

Implementasi Aplikasi Keamanan Data Karyawan Pada PT. Jaya Diesel Menggunakan Metode Affine Chiper Dan Rsa Berbasis Web

Implementation of Employee Data Security Application at Pt. Jaya Diesel Uses Web-Based Affine Chiper and Rsa Methods

Kevin Zulkarnaen Tohonan Siagian^{a,1}, Budi Triandi^{b,2}

^aInformatika Univeristas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A, Medan, 20241 - 20244, Indonesia

^b Informatika Univeristas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A, Medan, 20241 - 20244, Indonesia
kevinsiagian77@gmail.com¹, buditriandi@gmail.com²

ABSTRAK

PT. Diesel Jaya adalah spesialis di bidang mesin diesel sejak puluhan tahun lalu. Ketekunan dan pengalaman membawa perusahaan sampai sekarang ini, menjadi salah satu supplier terkemuka untuk mesin diesel dan suku cadang, Pt. Diesel Jaya berdedikasi untuk menyediakan suku cadang dengan kualitas tinggi untuk keperluan mesin. Pada saat ini Pt. Jaya Diesel belum memiliki aplikasi yang melakukan pengamanan data yang berguna untuk mengamankan data karyawan, sehingga kapan saja data karyawan bisa mengalami kebocoran atau hilang data diakibatkan oleh orang-orang yang tidak bertanggung jawab. RSA (Rivest Shamir Adleman) merupakan salah satu algoritma public key yang populer dipakai dan bahkan hingga saat ini algoritma RSA masih dianggap aman dan Affine Cipher adalah perluasan dari Caesar Cipher, yang menggalikan plaintext dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Kecurangan data karyawan tersebut dapat diatasi dengan memanfaatkan metode Affine Cipher dan RSA secara enkrip dan deskrip. Dengan memanfaatkan algoritma Affine Cipher dan RSA ini sistem akan mengenkripsi data asli yang diinputkan pengguna menjadi ciphertext dengan menggunakan key

Kata Kunci: PT. Jaya Diesel, Rivest Shamir Adleman, Affine Cipher

ABSTRACT

PT. Diesel Jaya has been a specialist in the field of diesel engines for decades. Perseverance and experience have brought the company to where it is today, becoming one of the leading suppliers of diesel engines and spare parts, Pt. Diesel Jaya is dedicated to providing high quality spare parts for engine needs. At this time Pt. Jaya Diesel does not yet have an application that provides data security which is useful for securing employee data, so that at any time employee data could experience data leaks or loss due to irresponsible people. RSA (Rivest Shamir Adleman) is a public key algorithm that is popularly used and even today the RSA algorithm is still considered safe and Affine Cipher is an extension of Caesar Cipher, which extracts plaintext with a value and adds it with a shift. This employee data fraud can be overcome by utilizing the Affine Cipher and RSA methods with encryption and description. By utilizing the Affine Cipher and RSA algorithms

keywords: : Pt. Jaya Diesel, Rivest Shamir Adleman, Affine Cipher

Info Artikel :

Disubmit: 10 Februari 2024

Direview: 22 Maret 2024

Diterima : 24 April 2024

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

1. PENDAHULUAN

Terdapat banyak metode pengamanan data yang bisa dimanfaatkan untuk mencegah adanya kecurangan ataupun manipulasi data salah satunya menggunakan *kriptografi* ataupun teknik penyamaran lainnya. *Kriptografi* adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi, pengertian *kriptografi* modern adalah tidak saja berurusan hanya dengan menyembunyikan pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi RSA (Rivest Shamir Adleman) merupakan salah satu *algoritma public key* yang populer dipakai dan bahkan hingga saat ini

algoritma RSA masih dianggap aman dan *Affine Cipher* adalah perluasan dari *Caesar Cipher*, yang menggalikan *plaintext* dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Kecurangan data karyawan tersebut dapat diatasi dengan memanfaatkan metode *Affine Cipher* dan RSA secara *enkrip* dan *deskrip*.

Penelitian yang dilakukan oleh Raja Nasrul Fuad, Haikal Nando Winata, dkk. “**Aplikasi Keamanan File Audio Wav (Waveform) Dengan Terapan Algoritma Rsa**”. Perangkat lunak (*software*) dapat melakukan penyandian data audio dengan menerapkan *algoritma* RSA dan struktur data audio WAV. Ukuran berkas audio WAV menjadi bertambah besar setelah dilakukan enkripsi menggunakan algoritma RSA berdasarkan besar kunci yang digunakan. [1].

Penelitian yang dilakukan oleh Heri Santoso, M. Fakhriza “**Perancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma Rsa**”. Penelitian ini menghasilkan Perangkat lunak (*software*) dapat melakukan penyandian data audio dengan menerapkan algoritma RSA dan struktur data audio WAV. Ukuran berkas audio WAV menjadi bertambah besar setelah dilakukan enkripsi menggunakan algoritma RSA berdasarkan besar kunci yang digunakan. [2].

Penelitian yang dilakukan oleh I Wayan Swendra Putra Arta. “**Penerapan Algoritma Triple Transposition Vigenere Cipher Dan Algoritma Rsa Dalam Keamanan Login**”. Penelitian ini menghasilkan Masalah keamanan berada di urutan kedua atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu kinerja sistem, seringkali keamanan dikurangi atau ditiadakan. Jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka sulit memisahnya dengan proses login. Login bertujuan untuk memberikan layanan keamanan pada sistem. Saat melakukan login pengguna akan memasukkan password dimana password tersebut bersifat privasi dan rahasia. Oleh karena itu, masalah keamanan menjadi masalah yang sangat penting mengingat internet merupakan jaringan publik yang saling terhubung dalam suatu jaringan dan akan sangat berbahaya jika password yang dimasukkan user tersebut tidak dienkripsi sebelum dikirim ke server melalui jaringan. *Triple Transposition Vigenere Cipher* adalah metode enkripsi dengan cara mengulang teknik *Vigenere Cipher* yang setiap *plaintext* nya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya. [3].

Penelitian yang dilakukan oleh Saiful Rohman Cholil, dkk. “**Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA**” Penelitian ini menghasilkan Perkembangan teknologi informasi yang semakin pesat memberi pengaruh yang besar, Salah satunya adalah kriptografi dimana pesan disamarkan menjadi pesan tersandi. Dalam proses penyandian, penyandian yang digunakan adalah Enigma dan RSA (*Rivest Shamir Adleman*). Dimana Enigma sebagai proses penyandian simetris pada pesan dan RSA (*Rivest Shamir Adleman*) sebagai proses penyandian asimetris pada kunci sehingga terjadinya *Kriptografi Hybrid*. *Kriptografi Hybrid* sebenarnya metode yang sangat aman dikarenakan memakai dua jenis algoritma yaitu algoritma simetris dan asimetris, untuk algoritma simetris *Ciphertext* yang dihasilkan akan sama panjang dengan *Plaintext* yang di enkripsi, lain halnya dengan algoritma asimetris yang berfungsi hanya untuk proses enkripsi kunci pada penelitian ini, karena jika algoritma asimetris dipakai untuk enkripsi maka *Ciphertext* yang dihasilkan akan lebih besar jumlah datanya. [4].

Penelitian yang dilakukan oleh Muhamad Yazir Rizki dan Anggraeni Ridwan “**Penerapan Algoritma Affine Cipher Dan Algoritma Coloumnar Transposition Dalam Keamanan Teks**”. Penelitian ini menghasilkan Dengan adanya proses enkripsi dandekripsi pada keamanan teks dengan menggunakan algoritma *affine cipher* dan algoritma *coloumnar transposition*, teks dapat diamankan dari orang – orang yang tidak berkepentingan. Proses pengamanan teks dengan mengkombinasikan algoritma *affine cipher* dan algoritma *coloumnar transposition* bertujuan agar mempersulit analisis sandi. Perancangan aplikasi

dengan *visual basic studio* 2008 bertujuan untuk mengimplementasikan hasil enkripsi dan dekripsi untuk keamanan teks[5].

A. Sistem

Sistem yaitu dari bahasa Inggris yang disebut dengan *system*, arti sistem sendiri yaitu susunan, misalnya apa yang terkandung dalam kata sistem sensorik menyiratkan sistem sensorik, kerangka kerja jaringan menyiratkan tindakan jaringan, dll. Sistem diartikan sebagai sekelompok kumpulan komponen yang terhubung dan terkait satu sama lain dan masing-masing membentuk satu kesatuan yang utuh. [6].

B. Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. *Kriptografi* adalah ilmu pengetahuan dan seni menjaga *message* agar tetap aman. Tujuan penerapan *kriptografi* adalah untuk membuat sesuatu yang tersembunyi, dapat suatu pesan rahasia berupa teks, suara, gambar dan video. [7]

C. Metode Rivest Shamir Aldeman

Algoritma Rivest Shamir Aldeman (RSA) adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah *algoritma* pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk *enkripsi* (*encryption*) dan salah satu penemuan besar pertama dalam *kriptografi* kunci publik. RSA masih digunakan secara luas dalam protokol-protokol keamanan *SSL/TLS*, *SET*, *SSH*, *S/MIME*, *PGP*, *DNSSEC*[8].

D. Metode Affine Cipher

Affine cipher adalah perluasan dari *caesar cipher*, yang menggalikan *plainteks* dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Secara matematis enkripsi *plainteks* P menghasilkan *cipherteks* C dinyatakan dengan fungsi kongruen[9].

E. Hyper Text Preprocessor (PHP)

PHP merupakan singkatan dari “*Hypertext Preprocessor*”. PHP adalah sebuah bahasa *scripting* yang terpasang pada HTML. Sebagai besar sintaknya mirip dengan bahasa pemrograman C, Java, ASP dan Perl ditambah beberapa fungsi PHP yang Spesifik dan mudah dimengerti. PHP digunakan untuk membuat tampilan *web* menjadi lebih dinamis, dengan PHP anda bisa menampilkan atau menjalankan beberapa *file* dalam 1 *file* dengan cara *include* dan *require*. PHP itu sendiri sudah dapat berinteraksi dengan beberapa *Database* walaupun dengan kelengkapan yang berbeda yaitu DBM, MySQL, *Oracle* [10].

F. MySQL

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL atau yang dikenal dengan DBMS (*Database management system*), *Database* ini *multithread*, *multi-user*. MySQL bersifat RDBMS (*Relational Database Management System*). MySQL bekerja dengan SQL Language (*Structure Query Language*) yang dapat diartikan bahwa MySQL merupakan standar penggunaan *Database* didunia untuk pengolahan data. Perintah yang sering digunakan dalam MySQL adalah *SELECT* (Mengambil), *INSERT* (Menambah), *UPDATE* (Mengubah), dan *DELETE* (Menghapus) [11].

G. Unified Modelling Language (UML)

UML merupakan singkatan dari *Unified Modeling Language* yang merupakan sekumpulan alat yang digunakan untuk melakukan abstraksi terhadap sebuah sistem atau perangkat lunak berbasis objek. UML juga menjadi salah satu cara untuk mempermudah pengembangan aplikasi yang berkelanjutan. Aplikasi atau sistem yang tidak terdokumentasi biasanya dapat menghambat pengembangan karena developer

harus melakukan penelusuran dan mempelajari kode program. UML juga dapat menjadi alat bantu untuk transfer ilmu tentang sistem atau aplikasi yang akan dikembangkan dari satu developer ke developer lainnya [12].

1. *Use case Diagram*

Use case diagram merupakan gambaran graphical dari beberapa atau semua aktor, *use case*, dan interaksi yang memperkenalkan suatu sistem. *Use case* secara sederhana sesungguhnya merupakan sebuah sarana bantu untuk mendefinisikan apa yang ada di luar sistem (aktor) dan apa yang harus dilakukan oleh sistem yang sedang dikembangkan.

2. *Activity Diagram*

Activity diagram merupakan diagram ini menggambarkan tentang aktifitas yang terjadi pada sistem. Dari pertama sampai akhir, diagram ini menunjukkan langkah – langkah dalam proses kerja sistem yang kita buat.

3. *Sequence Diagram*

Sequence diagram merupakan diagram yang menjelaskan interaksi objek yang berdasarkan urutan waktu. *Sequence diagram* dapat menggambarkan urutan atau tahapan yang harus dilakukan untuk dapat menghasilkan sesuatu seperti pada *use case diagram*.

4. *Class Diagram*

Ini mewakili hubungan antara kelas dan setiap kelas dalam model desain sistem, serta aturan dan tanggung jawab entitas yang menentukan perilaku sistem. Diagram kelas juga menunjukkan atribut dan operasi kelas, serta kendala yang terkait dengan objek yang terkait dengan kelas. Diagram kelas biasanya mencakup kelas (classes), hubungan, asosiasi, generalisasi dan agregat, atribut (atribut), operasi (operasi/metode), visibilitas, operasi, atau tingkat akses dari objek eksternal ke atribut. Hubungan antar kelas memiliki deskripsi yang disebut multiplicity atau kardinalitas.

2. METODE PENELITIAN

A. Pengumpulan Data

Berikut ini adalah beberapa teknik pengumpulan data yang peneliti lakukan untuk melengkapi bahan penelitian:

1. Penelitian Lapangan (*Field Research*)

Yaitu metode penelitian yang dilakukan dengan peninjauan langsung ke lokasi penelitian melalui langkah-langkah berikut :

- a. Pengamatan (*Observation*)

Melakukan pengamatan secara langsung ke tempat objek pembahasan yang ingin diperoleh yaitu bagian-bagian penting dalam pengambilan data seperti data karyawan.

- b. Wawancara (*Interview*)

Teknik ini digunakan secara langsung bertatap muka dengan pihak bersangkutan yaitu Zulkipli S.H. Selaku HRD untuk mendapatkan informasi serta data karyawan.

- c. Sample (*Sampling*)

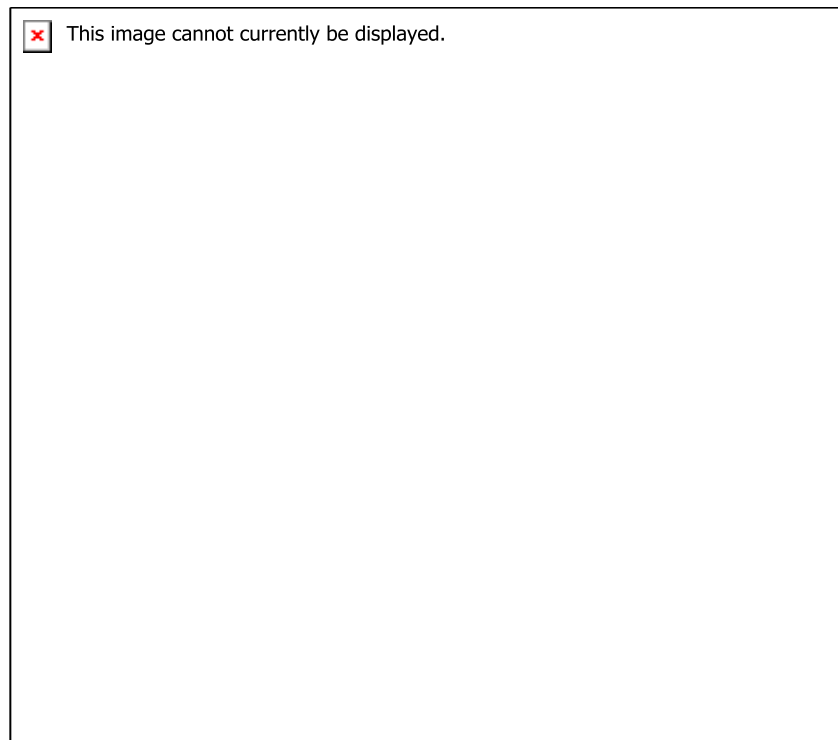
Yaitu meneliti dokumen apa yang dibutuhkan dalam pengambilan data yang sesuai dengan judul penulis yaitu menggunakan metode untuk merancang sistem keamanan data.

2. Metode Penelitian Pustaka (*Library Research*)

Pada teknik ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi. Bacaan yang dikutip dapat berupa teori atau pendapat dari beberapa bacaan. Hal ini dimaksudkan untuk memberikan landasan teori yang kuat melalui buku-buku, jurnal yang berhubungan dengan penulisan skripsi ini.

B. Metode Perancangan

Dalam metode penelitian ini digunakan teknik-teknik analisis, klasifikasi masalah, terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis buat. Langkah-langkah yang dilakukan penulis untuk mencapai tujuan perancangan ditunjukkan pada Gambar 1 berikut ini:



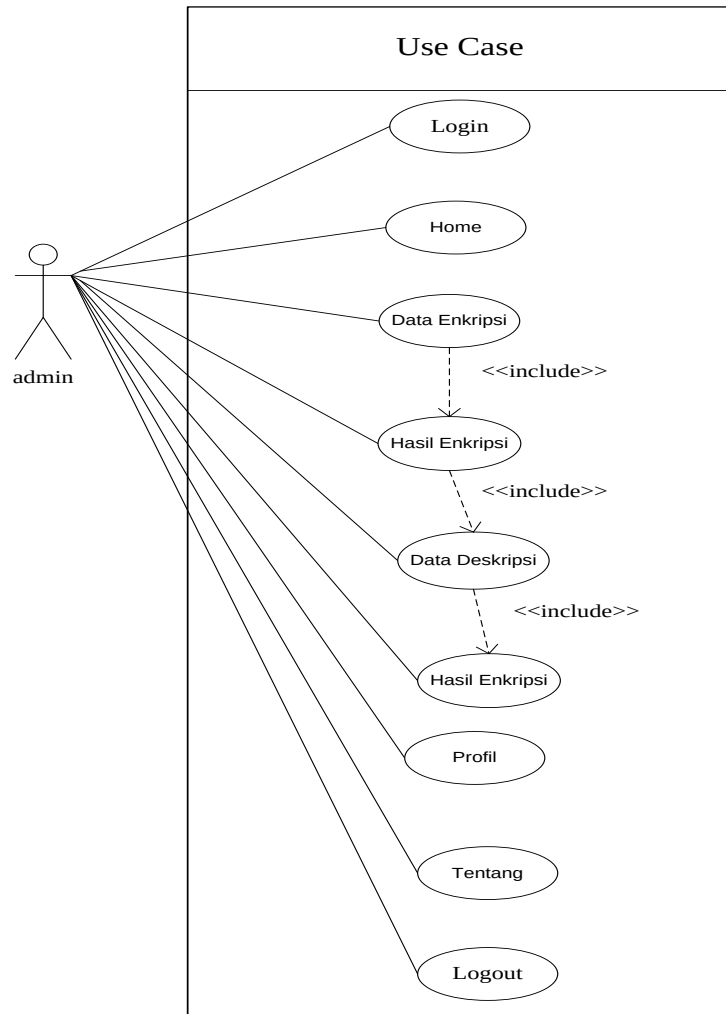
Gambar 1. Diagram *Waterfall*

3. HASIL DAN PEMBAHASAN

Perkembangan sistem keamanan sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Teknologi juga memberikan kemudahan untuk bertukar informasi sehingga keamanan data tidak dapat lepas dari berbagai aspek kegiatan manusia yang memungkinkan dapat menjaga kerahasiaan informasi tersebut, namun dalam implementasinya masih terdapat kecurangan dan ancaman terhadap data khususnya apada data keamanan karyawan Pada saat ini perusahaan belum memiliki aplikasi yang melakukan pengamanan data yang berguna untuk mengamankan data karyawan, sehingga kapan saja data karyawan bisa mengalami kebocoran atau hilang data diakibatkan oleh orang-orang yang tidak bertanggung jawab

A. *Desain Sistem*

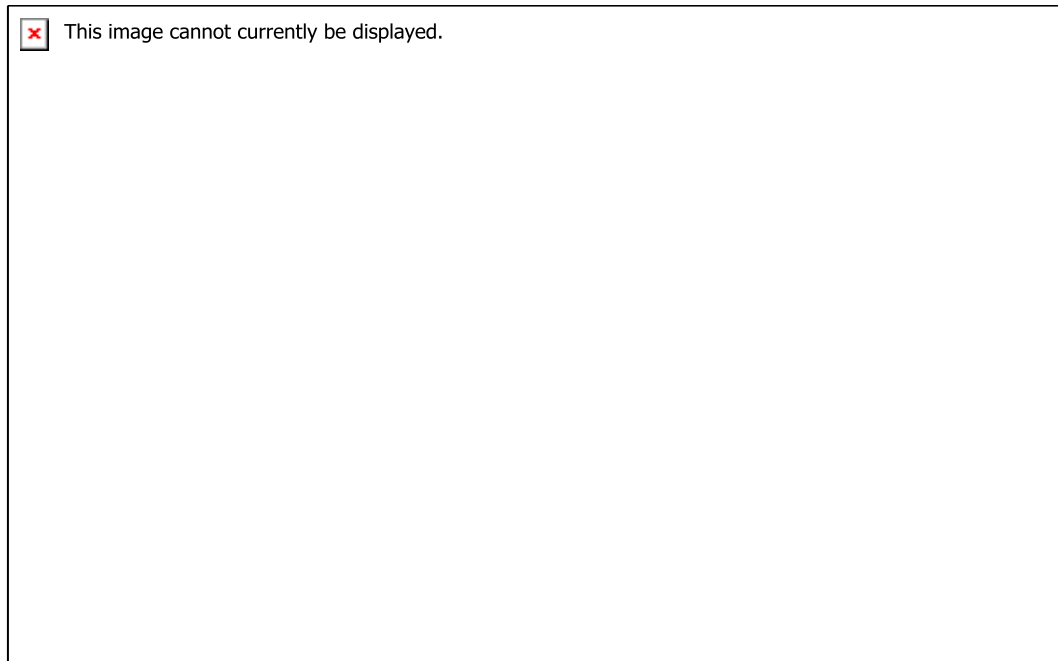
Desain sistem yang peneliti gunakan adalah pemodelan *Unified Modeling Language* (UML). Berikut ini adalah beberapa pemodelan *Unified Modeling Language* (UML) yang peneliti gunakan:



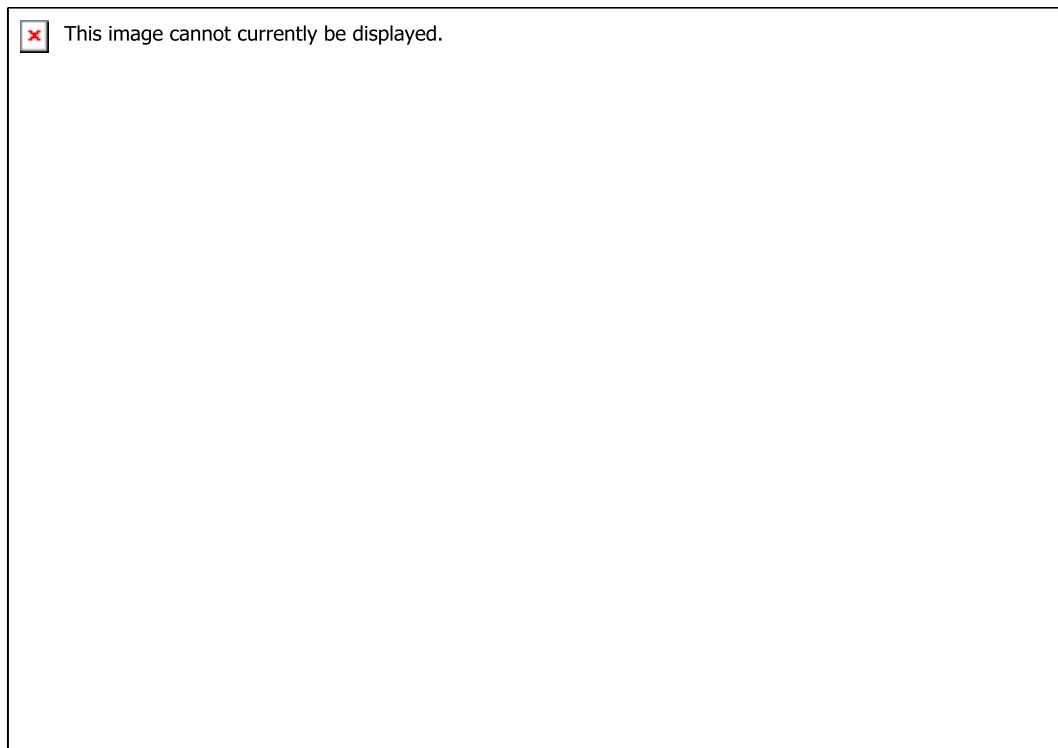
Gambar 4. Use Case Diagram

B. Tampilan Hasil

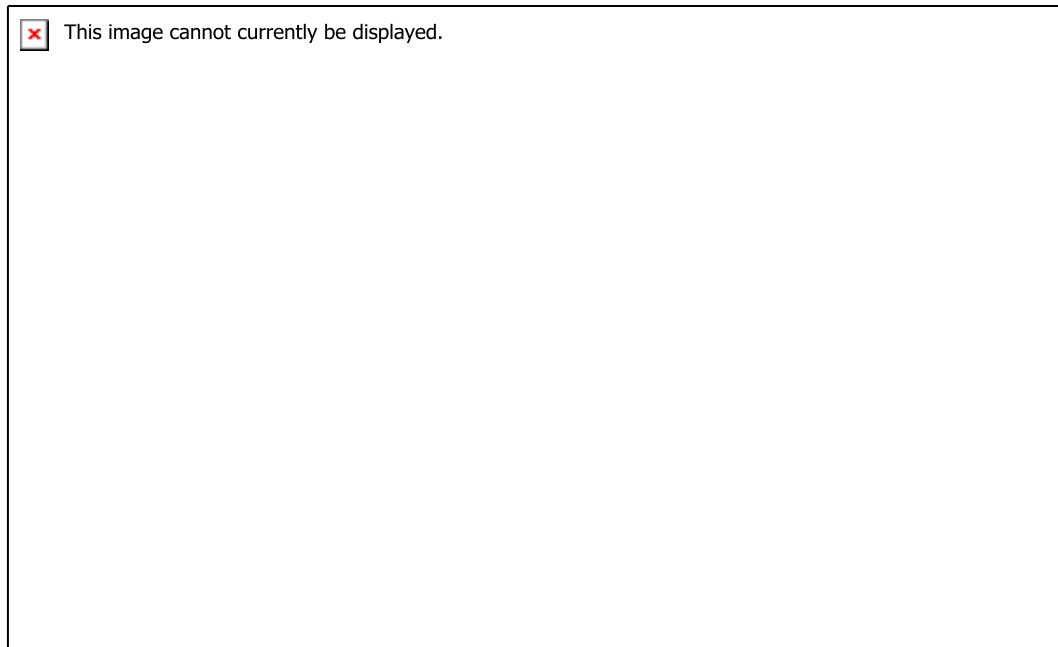
Tampilan hasil dari aplikasi Sistem informasi Eksekutif Data Alumni Pada Sekolah SMP Swasta Generasi Bangsa Martubung Menggunakan Metode EFS Berbasis Web dapat dilihat sebagai berikut:



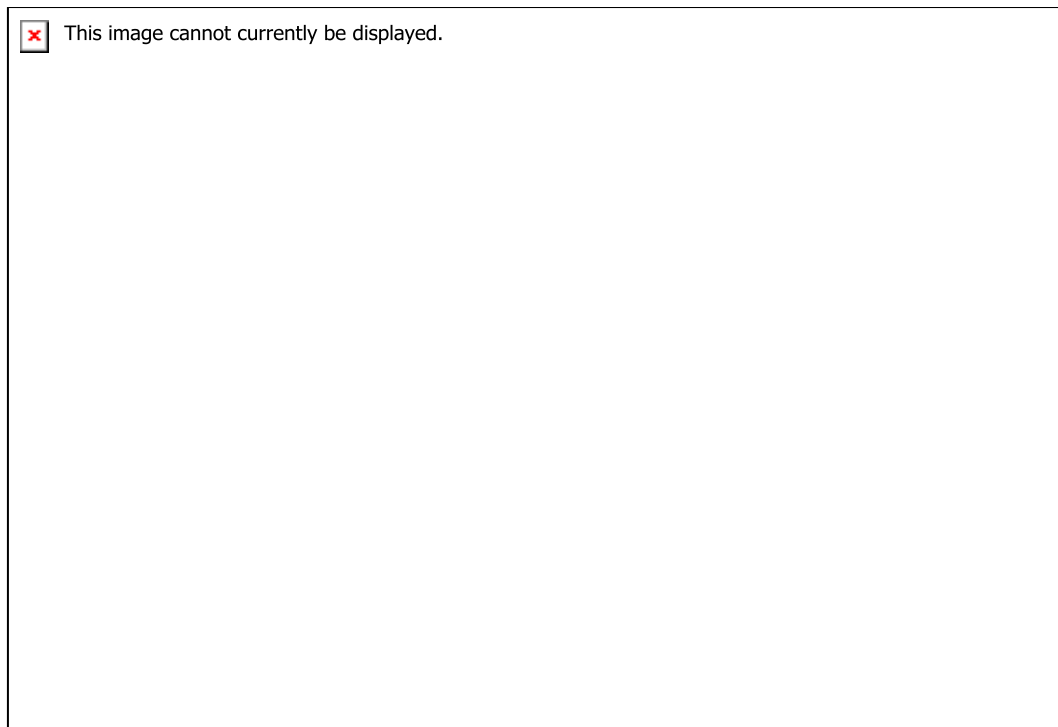
Gambar 5. Tampilan *Form Login*



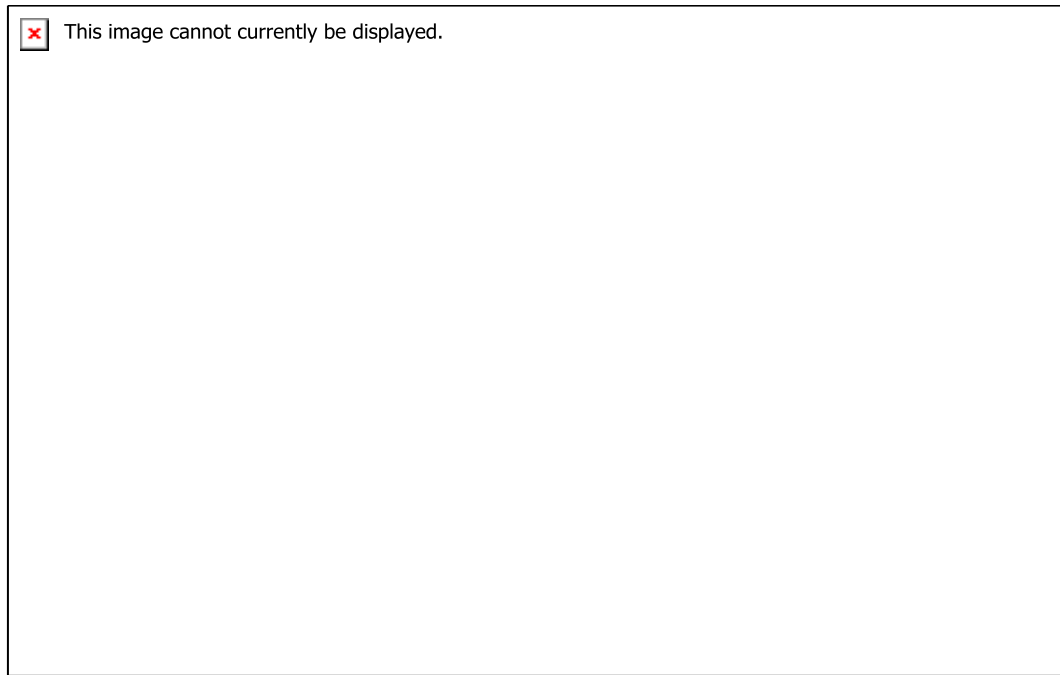
Gambar 6. Tampilan *Form Data Home*



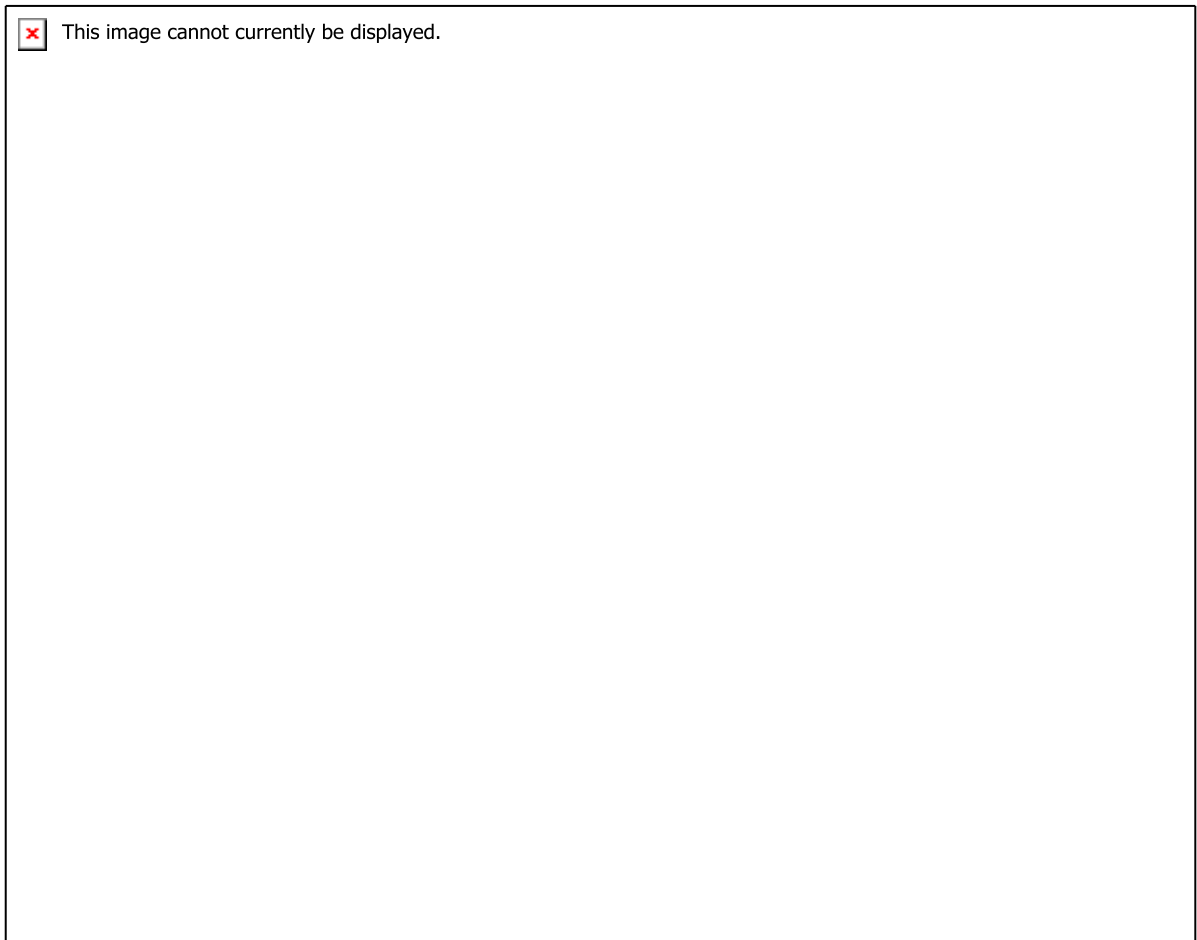
Gambar 7. Tampilan *Form Data Enkripsi*



Gambar 8. Tampilan *Form data Dekripsi*.



Gambar 8. Tampilan *Form* Data Ekripsi File



Gambar 9. Tampilan *Form Data Deskripsi***C. Skenario Pengujian**

Uji coba terhadap sistem bertujuan untuk memastikan bahwa sistem sudah berada pada kondisi siap pakai. Instrumen yang digunakan untuk melakukan pengujian ini yaitu dengan menggunakan *Blackbox Testing*:

Tabel 2. Skenario Pengujian *Admin (Black Box Testing)*

Form Uji	Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
Pengujian Login (Admin)			
Login	Memasukkan username dan password dengan benar	Sistem akan menerima akses login kemudian langsung menampilkan halaman admin	Valid
	Memasukkan Username dan Password dengan salah	Sistem akan menolak akses login dan akan muncul pesan pemberitahuan	Valid
Pengujian Data Enkripsi (Admin)			
Data Enkripsi	Pengujian aksi enkripsi data dengan mengklik tombol data	Sistem akan men enkripsi data setelah di klik tombol data	Valid
Pengujian Data Deskripsi (Admin)			
Data Deskripsi	Pengujian aksi Deskripsi data dengan mengklik tombol data	Sistem akan menampilkan hasil deskripsi data setelah di klik tombol data	Valid
Pengujian Data Enkripsi Fille (Admin)			
Data Enkripsi Fille	Komponen yang diuji adalah unduh file asli pada halaman data enkripsi	Data akan menampilkan data asli yang sudah di unduh	Valid
	Pengujian aksi download file data dengan megklik data download	Sistem akan menampilkan download file data yang sudah di download	Valid
	Pengujian aksi download file data dengan megklik data download	Sistem akan menampilkan download file data yang sudah di download	Valid

Pengujian Data Enkripsi Fille (Admin)			
Data Dekripsi Fille	Komponen yang diuji adalah tambah data pada halaman data	Data yang di klik akan tampil pada halaman data	Valid
	Pengujian aksi hapus data dengan mengklik tombol hapus	Sistem akan menghapus data setelah di klik tombol hapus	Valid
	Pengujian aksi		

Setelah dilakukan tahap uji sistem maka penulis mengetahui apakah aplikasi yang dibuat sesuai dengan hasil yang diharapkan. Dimana dari hasil pengujian menggunakan metode *black box* penulis dapat mengambil kesimpulan bahwa hasil *output* sistem sesuai dengan yang diharapkan dan setiap menu yang dijalankan *valid*.

D. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

Adapun kelebihan sistem yang telah dibuat diantaranya yaitu:

1. Tampilan sistem yang menarik dan mudah dipahami
2. Data-data yang disimpan ada database dapat ditambah,edit dan hapus langsung dari aplikasi oleh admin tanpa harus mengubah database

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu:

1. Fitur dalam aplikasi masih terbatas, sehingga kedepannya dibutuhkan pengembangan aplikasi agar lebih menarik, efektif dan efisien.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama sistem pendukung keputusan pemilihan berbasis web untuk pengamanan file (isi file) dengan menggunakan algoritma affine cipher dan rsa dapat ditarik kesimpulan sebagai berikut:

1. Kombinasi affine cipher dan algoritma rsa dapat membantu meningkatkan data, jika dibandingkan dengan hanya menggunakan satu metode saja. Menggunakan perhitungan dengan struktur alphabetis dan dipadukan dengan menggunakan memfaktoran bilangan prima dapat meningkatkan sistem keamanan data, sehingga data yang tersimpan akan semakin terjaga.
2. Dalam proses pembuatan aplikasi berbasis web yang baru dapat diketahui bahwa untuk pengamanan file (isi file) yang baik, tahap-tahap yang perlu dilakukan adalah dengan mempelajari sistem yang ada, kemudian mendesain sistem dan melakukan perhitungan dengan kriteria-kriteria pemilihan.
3. Dengan adanya sistem ini maka akan sangat membantu untuk pengamanan file (isi file) dalam pengamanan suatu file

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberi dukungan terhadap penelitian ini.

REFERENSI

- [1] Fuad, R. N., & Winata, H. N. (2017). Aplikasi keamanan *file audio wav (waveform)* dengan terapan algoritma RSA. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 1(2), 113-119.
- [2] Santoso, H., & Fakhriza, M. F. M. (2018). Perancangan aplikasi keamanan *file audio format wav (waveform)* menggunakan algoritma RSA. *Algoritma: Jurnal Ilmu Komputer Dan Informatika*, 2(1).
- [3] Damanik, M. A., & Buulolo, E. (2017). Penerapan Algoritma *Triple Transposition Vigenere Cipher* Dan *Algoritma RSA* Dalam Keamanan Login. *Informasi dan Teknologi Ilmiah (INTI)*, 5(1), 76-80.
- [4] Prasetyo, Y., & Triandi, B. (2018). Perancangan Aplikasi Pengamanan *File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA* *Designing Application for Safeguarding Text Files with Hybrid Schemes Using Enigma Algorithms and RSA Algorithms*. 46. *IT J*, 6(1), 2252-746.
- [5] Siregar, I. M. (2019). Penerapan *Algoritma Affine Cipher* Dan *Algoritma Coloumnar Transposition* Dalam Keamanan Teks. *Jurnal Informatika Kaputama (JIK)*, 3(1), 6-12