PERANCANGAN APLIKASI KRIPTOGRAFI PADA DOKUMEN PENGARSIPAN DENGAN MENGGUNAKAN ALGORITMA *TRIPLE* DES BERBASIS WEB

Bagas Putra Pratama[1], Wasis Haryono[2]

[1]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang,Jl. Surya Kencana No.1, Pamulang – Tanggerang Selatan, 15417, Indonesia
e-mail: [1]bagasputrapratama18@gmail.com

[2]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang,Jl. Surya Kencana No.1, Pamulang – Tanggerang Selatan, 15417, Indonesia
e-mail: [2]wasish@unpam.ac.id

Abstract

Along with the rapid development of technology and communication, it will be easier for us to exchange data quickly. But sometimes the security of the data exchange is less realized by us. Lack of safeguarding the security aspect in terms of data exchange has one of the impacts of negative developments in technological development, namely data theft, data theft is one of the problems most feared by communication networks. With data theft, safeguarding security aspects in information exchange and data storage is considered important. Security is needed because a lot of data is confidential and cannot be changed by parties who do not have the right to change it.For secure these data files, cryptography can be used. Therefore, users of data files need assistance for the security of the data files they store. In this case a security system is needed to secure confidential document files. For this reason, a document archiving, security system was designed. The security system design process is carried out using the Triple DES algorithm with the PHP programming language. With this web-based document security system, a system is designed that can perform all data security, search, and download processes that are processed through a web-based application.So that security, searching and downloading archives can be done easily, and in the end it can produce a proper security system.

Keywords: Cryptography, Archives, Triple DES,PHP.

Abstrak

Seiring dengan perkembangannya teknologi dan komunikasi yang begitu pesat, akan memudahkan kita untuk melakukan pertukaran data secara cepat. Namun terkadang keamanan penukaran data tersebut kurang disadari oleh kita. Kurangnya penjagaan aspek keamanan dalam hal pertukaran data tersebut memiliki salah satu dampak perkembangan negatif dalam perkembangan teknologi yaitu ada pencurian data, pencurian data merupakan satu masalah yang paling ditakuti oleh jaringan komunikasi. Dengan adanya pencurian data maka penjagaan aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting. Keamanan sangat dibutuhkan karena banyak data yang bersifat rahasia dan tidak bisa dirubah oleh pihak yang tidak berhak untuk merubahnya.Untuk mengamankan *file* data tersebut maka dapat menggunakan kriptografi. Oleh karena itu, pengguna *file* data membutuhkan bantuan untuk keamanan *file* data yang disimpannya. Dalam hal ini sistem keamanan diperlukan untuk mengamankan *file* dokumen yang bersifat rahasia. Untuk itu dibuatlah perancangan sistem keamanan dokumen pengarsipan. Proses perancangan sistem keamanan ini dilakukan dengan menggunakan algoritma *Triple* DES dengan bahasa pemrograman PHP. Dengan adanya sistem keamanan dokumen berbasis web ini, maka dirancang sebuah sistem yang dapat melakukan semua proses keamanan data, pencarian, pengunduhan yang diproses melalui aplikasi berbasis web. Sehingga keamanan, pencarian dan pengunduhan arsip bisa dilakukan dengan mudah, dan pada akhirnya bisa menghasilkan suatu sistem keamanan yang tepat.

Kata kunci : Kriptografi, Arsip, *Triple* DES, PHP.

1. PENDAHULUAN

Seiring dengan perkembangannya teknologi dan komunikasi yang begitu pesat, akan memudahkan kita untuk melakukan pertukaran data secara cepat. Namun terkadang keamanan penukaran data tersebut kurang disadari oleh kita. Kurangnya penjagaan aspek keamanan dalam hal pertukaran data tersebut memiliki salah satu dampak perkembangan negatif dalam perkembangan teknologi yaitu ada pencurian data, pencurian data merupakan satu masalah yang paling ditakuti oleh jaringan komunikasi. Dengan adanya pencurian data maka penjagaan aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting.

Keamanan sangat dibutuhkan karena banyak data yang bersifat rahasia dan tidak bisa dirubah oleh pihak yang tidak berhak untuk merubahnya. Untuk mengamankan file data tersebut maka dapat menggunakan kriptografi. Oleh karena itu, pengguna filedata membutuhkan bantuan untuk keamanan file data yang disimpannya.

PT. Herysapta Contultant adalah perusahaan yang bergerak dalam bidang Konsultan Pajak dan Akuntansi hasil survey sementara peneliti mendapatkan bahwa PT. Herysapta Consultant menghasilkan kurang lebih 111 dokumen dari berbagai jenis atau pola dokumen setiap bulannya. Atas hal tersebut peneliti meneliti, mengambil sampel pendataan, pencatatan arsip dan dilakukan survey pada PT. Herysapta Consultant di Jl. Raya Nusantara Anyelir 6 No.115 Depok, Pancoran Mas Kota Depok, Jawa Barat.

Setelah dilakukan proses survey awal terhadap penataan arsip, peneliti menemukan bahwa proses pengolahan arsip yang dilakukan oleh PT. Herysapta masih dilakukan secara copy file dari folder ke folder, yang menimbulkan permasalahan seperti tidak adanya sistem yang membatasi hak akses user, susah mencari data, tidak ada keamanan pada dokumen, serta belum adanya keamanan yang menggunakan algoritma kriptografi.

2. PENELITIAN YANG TERKAIT

Adapun peneliti terkait menggunakan kritografi Triple DES untuk mengamankan dokumen. Dalam penulisan, peneliti menggunakan referensi tinjauan pustaka yang berhubungan dengan kegiatan ini. Referensi yang digunakan sebagai sumber informasi peneliti ini di dapat dari materi kuliah, jurnal, beberapa penulisan dan karya ilmiah yang berkaitan dengan pembahasan pada penelitian ini adalah ”Perancangan Aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple DES Berbasis Web”**.** Adapun referensi atau jurnal pendukung sebagai berikut :

Penelitian ini dilakukan oleh Joko Susanto [1] (Universitas Tanjungpura, 2016) yang berjudul **“Aplikasi Enkripsi Dan Dekripsi Untuk Keamanan Dokumen Menggunakan Triple DES Dengan Memanfaatkan USB Flash Drive”** yang membahas tentang keamanan dan kerahasiaan data dan informasi pada teks dokumen dengan menggunakan metode *Triple* DES dengan tujuan untuk mengamankan dokumen menggunakan USB agar tidak bisa dibaca oleh pihak luar (ISSN : 2338-493XVolume 04, No.2 2016).

Penelitian ini dilakukan oleh Zahrul Basim (Universitas Budi Luhur, 2020) yang berjudul [3]**“Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su’udiyyah”** yang membahas tentang keamanan dokumenfilepada SMK As-Su’udiyyah degan menggunakan Algoritma RC4 Dan 3DES dengan tujuan untuk mengamankan data rahasia SMK As-Su’udiyyah dari pihak yang tidak bertanggung jawab dengan membuat aplikasi pengamanan data menggunakan metode kriptografi dan steganografi (ISSN : 2721-4788VOLUME 3, NO 4, JULI 2020).

Penelitian ini dilakukan oleh Elvara Delfriantina Saragih [2] (STMIK Budi Darma, 2018) yang berjudul **“Implementasi Algoritma *Triple* DES Dan Algoritma Advances Encryption Standard Dalam Penyandian *File* Teks”** yang membahas tentang Yang membahas mengenai penyandian keamanan *file* teks dengan menggunakan algoritma *Triple* DES dan AES dengan tujuan untuk meningkatkan keamanan file agar tidak bisa dimengerti oleh orang yang tidak diizinkan untuk mengakses file tersebut(ISSN 2339-210XVolume 6, Nomor 1, Oktober 2018).

3. METODE PENELITIAN

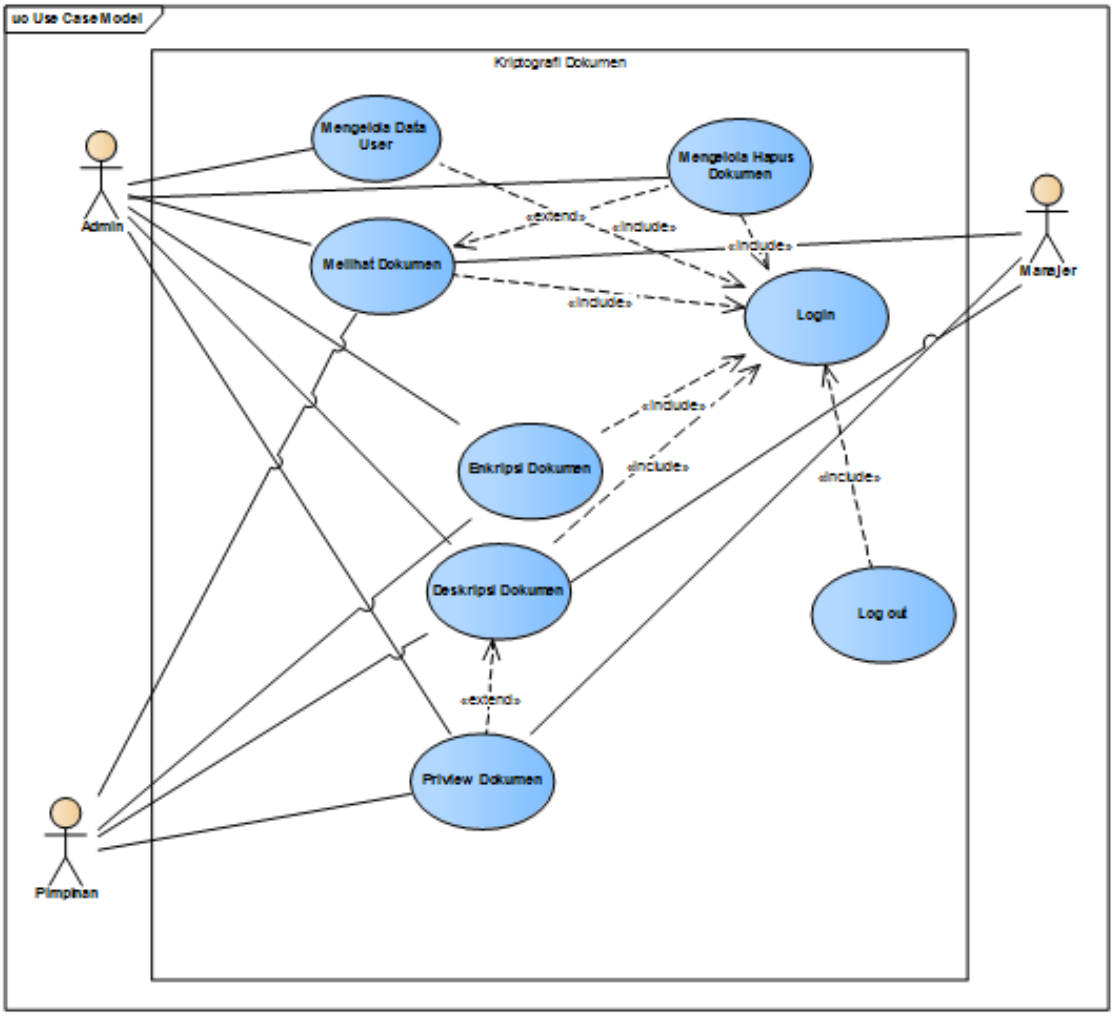
Metodologi yang digunakan adalah metode observasi yang melakukan pengenalan atau penelitian langsung dari objek yang sedang berjalan, studi pustaka yang mempelajari teori-teori yang berkaitan dengan penulisan melalui buku-buku atau jurnal penelitian ilmiah dan wawancara guna untuk mendapatkan data-data

atau permasalahan yang sedang dialami ditempat tersebut.

a. Pengumpulan Data
   Pengumpulan data diambil dari sumber buku dan jurnal serta sumber-sumber lain yang tercantum pada daftar pustaka
b. Wawancara
   Melakukan proses wawancara guna untuk mengetahui permasalahan yang sedang terjadi di PT.Herysapta Consultant.
c. Analisa Sistem Berjalan
   a) Admin mendapatkan dokumen.
   b) Karyawan menyelesaikan perhitungan pajak.
   c) Karyawan menyimpan dokumen berdasarkan nama klien dan jenis dokumen.
   d) Karyawan print dokumen untuk arsip hardcopynya.
   e) Admin melakukan pengecekan berkala.
d. Analisa Sistem Usulan
   a) Dokumen yang tersimpan akan dienkripsi oleh sistem dengan algoritma Triple DES.
   b) Ekstensi dokumen akan berubah menjadi .rda setelah dokumen terenkripsi.
   c) Dokumen tidak dapat dipreview setelah dienkripsi kedalam sistem jika dokumen belum dideskripsi kembali.
   d) Dokumen tidak dapat dibaca walaupun pengguna merubah ekstensinya secara manual.
   e) Aktor yang dapat mengakses aplikasi ini ada 3 (tiga) yaitu admin, pimpinan dan manajer.

Dibawah ini adalah gambaran sistem usulan yang akan di implementasikan pada proses enkripsi dokumen yang akan diterapkan di PT.Herysapta Consultant :

a. Use Case Diagram
   Berikut adalah use case diagram kriptografi :

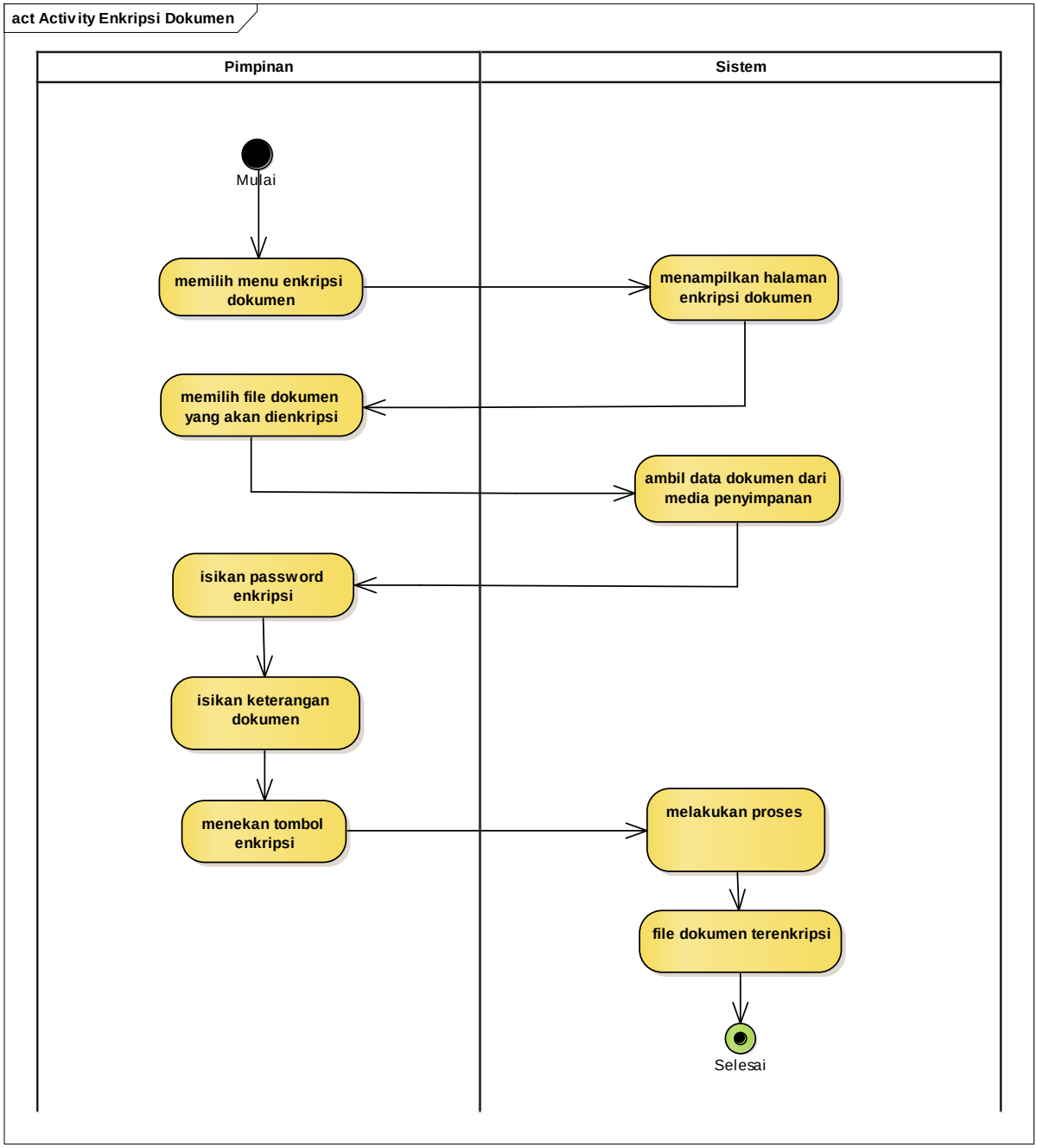


Gambar 1 Use Case Diagram Kriptografi

Keterangan :

Gambar diatas merupakan use case diagram kriptografi yang dimana ada admin, pimpinan dan manajer. Dimana admin dapat mengelola data user, admin dapat mengelola hapus dokumen, admin dapat melihat dokumen, admin dapat mengenkripsi dokumen, admin dapat mendeskripsi dokumen dan admin dapat melihat dokumen. Lalu pimpinan juga dapat melihat dokumen, pimpinan dapat mengenkripsi dokumen, pimpinan dapat mendeskripsi dokumen dan pimpinan juga dapat mempreview dokumen. Kemudian manajer dapat melihat dokumen, manajer dapat mendeskripsi dokumen dan manajer juga dapat melihat dokumen.

b. Activity Diagram Enkripsi Dokumen

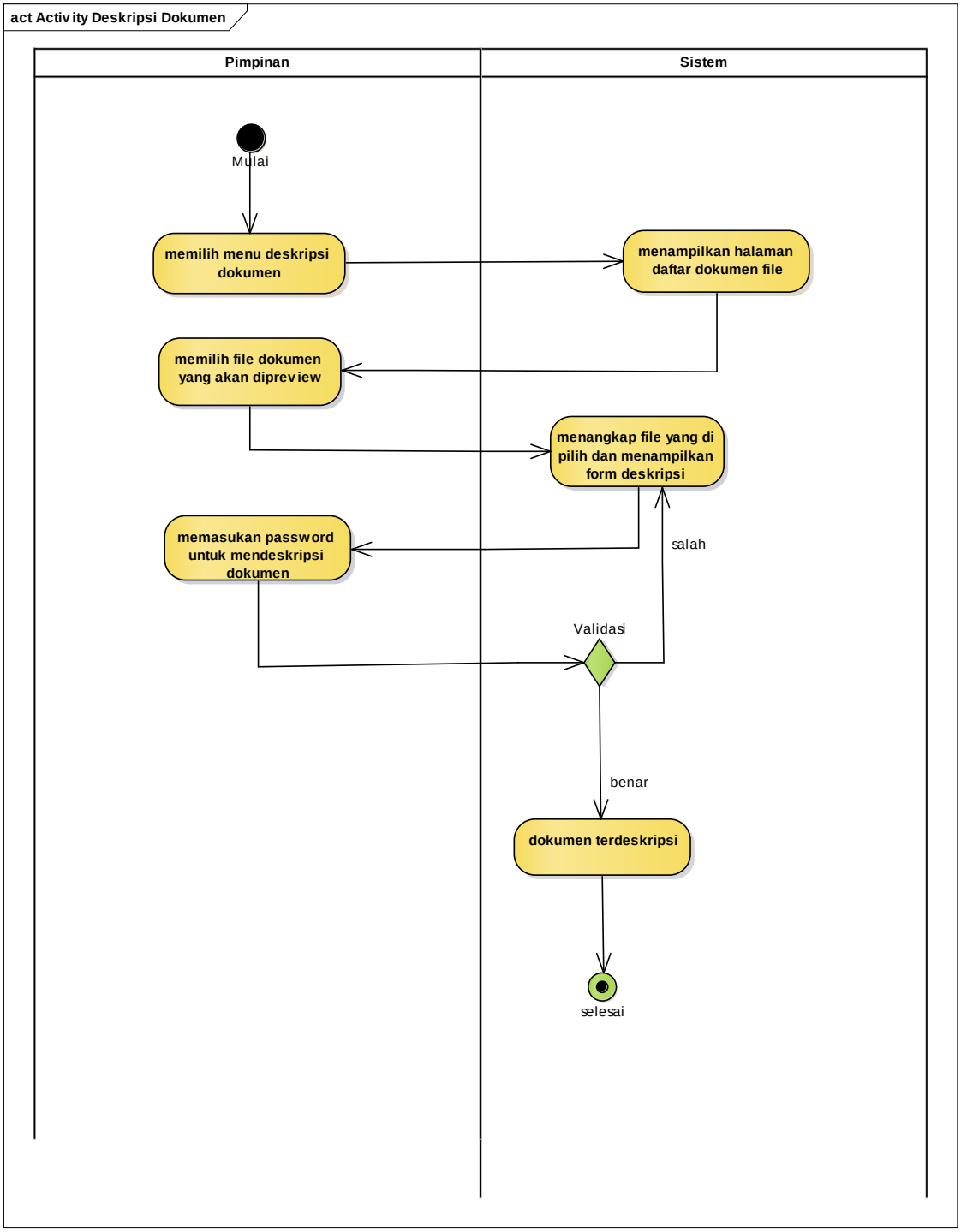


Gambar 2 Activity Diagram Enkripsi Dokumen

Keterangan :

Gambar diatas menjelaskan aktivitas diagram proses enkripsi dokumen pada aplikasi yang akan dibuat. Dimulai oleh admin yang melakukan pilih menu enkripsi lalu sistem menampilkan halaman enkripsi kemudian admin memilih file dokumen yang akan dienkripsi lalu sistem akan mengambil data dokumen dari media penyimpanan, admin mengisi password enkripsi dan keterangan dokumen lalu sistem akan mengenkripsi dokumen dan selesai.

c. Activity Diagram Deskripsi Dokumen



Gambar 3 Activity Diagram Deskripsi Dokumen

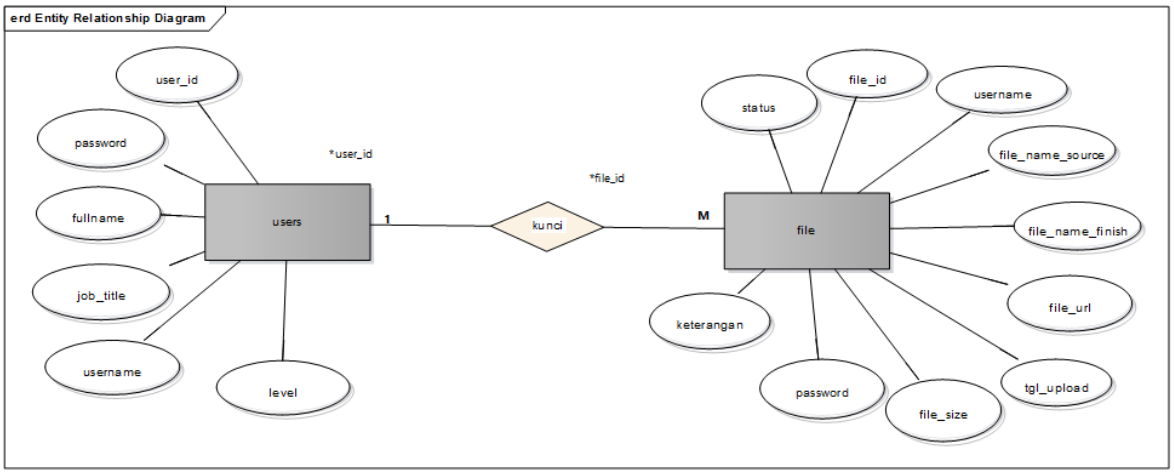
Keterangan :

Gambar diatas menjelaskan aktivitas diagram proses Deskripsi dokumen pada aplikasi yang akan dibuat. Dimulai oleh admin yang memilih menu deskripsi dokumen, lalu sistem akan menampilkan halaman deskripsi dokumen, admin memilih file dokumen yang akan dideskripsi lalu sistem akan menampilkan form deskripsi dokumen, admin memasukan password untuk mendeskripsi dokumen, jika password salah maka sistem akan mengembalikan kehalaman deskripsi dokumen, jika benar sistem akan mendeskripsi dokumen.

d. Perancangan Basis Data

Perancangan basis data adalah proses untuk menentukan dan mengatur data yang dibutuhkan untuk mendukung suatu rancangan sistem.

1) ERD (Entitas Relationship Diagram)

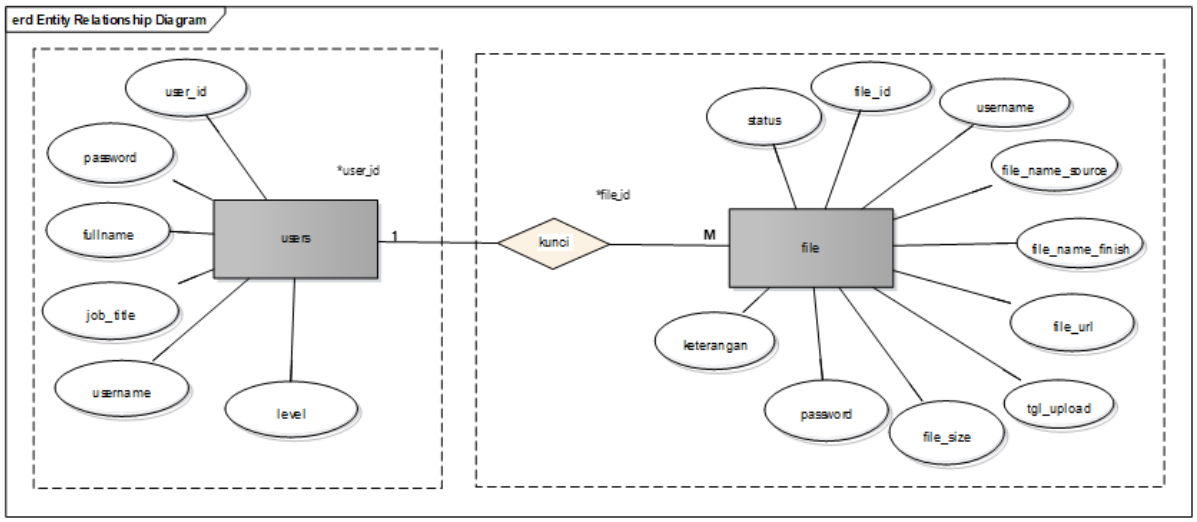


Gambar 4 Entitas Relationship Diagram Kriptografi

Keterangan:

Gambar diatas merupakan ERD (Entity Relationship Diagram) yang digunakan untuk merancang suatu basis data. Dimana digambar tersebut terdapat 2 entitas yaitu users dan file, masing-masing entitas mempunyai atribut, entitas users mempunyai atribut user_id, password, fullname, job_title, username dan level lalu entitas file mempunyai atribut status, file_id, username, file_name_source, file_name_finish, file_url, tgl_upload, file_size, password dan keterangan.

2) Transformasi ERD ke LRS

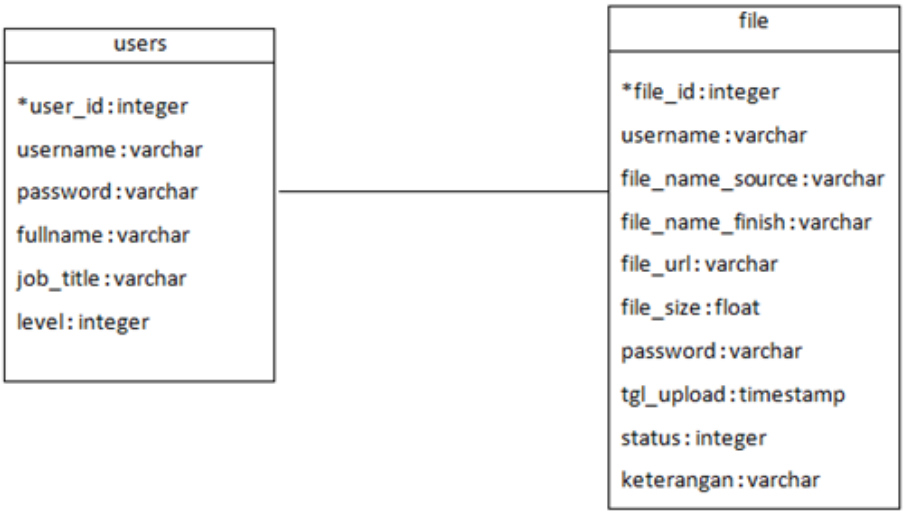


Gambar 5 Transformasi ERD ke LRS Kriptografi

Keterangan :

Gambar diatas adalah gambar dari transformasi ERD ke LRS yang membentuk data-data dari diagram hubungan entitas ke suatu LRS.

3) LRS (Logical Record Structure)



Gambar 6 Logical Record Structure Kriptografi

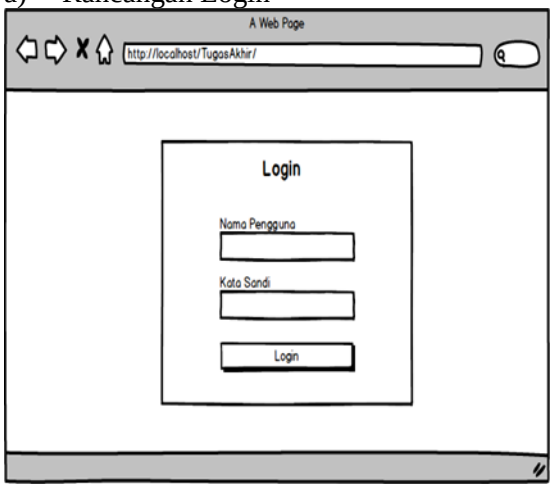
Keterangan :

Gambar diatas merupakan LRS (Logical Record Structure) adalah objek yang ditangkap dari struktur record-record pada tabel yang terbentuk dari relasi antar himpunan entitas.

e. Rancangan Antar Muka

Berikut adalah rancangan antar muka yang sudah penulis rancang dan dibuat :

a) Rancangan Login



Gambar 7 Mockup Login

Keterangan :

Gambar diatas merupakan rancangan antar muka Login, yang dimana admin, pimpinan dan manajer harus login dahulu sebelum melakukan proses enkripsi dan deskripsi.

b) Rancangan Enkripsi Dokumen

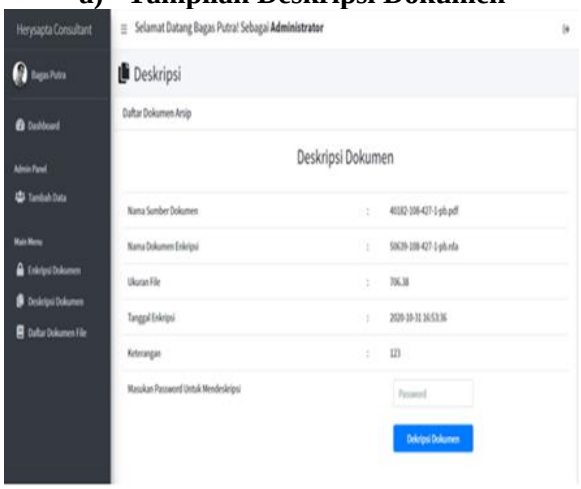
Gambar 8 Tampilan Enkripsi Dokumen

Keterangan :

Gambar diatas adalah tampilan enkripsi dokumen, admin, pimpinan dan manajer memilih menu enkripsi dokumen, lalu memilih file dokumen yang ingin dienkripsi dimedia penyimpanan, kemudian memasukan password atau key, lalu isi keterangan dan

tekan tombol enkripsi. Dan sistem akan memberikan persan dokumen berhasil terenkripsi.

a) Tampilan Deskripsi Dokumen

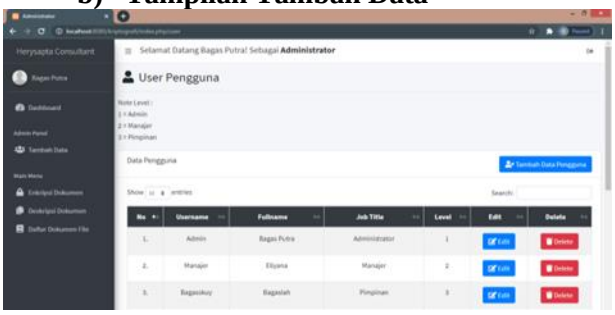


Gambar 9 Tampilan Deskripsi Dokumen

Keterangan :

Gambar diatas adalah tampilan deskripsi dokumen, admin, pimpinan dan manajer memilih menu, daftar dokumen kemudian memilih file dokumen yang akan dideskripsi lalu sistem akan mengarahkan ke form deskripsi, kemudian admin, pimpinan dan manajer mengisikan password atau key yang sesuai saat mengenkripsi dokumen, jika password valid maka deskripsi dokumen berhasil dan jika tidak berhasil maka harus memasukkan ulang password atau key dengan benar.

b) Tampilan Tambah Data



Gambar 10 Tampilan Tambah Data

Keterangan :

Gambar diatas adalah tampilan tambah data yang bisa diakses oleh admin, admin memilih menu tambah data kemudian admin akan ditampilkan halaman tambah data dimana terdapat data user yang ada didalam tabel dan terdapat 2 tombol edit dan delete.

4. HASIL DAN PEMBAHASAN

a. Hasil Pengujian BlackBox

Dibawah ini adalah pengujian black box yang telah penulis buat, dimana terdapat login, menu tambah data pengguna, menu edit data pengguna, menu delete data pengguna, menu enkripsi dokumen, menu deskripsi dokumen, menu daftar dokumen file, menu daftar dokumen file delete.

Tabel 4.1 Black Box Testing

No	Detail Uji	Keterangan
1	*Login*	*Valid*
2	Menu Tambah Data Pengguna	*Valid*
3	Menu *Edit* Data Pengguna	*Valid*
4	Menu *Delete* Data Pengguna	*Valid*
5	Menu Enkripsi Dokumen	*Valid*
6	Menu Deskripsi Dokumen	*Valid*
7	Menu Daftar Dokumen *File*	*Valid*
8	Menu Daftar Dokumen *FileDelete*	*Valid*

Keterangan :

Tabel diatas merupakan tabel dari black box testing yang dimana terdapat 8 halaman yang telah diuji, jika pengujian dinyatakan berhasil maka keterangannya adalah valid.

b. Hasil Kuesioner

Berikut adalah hasil kuesioner yang sudah penulis berikan kepada 3 aktor yaitu, admin, pimpinan perusahaan dan manajer yang bertempat di PT.Herysapta Consultant tanggal 23-November-2020 dan hasilnya dapat disimpulkan didalam tabel dibawah ini :

Tabel 4.2 Kuesioner Keseluruhan

Penilaian	Jumlah	Skor	Jumlah x Skor
Sangat Setuju(5)	21	5	105
Setuju(4)	33	4	132
Cukup(3)	30	3	90
Tidak Setuju(2)	5	2	10
Sangat Tidak Setuju(1)	0	1	0
Total			337

kuesioner yang sudah diisi oleh beberapa aktor diantaranya admin, pimpinan dan manajer. Perhitungan hasil kuesioner dapat dijelaskan pada rumus dibawah ini :

Skor maksimal = jumlah responden x jumlah soal x 5

Admin : 1 x 33 x 5 = 165
Pimpinan : 1 x 23 x 5 = 115
Manajer : 2 x 17 x 5 = 170

Total : 165 + 115 + 170 = 450
Persentase :337 / 450 x 100%
Hasil : 74,88%

Berdasarkan hasil kuesioner yang telah penulis berikan ke3aktor (admin, pimpinan dan manajer) yang telah mengisi kuesioner tersebut, dapat disimpulkan bahwa Perancangan Aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple DES Berbasis Web (Studi Kasus : PT.Herysapta Consultant) memiliki nilai 74,88% **(BAIK)**dari skala 100% (sangat tinggi) dianggap layak dan dapat bermanfaat untuk mengamankan file dokumen pengarsipan pada PT.Herysapta Consultant.

5. KESIMPULAN

Dengan membuat aplikasi kriptografi dokumen pengarsipan ini dapat membantu pihak perusahaan khususnya admin dan pihak-pihak yang terlibat antara lain pimpinan perusahaan dan manajer yang dapat mengoperasikannya, dan penulis dapat menyimpulkan bahwa :

a. Aplikasi ini dapat menjadi solusi dalam melalukan proses keamanan sistem yang membatasi hak akses *user* terhadap sistem.
b. Aplikasi ini dapat menjadi solusi dalam melakukan proses pengamanan dokumen pengarsipan.
c. Aplikasi ini dapat menjadi solusi dalam sistem keamanan dokumen karena sudah menggunakan algoritma kriptografi.

UCAPAN TERIMAKASIH

Ucapan terima kasih penulis berikan kepada pihak yang membantu penulis ataupun memberikan dukungan terkait dengan penelitian yang dilakukan seperti bantuan fasilitas penelitian, support keluarga dan teman-teman yang sudah membantu.

DAFTAR PUSTAKA

[1] Susanto, J., & Ilhamsyah, T. R. 2016. APLIKASI ENKRIPSI DAN DEKRIPSI UNTUK KEAMANAN DOKUMEN MENGGUNAKAN TRIPLE DES DENGAN MEMANFAATKAN USB FLASH DRIVE. *Jurnal Coding, Sistem Komputer Untan Volume 04, No.2*,1-12.
[2] Saragih, E. D., Hasibuan, N. A., & Bu'ulolo, E. 2018. IMPLEMENTASI ALGORITMA TRIPLE DES DAN ALGORITMA ADVANCED ENCRYPTION STANDARD DALAM PENYANDIAN FILE TEKS. *Jurnal Majalah Ilmiah INTIVolume 6, Nomor 1,* 1-7.
[3] Basim, Z., & Painem, P. 2020. Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah. *Jurnal SKANIKAVOLUME 3, NO 4*,1-8.
[4] Delimayanti, M. K., & Sudirko, D. 2015. Perancangan dan Realisasi Aplikasi Berbasis Web untuk Enkripsi dan Dekripsi Data dengan Algoritma 3DES dan Twofish.
[5] Kartika, K. H.PERANCANGAN SISTEM KRIPTOGRAFI PADA DOCUMENT MENGGUNAKAN ALGORITMA TRIPLE DES DAN RSA.*Jurnal Inteksis STIMIK Widya Dharma.*
[6] M. Niki Ratama, "Perancangan Sistem Informasi Sosial Learning Untuk Mendukung Pembangunan Kota Tangerang Dalam Meningkatkan Smart city Berbasis Android," SATIN - Sains dan Teknologi Informasi, vol. 5, 2019.
[7] N. R. Munawaroh, "Penerapan Teknologi Augmented reality Pada Matakuliah Pengantar Teknologi Informasi Di Universitas Pamulang Berbasis Android," SATIN - Sains dan Teknologi Informasi, vol. 5, 2019.