SKANIKA: Sistem Komputer dan Teknik Informatika
Volume 5, Nomor 1, Januari 2022, Halaman 1-10 E-ISSN: 2721-4788

Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi

Arther Ignasius Suranta[1], Dolly Virgian Shaka Yudha Sakti[2*]
[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia
E-mail: [1]1511501312@student.budiluhur.ac.id, [2*]dolly.virgianshaka@budiluhur.ac.id
(* : corresponding author)

Abstrak

PT Gunung Geulis Elok Abadi adalah perusahaan yang bergerak di beberapa bidang seperti food court, hotel, dan lain – lain. Perusahaan ini terdapat data dokumen yang bersifat penting dan tidak semua orang boleh melihat ataupun mengambil data tersebut secara mudah. Permasalahannya adalah perusahaan ini tidak memiliki sistem untuk pengamanan data khususnya dibagian dokumen yang penting untuk perusahaan sebagai pencegahan dari orang yang melakukan penyadapan data. Solusi dari permasalahan tersebut adalah merancang suatu aplikasi yang dapat mengamankan data agar tidak dapat digunakan oleh orang lain. Perancangan aplikasi ini menggunakan algoritma AES-128 untuk proses enkripsi dan dekripsi data. Hasil dari percobaan enkripsi dan dekripsi dari dua pulu file, menunjukkan rata – rata waktu enkripsi yaitu 12.769 milisecond dan rata – rata waktu dekripsi yaitu 18.075 milisecond.

Kata kunci: keamanan data, enkripsi, AES-128, dokumen

Abstract

PT Gunung Geulis Elok Abadi is a company engaged in several fields such as food courts, hotels, and others. This company has important document data and not everyone can see or retrieve the data easily. The problem is that this company does not have a system for data security, especially in the document section that is important for the company as a prevention from people who intercept data. The solution to these problems is to design an application that can secure data so that it cannot be used by others. The design of this application uses the AES-128 algorithm for the encryption and decryption of data. The results of the encryption and decryption experiments of twenty files, show the average encryption time is 12,769 milliseconds and the average decryption time is 18,075 milliseconds.

Keywords: data security, encrytion, AES-128, document

1. PENDAHULUAN

Pesatnya perkembangan teknologi membuat semua kalangan memanfaatkannya untuk banyak kegiatan, terutama pengelolaan data[1]. Tidak hanya data yang bersifat umum, tapi juga data yang bersifata rahasia[2]. Beberapa contoh data yang memanfaatkan tekonlogi pada PT. Gunung Geulis Elok Abadi diantaranya data keuangan, data bahan baku, informasi data member. Dokumen / data tersebut tidak diperkenankan untuk diakses ataupun dibuka oleh orang sembarangan orang, hanya orang tertentu yang diperkenankan mengakses dokumen tersebut [3].

Perusahaan ini masih menyimpan data yaitu arsip dokumen digital di dalam suatu folder pada komputer tanpa adanya sistem pengamanan data. Perusahaan ini juga tidak memiliki sistem penyimpanan dan pengamanan database mengenai arsip dokumen. Perusahaan ini juga tidak memiliki database yang berfungsi sebagai media penyimpanan file dokumen sehingga apabila para pegawai membutuhkan suatu file, mereka harus meminta kepada pegawai yang mempunyai file bersangkutan.

Berdasarkan hal tersebut, diperlukan suatu aplikasi pengamanan arsip dokumen berbasis web yang dapat mengamankan data dari kebocoran data dari pihak lain. Tidak hanya pengamanannya saja, tapi kebutuhan berikutnya adalah manajemen pengelolaan dokumen. Pada penelitian ini dibuat manajemen pengelolaan file yang dikombinasikan dengan pengamanan data berupa enkripsi dan dekripsi.

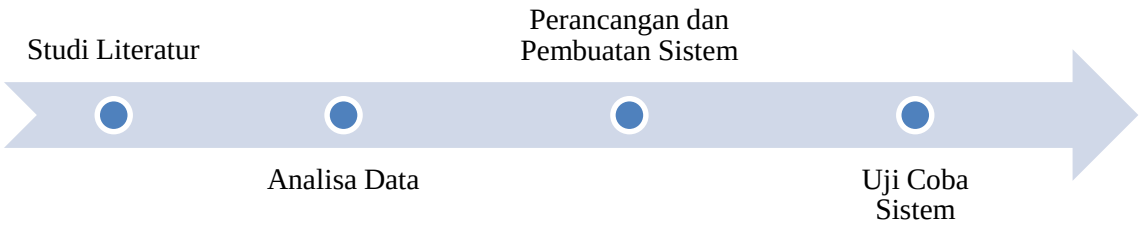
Banyak penelitian sebelumnya yang telah menerapkan kriptografi untuk pengamanan data. Salah satu diantaranya menerapkan kriptografi untuk pengamanan data pada aplikasi berbasis desktop[1], [3]–[6]. Kekurangan aplikasi berbasis desktop diantaranya adalah harus dilakukan instalasi atau konfigurasi di setiap komputer yang akan menggunakan aplikasinya. Penerapan kriptografi di dalam penelitian lain melakukan pengamanan data pada aplikasi berbasis mobile[7][8]. Masih mirip dengan aplikasi berbasis desktop, aplikasi berbasis mobile juga masih harus dilakukan instalasi pada smartphone yang akan digunakan.

Penelitian sebelumnya juga sudah banyak membangun aplikasi keamanan data berbasis web[2], [9]. Salah satu kelebihan dibangun aplikasi keamanan data berbasis web, pengguna cukup menggunakan browser dan menuju alamat server web. Aplikasi berbasis web bisa diakses asalkan perangkat yang digunakan terhubung dengan jaringan yang sama dengan server web.

Pada penelitian ini digunakan algoritma AES karena menurut penelitian sebelumnya kecepatan enkripsi dan dekripsi AES masih lebih baik jika dibandingkan dengan beberapa algoritma lain[10], [11]. Perbandingan AES pada penelitian lain menyatakan bahwa enkripsi dan dekripsi dilakukan pada gambar, hasil dari proses algoritma AES masih lebih baik [12].

2. METODE PENELITIAN

Tahapan yang dilakukan pada penelitian ini dimulai dari mempelajari literature tentang kriptografi, khususnya algoritma AES. Berikutnya melakukan analisa data pada instansi, mempelajari data apa yang akan dilakukan pengamanan. Selanjutnya merancang skema aplikasi yang akan dibuat berdasarkan studi literature dan analisa data, sekaligus membuat sistem / aplikasi pengamanan data berbasis web. Setelah aplikasi selesai dibuat dilakukan uji coba sistem. Tahapan ini seperti terlihat pada Gambar 1.



Gambar 1. Metode Penelitian

a. Studi Literatur

Literatur yang dipelajari adalah buku terkait teori kriptografi dan juga dua belas paper penelitian berupa paper journal dan prosiding. Buku terkait teori kriptografi digunakan untuk mempelajari hal mendasar tentang kriptografi. Sedangkan paper penelitian digunakan untuk mempelajari penerapan yang pernah dilakukan pada penelitian sebelumnya.

b. Analisa Data

Pada tahapan analisa, dilakukan wawancara dengan pihak PT.Gunung Geulis Elok Abadi. Selain wawancara, dilakukan sedikit obervasi terhadap data yang akan dilakukan pengamanan. Beberapa contoh data yang perlu diamankan diantaranya data keuangan, data bahan baku, dan informasi data member.

c. Perancangan dan Pembuatan Sistem

Tahapan perancangan dilakukan dengan membuat flowchart dan algoritmanya. Selanjutnya aplikasi dibuat menggunakan bahasa pemrograman PHP dan basis data MySQL.

d. Uji Coba Sistem

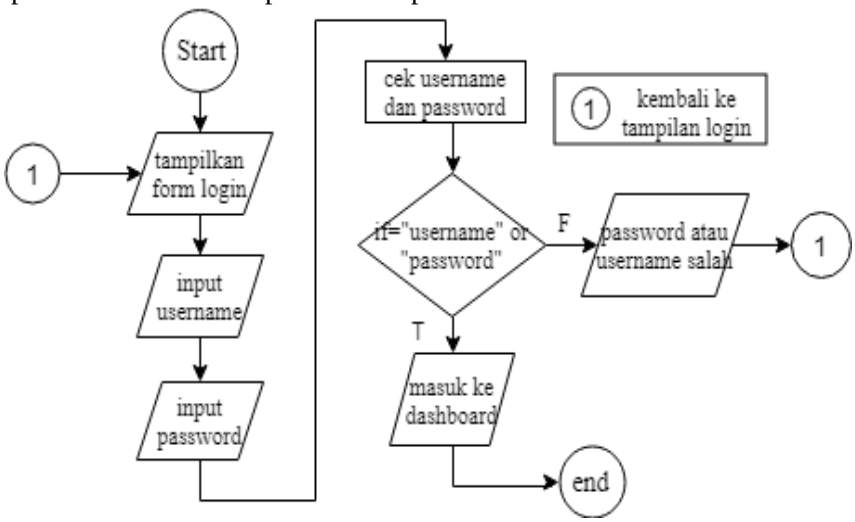
Metode ini dilaksanakan dengan pengujian terhadap aplikasi untuk melihat apakah sudah berjalan dengan baik. Selain itu pengujian dilakukan untuk melihat perbandingan besaran file

sebelum enkripsi, setelah enkripsi dan juga setelah dekripsi. Pengujian ini juga dilakukan untuk melihat kecepatan proses enkripsi dan dekripsi.

3. HASIL DAN PEMBAHASAN

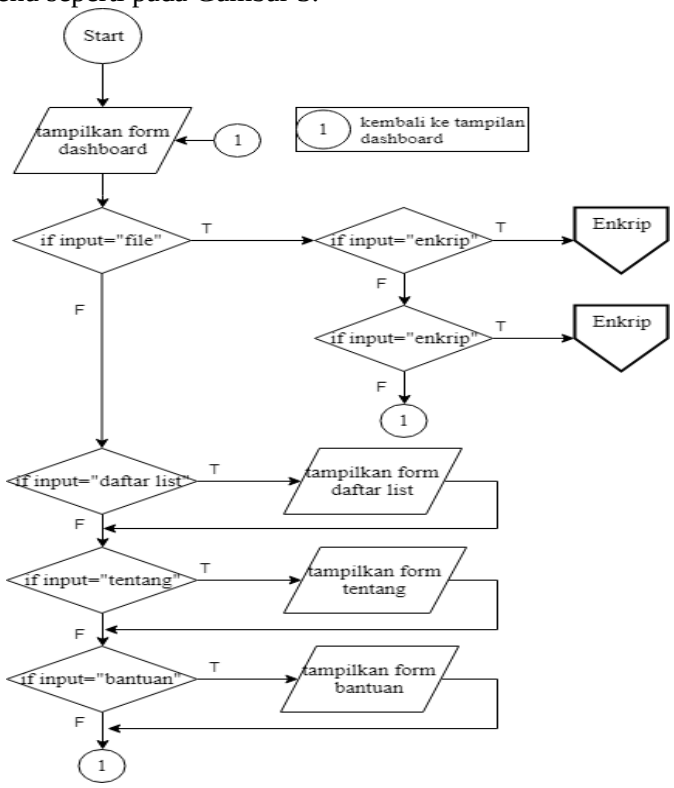
3.1. Flowchart

Proses diawali dengan adanya tampilan login sebagai tampilan awal, kemudian *user* mengisi *username* dan *password*. Setelah itu database akan mengecek *username* dan *password* telah sesuai atau belum. Apabila sesuai maka user dapat masuk ke aplikasi. Apabila tidak, maka user tidak dapat masuk ke dalam aplikasi enkripsi.



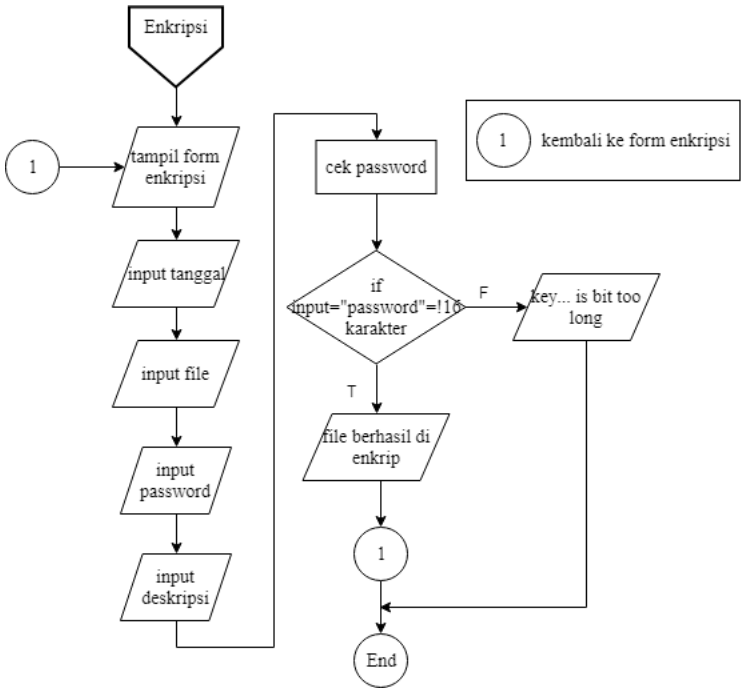
Gambar 2. Flowchart Login

Setelah berhasil login, pengguna akan diarahkan pada dashboard yang akan disediakan beberapa pilihan menu seperti pada Gambar 3.



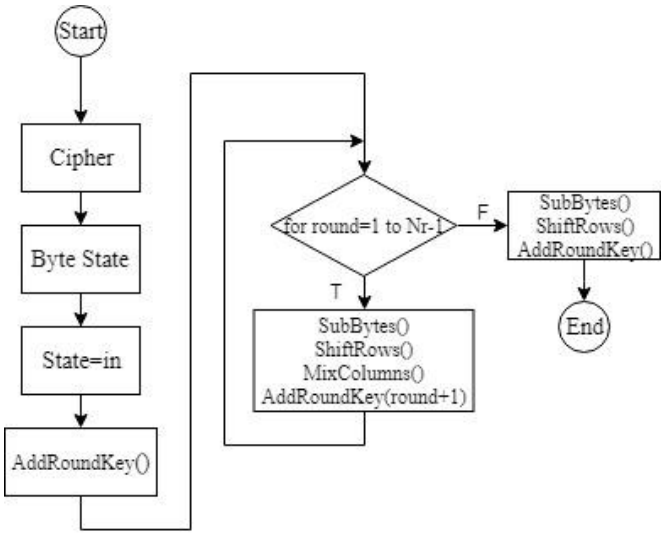
Gambar 3. Flowchart Dashboard

Pilihan pertama yang tersedia pada dashboard adalah Menu File seperti pada Gambar 4. Flowchart ini dimulai dari tampilan form enkripsi lalu user akan meng input beberapa bagian seperti bagian tanggal, dokumen yang ingin dienkrip, *password* untuk menguci dokumen dan keterangan. Lalu sistem akan melakukan pengecekan terhadap password yang di input. Apabila password sesuai dengan aplikasi maka dokumen akan terenkripsi. Bila tidak maka akan muncul *key*. bit long karena jumlah karakter *password* yang dimasukkan tidak sesuai.



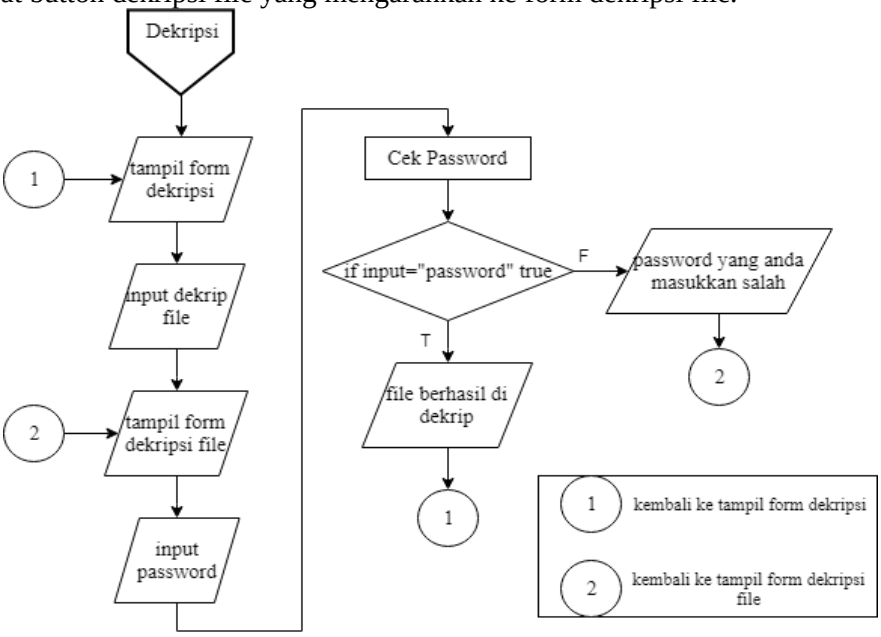
Gambar 4. Flowchart Form Enkripsi

Proses Enkripsi AES-128 sendiri digambarkan pada flowchart Gambar 5. Proses diawali dengan pengubahan dari plaintext menjadi ciphertext. Lalu proses dilanjutkan dengan byte yang berasal dari plaintext berubah menjadi state. Setelah itu, dilakukannnya proses AddRoundKey. Proses transformasi AddRoundKey selesai, dilanjutkan dengan proses looping. Proses dilanjutkan lagi ke 4 transformasi dimulai dari SubByte sampai dengan AddRoundKey. Bila proses transformasi selesai, dilanjutkan dengan proses SubByte sampai AddRoundKey tanpa adanya transformasi MixColumns.



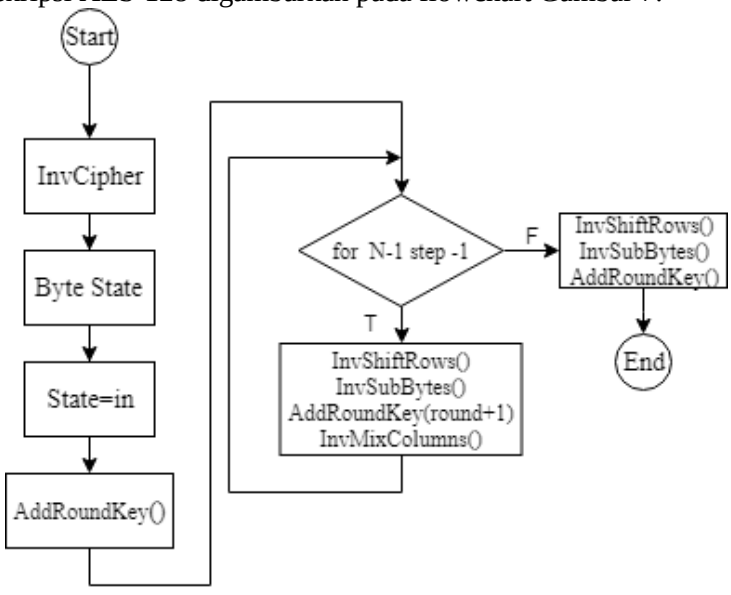
Gambar 5. Flowchart Enkripsi

Flowchart form dekripsi dimulai dengan tampilan form dekripsi. Tampilan form dekripsi terdiri dari beberapa bagian seperti nama file, nama file enkripsi, path file status, aksi. Pada bagian aksi terdapat button dekripsi file yang mengarahkan ke form dekripsi file.



Gambar 6. Flowchart Form Dekripsi

Proses dekripsi AES-128 digambarkan pada flowchart Gambar 7.



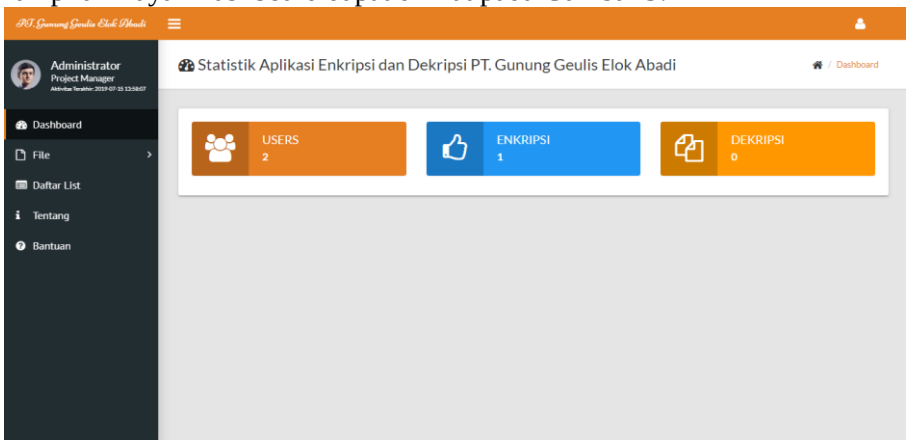
Gambar 7. Flowchart Dekripsi.

3.2. Tampilan Layar

Setelah program dirancang, berikutnya dibuat sesuai dengan yang dirancang, dibuatlah program berbasis web. Untuk masuk ke dalam aplikasi, pengguna akan dihadapakan pada halaman awal yaitu halaman login. Tampilan login terdiri beberapa bagian seperti adanya tulisan tempat perusahaan, pengisian username dan password dan adanya button login untuk masuk ke aplikasi enkripsi data. Halaman Login dapat dilihat pada Gambar 8.

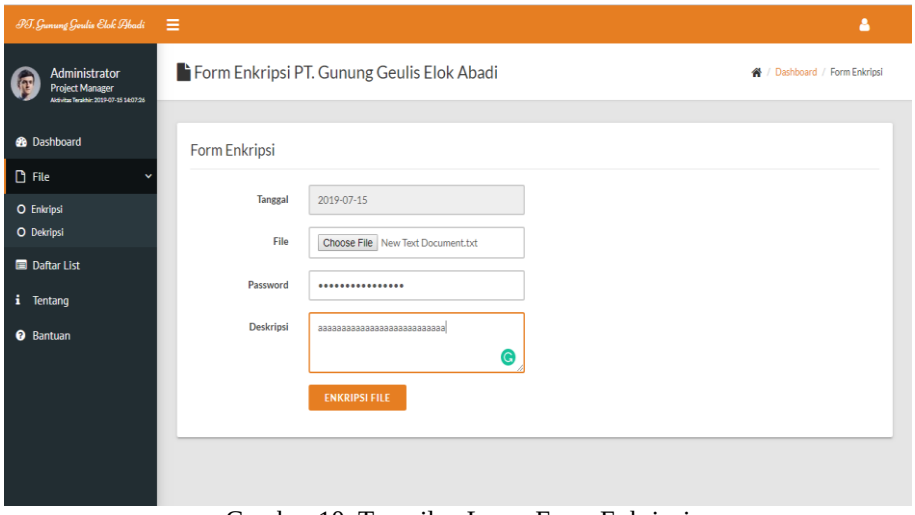
Gambar 8. Tampilan Layar Halaman Login

Setelah berhasil login, pengguna akan dihadapkan dengan dashboard yang berisi informasi jumlah pengguna yang terdaftar, jumlah file yang pernah dienkripsi dan juga di dekripsi. Tampilan Layar Dashboard dapat dilihat pada Gambar 9.



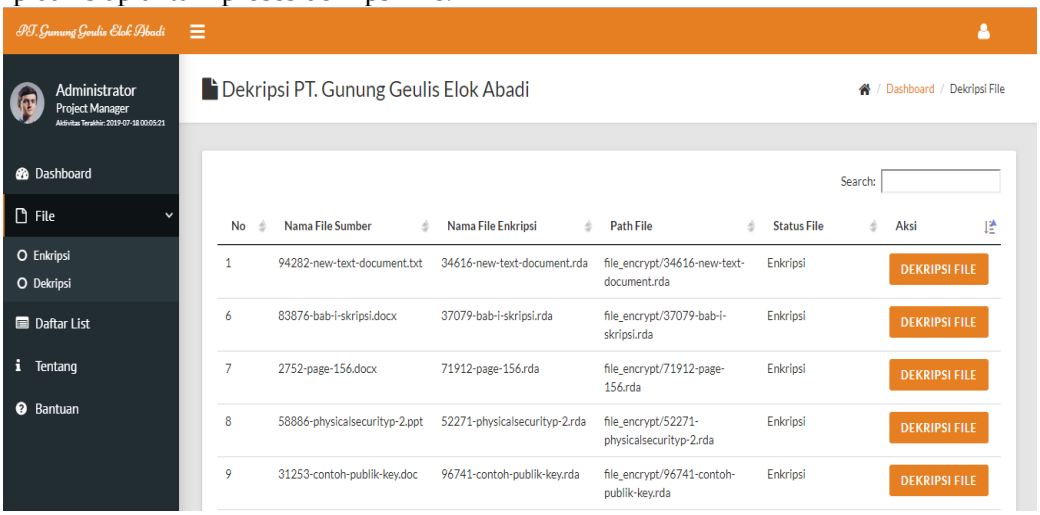
Gambar 9. Tampilan Layar Dashboard

Form Enkripsi adalah tempat dimana user dapat melakukan enkripsi dokumen file. Pada tampilan layar form enkripsi terdapat beberapa bagian yang harus disi seperti pengisian tanggal, memilih file yang ingin dienkrip, mengisi password dan dekripsi atau keterangan mengenai file yang akan dienkripsi. Tampilan layar form enkripsi dapat dililhat pada Gambar 10.



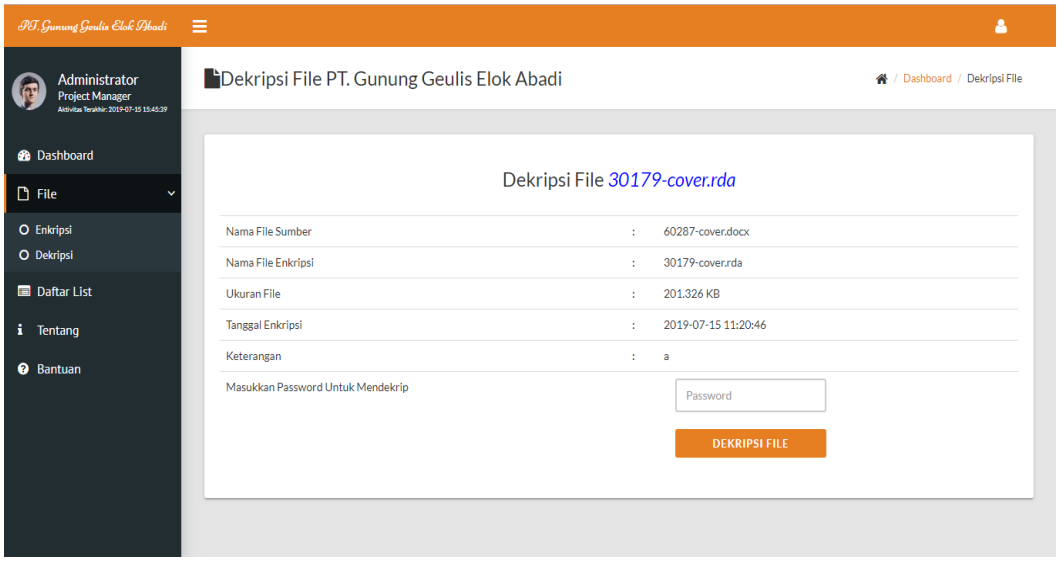
Gambar 10. Tampilan Layar Form Enkripsi

Untuk melakukan dekripsi, akan tampil List File Dekripsi seperti pada Gambar 11. Disini terlihat informasi seperti nomor, nama file, nama file enkripsi, path file, status dan aksi. Pada bagian aksi, terlihat bagian berwarna oranye yang menandakan status suatu file dalam keadaan enkrip dan siap untum proses dekripsi file.



Gambar 11. List File Dekripsi

Setelah tombol Dekripsi diklik maka akan menampilkan form Dekripsi seperti pada Gambar 12. Tampilan form dekripsi file menampilkan beberapa informasi yang sama pada tampilan form enkripsi. Terdapat masukkan *password* untuk mendekrip dokumen dari cipher file menjadi plain file. *Password* yang dimasukkan harus sama dengan *password* saat melakukan proses enkripsi sebelumnya.



Gambar 12. Tampilan Layar Form Dekripsi

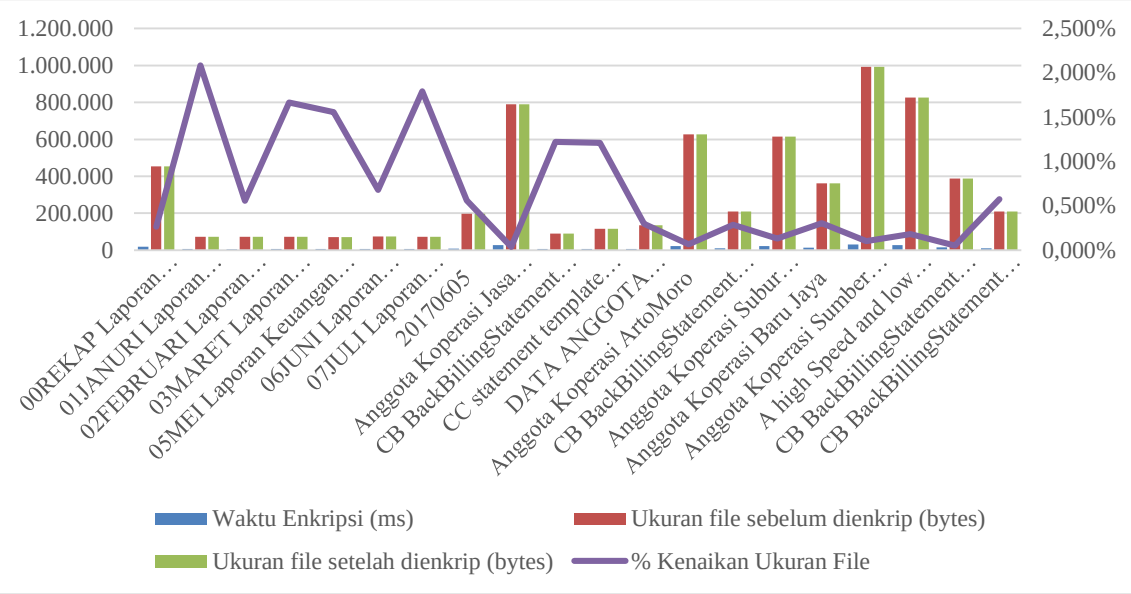
3.3. Pengujian

Setelah aplikasi dibuat, dilakukan pengujian blackbox berupa uji coba terhadap jalannya aplikasi. Skema pengujian yang dibuat diantaranya adalah dengan melakukan enkripsi dua puluh file dan selanjutnya didekripsi kembali. Tidak hanya melihat keberhasilan enkripsi dan dekripsi, pengujian ini juga mengukur kecepatan proses enkripsi dan dekripsi yang terjadi, dan juga melihat perubahan ukuran file setelah proses enkripsi dan dekripsi.

File yang ada pada tempat riset dan bisa dilakukan pengujian berukuran di bawah 2 MB. Hasil dari pengujian Enkripsi terhadap file tersebut, aplikasi dapat berjalan dengan baik. Selain

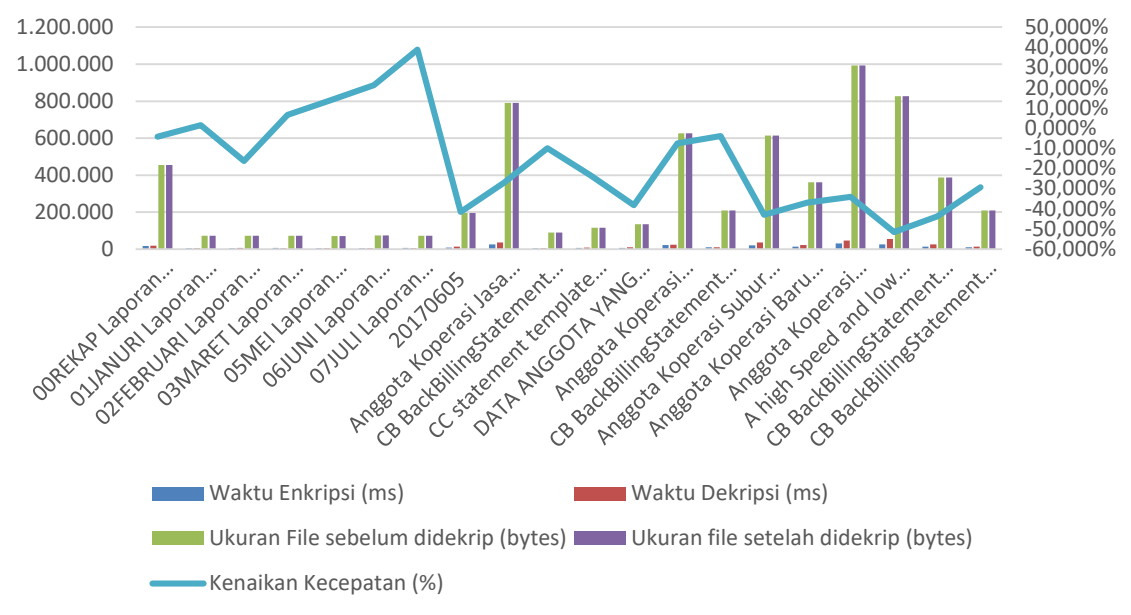
itu berdasarkan pengujian Enkripsi yang sudah dilakukan, didapat data seperti pada Gambar 12. Terlihat untuk proses enkrip file yang diuji masih tergolong cukup cepat karena masih di bawah satu detik. Hal lain yang bisa dilihat adalah, semakin kecil file yang dilakukan enkripsi, maka semakin besar kenaikan ukuran file.

Presentase kenaikan ukuran file terjadi pada proses enkripsi file "01JANURI Laporan Keuangan Lengkap". Awalnya memiliki ukuran 71.913bytes, setelah proses enkripsi menjadi 71.928bytes, naik sebesar 2,086%. Lama waktu proses enkrip 5.851 milisecond. Sementara presentasi kenaikan terkecil ada pada file "Anggota Koperasi Sumber Dana" awalnya memiliki ukuran 992.486bytes setelah melalui proses enkripsi menjadi 992.496bytes, naik sebesar 0,101%. Lama waktu proses enkrip adalah 30.561 milisecond.



Gambar 13. Pengujian Enkripsi

Pengujian proses dekripsi menggunakan file yang telah melalui proses enkripsi sebelumya. Berdarkan pengujian dekripsi didapat data seperti terlihat pada Gambar 14. Ukuran file yang sudah dilakukan dekripsi ternyata tidak berubah dari ukuran sebelum didekripsi. Untuk waktu proses dekripsi, masih cukup cepat seperti pada waktu proses enkripsi. Sedangkan jika dibandingkan antara waktu proses enkripsi dengan dekripsi pada masing-masing file, belum ditemukan keseragaman pada kenaikan atau penurunan kecepatannya. Beberapa file mengalami kenaikan kecepatan, beberapa lain mengalami penurunan kecepatan. Rata-rata waktu proses enkripsi adalah 12.769 milisecond, sedangkan rat-rata waktu proses dekripsi adalah 18.075 milisecond.



Gambar 14. Pengujian Dekripsi

4. KESIMPULAN DAN SARAN

Dari hasil analisis dapat diambil beberapa kesimpulan, yang pertama dengan adanya aplikasi enkripsi – dekripsi file menggunakan algoritme AES-128 dapat meningkatkan keamanan dokumen dari serangan pihak lain. Berikutnya hasil dari percobaan enkripsi sebanyak 20 file, presentase kenaikan ukuran file sekitar 0.038% sampai dengan 2.086%. Selain itu hasil dari percobaan enkripsi dan dekripsi dari 20 file menunjukkan rata – rata waktu enkripsi yaitu 12.769 milisecond dan rata – rata waktu dekripsi yaitu 18.075 milisecond. Waktu rata-rata proses dekripsi sedikit lebih lama dari pada waktu proses enkripsi.

Untuk pengembangan pada penelitian berikutnya akan lebih baik jika menggunakan dua algoritme pada proses enkripsi data agar lebih aman lagi. Misalnya saja penggunaan dua algoritme simetris atau kombinasi antara algoritme asimetris dan algoritme simetris.

DAFTAR PUSTAKA

[1] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *Jurnal Format*, vol. 6, no. 2, pp. 2089–5615, 2016.

[2] H. Agung and B. Budiman, "Implementasi Affine Chiper dan RC4 pada Enkripsi file Tunggal," in *Prosiding SNATIF*, pp. 243–250, 2015.

[3] D. Darwis, R. Prabowo, and N. Hotimah, "Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 5, no. 4, pp. 389-394, 2018.

[4] A. Latif, "Implementasi Kriptografi Menggunakan Metode Advanced Encryption Standar (AES) untuk Pengamanan Data Teks," *Jurnal Ilmu Mustek Anim*, vol. 4, no. 2, pp. 163-172, 2015.

[5] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, pp. 52-58, 2018.

[6] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting Data Hiding," *Journal of Applied Intelligent System*, vol. 1, no. 3, pp. 179–190, 2016.

[7] Y. Laia *et al.*, "File Cryptography with AES and RSA for Mobile Based on Android," *Jornal Physics: Conf. Series*, vol. 1007, no. 1, 2018.

[8] Y. Prihartono and G. Bagio, "Pengembangan Aplikasi Pengamanan File Sebagai Solusi Keamanan Data pada Smartphone Berbasis Android," in *Seminar Nasional Sistem Informasi Indonesia*, 2016, pp. 69–76.

[9] W. Pramusinto, Subandi, B. H. Prasetyo, and D. Anubhakti, "Aplikasi Pengamanan File dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman," *Jurnal. BIT*, vol. 16, no. 2, pp. 47–53, 2020.

[10] D. A. Meko, "Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *Jurnal Teknologi Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[11] M. A. Muin, A. Setyanto, and Sudarmawan, "Perbandingan Algoritma AES256 dan Blowfish," *Jurnal Transformasi (Informasi Pengembangan Iptek)*, vol. 14, no. 1, pp. 84-91, 2018.

[12] A. Siswanto, A. Syukur, and I. Husna, "Perbandingan Metode Data Encryption Standard (Des) dan Advanced Encryption Standard (AES) Pada Steganografi File Citra," *Seminar Nasasional Teknologi Informasi Dan Komunikasi (SEMNATIK)*, vol. 1, no. 1, pp. 229-236, 2018.