

Implementasi Algoritma *Advance Encryption Standard* (AES) Pada Keamanan Dokumen Keuangan (Studi Kasus : CV.Multikreasi Bersama)

Apriliana Tumanggor¹, Humuntal Rumapea², Arina Silalahi³
^{1,2,3}Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

Histori Artikel:

Received, mar, 2021
Revised, sep, 2022
Accepted, nov, 2022

Keywords:

Keamanan dokumen,
kriptografi,
AES-128

ABSTRAK

Perkembangan teknologi saat ini sangat mempengaruhi kehidupan manusia dalam setiap kegiatannya. CV. Multi Kreasi Bersama merupakan suatu perusahaan yang bergerak dibidang penjualan alat dan bahan kimia yang terletak di pusat kota Medan. Pada saat ini pengamanan file investigasi dilakukan secara manual, yaitu menyimpan file investigasi kedalam arsip tempat penyimpanan, hal itu bisa membuat file investigasi kondisinya sering terjadi kehilangan atau bocornya file penting karena kemudahan untuk mengakses file tersebut. Keamanan dan kerahasiaan data adalah salah satu aspek yang sangat penting dalam dunia teknologi pada saat ini. Disebabkan munculkan ilmu pengetahuan yang memungkinkan Teknik – teknik untuk melakukan kejahatan pada informasi, sehingga dapat merugikan pemilik informasi. Untuk permasalahan yang ada, Maka dilakukan sebuah perancangan dengan merancang sistem keamanan yang dapat digunakan untuk melindungi data berupa file dengan teknik kriptografi dengan menggunakan sebuah metode untuk mengimplementasikan Teknik kriptografi adalah metode AES-128 bit. Dengan adanya aplikasi kriptografi dengan metode AES 128 ini dapat mengamankan file dokumen penting yang ada di CV. Multi Kreasi dan Algoritma AES-128 bit ini berhasil diterapkan pada CV. Multi Kreasi yang dapat menghasilkan beberapa file yang dapat di input pada sistem.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Penulis Koresponden:

Apriliana Tumanggor,
Fakultas Ilmu Komputer,
Universitas Methodist Indonesia, Medan,
Jl. Hang Tuah No.8, Medan - Sumatera Utara.
Email: apriltmgr12@gmail.com

1. PENDAHULUAN

Teknologi komputer dan telekomunikasi saat ini telah mengalami kemajuan dan sudah menjadi suatu kebutuhan yang penting bagi setiap orang, karena banyaknya pekerjaan yang dapat diselesaikan dengan cepat. Salah satu dampak negatif di dalam perkembangan teknologi adalah adanya pencurian data. Dengan adanya pencurian data maka sisi keamanan dalam pertukaran informasi dan penyimpanan data dianggap penting. Salah satu data yang penting yaitu masalah keuangan, data keuangan merupakan sebuah data yang berisifat sensitif. Sehingga banyak kejahatan yang terjadi[1]. Untuk menjaga keamanan data ini di perlukan sistem yang mampu untuk

mengamankan data keuangan. Terdapat beberapa algoritma dalam kriptografi, salah satunya yaitu AES. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan ketika pesan dikirimkan dari suatu tempat ke tempat lain [2] Dipilihnya algoritma AES (Advanced Encryption Standard) karena dirancang khusus untuk keamanan tingkat tinggi serta ketahanan terhadap berbagai jenis serangan, bahkan kesederhanaan rancangan, kekompakan kode dan kecepatan men-enkripsi dan deskripsi setiap file atau data.

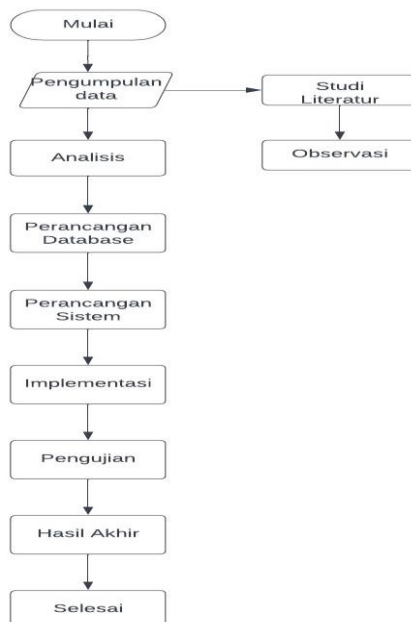
CV. Multi Kreasi Bersama merupakan suatu perusahaan yang bergerak dibidang penjualan alat dan bahan kimia yang terletak di pusat kota Medan. Adanya dampak negatif dari perkembangan teknologi maka keamanan data dalam penyimpanan file atau data menjadi sangat penting. Belum tentu dalam penyimpanan data dapat lebih aman dari pencurian file atau data, sehingga keamanan informasi atau data menjadi bagian penting dalam perkembangan teknologi. Untuk mengatasi masalah maka diperlukan cara untuk mengamankan data tersebut agar data tersebut tidak disalah gunakan. Dengan menggunakan teknik kriptografi/enkripsi. Proses enkripsi pada AES merupakan transformasi terhadap state secara berulang dalam 10 ronde [3]

Maka Pada penelitian ini bertujuan untuk membangun sistem keamanan AES pada keuangan dengan algoritma AES-128 dan di aplikasi enkripsi berbasis web. Untuk mengamankan file berupa informasi dapat terlindungi dengan baik. Manfaat dari penelitian ini membantu dalam mengamankan dokumen keuangan pada perusahaan CV.Multi Kreasi Bersama dan memberikan informasi file dokumen yang telah di proses ke AES.

2. METODE PENELITIAN

2.1 Framework Penelitian

Framework Penelitian adalah suatu kerangka kerja yang dilakukan dalam penelitian yang terdiri dari beberapa tahapan, adapun tahapan-tahapan yang akan dilakukan dalam penelitian ini yang terdiri dari beberapa tahapan untuk dapat menentukan proses dalam penelitian diantara dapat dilihat pada gambar 1.



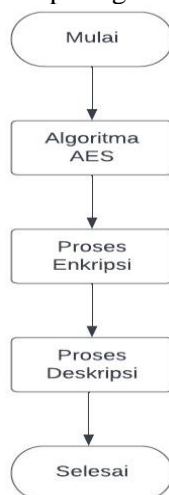
Gambar 1. tahapan penelitian

Pengumpulan Data

Pengumpulan data adalah teknik atau cara yang dilakukan oleh peneliti untuk mengumpulkan data. Pengumpulan data saat ini digunakan dalam penelitian adalah data dari juli tahun 2021 sampai dengan oktober 2021. Data tersebut seperti penjualan barang, dan data pembelian barang. Adapun pengumpulan data yang dilakukan penelitian yaitu Studi Literatur dan observasi. Observasi dilaksanakan perusahaan Cv. Multikreasi.

2.2 Analisis Sistem

Analisis sistem merupakan suatu teknik atau metode pemecahan masalah dengan cara menguraikan sistem keamanan kedalam komponen-komponen pembentuk, untuk mengetahui bagaimana komponen-komponen tersebut bekerja dan saling berinteraksi satu sama lain. Maka dibutuhkan merancang analisis sistem dengan metode Algoritma encryption standard (AES). Dalam merancang analisis sistem keamanan dengan metode AES ada beberapa tahapan-tahapan penelitian membangun sistem keamanan AES dapat dilihat pada gambar 2.



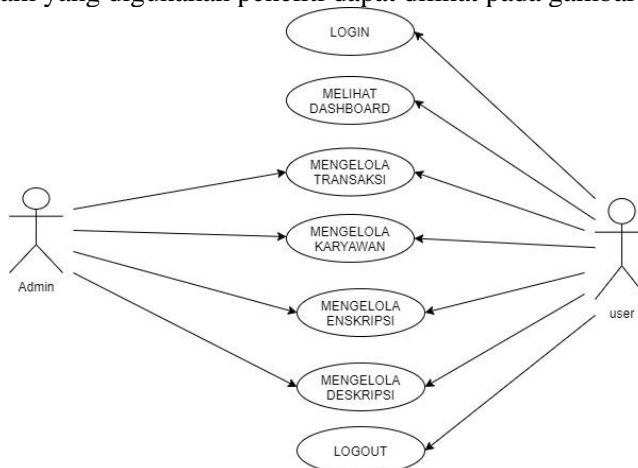
Gambar 2. Tahapan analisis sistem

2.3 Perancangan Sistem

Pada penelitian ini Perancangan sistem dilakukan setelah mendapatkan gambaran jelas mengenai apa yang harus dikerjakan. perancangan ini menggunakan UML (*Unified Modeling Language*) adalah sebuah bahasa yang berdasarkan grafik/gambar untuk memvisualisasi, menspesifikasikan, membangun, dan pendokumentasian dari sebuah sistem pengembangan software berbasis OO (*Object-Oriented*). Sebuah bahasa model adalah sebuah bahasa yang mempunyai vocabulary dan konsep tatanan / aturan penulisan serta secara fisik mempresentasikan dari sebuah sistem. [4] Pada penelitian ini dalam membangun website, dalam penelitian menggunakan 4 jenis diagram, yaitu *use case* diagram, *activity* diagram, *sequence* diagram dan *class* diagram.

1. Use Case diagram

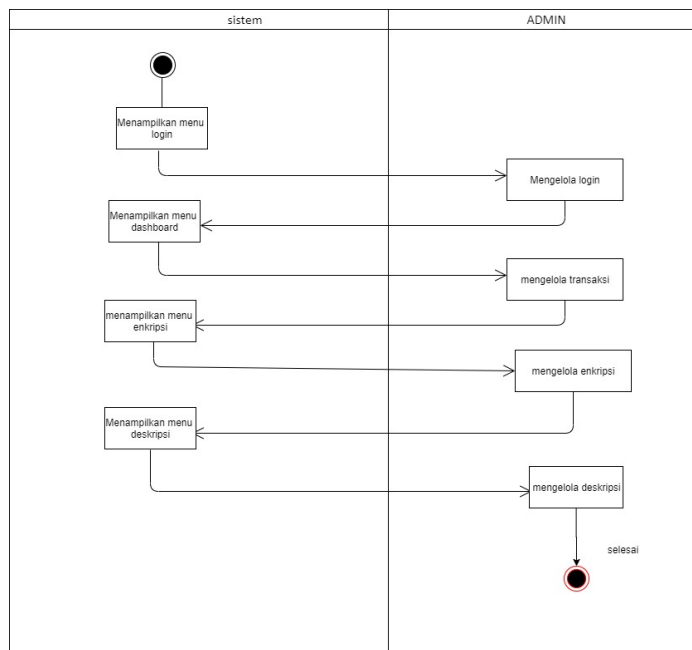
Use case diagram adalah suatu urutan interaksi yang saling berkaitan antara sistem dan aktor. *Use case* harus mampu menggambarkan urutan aktor yang menghasilkan nilai yang terukur [5]. Adapun *use case* diagram yang digunakan peneliti dapat dilihat pada gambar 3.



Gambar 3. use case diagram

2. Activity Diagram

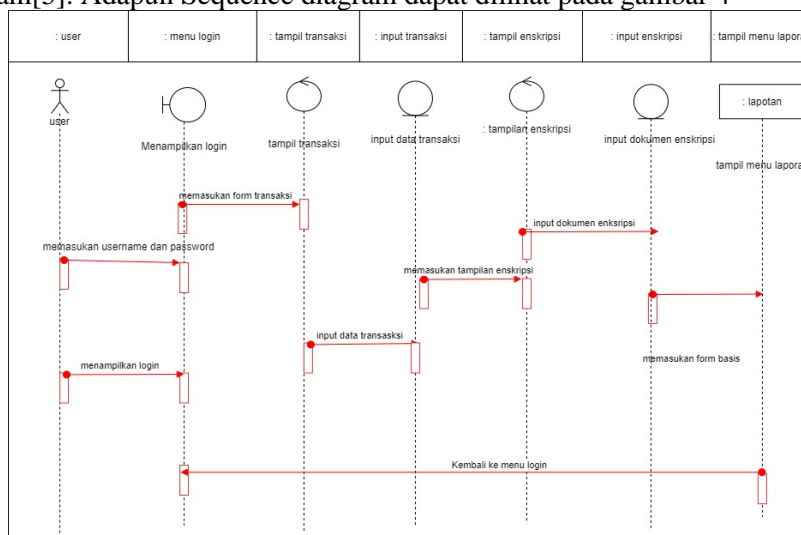
Activity Diagram menunjukkan aktivitas sistem dalam bentuk serangkaian tindakan, bagaimana setiap tindakan dimulai, dan keputusan yang mungkin terjadi sebelum tindakan berakhir. Diagram aktivitas juga dapat menggambarkan proses beberapa tindakan pada saat yang bersamaan. Diagram aktivitas adalah aktivitas, objek, status, transisi status, dan peristiwa. Dengan kata lain, diagram alur kerja aktivitas menggambarkan perilaku sistem dari aktivitas [5]. Activity diagram dapat dilihat pada gambar 4.



Gambar 4. activity diagram

3. Sequence Diagram

Sederhananya, *sequence* diagram adalah deskripsi langkah demi langkah, termasuk urutan waktu (*sequence*) perubahan logis yang harus dilakukan untuk menghasilkan sesuatu berdasarkan *use case* diagram[5]. Adapun Sequence diagram dapat dilihat pada gambar 4



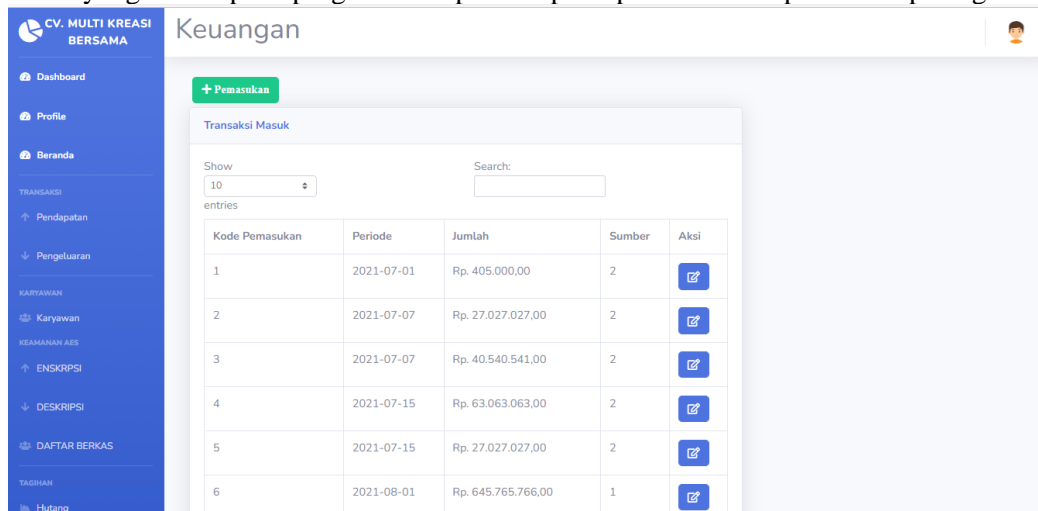
Gambar 5. sequence diagram

3. HASIL DAN PEMBAHASAN

Tampilan program

Pada penelitian ini hasil program website keuangan dengan metode aes 128 dengan menggunakan bahasa pemrograman php yang dikerjakan oleh peneliti. Pada tampilan program admin mengelola data ke dalam program dengan menginput data pemasukan ke dalam database, akan tampil

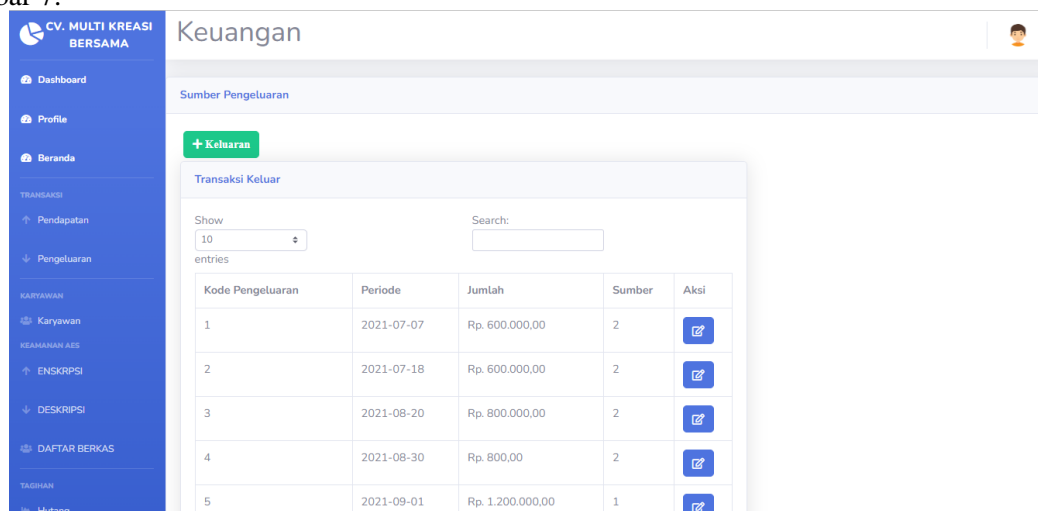
pada program web. Pada tampilan program admin dan user dapat menginput data mengklik pemasukan yang tertera pada program. Adapun tampilan pemasukan dapat dilihat pada gambar 6.



Kode Pemasukan	Periode	Jumlah	Sumber	Aksi
1	2021-07-01	Rp. 405.000,00	2	
2	2021-07-07	Rp. 27.027.027,00	2	
3	2021-07-07	Rp. 40.540.541,00	2	
4	2021-07-15	Rp. 63.063.063,00	2	
5	2021-07-15	Rp. 27.027.027,00	2	
6	2021-08-01	Rp. 645.765.766,00	1	

Gambar 6. tampilan program pemasukan

Pada tampilan pengeluaran maka admin menginput transaksi pengeluaran keuangan pada program. Disini berfungsi untuk melihat data pengeluaran yang dimana setiap data akan diinput di database akan tampil pada pada program pengeluaran disini, user juga dapat menambahkan setiap transaksi pengeluaran dengan mengklik keluaran. Adapun tampilan pengeluaran dapat dilihat pada gambar 7.



Kode Pengeluaran	Periode	Jumlah	Sumber	Aksi
1	2021-07-07	Rp. 600.000,00	2	
2	2021-07-18	Rp. 600.000,00	2	
3	2021-08-20	Rp. 800.000,00	2	
4	2021-08-30	Rp. 800,00	2	
5	2021-09-01	Rp. 1.200.000,00	1	

Gambar 7. tampilan program pengeluaran

Tampilan enkripsi

Pada tahapan enkripsi disini menampilkan berkas file data fakturan penjualan.pdf untuk di input pada program enkripsi. File ini akan dikelola oleh admin untuk menampilkan di program enkripsi. Adapun tampilan file fakturapenjualan.pdf dapat dilihat pada gambar 8



CV. MULTI KREASI BERSAMA
 Jl. K.H. Wahid Hasyim No. 6 P Medan
 Telp. : (061) 4150107
 Fax. : (061) 4150107

Supplier :
 • Chemical
 • Laboratory Equipments
 • Glassware
 • Alat Praktikum Sekolah
 • Alat Peraga Pendidikan

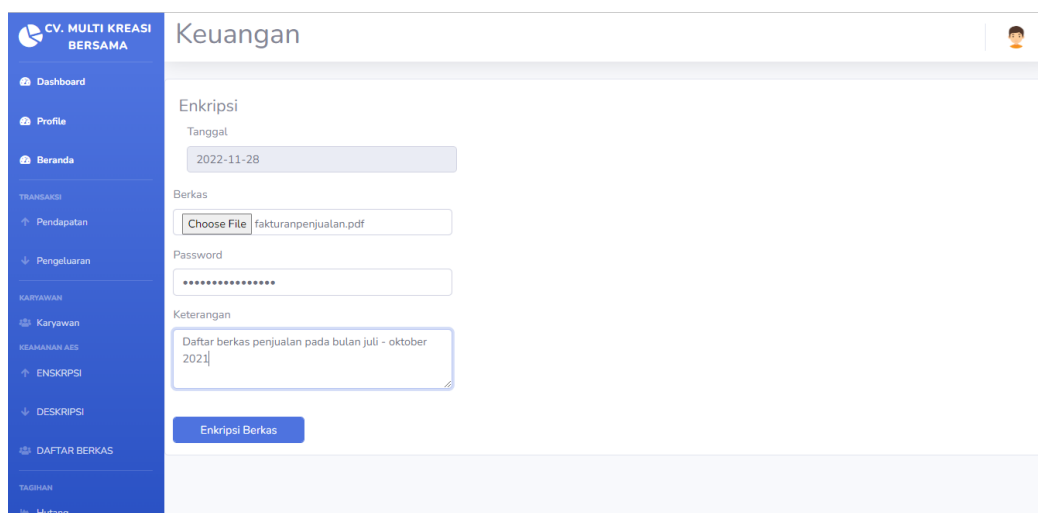
FAKTUR PENJUALAN

Faktur Penjualan Alat dan Bahan Kimia
 BULAN JULI 2021
 SMA SW METHODIST SIANTAR
 Jln Pane No.34, Kebun Sayur, Siantar

No.	Daftar Jual Alat dan Bahan praktikum IPA	Kemasan Volume	Harga Satuan/Rp	Jumlah Harga/Rp
1.	Mikroskop Digital Trinocular Habis pakai	2 unit	18.592.500	37.185.000,
2.	Larutan Ag No3 100 ml	10 btl	111.000,	1.110.000,
3.	Sumbu kompor	6 mtr	33.300,	199.800,
4.	Larutan Moolish	6 btl	166.500,	999.000,
5.	NaOH Pa 500 gr	4 btl	527.250,	2.109.000,
6.	Tissu Passio	6 bks	49.950,	299.700,
7.	Larutan CHCL3 100 ml	6 btl	111.000,	666.000,
8.	Larutan NH4OH 100 ml	5 btl	111.000	555.000,
9.	Larutan CH2HSOH 100 ml	5 btl	111.000,	555.000,
10.	Larutan HNo3 100 ml	5 btl	111.000,	555.000,
11.	Larutan NH3 100 ml	5 btl	111.000,	555.000,
12.	Larutan Aceton 100 ml	5 btl	111.000,	555.000,
13.	Urea	5 kg	33.300,	166.500,

Gambar 8. tampilan file fakturapenjualan

Selanjutnya akan admin menginput Pada program enkripsi disini berfungsi untuk mengamankan dokumen aes pada yang telah di input. Enkripsi ini akan menjadi update jika ada data yang telah di input user. Adapun tampilan enkripsi berkas dapat dilihat pada gambar 9.



CV. MULTI KREASI BERSAMA Keuangan

Enkripsi

Tanggal
2022-11-28

Berkas
Choose File fakturapenjualan.pdf

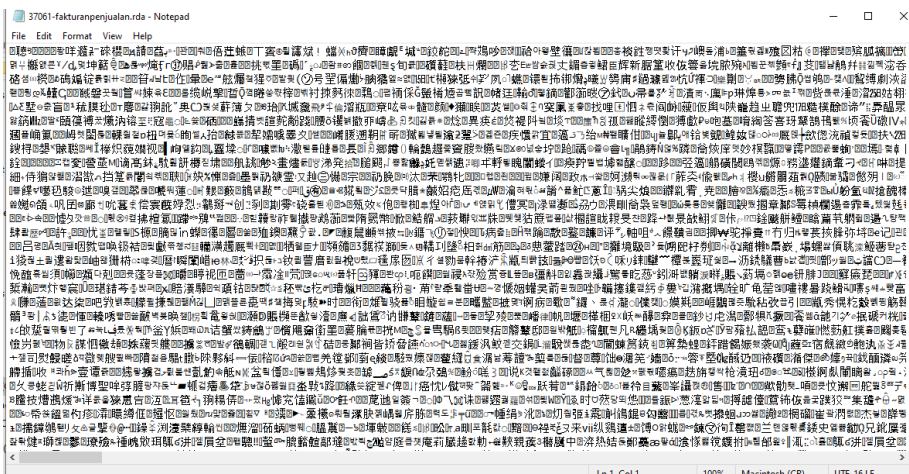
Password

Keterangan
Daftar berkas penjualan pada bulan juli - oktober 2021

Enkripsi Berkas

Gambar 9. tampilan enkripsi

Setelah melakukan proses enkripsi maka akan tampil file dengan ekstensi rda, tampilan file akan berubah dengan file yang tidak diketahui nama atau bahasa tidak jelas. Adapun tampilan hasil enkripsi file dapat dilihat pada gambar 10



Gambar 10. tampilan hasil proses enkripsi

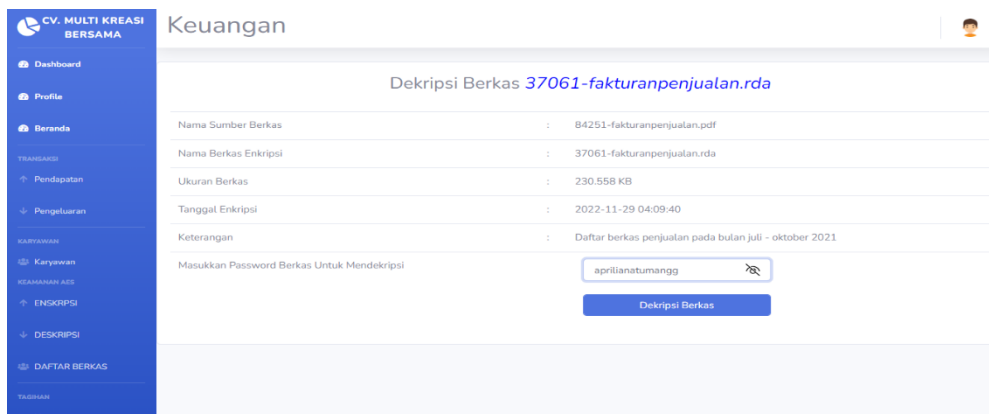
Tampilan deskripsi

Pada tampilan deskripsi disini berfungsi untuk mengamankan dokumen aes pada yang telah di input. Deskripsi ini akan menjadi update jika ada data yang telah di input user. Adapun tampilan deskripsi berkas dapat dilihat pada gambar 11.



Gambar 11. tampilan program deskripsi

Selanjutnya akan tampil pada program deskripsi, maka user menginput kembali password yang telah di input pada program deskripsi. Ketika proses deskripsi maka tampilan file dengan format pdf akan muncul kembali file seperti pada gambar diatas. Adapun tampilan deskripsi berkas dapat dilihat pada gambar 12



Gambar 12. tampilan deskripsi berkas

4. KESIMPULAN

Kesimpulan dari penelitian skripsi ini adalah:

1. Kriptografi dengan metode AES 128 bit dapat melakukan proses enkripsi dan dekripsi data keuangan pada CV. Multi Kreasi Bersama dalam bentuk file pdf.
2. Penelitian ini menghasilkan satu kemajuan teknologi yang dapat mengamankan data yang bersifat sensitive.

REFERENSI

- [1] H. G. Simanullang and A. P. Silalahi, "Algoritma Blowfish Untuk Meningkatkan Keamanan Database Mysql," vol. 4, no. 1, pp. 10–14, 2018.
- [2] A. Azzam Ajhari, "IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN AES-128 UNTUK PENGAMANAN PESAN DAN ONE TIME PASSWORD REGISTRASI AKUN PADA APLIKASI CHATting BERBASIS ANDROID DI SMA HANG TUAH 1 JAKARTA," 2018.
- [3] G. S. Yudha and R. H. Laluma, "Sistem Keamanan Jaringan Dalam Ujian Online Sma/Smk Menggunakan Metode Algoritma Advanced Encryption Standard (Aes)," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 4, no. 2, p. 71, 2019, doi: 10.32897/infotronik.2019.4.2.261.
- [4] A. Mubarak, "Rancang Bangun Aplikasi Web Sekolah Menggunakan Uml (Unified Modeling Language) Dan Bahasa Pemrograman Php (Php Hypertext Preprocessor) Berorientasi Objek," *JIKO (Jurnal Inform. dan Komputer)*, vol. 2, no. 1, pp. 19–25, 2019, doi: 10.33387/jiko.v2i1.1052.
- [5] Suendri, "Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan)," *J. Ilmu Komput. dan Inform.*, vol. 3, no. 1, pp. 1–9, 2018.