybercriminal attacks that target user and business data. In placing an order, market participants place an order by contacting the company, in this case a customer service officer (CS), then asking for the desired number of products. However, in making order transactions, companies provide lower prices to market business actors who order in large quantities compared to the average price that already exists in the market, so that business people who know this price difference and order quantities do not protest much against the company. Existing constraints can be minimized with web-based technology, which is a computer technology capable of storing data computerized and supported by the Caesar Cipher and Base64 methods, which are cryptographic algorithms for encoding and decoding data into ASCII format, which is based on numbers. base 64 and is also a substitution method that has a working way of exchanging one letter with another so that the ordering data can be confidential and safe from the threat of cyber attacks.

Keywords : Data Security, Caesar Cipher, Base64

Info Artikel :

Disubmit: 12 Juni 2024

Direview: 11 Juli 2024

Diterima : 15 Agustus 2024

Copyright © 2024 - Journal UPU. All rights reserved..

1. PENDAHULUAN

Keamanan data adalah suatu upaya perlindungan data di dalam sebuah sistem, yang bertujuan untuk melawan otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi. Keamanan data merupakan langkah yang sangat penting dalam mengelola suatu data. Keamanan merupakan aspek penting dari suatu data atau informasi, dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi [1]

Dalam melakukan perjalanan bisnis, data merupakan salah satu bagian terpenting dalam lingkungan bisnis. Data yang memuat informasi, baik identitas seseorang, produk, maupun penjualan merupakan hal privasi baik bagi pebisnis maupun konsumen. Data yang seharusnya bersifat rahasia, menjadi target utama bagi penjahat *cyber* dan juga kompetitor bisnis.

Pebisnis yang memegang data, baik data perusahaan itu sendiri maupun data konsumen seharusnya menyiapkan data berada dalam kondisi yang aman dari serangan *cyber* dan juga pihak-pihak yang tidak bertanggungjawab yang ingin melakukan pencurian data. Data yang disimpan oleh Pebisnis, akan lebih baik jika disimpan bukan dalam bentuk aslinya, namun dalam bentuk enkripsi. Enkripsi yang merupakan suatu proses dilakukannya perubahan dari suatu bentuk data yang dapat dimengerti, menjadi tidak dapat dimengerti. Enkripsi yang menerapkan ilmu kriptografi didalamnya, yakni ilmu penyimpanan pesan, data atau informasi dengan menerapkan logika-logika tertentu, sehingga data asli yang tersimpan, menjadi tidak dapat terbaca oleh penjahat *cyber* dan pihak yang tidak bertanggungjawab lainnya, sehingga ketika terjadi kebocoran data, data menjadi lebih aman dan data yang didapat menjadi tidak mudah untuk dibaca.

Menurut Muhammad Rizki Zulfikar, Sri Mulyati (2022) dengan judul penelitian “Penerapan Kriptografi *Caesar Cipher* dan *Vigenere Cipher* untuk Mengamankan *Database* Barang *Belting* pada PT. Multi Mitra Usaha Bersama”. Penelitian ini menggunakan sistem dengan *pemrograman PHP* dan berbasis *web*. Sistem ini menggunakan metode penggabungan dua algoritma klasik, yakni *Caesar Cipher* dan *Vigenere Cipher*, hasil dari penelitian ini menunjukkan bahwa sistem keamanan yang teraplikasi didalam teknologi berbasis web, dapat mengamankan data-data barang yang ada didalam *database* sehingga data yang ada menjadi lebih aman. Tujuan dari penelitian ini adalah mengimplementasikan algoritma kriptografi klasik ke dalam sebuah sistem keamanan yang berbasis *web*. [2]

Penelitian yang dilakukan Anjur S Manullang, dkk (2020) dengan judul penelitian “Penyandian *Database* Menggunakan Metode *Base64* dan *Rot13*”. Penelitian ini dilakukan menggunakan dua algoritma klasik, yaitu *Base64* dan *Rot13*. *Rot13* yang merupakan singkatan dari “*Rotate by 13*” yang merupakan salah satu variasi dari metode *Caesar Cipher*, dinamakan algoritma *Rot13* karena algoritma *Caesar Cipher* tersebut di geser sebanyak 13 kali huruf *plaintext* nya sehingga menghasilkan sebuah *ciphertext* dalam putaran yang ke-13. Dari penelitian menggunakan dua algoritma ini, didapatkan hasil bahwa sistem dapat mengamankan *database* yang ada didalam server dengan *double protection* sehingga lebih aman dan sulit untuk di *hack*. [3]

Berdasarkan penelitian yang dilakukan Sri Vivi Wahdini, dkk (2021) dimana melakukan penelitian mengenai “Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi”. Hasilnya menunjukkan bahwa dengan mengimplementasikan algoritma kriptografi kedalam sebuah sistem yang berbasis teknologi web, dapat meningkatkan keamanan sebuah data yang akan diakses kepada berbagai pihak. Data yang akan dikirimkan ke pihak pusat, menjadi terjamin keamanan nya karena dilakukan proteksi terhadap data dengan melakukan proses enkripsi kepada data tersebut. [4]

Menurut penelitian yang dilakukan oleh Ali Aman dan Budi Triandi (2020) dengan judul penelitian “Validasi Formulir Pelanggaran Pemilu pada Bawaslu Sumatera Utara Menggunakan *QR-Code* dan *Base64*”. Penelitian ini dilakukan dengan menggunakan teknologi berbasis *Web*. Dari penelitian ini, didapatkan hasil bahwa sistem validasi formulir yang berbasis *web* ini dapat mengelola seluruh data yang berhubungan dengan pelanggaran pemilu sehingga dapat mempermudah bagi instansi Bawaslu Sumatera Utara untuk melakukan validasi terhadap formulir pengaduan pelanggaran pemilu sehingga pengaduan tersebut lebih terstruktur, sistematis, dan berada diluar jaringan. Dengan perpaduan *QR-Code* dan *Base64*, data-data pengaduan pelanggaran pemilu yang termasuk didalamnya beberapa data yang bersifat rahasia dapat menjadi lebih aman dan terjamin datanya. [5]

Berdasarkan penelitian yang dilakukan Obby Oktafianto dan Achmad Solichin (2019) dimana melakukan penelitian mengenai “Pengamanan Data Penjualan pada CV. Monochrome dengan Kriptografi Algoritma *Caesar Cipher* dan *RSA*”. Hasilnya menunjukan bahwa sistem yang berjalan sangat bermanfaat bagi perusahaan karena data yang disimpan sudah terenkripsi dengan keamanan yang berlapis sehingga ketika terjadi kebocoran atau pencurian data, maka akan lebih sulit untuk membaca data karena proteksi keamanan enkripsi yang berlapis. [6]

Penelitian sistem keamanan data penjualan berbasis web menggunakan metode *Caesar cipher* dan *base 64*. Kriptografi merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi (cryptography) adalah penggabungan kata “*Crypto*” yang berarti rahasia dan “*graphy*” yang berarti tulisan, bisa disimpulkan bahwa kriptografi adalah seni dan seni untuk menjaga keamanan data dari pihak ketiga, yang hanya bisa diketahuioleh pihak pengirim dan penerima. [7] Kriptografi berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan

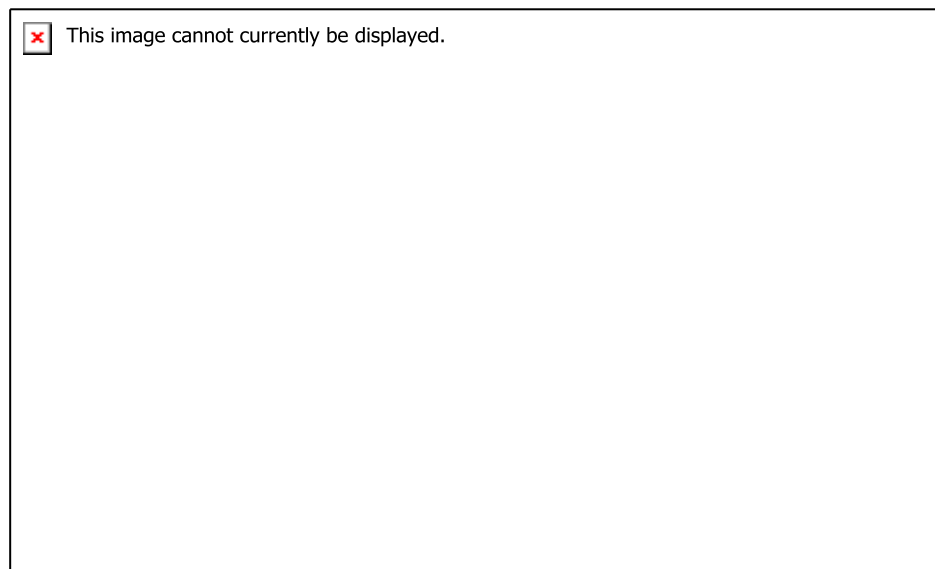
data jelas(plaintext) ke dalam bentuk data sandi(ciphertext) yang tidak dapat dikenali. Base64 merupakan salah satu algoritma untuk garbling dan decoding suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan encoding(penyadiran) terhadap data binary. Umumnya digunakan pada berbagai aplikasi seperti-mail via MIME, data XML, atau untuk keperluan garbling URL. Prinsip encodingnya adalah dengan memilih kumpulan dari 64 karakter yang dapat di print(printable), dengan demikian data dapat disimpan dan ditransfer melewati media yang didesain untuk menangani data tekstual, penggunaan lain garbling Base64 adalah untuk melakukan obfuscation atau pengacakan data. Skema enkripsi Base64 biasanya juga digunakan ketika diperlukan sandi terhadap data biner yang didesain untuk menangani data. Sehingga memungkinkan pelanggan dan penjual untuk mengamankan data transaksi.

2. METODE PENELITIAN

Metode merupakan suatu cara atau teknik yang sistematis untuk mengerjakan suatu kasus. Metode yang digunakan oleh peneliti adalah penelitian kuantitatif. Penelitian kuantitatif adalah metode penelitian yang bersifat deskriptif dan lebih banyak menggunakan analisis.

A. Metode Pengembangan Sistem

Metodologi penelitian merupakan tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Metode penelitian yang dilakukan dalam penelitian ini adalah dengan menggunakan metode *waterfall* (air terjun) dalam pengembangan sistem. metode waterfall adalah sebuah metode pengembangan sistem dimana antar satu fase ke fase yang lain dilakukan secara berurutan [8] Dalam proses implementasi metode Waterfall ini, sebuah langkah akan diselesaikan terlebih



dahulu dimulai dari tahapan yang pertama sebelum melanjutkan ke tahapan yang berikutnya dapat dilihat pada Gambar 1.

Gambar 1. Metode Pengembangan Sistem

1. *Analysis*, pada tahap ini layanan sistem, kendala, dan tujuan ditetapkan oleh hasil konsultasi dengan pengguna yang kemudian didefinisikan secara rinci untuk mengetahui mengenai sistem. Sistem yang harus dipenuhi yaitu dapat memberikan informasi.
2. *Design*, pada tahap ini developer mengalokasikan kebutuhan-kebutuhan sistem baik perangkat keras maupun perangkat lunak dengan membentuk arsitektur sistem secara keseluruhan. Perancangan sistem melibatkan identifikasi dan penggambaran abstraksi sistem dasar perangkat lunak dan hubungannya.
3. *Implementation*, tahap ini keseluruhan dari desain sistem yang telah disusun sebelumnya diubah menjadi kode-kode program dan modul-modul yang nantinya diintegrasikan menjadi sebuah sistem yang lengkap sesuai dengan kontrak.
4. *Testing*, tahap ini merupakan proses ujicoba terhadap aplikasi yang telah selesai dirancang dilakukan, pengujian ini dilakukan untuk mengetahui apakah aplikasi sudah berjalan sesuai dengan baik yang telah ditetapkan agar hasil tujuan pembangunan aplikasi sesuai dengan kontrak.
5. *Maintenance*, tahapan ini adalah tahap terakhir dari seluruh rangkaian kegiatan perancangan aplikasi, dimana pada tahap ini terjadinya proses perbaikan sistem. seperti terjadi kesalahan-kesalahan pada tahapan-tahapan sebelumnya, meningkatkan penggunaan dan layanan sistem agar lebih baik

C. Caesar Cipher

Merupakan salah satu kriptografi yang paling tua dan paling sederhana yang ditemukan oleh Julius Caesar. Caesar Cipher adalah salah satu metode kriptografi klasik, alasan metode ini dinamakan Caesar Cipher adalah saat Julius Caesar berkomunikasi dengan para panglimanya [9] Kriptografi Caesar ini merupakan kriptografi substitusi karena setiap huruf akan digantikan huruf lain. Huruf-huruf yang akan diganti, akan ditambah dengan geseran (*rotation*) yang diinginkan, misalnya jika huruf "A" memiliki geseran 3 kali, sehingga huruf "A" tersebut akan berubah menjadi huruf "D".

Algoritma enkripsi *Caesar Cipher* :

$$C_i = P_i + 3$$

Algoritma dekripsi *Caesar Cipher* :

$$P_i = C_i - K_i$$

Contoh Proses Enkripsi :

Plaintext : AHMAD

Solusi :

Ascii Plaintext :

$$A = 65$$

$$H = 72$$

$$M = 77$$

$$A = 65$$

$$D = 68$$

Enkripsi :

$$C_1 = A + 3$$

$$= 65 + 3$$

$$= 68 = D$$

$$C_2 = H + 3$$

$$= 72 + 3$$

$$= 75 = K$$

$$C_3 = M + 3$$

$$= 77 + 3$$

$$= 80 = P$$

$$C_4 = A + 3$$

$$= 65 + 3$$

$$= 68 = D$$

$$C_5 = D + 3$$

$$= 68 + 3$$

$$= 71 = G$$

Chipertext : DKPDG

Contoh Proses Dekripsi :

$$C_1 = D - 3$$

$$= 68 - 3$$

$$= 65 = A$$

$$C_2 = K - 3$$

$$= 75 - 3$$

$$= 72 = H$$

$$C_3 = P - 3$$

$$= 80 - 3$$

$$= 77 = M$$

$$C_4 = D - 3$$

$$= 68 - 3$$

$$= 65 = A$$

$$C_5 = G - 3$$

$$= 71 - 3$$

$$= 68 = D$$

Plaintext : AHMAD

C. Base 64

Base64 merupakan salah satu algoritma untuk *encoding* dan *decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyadian) terhadap data *binary*. [8]. Umumnya digunakan pada berbagai aplikasi seperti *e-mail* via MIME, data XML, atau untuk keperluan *encoding* URL. Prinsip *encoding*nya adalah dengan memilih kumpulan dari 64 karakter yang dapat di *print* (*printable*), dengan demikian data dapat disimpan dan ditransfer melewati media yang didesain untuk menangani data tekstual, penggunaan lain *encoding* Base64 adalah untuk melakukan *obfuscation* atau pengacakan data. Skema enkripsi Base64 biasanya juga digunakan ketika diperlukan sandi terhadap data biner yang didesain untuk menangani data. Algoritma Base64 tidak menggabungkan hasil prosesnya tetapi mengubah suatu nilai ke bentuk nilai lainnya tanpa menggabungkan hasilnya dan tidak memerlukan kunci.[11] Algoritma kriptografi Base64 ini sebenarnya menggunakan algoritma kunci simetris atau disebut juga algoritma kriptografi konvensional, yaitu algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. [12]

Karakter yang dihasilkan pada transformasi Base64 ini terdiri dari A sampai Z, a sampai z dan 0 sampai 9, serta ditambah simbol “ ” dan “/ ” serta satu buah karakter sama dengan(=) di karakter terakhir yang di pakai untuk pengisian pad atau dengan penyesuaian menggenapkan binary. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan.

Teknik encoding Base64, jika satu senarai(string) bytes yang akan disandikan dengan Base64 maka caranya adalah:

- Masukkan kata yang akan di garbling dengan Base64, contoh “ Ahmad ”
- Ambil nilai double dari ASCII setiap karakter yaitu

A = 65, binary = 01000001

h = 104, binary = 01101000

m = 109, binary = 01101101

a = 97, binary = 01100001

d = 100, binary = 01100100

- Deretan double dari “ Ahmad ” 01000001 01101000 01101101 01100001 01100100.

Deretan binary(dijadikan 1 baris panjang) dari" Ahmad"

0100000101101000011011010110000101100100

Proses per 6 bit, setiap 6 bit akan mewakili 1 karakter Base64

0100000101101000011011010110000101100100.

Maka menjadi 010000-010110-100001-101101-011000-010110-0100.

Panjang kata bukan kelipatan 3, akan padding “ = ” sepanjang 1 karakter.

Maka hasil dari garbling nya adalah

double Desimal Base64

00010000 16 Q

00010110 22 W

00100001 33 h

00101101 45 t

00011000 24 Y

00010110 22 W

00010000 16 Q

Hasil garbling Base64, dengan padding “ QWhYWQ = ”

D. Enkripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau chipper.

E. Dekripsi

Dekripsi adalah satu kaedah upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri. Dalam keilmuan, deskripsi diperlukan agar peneliti tidak melupakan pengalamannya dan agar pengalaman tersebut dapat dibandingkan dengan pengalaman peneliti lain, sehingga mudah untuk dilakukan pemeriksaan dan kontrol terhadap dekripsi tersebut. Pada umumnya dekripsi menegaskan sesuatu, seperti apa sesuatu itu kelihatannya, bagaimana bunyinya, bagaimana rasanya, dan sebagainya. Dekripsi yang detail diciptakan dan dipakai dalam disiplin ilmu sebagai istilah teknik. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal [13]

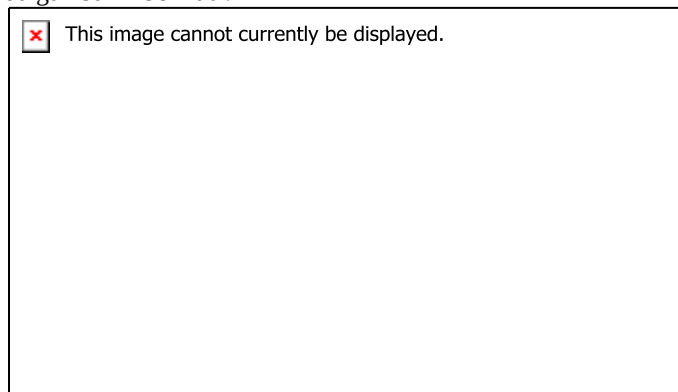
3. HASIL DAN PEMBAHASAN

A. Tampilan Sistem

Berikut ini dijelaskan tentang tampilan hasil dari penerapan metode old kriptografi yaitu kombinasi algoritma Base64 dengan Caesar Cipher dalam Aplikasi Keamanan Data Penjualan untuk mengamankan data penjualan baik dari serangan penjahat cyber dan juga dari para pedagang dapat dilihat sebagai berikut :

1. Tampilan Login

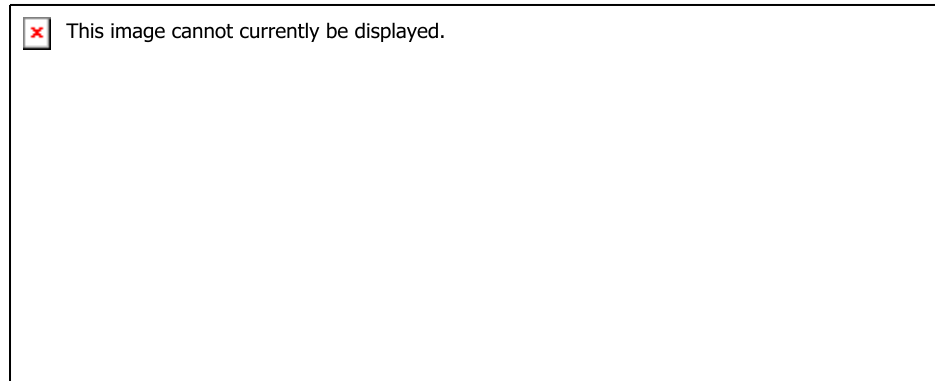
Halaman *Login* merupakan halaman yang akan muncul ketika Pengguna membuka *website* aplikasi keamanan data. Dapat dilihat pada gambar 2 berikut :



Gambar 2 Tampilan *Login*

2. Tampilan Dashboard

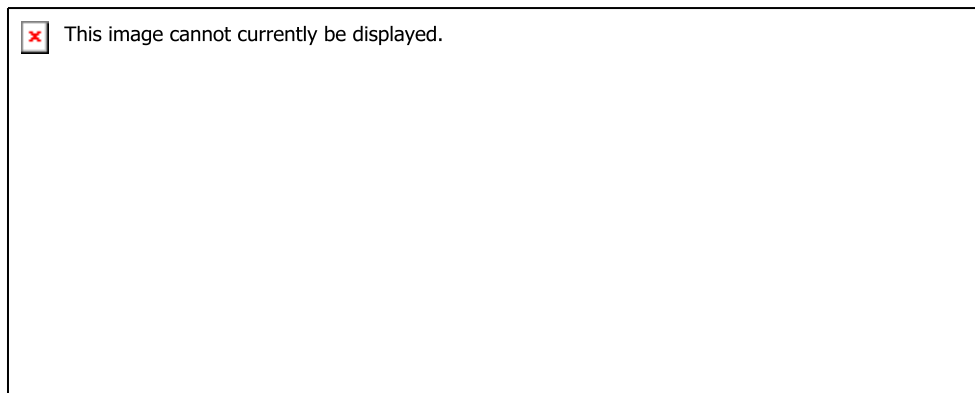
Halaman *Dashboard* merupakan halaman yang akan muncul ketika Pengguna berhasil *login*. Dapat dilihat pada gambar 3 berikut :



Gambar 3 Tampilan *Dashboard*

3. Tampilan Halaman *Order*

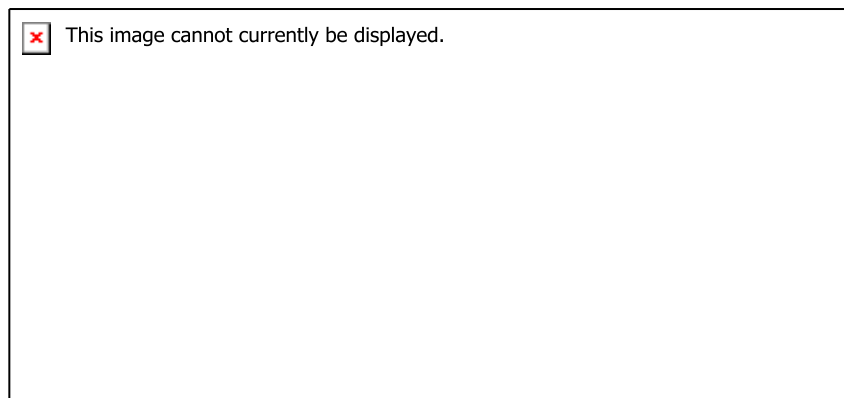
Halaman *Order* merupakan halaman yang digunakan Pengguna untuk mengatur segala aktifitas mengenai data pesanan seperti tambah, ubah, dan hapus *order*. Dapat dilihat pada gambar 4 berikut :



Gambar 4 Tampilan Halaman *Order*

4. Tampilan Halaman Detail *Order*

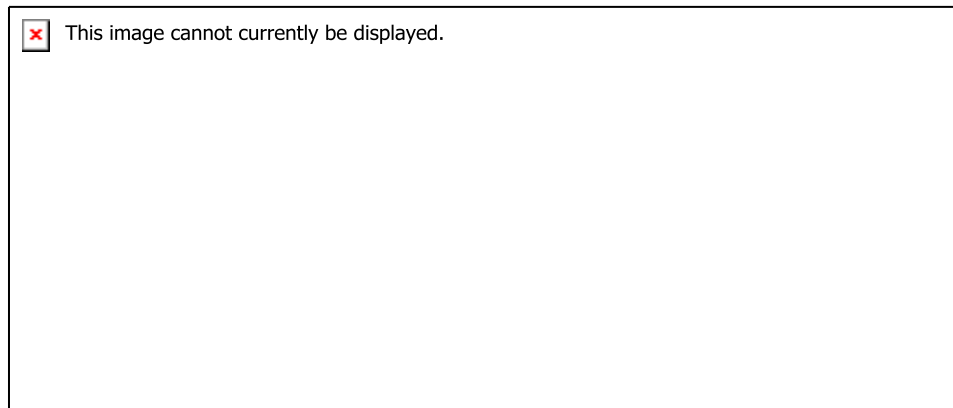
Halaman detail *order* merupakan halaman yang digunakan Pengguna untuk melihat detail pesanan baik berupa data *plaintext* maupun data yang telah terenkripsi yang dilakukan oleh pelaku bisnis, dapat dilihat seperti gambar 5 berikut :



Gambar 5 Tampilan Halaman Detail *Order*

5. Tampilan Halaman *History*

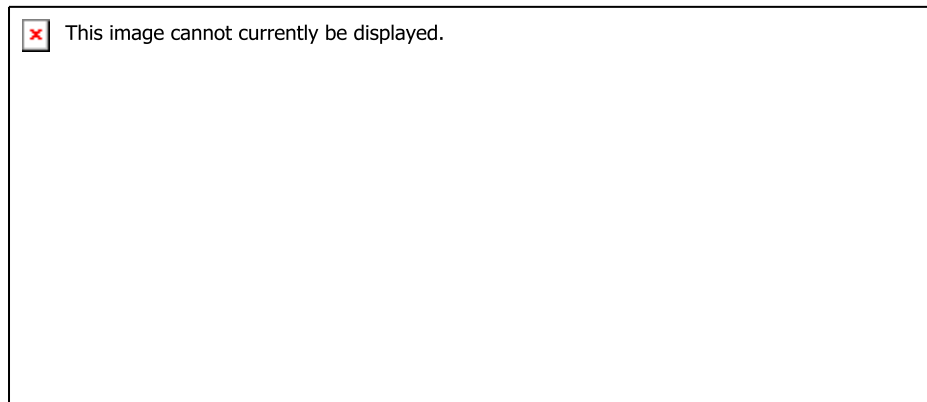
Halaman *history* merupakan halaman yang digunakan Pengguna untuk melihat data pesanan yang dilakukan oleh pelaku bisnis pasar, dapat dilihat seperti gambar 6 berikut :



Gambar 6 Tampilan Halaman *History*

6. Tampilan Halaman *Track*

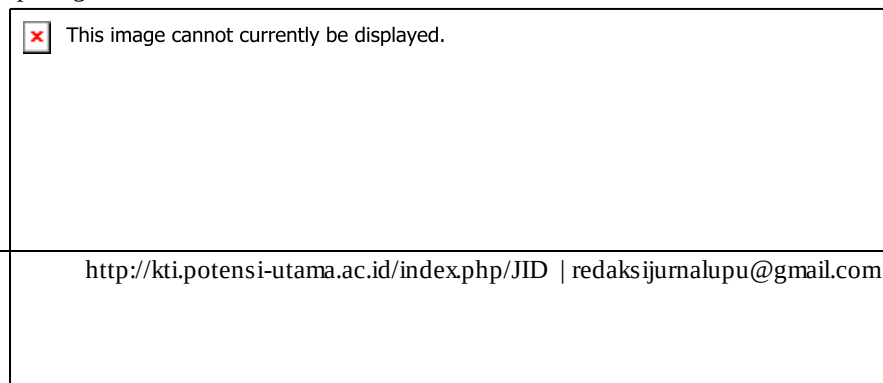
Halaman *track* merupakan halaman yang digunakan oleh pengguna untuk melakukan *tracking* dan mengubah status proses terhadap pesanan yang dilakukan oleh pelaku bisnis. Dapat dilihat pada gambar 7 berikut :



Gambar 7 Tampilan Halaman *Track*

7. Tampilan Halaman Laporan

Halaman laporan merupakan halaman yang akan menampilkan hasil total pesanan dalam jangka waktu perbulan. Dapat dilihat pada gambar 8 berikut :



Gambar 8 Tampilan Laporan

B. Hasil Pengujian

Skenario pengujian aplikasi ini dilakukan oleh Admin. Sedangkan metode yang digunakan pada aplikasi keamanan data penjualan pada pabrik tahu SS ini menggunakan metode *black box testing*. Adapun hal-hal yang di ujikan menggunakan metode *black box testing* ini adalah :

Tabel 1 *Black Box Testing Login*

Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
Username dan Password : admin, admin / operator, operator	Akan <i>redirect</i> ke halaman <i>Dashboard</i> .	Menampilkan Halaman <i>Dashboard</i> .	[✓] diterima [] ditolak

Tabel 2 *Black Box Testing Order*

Data Masukk0an	Yang Diharapkan	Pengamatan	Kesimpulan
Klik “Order”	Menampilkan halaman <i>order</i>	Berhasil menampilkan halaman <i>order</i>	[✓] diterima [] ditolak
Klik “Tambah”	Menambahkan <i>list order</i>	Berhasil menambah <i>list order</i>	[✓] diterima [] ditolak
Klik “Edit”	Mengubah <i>order</i>	Berhasil mengubah data <i>order</i>	[✓] diterima [] ditolak
Klik “Hapus”	Menghapus <i>order</i>	Berhasil menghapus data <i>order</i>	[✓] diterima [] ditolak
Klik “Lihat Data”	Menampilkan halaman detail <i>order</i>	Berhasil menampilkan halaman detail <i>order</i>	[✓] diterima [] ditolak

Tabel 3 *Black Box Testing Detail Order*

Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik “Kembali”	Menampilkan halaman <i>order</i>	Berhasil menampilkan halaman <i>order</i>	[✓] diterima [] ditolak
Klik “ <i>Encrypt</i> ”	Melakukan proses enkripsi terhadap data	Berhasil melakukan enkripsi terhadap data	[✓] diterima [] ditolak
Klik “ <i>Decrypt</i> ”	Melakukan proses dekripsi terhadap data	Berhasil melakukan dekripsi terhadap data	[✓] diterima [] ditolak
Klik “Edit”	Mengubah <i>order</i>	Berhasil mengubah data <i>order</i>	[✓] diterima [] ditolak

Tabel 4 *Black Box Testing History*

Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik “ <i>History</i> ”	Menampilkan halaman <i>history</i>	Berhasil menampilkan halaman <i>history</i>	[✓] diterima [] ditolak
Klik “ <i>Track</i> ”	Menampilkan halaman <i>track</i>	Berhasil menampilkan halaman <i>track</i>	[✓] diterima [] ditolak

Tabel.5 *Black Box Testing Track*

Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
---------------	-----------------	------------	------------

Klik “Ubah Status Orderan”	Menambahkan status proses <i>orderan</i>	Berhasil menambah status proses <i>orderan</i>	[✓] diterima [] ditolak
----------------------------	--	--	-----------------------------

Tabel 6 *Black Box Testing* Riwayat

Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik “Laporan”	Menampilkan halaman laporan	Berhasil menampilkan halaman laporan	[✓] diterima [] ditolak
Klik <i>icon</i> “kalender” dan <i>icon</i> “mata”	Memilih data bulan yang akan ditampilkan	Berhasil memilih dan menampilkan laporan data <i>orderan perbulan</i>	[✓] diterima [] ditolak

4. KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Aplikasi Sistem Keamanan berbasis *web* ini adalah sebuah perancangan sistem yang berfungsi untuk mengamankan data penjualan berdasarkan hasil pemesanan yang dilakukan pelanggan atau pelaku dipasar, sehingga dapat mengamankan data penjualan dari pelanggan yang protes terhadap harga yang berbeda dan mengamankan dari serangan *cyber*.
2. Dengan adanya sistem yang telah menerapkan keamanan dengan kombinasi antar 2 (dua) algoritma, maka sistem yang berjalan akan lebih *powerfull* dalam mengamankan data penjualan.
3. Dengan adanya aplikasi yang berbasis digital, akan lebih mudah dalam melakukan proses pengamanan data penjualan

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberikan kesempatan pada penulis agar menyelesaikan karya tulis ilmiah ini. Penulis juga memberikan ucapan terimakasih yang sebesar-besarnya kepada keluarga yang telah memberikan dukungan yang sangat besar, dan kepada teman-teman penulis yang telah memberikan support sehingga penulis dapat menyelesaikan karya tulis ilmiah ini. Penulis berharap karya tulis ilmiah dapat bermanfaat untuk banyak orang.

REFERENSI

- [1] Pradipta, Anjar. 2016. Implementasi Metode Caesar Chiper Alfabeta Majemuk Dalam Kriptografi Untuk Pengamanan Informasi. Agustus 2016. Volume 5 No 3. Yogyakarta. STMIK AMIKOM Yogyakarta.
- [2] Zulfikar, Muhammad Rizqi, Mulyati, Sri, 2022. “Penerapan Kriptografi Caesar Cipher dan Vigenere Cipher Untuk Mengamankan Database Barang Belanja Pada PT. Multi Mitra Usaha Bersama” Jurnal SENAFTI, 1(1), 402-410.
- [3] Manullang, S. Anjur, Puspasari, Ratih, Verina, Wiwi, 2020. “Penyandian Database Menggunakan Metode Base64 dan Rot13” Jurnal Mahasiswa FTIK April 2020, Volume 1, No. 1 April 2020. Universitas Potensi Utama.
- [4] 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.

- [5] Aman Ali, Triandi Budi, 2020. “*Validasi Formulir Pelanggaran Pemilu Pada Bawaslu Sumatera Utara Menggunakan QR-CODE dan Base64*” Jurnal IT Journal, Vol. 8, No. 1 April 2020, 2252-746X.
- [6] Oktafianto, Obby, Solichin, Achmad, 2018. “*Pengamanan Data Penjualan Pada CV. Monochrome Dengan Kriptografi Algoritma Caesar Cipher dan RSA*” Jurnal SKANIKA, Volume 1, No. 1 Maret 2018.
- [7] Putri, Y. D., Rosihan, R., & Lutfi, S. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. *JIKO (Jurnal Informatika dan Komputer)*, 2(2), 87-94.
- [8] Gunadhi, E., & Nugraha, A. P. (2016). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *Jurnal Algoritma*, 13(2), 391-398.
- [9] Fachri, B., & Surbakti, R. W. (2021). Perancangan Sistem Dan Desain Undangan Digital Menggunakan Metode Waterfall Berbasis Website (Studi Kasus: Asco Jaya). *Journal Of Science And Social Research*, 4(3), 263-267.
- [10] Y. D. Putri, Rosihan dan S. Lutfi, “Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance,” Jurnal Informatika dan Ilmu Komputer (JIKO), vol. 2, no. 2, pp. 87-94, 2019.
- [11] Minami, R. (2019). Implementasi Algoritma Base64 untuk Mengamankan SMS pada Smartphone. *Building of Informatics, Technology and Science (BITS)*, 1(1), 28-33.
- [12] Aulia, R., Zakir, A., & Purwanto, D. A. (2018). Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 2(2), 146-151.
- [13] Aulia, R., Zakir, A., & Purwanto, D. A. (2018). Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 2(2), 146-151.
- [14] Perkasa, S., Syahrizal, M., & Simangunsong, P.B.N., 2017. “Implementasi Keamanan Data Teks Dengan Algoritma Modifikasi Caesar Cipher dan Mengkompresi File Menggunakan Algoritma Shannon Fano” Jurnal STMIK GI MDP Palembang.
- [15] Lovian, Tio, Fitri, Iskandar, 2022. “Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang” Jurnal Media Informatika Budidarma, Volume 6, No. 1 Januari 2022. ISSN : p-2614-5278; e-ISSN : 2548-8368.