JURNAL FASILKOM
Volume 13 No. 2 | Agustus 2023: 259-268

P-ISSN : 2089-3353
E-ISSN : 2808-9162

IMPLEMENTASI PENGARSIPAN ELEKTRONIK MENGGUNAKAN ENKRIPSI DAN DEKRIPSI DENGAN METODE AES DI UNISKA

Bagus Arianto[1], Harso Kurniadi[2] , Iin Kurniasari[3]
[1,2,3]Teknik Komputer, Fakultas Teknik, Universitas Islam Kadiri
[1]bagusarianto333@gmail.com*, [2]harsokurniadi@uniska-kediri.ac.id, [3]iin.kurniasari@uniska-kediri.ac.id

Abstract

Maintaining the security or privacy of document archives is the most crucial aspect nowadays. Archives containing sensitive information should not be stored in physical form and should not be accessible to unauthorized individuals. With the advancement of technology, manual archiving systems have evolved into more modern and efficient cloud-based archiving systems. At Universitas Islam Kadiri, a website-based archiving system has been implemented, similar to most other website-based archiving systems. However, the security of the archiving system is only present during the authentication process or when users log in. Therefore, there is a need to enhance the security system by creating an electronic archiving website with encryption and decryption capabilities. The website is developed using the advanced encryption standard (AES) and follows a research and development approach, utilizing the waterfall model. Testing of the archiving system on the electronic archiving website with encryption and decryption has shown that the archive files can be encrypted and decrypted smoothly as expected. Hence, it can be concluded that this created electronic archiving website with encryption is suitable for use.

Keywords: advanced encryption standard, AES, encryption, decryption, electronic archiving.

Abstrak

Menjaga keamanan atau privasi arsip dokumen merupakan aspek yang paling penting saat ini. Arsip dokumen yang memiliki informasi sensitif seharusnya tidak disimpan dalam bentuk fisik dan tidak boleh diakses oleh orang yang tidak memiliki izin terhadap berkas arsip tersebut. Seiring berkembangnya teknologi saat ini sistem pengarsipan yang dulunya dilakukan secara manual telah berkembang menjadi sistem pengarsipan berbasis *cloud* yang lebih modern dan efisien. Pada Universitas Islam Kadiri sistem pengarsipan berbasis *website* sebenarnya sudah diterapkan namun seperti kebanyakan sistem pengarsipan berbasis *website* lainnya. Keamanan dari sistem pengarsipan hanya terdapat pada saat proses autentikasi atau saat pengguna melakukan *login* saja. Sehingga perlu dilakukan peningkatan sistem keamanan satunya dengan dibuatnya *website* pengarsipan elektronik dengan enkripsi dan dekripsi. *Website* dibuat dengan enkripsi *advanced encryption standard* dan pembuatan *website* dilakukan menggunakan metode *research and development dimana* aplikasi dikembangkan dengan model *waterfall*. Dari hasil pengujian sistem yang telah dilakukan pada *website* pengarsipan elektronik menggunakan enkripsi dan dekripsi diperoleh hasil bahwa berkas arsip dapat dienkripsi dan didekripsi secara lancar sesuai dengan apa yang telah diharapkan. Sehingga dapat disimpulkan bahwa *website* pengarsipan elektronik dengan enkripsi yang telah dibuat ini layak untuk digunakan.

Kata kunci: advanced encryption standard , AES, enkripsi, dekripsi, pengarsipan elektronik.

1. Pendahuluan

Perkembangan teknologi pada era digital saat ini terus berkembang secara pesat seiring berjalanya waktu, sehingga memberikan banyak peningkatan salah satunya keamanan pada sistem informasi. Selain keamanan sistem informasi digitalisasi kini juga telah mengalami banyak perkembangan. Digitalisasi merupakan faktor penting yang perlu direalisasikan dalam berbagai bidang pada institusi untuk menunjang efisienasi waktu, biaya dan lain-lain.

Saat ini keamanan data merupakan aspek yang paling penting. Salah satu contoh adalah peningkatan sistem keamanan yaitu dengan pemanfaatan kriptografi atau teknik-teknik matematika dalam mengamankan suatu informasi atau pesan asli (*plainteks*) menjadi sebuah teks tersembunyi (*chiperteks*) dan kemudian diubah menjadi pesan asli kembali [1]. Saat ini banyak instansi termasuk Universitas Islam Kadiri berupaya meningkatkan sistem keamanannya untuk mencegah terjadinya kebocoran atau eksploitasi data. Salah satunya pada bidang pengarsipan, yaitu dibuatnya sistem pengarsipan elektronik berbasis *website* yang dilengkapi dengan fitur enkripsi. Pengarsipan berbasis *website* sebenarnya telah ada dan sudah diterapkan pada Universitas Islam Kadiri namun masih belum memanfaatkan fitur enkripsi pada berkas arsip yang akan diarsipkan.

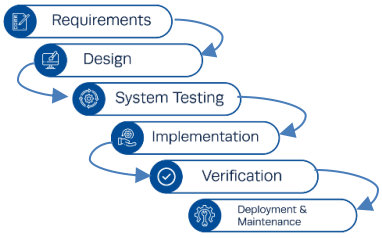
Pengarsipan manual masih dilakukan pada beberapa bidang saat ini, hal ini disebabkan oleh beberapa faktor diantaranya seperti terbatasnya sumber daya manusia dan berbagai faktor internal lainnya. Pengarsipan berkas secara manual akan menyebabkan terjadinya penumpukan data arsip yang ada [2]. Sehingga dapat menyulitkan dalam pencarian arsip yang telah lama tersimpan. Berkas arsip yang tidak dikelola dengan baik dapat berakibat pada rusak atau bahkan hilangnya kertas surat atau arsip tersebut [3]. Selain itu berkas yang tidak dikelola dengan baik menyulitkan karyawan dalam melakukan pencarian berkas arsip jika suatu-waktu arsip itu diperlukan.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Mengenkripsi berkas merupakan hal yang wajib dilakukan terlebih lagi jika berkas tersebut berisi informasi penting yang bersifat sensitif seperti arsip. Berdasarkan uraian dari masalah diatas peneliti membuat sebuah rancang bangun aplikasi pengarsipan elektronik menggunakan enkripsi dan dekripsi dengan metode *advanced encryption standard* sebagai solusi dari permasalahan yang ada. Peneneliti menggunakan algoritma *advanced encryption standard* dikarenakan algoritma ini cukup sulit dipecahkan saat ini [1]. Jika berkas arsip sudah dienkripsi menggunakan algoritma *advanced encryption standard* dan tidak didekripsikan dengan kunci yang telah dibuat sebelumnya, maka berkas tersebut tidak bisa dibaca dan diunduh sehingga mustahil untuk orang dapat memahami apa isi dari berkas tersebut.

2. Metode Penelitian

Metode yang digunakan dalam merancang aplikasi pengarsipan elektronik menggunakan enkripsi dan dekripsi dengan metode *advanced encryption standard* ini adalah metode penelitian dan pengembangan atau *research and development* (R&D). Aplikasi dikembangkan dengan menggunakan model *waterfall* atau air terjun. Model *waterfall* merupakan model klasik dengan pendekatan sistematis dan berurutan terhadap tingkat kemajuan sistem dalam semua analisis, desain, kode, pengujian, dan pemeliharaan [4]. Dalam model *waterfall* tahap awal dimulai dari perencanaan atau *requirement*, *design system*, *coding and testing* (penulisan sinkode program atau implementasi), *integration and testing* (verifikasi penerapan atau pengujian program), lalu yang terakhir adalah *operation and maintenance* [5]. Berikut adalah gambar tahapan dalam metode *waterfall* :



Gambar 1. Model *Waterfall*

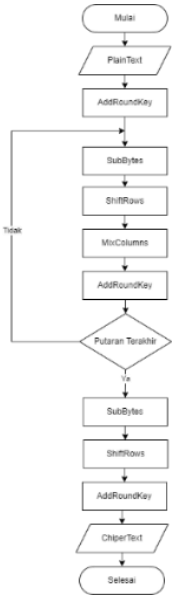
2.1. *Advanced Encryption Standard*

AES atau (*Advanced encryption standard)* adalah standar enkripsi kunci simetris yang dapat digunakan untuk mengamankan data, dikembangkan oleh kriptografer dari Belgia Joan Daemen dan Vincent Rijmen [6]. *Advanced encryption standard* atau disingkat AES merupakan standar algoritma kriptografi terbaru yang dipublikasikan oleh *National Institute of Standards and Technology* dan faktanya *advanced encryption standard* sendiri hampir mustahil untuk dipecahkan kuncinya secara paksa [7]. *Advanced encryption standard* terdiri dari tiga jenis yaitu AES-128, AES-192, dan AES-256. Pada dasarnya jenis enkripsi ini memiliki ukuran blok yang sama yaitu 128 bit yang membedakan hanya jumlah putaran [6]. Berikut adalah tabel perbedaan jenis *advanced encryption standard* :

Tabel 1. Jenis-Jenis *Advanced Encryption Standard*

No	Jenis	Ukuran Blok	Putaran	Panjang
1	AES 128	128 Bit	10 Putaran	128 Bit
2	AES 192	128 Bit	12 Putaran	192 Bit
3	AES 256	128 Bit	14 Putaran	256 Bit

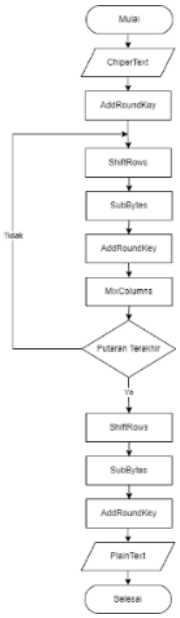
Dalam proses enkripsi *advanced encryption standard* terdiri dari empat jenis transformasi byte diantaranya *addroundkey, subbytes, shiftrows, dan mixcolumns* [6]. Keempat jenis transformasi *byte* tersebut merupakan bagian wajib dari setiap proses enkripsi *advanced encryption standard*. Transformasi ini digunakan untuk memperkenalkan kompleksitas pada blok data yang akan dienkripsi sehingga membuatnya sulit untuk dipecahkan [1]. Setiap jenis transformasi memiliki fungsi dan tujuan masing-masing, setelah itu diproses untuk penggabungan dalam beberapa putaran enkripsi untuk menghasilkan kunci yang aman dan dapat diandalkan untuk mengamankan data. Berikut adalah gambaran *flowchart* pada proses penguncian atau enkripsi berkas menggunakan metode *advanced encryption standard* :



Gambar 2. Flowchart Proses Enkripsi

Selanjutnya yaitu proses pengembalian berkas menjadi format asli atau dekripsi pada *advanced encryption standard* hampir sama dengan proses enkripsi, tetapi prosesnya dilakukan dalam urutan yang berlawanan. Proses ini membutuhkan kunci yang sama saat digunakan pada proses enkripsi untuk membantu membuka berkas arsip yang terenkripsi. Blok-blok data dalan proes dekripsi yang telah diterenkripsi diproses melalui serangkaian transformasi yaitu *AddRoundKey, InvShiftRows, InvSubBytes,* dan *InvMixColumn* [8]. Berikut adalah tampilan *flowchart*nya :

P-ISSN : 2089-3353
E-ISSN : 2808-9162



Gambar 3. *Flowchart* Proses Dekripsi

Kecepatan saat menjalankan proses enkripsi dan dekripsi tidak dipengaruhi oleh format berkas saja, melainkan dipengaruhi oleh perangkat keras , ukuran berkas serta panjang kunci yang dipakai. Semakin besar ukuran berkas asli (*plainteks*) maka semakin lama waktu yang dibutuhkan untuk memrosesnya. Selain itu proses enkripsi dan dekripsi dengan panjang kunci 128 bit membutuhkan waktu lebih cepat dibandingkan menggunakan panjang kunci 192 bit dan 256 bit [9].

2.2. Rancangan Kebutuhan Sistem

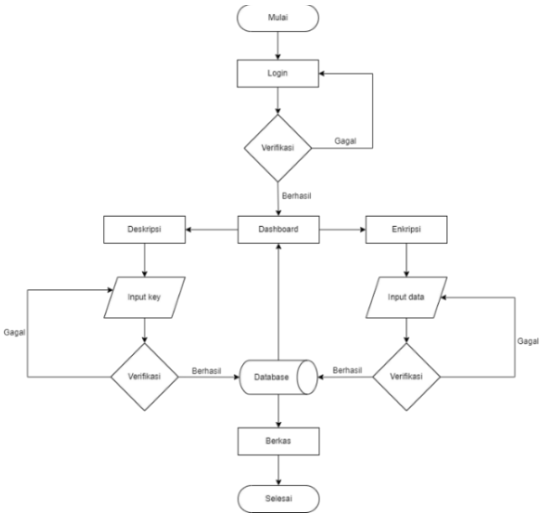
Kebutuhan sistem berperan penting dalam pengembangan sistem yang akan dibuat. Dengan memahami kebutuhan pengguna dan masalah yang ada, peneliti dapat merancang dan mengimplementasikan pada sistem. Sehingga dapat menghasilkan solusi untuk memenuhi kebutuhan. Pada tahapan ini, kebutuhan sistem dihasilkan berdasarkan hasil analisis terhadap sistem yang berjalan dan analisis terhadap dokumen sistem [10]. Berikut adalah tabel rancangan kebutuhan sistem yang telah dibuat :

Tabel 2. Kebutuhan Sistem

No	Hasil Analisa	Keluaran
1	Sistem	Sistem dapat menampilkan *form login*, mengenkripsi berkas arsip, mendekripsi berkas arsip, mengunduh berkas yang telah didekripsi, menghapus berkas arsip dan mengunci ulang berkas arsip yang telah didekripsi.
2	Pengguna	Pengguna dapat menginput berkas arsip (enkripsi), melihat dan mengunduh berkas arsip (dekripsi) serta mengunci dan menghapus berkas arsip.

2.3. Analisa Alur Sistem

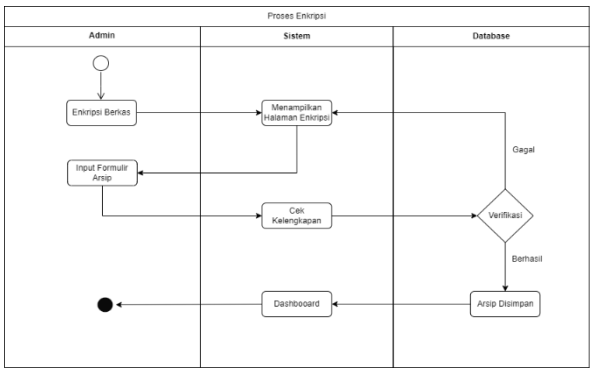
Dalam rancangan yang telah dibuat, format berkas arsip yang dapat dienkripsi berupa format yang umum digunakan dari *Microsoft Office* yaitu *word*, excel, dan *power point* termasuk, pdf dan txt serta format jpg dan png pada gambar. *Flowchart* adalah rangkaian bagan yang menggambarkan urutan suatu proses kegiatan dalam mencapai tujuan yang diinginkan [11]. Dalam rancangan analisa sistem *flowchart* dapat membantu dalam identifikasi dan mengatasi masalah yang ada dalam sistem dan membantu dalam perencanaan sistem yang akan dikembangkan [11]. Berikut adalah *flowchart* dari rancangan sistem yang telah dibuat :



Gambar 4.Analisa Alur Sistem

2.4. Desain Sistem

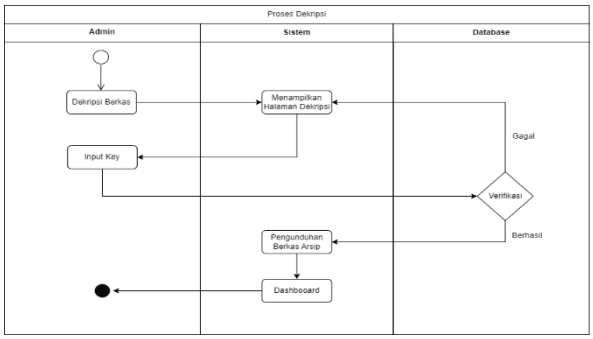
Arsitektur atau desain sistem adalah gambaran cara kerja sistem, sehingga mempermudah pemahaman *user* mengenai cara kerja sistem informasi [12]. *Activity* diagram dibuat untuk rancangan pada rancang bangun aplikasi dan menggambarkan semua proses yang ada pada sistem informasi ini [4]. Berikut adalah rancangan desain *actifity* diagram proses enkripsi yang telah dibuat :



Gambar 5. Desain Sistem Enkripsi

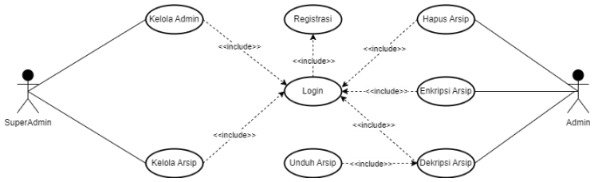
Selain desain sistem enkripsi peneliti juga membuat desain sistem dekripsi. Berikut adalah desain sistem proses dekripsi yang telah dibuat.

P-ISSN : 2089-3353
E-ISSN : 2808-9162



Gambar 6. Desain Sistem Dekripsi

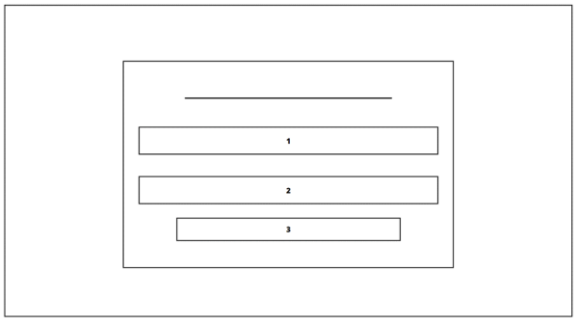
Selain *activity* diagram peneliti juga membuat rancangan *usecase* yang akan digunakan. Berikut adalah desain rancangan *usecase* yang telah dibuat :



Gambar 7. Desain *Usecase*

2.5. Desain Aplikasi

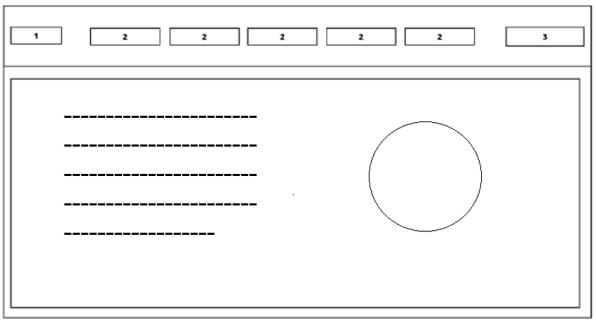
Desain aplikasi yaitu dokumentasi yang menjelaskan secara singkat bagaimana aplikasi yang akan dikembangkan akan terlihat dan bekerja. Ringkasan ini biasanya berisi informasi tentang tampilan antarmuka, fitur dan fungsionalitas. Selanjutnya adalah desain rancangan halaman *login*, berikut merupakan desain rancangan aplikasi yang telah dibuat.



Gambar 8. Desain Halaman *Login*

Berikut keterangan yang terdapat pada gambar 8 :
1. Keterangan pada angka 1 merupakan formulir untuk menemasukan *username*
2. Keterangan nomor 2 merupakan formulir *password*
3. Keterangan nomor 3 merupakan tombol masuk

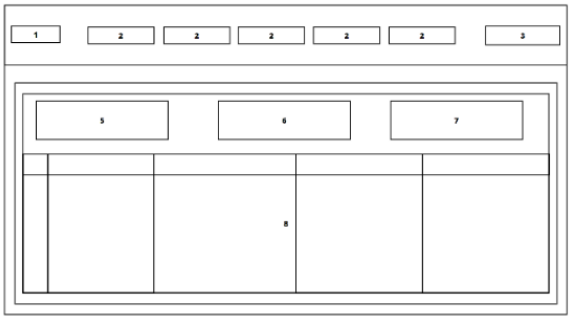
Pada Gambar 9 merupakan desain rancangan aplikasi yang telah dibuat pada halaman beranda. Berikut adalah tampilan halaman beranda.



Gambar 9. Desain Tampilan Beranda

Berikut keterangan yang terdapat pada gambar 9 :
1. Keterangan nomor 1 merupakan logo dari *website*.
2. Keterangan nomor 2 merupakan tombol menu yang terdiri dari menu beranda, dekripsi, enkripsi, bantuan dan tentang aplikasi.
3. Keterangan nomor 3 merupakan menu profil dan menu *logout*.
4. Keterangan kotak nomor 4 merupakan menu utama yang disajikan dalam *website* atau *welcome page*.

Pada gambar 10 dibawah ini merupakan desain rancangan aplikasi yang telah dibuat pada halaman berkas disimpan.

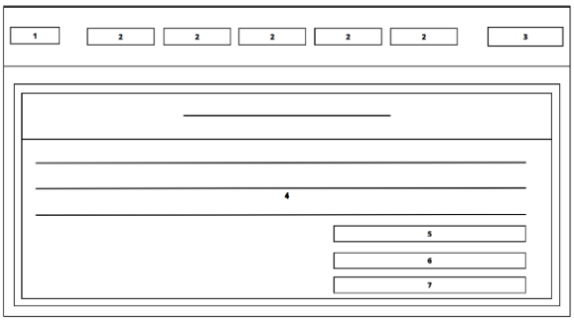


Gambar 10. Halaman Berkas Disimpan

Berikut keterangan yang terdapat pada gambar 10 :
1. Keterangan nomor 1 merupakan logo dari *website*.
2. Keterangan nomor 2 merupakan tombol menu yang terdiri dari menu beranda, dekripsi, enkripsi, bantuan dan tentang aplikasi.
3. Keterangan nomor 3 merupakan menu profil dan menu logout.
4. Keterangan nomor 4 merupakan tombol kunci ulang berkas.
5. Keterangan nomor 5 merupakan tombol menu enkripsi.
6. Keterangan nomor 6 merupakan tombol menu pusat bantuan.
7. Keterangan nomor 7 merupakan tampilan berkas tersimpan.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

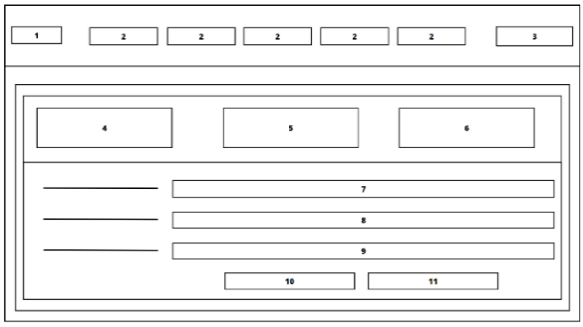
Pada gambar 11 dibawah ini adalah desain rancangan aplikasi yang telah dibuat pada halaman proses dekripsi.



Gambar 11. Halaman Proses Dekripsi

Berikut keterangan yang terdapat pada gambar 11 :
1. Keterangan nomor 1 merupakan logo dari *website*.
2. Keterangan nomor 2 merupakan tombol menu yang terdiri dari menu beranda, dekripsi, enkripsi, bantuan dan tentang aplikasi.
3. Keterangan nomor 3 merupakan menu profil dan menu logout.
4. Keterangan nomor 4 detail berkas yang akan didekripsi.
5. Keterangan nomor 5 formulir key dekripsi.
6. Keterangan nomor 6 tombol proses dekripsi.
7. Keterangan nomor 7 tombol batal.

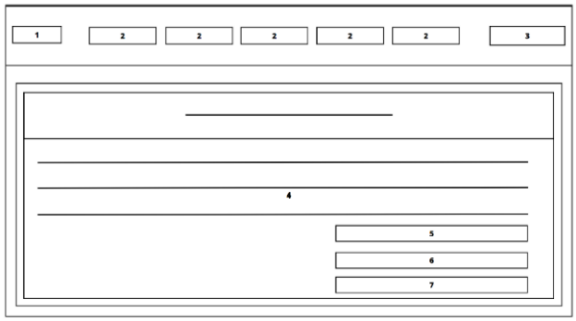
Pada gambar 12 dibawah ini merupakan desain rancangan aplikasi yang telah dibuat pada halaman proses enkripsi.



Gambar 12. Halaman Proses Enkripsi

Berikut keterangan yang terdapat pada gambar 12 :
1. Keterangan nomor 1 merupakan logo dari *website*.
2. Keterangan nomor 2 merupakan tombol menu yang terdiri dari menu beranda, dekripsi, enkripsi, bantuan dan tentang aplikasi.
3. Keterangan nomor 3 merupakan menu profil dan menu logout.
4. Keterangan nomor 4 jumlah berkas dienkripsi.
5. Keterangan nomor 5 tombol untuk melihat berkas.
6. Keterangan nomor 6 total berkas didekripsi.
7. Keterangan nomor 7 formulir penginputan judul berkas.
8. Keterangan nomor 8 formulir upload berkas.
9. Keterangan nomor 9 formulir *key* atau *password* berkas.
10. Keterangan nomor 10 tombol konfirmasi upload berkas.
11. Keterangan nomor 11 tombol batal.

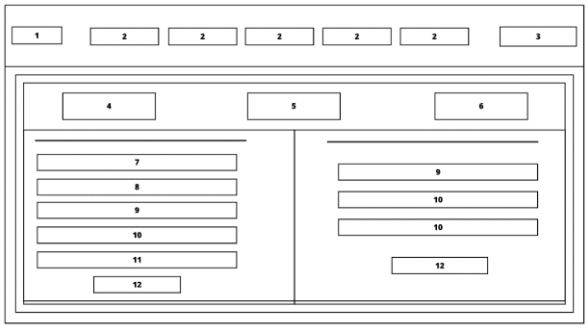
Gambar 13 merupakan desain desain aplikasi yang telah dibuat pada halaman hapus arsip. Berikut adalah desain yang telah dibuat.



Gambar 13. Halaman Hapus Arsip

Berikut keterangan yang terdapat pada gambar 13 :
1. Keterangan nomor 1 merupakan logo dari *website*.
2. Keterangan nomor 2 merupakan tombol menu yang terdiri dari menu beranda, dekripsi, enkripsi, bantuan dan tentang aplikasi.
3. Keterangan nomor 3 merupakan menu profil dan menu logout.
4. Keterangan nomor 4 detail berkas yang akan dihapus.
5. Keterangan nomor 5 formulir key hapus berkas.
6. Keterangan nomor 6 tombol proses hapus.
7. Keterangan nomor 7 tombol batal.

Gambar 14 merupakan desain desain aplikasi yang telah dibuat pada halaman kelola akun.



Gambar 14. Halaman Kelola Akun

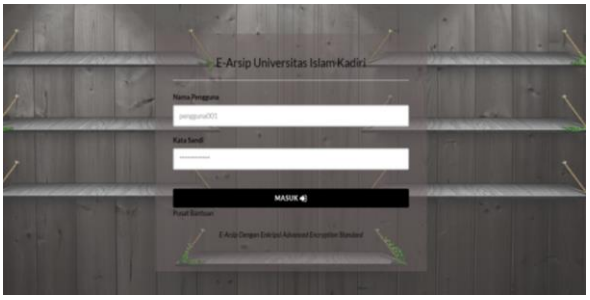
. Berikut keterangan yang terdapat pada gambar 14 :
1. Keterangan nomor 1 merupakan logo dari *website*.
2. Keterangan nomor 2 merupakan tombol menu yang terdiri dari menu beranda, dekripsi, enkripsi, bantuan dan tentang aplikasi.
3. Keterangan nomor 3 merupakan menu profil dan menu logout.
4. Keterangan nomor 4 jumlah berkas dienkripsi.
5. Keterangan nomor 5 tombol untuk melihat berkas.
6. Keterangan nomor 6 total berkas didekripsi.
7. Keterangan nomor 7 merupakan inputan nama pengguna.
8. Keterangan nomor 8 merupakan inputan *username* untuk *login*.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

9. Keterangan nomor 9 merupakan inputan *password* untuk *login*.
10. Keterangan nomor 10 merupakan inputan konfirmasi *password*.
11. Keterangan nomor 10 merupakan menu untuk memilih *role* akun.
12. Keterangan nomor 10 merupakan tombol untuk memproses perintah.

3. Hasil dan Pembahasan

Penelitian ini menghasilkan sebuah aplikasi yang dibernama "KEDOK AES" atau Keamanan Dokumen Dengan Metode *Advanced Encyption Standard*. Aplikasi ini berbasis *website* yang dapat diakses dari perangkat *desktop* atau *mobile*. Bahasa pemrograman yang digunakan adalah *php* dangan *MySQL* sebagai basis datanya. *PHP* merupakan bahasa pemrograman *open-source* sehingga pengguna bebas menggunakan bahasa pemrograman *PHP*. *PHP* dapat digunakan di Linux, Mac OS, Solaris dan semua versi *Windows* [13]. Berikut adalah implementasi dari hasil rancangan yang telah dibuat sebelumnya :



Gambar 15. Implementasi Halaman *Login*

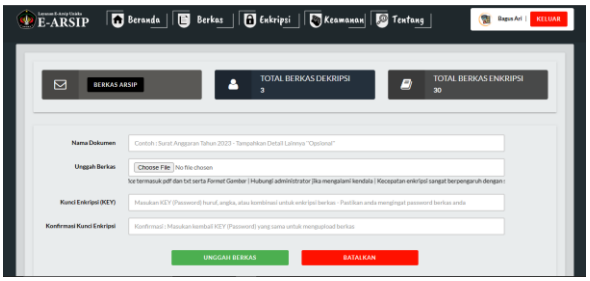
Gambar 15 merupakan implementasi dari halaman *login* yang telah dibuat. Berikut adalah penjelasan dari fitur-fiturnya.

Tabel 3. Fitur Halaman *Login*

No	Fitur	Keterangan
1	*Username*	Formulir ini akan digunakan pengguna untuk menginputkan *username*
2	*Password*	Formulir ini akan digunakan pengguna untuk menginputkan *password*
3	Masuk	Tombol ini akan digunakan pengguna untuk proses masuk setelah memsaukan *username* dan *password*.

Gambar 16. Halaman *Dashboard*

Gambar 16 merupakan implementasi dari halaman *dashboard*. Halaman ini akan disajikan setelah pengguna berhasil melewati proses verifikasi atau *login*. Disini *dashboard* berisi logo dari tempat penelitian serta keterangan mengenai aplikasi yang telah dibuat.

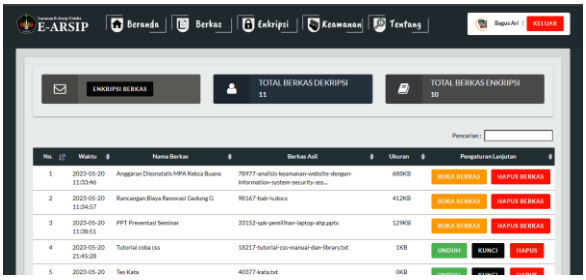


Gambar 17. Formulir Enkripsi Berkas Arsip

Gambar 17 merupakan implementasi dari halaman Enkripsi. Pada halaman ini pengguna dapat melakukan proses enkripsi berkar arsip. Berikut adalah penjelasan dari fitur-fiturnya :

Tabel 4. Fitur Enkripsi Berkas

No	Fitur	Keterangan
1	Nama Dokumen	Pengguna diwajibkan memasukkan nama dokumen pada formulir ini.
2	Unggah Berkas	Pada formulir ini pengguna harus memasukkan berkas dengan format yang telah ditetapkan.
3	Kunci (KEY)	*Password* atau *key* adalah kunci yang harus dibuat pengguna untuk mengunci berkas. *Password* wajib diisi minimal 8 karakter.
4	Konfirmasi KEY	Formulir konfirmasi digunakan supaya pengguna ingat dengan *password* yang dibuat sebelumnya.



Gambar 18. Implementasi Arsip Tersimpan

Gambar 18 merupakan implementasi dari halaman berkas tersimpan. Pada halaman ini pengguna dapat melakukan beberapa tindakan seperti melihat atau mengunduh arsip, mengunci arsip dan menghapus arsip. Berikut adalah penjelasan dari fitur-fiturnya.

Tabel 5. Fitur Arsip Tersimpan

No	Fitur	Keterangan
1	Buka Berkas	Fitur ini digunakan untuk membuka berkas, dimana pengguna akan diarahkan ke halaman buka berkas.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

2	Unduh	Setelah berhasil membuka berkas fitur unduh akan tampil yang digunakan mengunduh berkas.
3	Kunci	Ketika pengguna berhasil membuka berkas pengguna dapat mengunci berkas supaya berkas arsip tetap aman.
4	Hapus	Fitur hapus digunakan untuk menghapus berkas, dimana pengguna akan diarahkan ke halaman hapus berkas.

Gambar 19. Proses Dekripsi Berkas

Gambar 19 merupakan implementasi dari halaman proses dekripsi berkas. Pada halaman ini pengguna dapat melakukan pengunduhan berkas setelah pengguna berhasil melewati proses verifikasi. Jika gagal maka berkas tidak akan bisa dilihat maupun diunduh. Berikut adalah penjelasan dari fitur-fiturnya.

Tabel 6. Fitur Proses Dekripsi

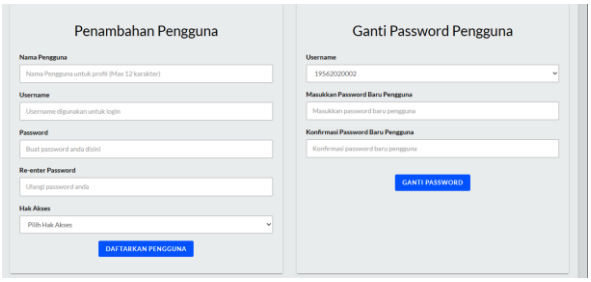
No	Fitur	Keterangan
1	Nama Berkas	Menampilkan informasi nama berkas.
2	Berkas Dokumen	Menampilkan nama dan format ekstensi asli dari berkas tang tersimpan.
3	Ukuran	Menampilkan ukuran berkas yang telah disimpan.
4	Waktu	Menampilkan informasi waktu berupa tanggal, bulan, tahun dan jam saat berkas diarsipkan.
5	*Key*	Formulir untuk memasukkan *password* atau *key* sebelum proses dekripsi berlangsung.
6	Dekripsi Berkas	Tombol untuk mengeksekusi berkas supaya dapat dienkripsi
7	Batal	Tombol untuk kembali ke menu penyimpanan berkas.

Gambar 20. Halaman Hapus Berkas

Gambar 20 merupakan implementasi dari halaman hapus berkas. Pada halaman ini pengguna dapat menghapus berkas yang sebelumnya telah diarsipkan setelah berhasil melewati proses verifikasi. Jika gagal maka berkas tidak akan dihapus dan harus melakukan verifikasi ulang. Berikut adalah penjelasan dari fitur-fiturnya.

Tabel 7. Fitur Halaman Hapus Berkas

No	Fitur	Keterangan
1	Nama Berkas	Menampilkan informasi nama berkas.
2	Berkas Dokumen	Menampilkan nama dan format ekstensi asli dari berkas tang tersimpan.
3	Ukuran	Menampilkan ukuran berkas yang telah disimpan
4	Waktu	Menampilkan informasi waktu berupa tanggal, bulan, tahun dan jam saat berkas diarsipkan.
5	*Key*	Formulir untuk memasukkan *password* atau *key* sebelum proses hapus berkas.
6	Hapus Berkas	Tombol untuk mengeksekusi berkas supaya dapat dihapus.
7	Batal	Tombol untuk kembali ke menu penyimpanan berkas.



Gambar 21. Halaman Kelola Pengguna

Gambar 21 merupakan halaman pengelolaan pengguna. Pada halaman ini admin dapat mengganti *password* penggunanya maupun menambahkan akun pengguna. Berikut adalah penjelasan dari fitur-fiturnya.

Tabel 8. Fitur Halaman Kelola Pengguna

No	Fitur	Keterangan
1	Nama Pengguna	Formulir untuk menambahkan inputan dari nama pengguna.
2	*Username*	Formulir untuk menambahkan inputan dari *username* yang digunakan untuk *login* apliaksi
3	*Passowrd*	Formulir untuk menambahkan inputan *password* yang digunakan untuk *login*.
4	Re-enter *Password*	Formulir untuk mengkonfirmasi password yang telah dibuat.
5	Hak Akses	Menu untuk memilih menyatakan akun bahwa akun yang didaftarkan itu berperan sebagai admin atau superadmin.
6	Daftarkan Pengguna	Tombol eksekusi untuk mendaftarkan pengguna baru.
7	Ganti *Password*	Tombol eksekusi untuk mengganti *password* pengguna.

3.1. Pengujian Sistem

Peneliti telah menguji coba dengan mengenkripsi dan mendekripsikan berkas dokumen dengan ukuran dan ekstensi yang berbeda-beda. Pengujian lainnya dilakukan dengan menghitung efisiensi waktu terhadap kecepatan dalam proses enkripsi dan dekripsi pada berkas, pengujian pengaruh ukuran berkas sebelum berkas dienkripsi dan dekripsi dan pengujian lainnya menggunakan metode *blackbox*. Berikut adalah spesifikasi *software* dan *hardware* yang digunakan :

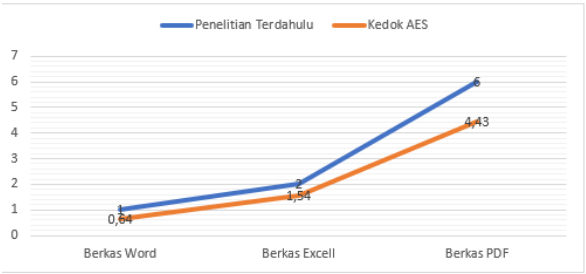
P-ISSN : 2089-3353
E-ISSN : 2808-9162

Tabel 9. Spesifikasi Perangkat

No	Hardware	Spesifikasi	*Software*	Versi
1	Prosesor	AMD A9	*Xampp*	3.3.0
2	Penyimpanan	SSD 128 Gb HDD 500 Gb	*Visual Studio Code*	1.78.2
3	RAM	8 Gb	*Microsoft Edge*	113.0.1774.42

3.2. Pengujian Efisiensi Aplikasi

Peneliti akan menguji efisiensi waktu dengan cara mengenkripsi dan mendekripsikan berkas dokumen dengan ukuran dan format yang berbeda-beda pada aplikasi keamanan dokumen dengan metode *advanced encyption standard* atau "KEDOK AES". Penelitianlain yang berjudul Implementasi Algoritma *Advanced Encryption Standard* 128 (Aes 128) Berbasis Web Pada Kedai Kopi Ngopiyuka! [14] akan dijadikan pembanding, karena semakin cepat proses enkripsi dan dekripsi maka semakin efisien aplikasi yang telah dibuat. Berikut adalah hasil perbandingan pengukuran dari kecepatan enkripsi :



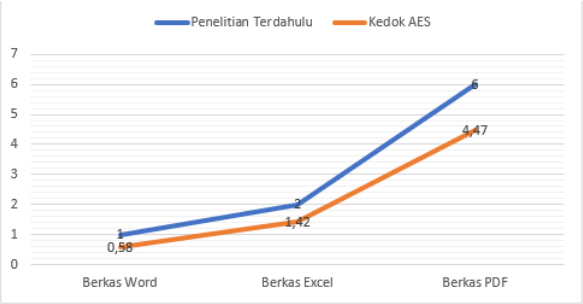
Gambar 22. Perbandingan Kecepatan Enkripsi

Pengujian pertama pada berkas *word* kecepatan enkripsi penelitian terdahulu membutuhkan waktu 1 detik sedangkan penelitian sekarang 0,64 detik maka dengan rumus hitung selisih waktu enkripsi yaitu selisih = waktu enkripsi pertama - waktu enkripsi kedua selisih = 1 - 0.64 = 0.36 detik dan persentase perubahan = (0.36 / 1) * 100 = 36%. Berikut tabel pengukuran yang lebih lengkap yang telah dibuat.

Tabel 10. Tabel Hasil Pengukuran Ukuran Berkas Enkripsi

Nama Berkas	Ukuran	Dekripsi *Old*	Dekripsi *New*	Selisih	Presentase Selisih
Word	27 Kb	1 *Sec*	0.64 *Sec*	0.36 *Sec*	36 %
Excel	58 Kb	2 *Sec*	1.54 *Sec*	0.46 *Sec*	23 %
PDF	212 Kb	6 *Sec*	4.43 *Sec*	1.57 *Sec*	26.17 %

Selanjutnya pengujian dekripsi dilakukan dengan membandingkan pada penelitian terdahulu dan akan dijadikan pembanding pada kecepatan dekripsi. Berikut adalah hasil perbandingan pengukuran dari kecepatan dekripsi :



Gambar 23 Perbandingan Kecepatan Enkripsi

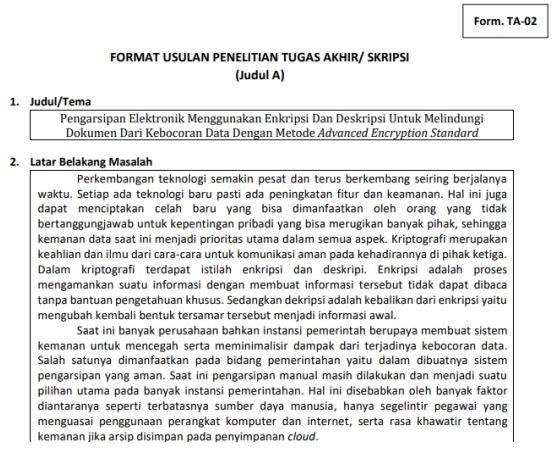
Pengukuran kecepatan dilakukan dengan rumus Selisih waktu enkripsi: Selisih = Waktu Enkripsi Pertama - Waktu Enkripsi Kedua Selisih = 1 - 0.58 = 0.42 detik. Persentase perubahan: Persentase Perubahan = (Selisih / Waktu Enkripsi Pertama) * 100 Persentase Perubahan = (0.42 / 1) * 100 = 42%. Berikut adalah hasil perbandingan pengukuran dari kecepatan dekripsi :

Tabel 11. Tabel Hasil Pengukuran Ukuran Berkas Dekripsi

Nama Berkas	Ukuran	Dekripsi *Old*	Dekripsi *New*	Selisih	Presentase Selisih
Word	27 Kb	1 *Sec*	0.58 Sec	0.42 *Sec*	42 %
Excel	58 Kb	2 *Sec*	1.42 *Sec*	1,58 *Sec*	29 %
PDF	212 Kb	6 *Sec*	4.47 *Sec*	1,53 *Sec*	25,5 %

3.3. Tampilan Berkas Setelah Enkripsi Dan Dekripsi

Saat berkas dienkripsi terdapat perubahan pada isi data berkas, sehingga berkas tidak dapat dibaca oleh orang yang tidak mengetahui apa kunci dari berkas tersebut. Berikut adalah salah satu contoh yaitu berkas pdf yang telah dienkripsi dan dekripsi.



Form. TA-02

FORMAT USULAN PENELITIAN TUGAS AKHIR/ SKRIPSI
(Judul A)

1. **Judul/Tema**

Pengarsipan Elektronik Menggunakan Enkripsi Dan Deskripsi Untuk Melindungi Dokumen Dari Kebocoran Data Dengan Metode *Advanced Encryption Standard*

2. **Latar Belakang Masalah**

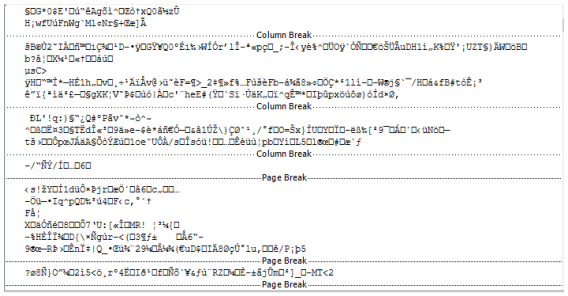
Perkembangan teknologi semakin pesat dan terus berkembang seiring berjalanya waktu. Setiap ada teknologi baru pasti ada peningkatan fitur dan keamanan. Hal ini juga dapat menciptakan celah baru yang bisa dimanfaatkan oleh orang yang tidak bertanggungjawab untuk kepentingan pribadi yang bisa merugikan banyak pihak, sehingga kemanan data saat ini menjadi prioritas utama dalam semua aspek. Kriptografi merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Dalam kriptografi terdapat istilah enkripsi dan deskripi. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Sedangkan dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Saat ini banyak perusahaan bahkan instansi pemerintah berupaya membuat sistem kemanan untuk mencegah serta meminimalisir dampak dari terjadinya kebocoran data. Salah satunya dimanfaatkan pada bidang pemerintahan yaitu dalam dibuatnya sistem pengarsipan yang aman. Saat ini pengarsipan manual masih dilakukan dan menjadi suatu pilihan utama pada banyak instansi pemerintahan. Hal ini disebabkan oleh banyak faktor diantaranya seperti terbatasnya sumber daya manusia, hanya segelintir pegawai yang menguasai penggunaan perangkat komputer dan internet, serta rasa khawatir tentang kemanan jika arsip disimpan pada penyimpanan *cloud*.

Gambar 24. Dokumen PDF Sebelum Dienkripsi

Sebelum berkas pdf dienkripsi isi dokumen akan menampilkan data seperti yang terdapat pada gambar 24. Dimana data masih bisa dibaca secara normal. Selanjutnya adalah tampilan berkas setelah dienkripsi.

P-ISSN : 2089-3353
E-ISSN : 2808-9162



Gambar 25. Dokumen PDF Setelah Dienkripsi

Setelah dienkripsi berkas akan menampilkan data yang bersifat acak seperti pada gambar 25 sehingga sangat tidak mungkin berkas dapat dibaca sebelum dilakukannya proses didekripsi.

3.4. Pengujian Aplikasi Menggunakan *Black Box*

Berdasarkan hasil pengujian telah diperoleh kesimpulan dengan menyesuaikan antara hasil yang diharapkan dan hasil pengujian. Pengujian aplikasi menggunakan metode *blackbox* dengan melibatkan 15 tester sehingga diperoleh hasil sebagai berikut :

Tabel 12. Pengujian Aplikasi Menggunakan *BlackBox*

ID	Deskripsi	Hasil Yang Diharapkan	Hasil Pengujian	Status
BB1	Melakukan *login* untuk menggunakan aplikasi Kedok AES.	Sistem akan menolak jika *username* dan *password* yang dimasukan salah.	Sistem akan memberitahu jika *username* dan *password* yang dimasukan salah.	Sukses
BB2	Melengkapi formulir pada proses enkripsi seperti nama berkas, berkas, kunci berkas, dan konfirmasi kunci berkas.	Jika formulir terpenuhi sistem akan menyimpan dan mengenkripsi berkas.	Sistem berhasil menyimpan dan mengenkripsi berkas sesuai syarat.	Sukses
BB3	Tidak melengkapi kolom pada formulir enkripsi lalu pengguna menekan tombol unggah berkas.	Sistem akan menolak sehingga proses enkripsi tidak dapat diteruskan.	Sistem dapat memberikan peringatan pada setiap kolom inputan jika belum dilengkapi.	Sukses
BB4	Mengupload arsip dokumen yang tidak sesuai dengan format yang didukung.	Sistem menolak berkas tersebut dan berkas tersebut tidak akan disimpan.	Sistem menolak dan memberitahu bahwa berkas tersebut tidak didukung.	Sukses
BB5	Meng*upload* arsip dokumen dengan ukuran melebihi kapasitas yang ditentukan.	Sistem akan menolak dan berkas tidak akan disimpan.	Sistem menolak dan memberikan pemberitahuan bahwa ukuran melebihi batas.	Sukses
BB6	Membuka berkas arsip yang telah dienkripsi.	Sistem akan memverifikasi jika *key* benar berkas akan terbuka jika salah berkas akan tetap terkunci.	Sistem dapat memverifikasi jika salah dan benar dalam melakukan input *key* untuk membuka berkas arsip.	Sukses
BB7	Menghapus berkas arsip.	Sistem akan memverifikasi *key*, jika benar berkas akan terhapus dan jika salah berkas akan tidak terhapus.	Sistem dapat memverifikasi *key*, jika benar berkas akan terhapus dan jika salah berkas akan tidak terhapus dan menampilkan pesan.	Sukses
BB8	Mengunci ulang berkas arsip yang telah didekripsi.	Sistem akan mengubah *value* ke posisi saat berkas belum terenkripsi.	Sistem dapat mengunci ulang berkas arsip yang telah didekripsi dan dan menghapus berkas asli yang telah didekripsi.	Sukses
BB9	Membuka berkas arsip dengan akun yang berbeda.	Jika mengetahui *key* dan *login* akun lain maka berkas akan tetap bisa dibuka	Sistem dapat membuka arsip jika berhasil *login* dan mengetahui *key*	Sukses
BB10	Mengunduh berkas arsip.	Berkas arsip tidak akan dapat diunduh jika tidak didekripsikan terlebih dahulu.	Sistem tidak memberikan akses terhadap berkas yang belum dienkripsi. Jika sudah didekripsi maka sistem menyediakan tombol untuk mengunduh arsip.	Sukses
BB11	Mengganti *password*	Admin harus memasukkan *password* lamanya untuk mengganti *password*.	Sistem menampilkan peringatan ketika *password* lama dan konfirmasi *password* tidak sesuai.	Sukses
BB12	Menambahkan pengguna	Superadmin memasukkan nama, *username* (id pengguna) dan *password* untuk menambahkan pengguna.	Sistem akan memperingatkan ketika terdapat username yang sama dan *password* yang tidak sesuai.	Sukses

4. Kesimpulan

Apliaksi keamanan dokumen dengan metode *advanced encyption standard* “Kedok AES” merupakan sebuah aplikasi berbasis *website* yang bekerja sama dengan

Biro Sistem Informasi Manajemen Universitas Islam Kadiri. Perancangan dan pengimplementasian telah sesuai dan sudah dilakukan uji coba aplikasi mengenkripsi dan mendekripsikan berkas dengan ekstensi dari *microsoft word* berupa *excel, power point*, pdf dan txt. Ujicoba efisiensi kecepatan enkripsi dan dekripsi telah dilakukan dengan membandingkan kecepatan enkripsi dan dekripsi dengan format dan jenis berkas yang sama dengan penelitian terdahulu dan menghasilkan data yang tertera pada pengujian efisiensi. Pengujian aplikasi ini menghasilkan nilai (36%), (23%) dan (26,17%) untuk selisih kecepatan enkripsi dan (42%), (29%) dan (25%) untuk selisih kecepatan dekripsi. Sehingga aplikasi Kedok AES memiliki rata-rata kecepatan enkripsi 28,39% dan kecepatan dekripsi 32,17% dimana prosesnya memakan waktu lebih sedikit.

Ucapan Terimakasih

Alhamdulillah atas izin-Nya peneliti senantiasa diberikan kesehatan serta kesabaran sehingga berhasil menyelesaikan jurnal ini. Tidak lupa peneliti mengucapkan terima kasih banyak kepada kedua orang tua karena selalu mendo'akan apa yang terbaik untuk anaknya dan jasa-jasanya yang telah diberikan selama ini salah satunya membiayai sekolah hingga lulus dan mendapatkan gelar S1. Terima kasih kepada bapak dan ibu dosen pembimbing yang senantiasa membimbing dengan sabar hingga jurnal ini terbit dan terima kasih kepada bapak dosen penguji yang senantiasa memberikan masukan selama ini. Peneliti juga berterima kasih kepada dosen, staf fakultas teknik, sahabat, teman-teman dan saudara yang telah mendukung selama ini.

Daftar Rujukan

[1] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, Nov. 2018, doi: 10.15408/jti.v11i2.7811.

[2] A. R. Riefnaldi, A. Aranta, and M. Muaidi, "Pembuatan Sistem Informasi Pengarsipan Surat Pada Kantor Desa Sandik Berbasis Website," *J. Begawe Teknol. Inf.*, vol. 2, no. 2, pp. 191–202, 2021, doi: 10.29303/jbegati.v2i2.557.

[3] A. Rohman, A. Syarif Hidaytullah, and Mg. Rohman, "Implementasi Metode Waterfall pada Rancang Bangun Sistem Pengarsipan Surat Berbasis Website," *Gener. J.*, vol. 6, no. 2, pp. 93–102, 2022, doi: 10.29407/gj.v6i2.17871.

[4] F. Fajriani, A. H. Jatmika, and L. M. Ulum, "Sistem Informasi Pengelolaan Arsip Surat Di Kantor Bpkad Provinsi Nusa Tenggara Barat Berbasis Web Dengan Php Mysql," *J. Begawe Teknol. Inf.*, vol. 1, no. 1, pp. 120–130, 2020, doi: 10.29303/jbegati.v1i1.158.

[5] M. Syafiih, N. Istifadah, and N. H. I. Arifin, "Sistem Informasi Jadwal Dan Pemesanan Tiket Keberangkatan Kapal Laut Di Pelabuhan Jangkar Berbasis Android," *J. Ilm. Inform.*, vol. 7, no. 2, pp. 107–116, Jan. 2023, doi: 10.35316/jimi.v7i2.107-116.

[6] R. Firdaus and R. R. Santika, "Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security," 2022.

[7] R. C. Halim and S. Sugiarto, "Penerapan Algoritma AES dalam Perancangan Aplikasi Media Sosial Berbasis Android," *J. ENTER*, vol. 1, pp. 368–379, 2018.

[8] K. Muttaqin and J. Rahmadoni, "Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," 2020. doi: 10.37385/jaets.v1i2.78.

[9] R. S. Nugroho and M. Arfa, "Pengelolaan Dokumen Digital Pendaftaran Pangan Olahan di Direktorat Registrasi Pangan Olahan Badan Pengawas Obat dan Makanan Jakarta," *Anuva J. Kaji. Budaya, Perpustakaan, dan Inf.*, vol. 5, no. 1, pp. 101–112, 2021, doi: 10.14710/anuva.5.1.101-112.

[10] A. Anisah, D. Wahyuningsih, E. Helmud, T. Suwanda, P. Romadiana, and D. Irawan, "Rancang Bangun Sistem Informasi Manajemen Arsip Digital," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 10, no. 3, pp. 419–425, 2021, doi: 10.32736/sisfokom.v10i3.1300.

[11] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 2, no. 1, pp. 31–42, 2020, doi: 10.54367/kakifikom.v2i1.666.

[12] R. N. Sarbini, D. E. Yuliana, and D. A. WK, "Rancang Bangun Sistem Informasi Akademik Berbasis Android," *J. Dedik.*, vol. 15, no. 0, pp. 134–139, 2018.

[13] A. Nurkholis and Y. B. Utomo, "RANCANG BANGUN SISTEM INFORMASI FAFA (FACTORY FIREWALL ADMINISTRATIVE) BERBASIS WEBSITE (Studi Kasus : PT Lotus Indah Textile Industries)," *J. Tek. Inform. Kaputama*, vol. 6, no. 2, pp. 789–796, 2022.

[14] M. H. Ibrahim, S. Mulyati, J. C. Chandra, D. Virgian, and S. Yudha, "IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD 128 (AES 128) BERBASIS WEB PADA KEDAI KOPI NGOPIYUKA ! WEB-BASED IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD 128 (AES 128) ALGORITHM AT NGOPIYUKA COFFEE SHOP !," vol. 2, no. April, pp. 141–148, 2023.