Terbit online pada laman web jurnal: **https://journal.budiluhur.ac.id/index.php/bit**

JURNAL BIT
(Budi Luhur Information Technology)

Vol. 18 No. 1 (2021) 09 - 18 ISSN Media Elektronik: **2685-127X**

Penerapan Algoritma Kriptografi Twofish Untuk Mengamankan Data File

Siswanto[1)], Anggun Saputro[2)], Gunawan Pria Utama[3)], Basuki Hari Prasetyo[*)]
[1)2)3)*)]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan. 12260
siswanto@budiluhur.ac.id[1)], anggunsputro@gmail.com[2)], gunawan.priautama@budiluhur.ac.id[3)],
basuki.hariprasetyo@budiluhur.ac.id[*)]

Abstract

The development of technology in the field of telecommunications makes people more and more often send data files in the form of doc, pdf, xls, voice, image, video via the internet. because the internet is a public medium that is vulnerable to intrusion and theft of information on data or files by unauthorized parties. The problem is that there are frequent changes or manipulation of the contents of data files from bank notes processing, cash pick-ups, document pick-ups, clearing items, atm & cdm service, atm cash replenishment, atm first line maintenance and atm second line maintenance. The purpose of this study is to prevent irresponsible people from knowing the reports that will be sent from the branch to the center by made applying the twofish cryptographic algorithm application to secure file data. The results of the tests carried out were 15 encrypted files, the average encrypted file size was 0.11%, the encryption process time was 9.5352 milliseconds and the decryption process time was 9.3294 milliseconds. In the UAT test, a questionnaire with a Likert scale scale of 5. has been used. As a result, the respondents agree (above 91.23%) that the overall application of the twofish algorithm to secure data files can be kept confidential.

Keywords: cryptography, twofish algorithm, UAT, data file.

Abstrak

Perkembangan teknologi dalam bidang telekomunikasi menjadikan orang semakin sering melakukan pengiriman data file berupa doc, pdf, xls, voice, image, video melalui internet. karena internet merupakan media umum yang rentan akan terjadinya penyusupan dan pencurian informasi terhadap data atau file oleh pihak yang tidak berhak. Masalahnya adalah sering terjadi perubahan atau manipulasi atas isi data file dari *bank notes processing, cash pick-up, document pick-up*, warkat kliring, atm & cdm *service, atm cash replenishment, atm first line maintenance* dan *atm second line maintenance*. Tujuan penelitian ini adalah mencegah orang yang tidak bertanggung jawab supaya tidak dapat mengetahui laporan yang akan dikirim dari cabang ke pusat dengan membuat aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data file. Hasil uji coba yang dilakukan sebanyak 15 buah file yang dienkripsi, maka rata-rata file yang dienkripsi ukurannya menjadi besar sebesar 0.11 %, lama waktu proses enkripsi sebesar 9,5352 milidetik dan lama waktu proses dekripsi sebesar 9,3294 milidetik. Pada pengujian UAT, telah digunakan kuesioner dengan *likert scale* skala 5. Hasilnya, para responden setuju (di atas 91,23%) bahwa secara keseluruhan aplikasi penerapan algoritma *twofish* untuk mengamankan data file dapat terjaga kerahasiannya.

Kata kunci: kriptografi, algoritma twofish, UAT, data file.

1. Pendahuluan

Perkembangan teknologi dalam bidang telekomunikasi menjadikan orang semakin sering melakukan pengiriman data file berupa doc, pdf, dll melalui internet. Kegiatan tersebut sangat beresiko, karena internet merupakan media umum yang rentan akan terjadinya penyusupan dan pencurian informasi terhadap aliran data oleh pihak yang tidak berhak. Saat ini hampir setiap sistem komputer terkoneksi dengan jaringan internet. Sistem sharing data dan akses jarak jauh menyebabkan masalah keamanan menjadi salah satu kelemahan komunikasi data

PT. Alpha – *Enterprise Management Solution* (Alpha-EMS) didirikan pada tanggal 14 Maret 2008, saat ini PT.Alpha-EMS berkedudukan di Jl. Wijaya

Diterima Redaksi : 30-03-2021 | Selesai Revisi : 23-04-2021 | Diterbitkan Online : 30-04-2021

*)*correspondent author*

IX No.21 Kebayoran Baru Jakarta Selatan PT.Alpha-EMS merupakan salah satu perusahaan *cash management* di Indonesia. PT. Alpha-EMS memiliki variasi produk jasa antara lain, *bank notes processing, cash pick-up, document pick-up*, warkat kliring, atm & cdm *service, atm cash replenishment, atm first line maintenance* dan mulai menjajaki *atm second line maintenance*. Guna menjawab dan memberikan solusi layanan kepada Bank dan retail, PT. Alpha-EMS memiliki 14 kantor cabang representatif, melingkupi seluruh Pulau Jawa, Pulau Bali, Pulau Lombok dan kepulauan sekitarnya, pulau Sumbawa serta Sumatera Utara, Pulau Sulawesi.

Permasalahan yang timbul di PT. Alpha-EMS data hanya disimpan di *sharing folder* dan bisa di buka oleh siapa pun. Sebab itu harus adanya pengucian file-file yang hanya dbuka oleh user yang memiliki akses tersebut.

Masalahnya adalah sering terjadi perubahan atau manipulasi atas isi data file dari *bank notes processing, cash pick-up, document pick-up*, warkat kliring, atm & cdm *service, atm cash replenishment, atm first line maintenance* dan *atm second line maintenance*. dasarkan kenyataan tersebut, perlu ada suatu pengamanan informasi pada saat pengiriman informasi.

Tujuan penelitian ini adalah mencegah orang yang tidak bertanggung jawab supaya tidak dapat mengetahui laporan yang akan dikirim dari cabang ke pusat dengan membuat aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data file.

Pada implementasi algoritma *twofish* pada keamanan data berbasis aplikasi *android* diharapkan akan dapat memproteksi masyarakat yang mengirimkan file dan folder menggunakan perangkat *mobile* [1].

Algoritma Twofish menggunakan jaringan feistel 16 putaran dan 4 kotak-S yang bergantung pada key. Terdapat empat macam key schedule dalam implementasinya yaitu: *full keying*, *partial keying*, minimal *keying*, dan *zero keying* dengan perbedaan dalam hal *key setup* [2],

Selain itu, *twofish* memiliki beberapa metode pengacakan yaitu matriks MDS, teknik PHT, dan teknik *whitening*. Hasil penerapan pada sistem informasi pengarsipan ini dilengkapi dengan proses enkripsi pada saat memasukkan (*input*) data menggunakan algoritma *twofish* di mana *key* akan diubah terlebih dahulu ke dalam bentuk *hexadecima*l sebelum digunakan untuk enkripsi [3].

User Acceptance Test (UAT) adalah suatu proses pengujian yang dilakukan oleh pengguna dengan hasil *output* sebuah dokumen hasil uji yang dapat dijadikan bukti bahwa *software* sudah diterima dan sudah memenuhi kebutuhan yang diminta. UAT tidak jauh beda dengan kuesioner pada tahap awal pembuatan aplikasi [4].

User acceptance testing (UAT) merupakan pengujian yang ditujukan di luar sistem yaitu *user*. Tujuan dari *user acceptance testing* adalah untuk mengetahui kelayakan dari perangkat lunak [5].

Pada penelitian sebelumnya, UAT dilakukan dengan metode *survey* yaitu dengan menyebar kuesioner kepada pengguna (petugas TPHD) yang sebelumnya sudah diberikan tutorial penggunaan sistem layanan haji. Model kuesioner menggunakan *likert scale* dengan skala 5 yaitu *strongly agree; agree; neutral/undecided; disagree; strongly disagree.* UAT digunakan untuk menjawab permasalahan perangkat lunak seputar *system metric;* usability*; satisfaction* dan beberapa *setting* pada masing – masing fungsi/fitur [6].

Pada proses enkripsi dan dekripsi dengan menggunakan algoritma *twofish* dalam proses pengiriman data menggunakan 128 bit setiap bloknya. Kunci yang digunakan pada saat enkripsi sama dengan saat dekripsi dengan panjang 128 bit. Aplikasi yang dibangun berhasil mengenkripsi dan mendekripsi *text* maupun file [7].

Perbandingan algoritma *blowfish* dan *twofish* untuk kriptografi file gambar. Hasil penelitian menunjukkan bahwa rata-rata perbandingan kecepatan dari algoritma *blowfish* dan algoritma *twofish* adalah 4355:4267 milidetik [8].

Implementasi algoritma kriptografi *twofish* untuk mengamankan pengiriman pesan suara Salah satu taknologi komunikasi suara yang digunakan dengan jaringan internet adalah *voice scrambbling*, Tetapi *voice scrambbling* mempunyai tingkat keamanan rendah. Solusi untuk meningkatkan keamanan rendah adalah dengan enkripsi pesan suara [9].

Pengamanan disposisi dokumen secara online menggunakan kriptografi *twofish* dan kompresi huffman pada CV. TMU. Berdasarkan 9 data pengujian diperoleh rata-rata proses encode 7,1 KByte/Second dan decode 6 KByte/Second [10].

Penerapan metode pengamanan data enkripsi dan deskripsi *twofish* pada PT. Gaya Makmur Tractor dapat membantu dalam pengiriman dan penerimaan pesan terjaga kerahasiaan [11].

Aplikasi enkripsi dan dekripsi untuk keamanan komunikasi data pada SMS (*Short Message Service)* berbasis android menggunakan algoritma *blowfish*. dapat mengatasi permasalahan SMS *snooping* dan SMS *interception* [12].

Analisis perbandingan kinerja algoritma *blowfish* dan algoritma *twofish* pada proses enkripsi dan dekripsi jika ditinjau dari estimasi waktu proses enkripsi dan dekripsi. Algoritma *blowfish* lebih cepat waktu eksekusinya dibandingkan dengan algoritma *twofish,* dan jika ditinjau dari besar ukuran file sebelum dan sesudah proses enkripsi dan dekripsi, algoritma *blowfish* dan algoritma *twofish* memiliki besar ukuran yang sama. [13].

Hasil dari penelitian aplikasi teknik enkripsi dan dekripsi file dengan algoritma *blowfish* pada perangkat *mobile* berbasis *android* ini menunjukkan

bahwa aplikasi yang dibangun mampu melakukan enkripsi dan dekripsi dengan baik [14].

Hasil Program sistem keamanan dengan sistem kriptografi algoritma *blowfish* dan *base64* pada Dinas Kependudukan Dan Pencatatan Sipil Kota Tangerang Selatan telah diuji coba, sehingga program dinyatakan sudah sesuai [15].

2. Metodologi Penelitian

Metode *penellitian* yang digunakan dalam penelitian ini, langkah-langkah sebagai berikut:

2.1 Analisa Masalah

Analisa masalah dilakukan dengan penelitian *langsung* di PT. ALPHA EMS yang beralamat di Jl. Wijaya IX No.21, RT.1/RW.5, Melawai, Kec. Kebayoran. Baru, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12160, Indonesia. Diobjek penelitian ini telah dilakukan pengambilan data laporan keuangan pada kantor cabang yang akan dikirim ke kantor pusat pada PT. Alpha EMS, pada tahun 2020.

Proses pengiriman data laporan keuangan pada kantor cabang yang perlu diamankan, sehingga pihak yang tidak bertanggung jawab tidak dapat melihat isi data laporan keuangan pada kantor cabang, untuk mengatasi permasalahan dalam pengamanan data laporan keuangan pada kantor cabang maka dicoba untuk mengembangkan aplikasi enkripsi data.

2.2 Analisa Algoritma

Mempelajari cara kerja algoritma *twofish* dapat dilihat pada gambar 1, menggunakan struktur sejenis *Feistel* dalam 16 putaran dengan tambahan teknik *whitening* terhadap *input* dan *output*. Teknik *whitening* adalah teknik melakukan operasi XOR terhadap kunci sebelum putaran pertama dan sesudah putaran akhir. Elemen di luar jaringan *feistel* normal yang terdapat dalam algoritma *twofish* adalah rotasi 1 bit. *Plaintext* dipecah menjadi empat kata 32-bit. Pada langkah *input whitening* terdapat *xor* dengan empat kata kunci. Selanjutnya diikuti oleh enam belas putaran. Pada setiap putaran, dua kata-kata pada sisi kiri digunakan sebagai masukan kepada fungsi g (Salah satu darinya diputar pada 8 bit pertama).

Fungsi g terdiri dari empat *byte-wide S-Box key dependent*, yang diikuti oleh suatu langkah pencampuran linier berdasar pada suatu matriks MDS. Hasil kedua fungsi g dikombinasikan menggunakan suatu *Pseudo Hadamard Transform* (PHT), dan ditambahkan dua kata kunci. Kedua hasil ini kemudian di-XOR ke dalam kata-kata pada sisi kanan (salah satunya diputar ke kanan 1 bit pertama, yang lainnya diputar ke kanan setelahnya). Yang kiri dan kanan dibelah dua kemudian ditukar untuk putaran yang berikutnya, pertukaran yang terakhir(putaran 16) dilakukan *undo swap*, dan yang empat kata di-XOR dengan lebih dari empat kata kunci untuk menghasilkan *ciphertext*. Secara formal, 16 byte plaintext $P_0,\ldots P_{15}$ yang yang pertama dipecah menjadi 4 kata $P_0,\ldots P_3$ dari 32 bit masing-masing menggunakan konvensi *little-endian* seperti persamaan (1).

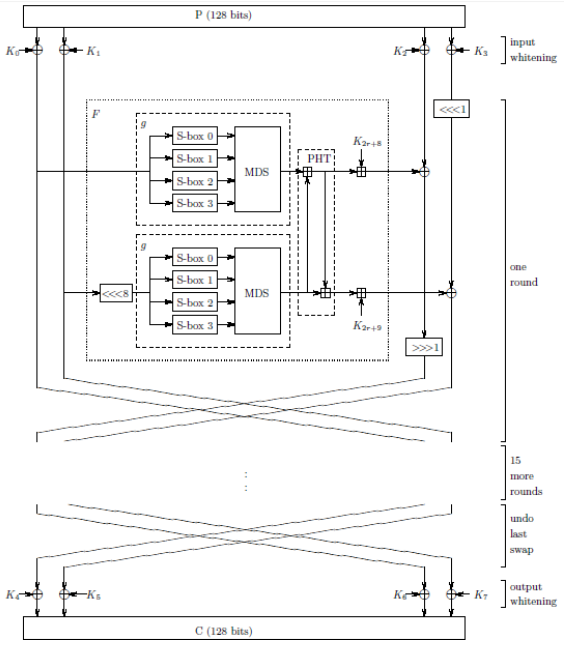
$$P(i) = \sum_{j=0}^{3} P(4i+j).2^{8j} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

$i = 0,\ldots,3$

Di dalam langkah whitening, kata-kata ini di-XOR dengan 4 kata dari kunci yang diperluas dengan persamaan (2).

$$R_{0,i} = P \oplus K_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

$i = 0,\ldots,3$



Gambar 1. Algoritma Twofish

Pada setiap 16 putaran, dua kata pertama digunakan sebagai masukan kepada fungsi F, yang juga mengambil angka bulat itu sebagai masukan. Kata yang ketiga di-XOR dengan keluaran pertama F dan kemudian diputar ke kanan satu bit. Kata keempat diputar ke kiri satu bit kemudian di-XOR dengan kata keluaran F Yang kedua.

Akhirnya, keduanya saling ditukar menghasilkan persamaan (3).

$$(F_{r,0}F_{r,1}) = F(F_{r,0}F_{r,1}r)$$

$$R_{r+1,0} = ROR(R_{r,2} \oplus F_{r,0},1)$$

$$R_{r+1,1} = ROL(R_{r,3},1) \oplus F_{r,1}$$

$$R_{r+1,2} = R_{r,0}$$

$$R_{r+1,3} = R_{r,1} \quad \ldots\ldots(3)$$

Untuk r = 0,…,15 (putaran). di mana ROR dan ROL adalah berfungsi memutar argumentasi pertama

(32-bit kata) ke kanan / ke kiri dengan angka bit-bit diindikasikan dengan argumentasi keduanya.

$$C_i = R_{16,(i+2) \bmod 4} \oplus K_{i+4} \quad \text{.....(4)}$$

i = 0,…,3

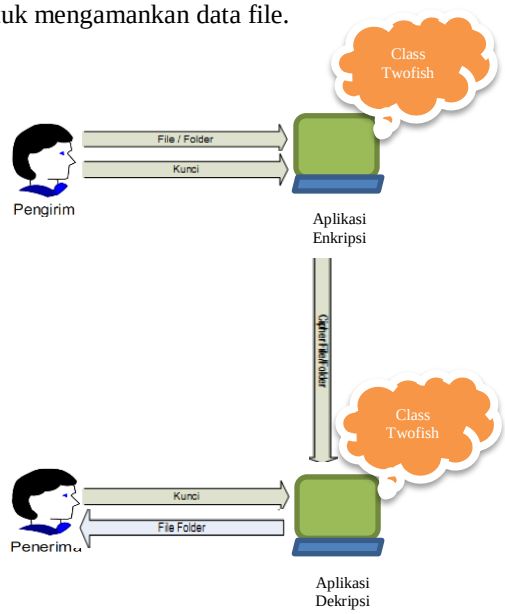
Empat kata dari *ciphertext* kemudian ditulis sebagai 16 byte $C_0,\ldots,C_{15}$ menggunakan konversi *little-endian* untuk *plaintext* seperti persamaan (4) dan (5).

$$c_i = \left\lfloor \frac{C\lfloor i/4 \rfloor}{2^{8(i \bmod 4)}} \right\rfloor \bmod 2^8 \quad \text{.....(5)}$$

i = 0,…,15

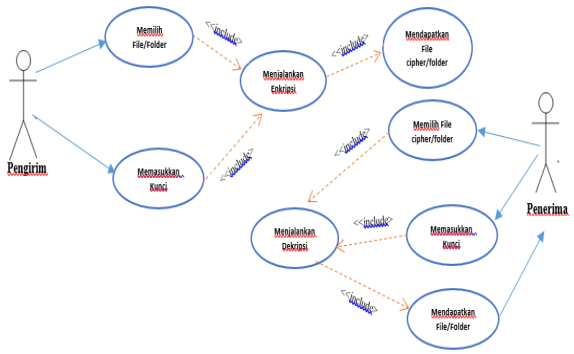
2.3 Mendesain Aplikasi

Gambaran aktifitas mengamankan data file dapat dimodelkan dalam *arsitektur aplikasi enkripsi dan deskripsi twofish* seperti gambar 1, desain use case diagram, desain *activity diagram* dan *user interface* aplikasi pengamanan data file yang akan digunakan untuk mengamankan data file.



Gambar 1. Arsitektur Aplikasi Enkripsi dan Deskripsi Twofish

Gambar 2. berikut ini merupakan use case diagram merupakan cerminan dari arsitektur aplikasi yang dirancang sebelumnya.

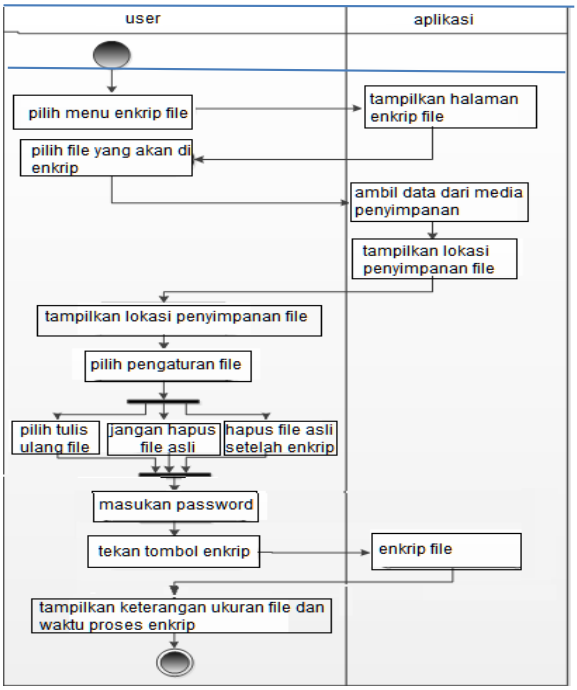


Gambar 2. Use Case Diagram Aplikasi

Diagram *use case* memperlihatkan lebih detail bagaimana sistem ini bekerja sesuai rancangan. Terdapat 8 *use case* di mana *use case* ini akan menjadi sub program dalam sistem, kedua *user* memiliki kunci yang sama untuk mengenkripsi dan mendeskripsi data file, penerima memiliki data file berupa *file cipher* dan kunci yang akan di masukkan ke dalam aplikasi untuk dapat memilhat data file.

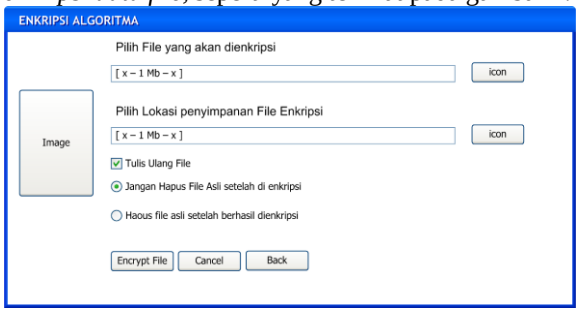
Data perusahaan sangat penting , data yang dimiliki perusahaan terdapat beberapa macam, seperti file doc , file pdf , file video , dan file lainnya. Yang tidak dapat dielakkan yaitu data perusahaan kadang harus disiapkan atau diarsipkan dalam 1 penyimpan identik , berangkat dari permasalah tersebut sistem yang dirancang ini dapat menerima bentuk file yang berbeda dan folder yang akan digunakan.

Gambar 3 berikut merupakan *activity diagram* proses enkripsi *twofish* bagaimana *user* dan sistem bekerja pada aplikasi mengamankan data file tersebut.



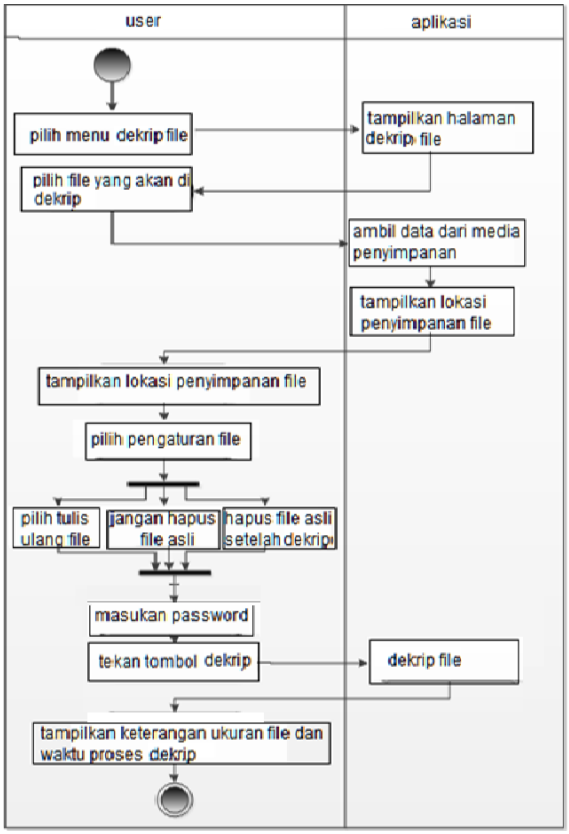
Gambar 3. Activity Diagram Proses Enkripsi Twofish

Tahap awal dalam perancangan adalah halaman *menu utama*, yang berisi halaman untuk memilih menu *enkripsi data file*, seperti yang terlihat pada gambar 4.



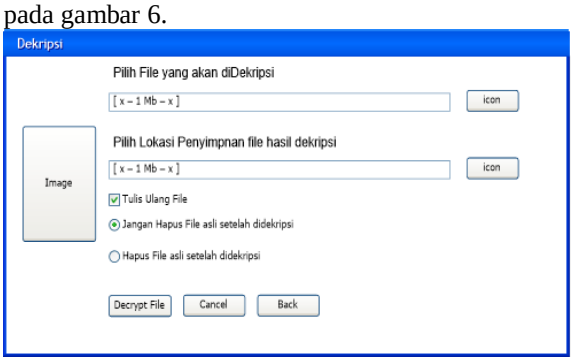
Gambar 4. Tampilan layar menu enkripsi data file

Gambar 5 berikut merupakan *activity diagram* proses dekripsi *twofish* bagaimana *user* dan sistem bekerja pada aplikasi mengamankan data file tersebut.



Gambar 5. Activity Diagram Proses Dekripsi Twofish

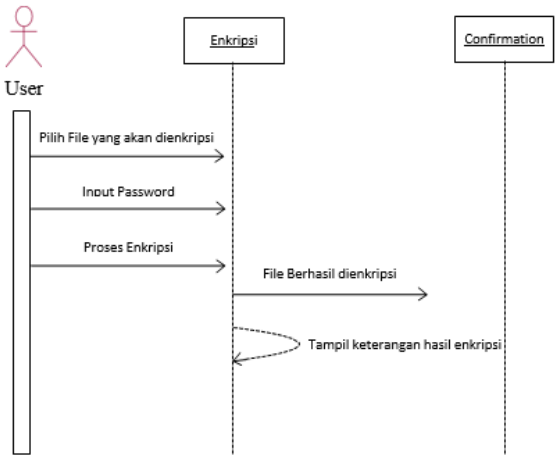
Pada menu *dekripsi data file cipher* akan langsung ditampilkan menu untuk melakukan *input* file cipher dan *input password* seperti yang terlihat pada gambar 6.



Gambar 6. Tampilan Layar Menu Dekripsi Data File Cipher

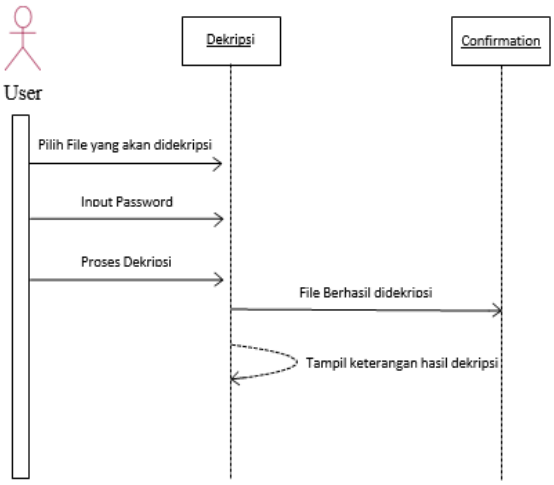
Pada saat *user* hendak mengirimkan pesan dengan enkripsi maka diperlukan untuk memasukan *password*/kunci rahasia yang terdiri dari 16 character dan *case sensitif*, diwajibkan bagi *user* untuk mengingat *password*/kunci rahasia yang dimasukkan, karena nantinya *secret key* ini akan digunakan kembali saat penerima data *file cipher* hendak membuka *data file/folder* ini kembali.

Pada gambar 7. Menggambarkan *sequence diagram* fungsi enkripsi interaksi antara user dan aplikasi pada saat mengirimkan data file, dimulai dari user mengenkripsi data file, kemudian pesan berhasil dienkripsi oleh aplikasi.



Gambar 7. Sequence Diagram Fungsi Enkripsi

Sedangkan pada gambar 8, menggambarkan *sequence diagram* fungsi dekripsi, user memilih file yang akan didekripsi. Kemudian input *password*, untuk mendekripsi maka pilih proses dekripsi. Kemudian setelah proses dekripsi selesai maka akan tampil keterangan hasil dekripsi.



Gambar 8. Sequence Diagram Fungsi Dekripsi

2.4 Membuat program Aplikasi

Membuat program aplikasi pengamanan data file yang akan digunakan untuk mengamankan pesan email dengan bahasa pemrograman PHP dan mengelola *file log* proses enkrip dan dekrip data file dengan MySql.

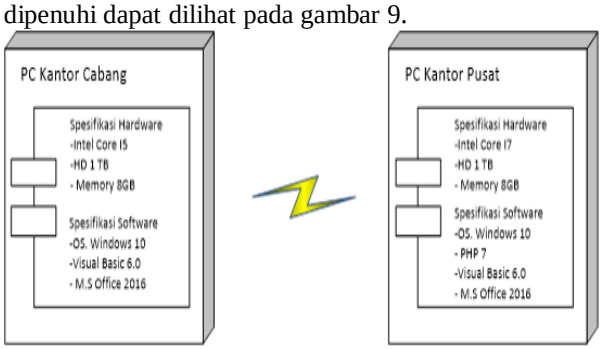
2.5 Merancang Pengujian Aplikasi

Pengujian aplikasi direncanakan dengan menggunakan metode pengujian *black box* dan *User Acceptence Test* (UAT).

3. Hasil Dan Pembahasan

3.1 Lingkungan Percobaan

Dalam melakukan uji coba untuk mengetahui hasil dari proses enkripsi dan dekripsi tersebut, maka kebutuhan lingkungan percobaan yang harus dipenuhi dapat dilihat pada gambar 9.



Gambar 9. Deployment Diagram Hardware dan Software

Adapun tahapan dari algoritma *Twofish* sebagai berikut:

a. Bit masukan disebut sebagai P_0, P_1, P_2, dan P_3, P_0 dan P_1 akan menjadi bagian kiri, dua lainnya akan menjadi masukan pada bagian kanan.
b. Kemudian melalui proses *whitening.*
c. Bagian kiri akan menjadi masukan untuk fungsi f, P_0 akan langsung menjadi masukan bagi fungsi g, sementara P_1 akan di-*rotate* 8-bit sebelum diproses oleh fungsi g.
d. Didalam fungsi g, bit-bit tersebut akan melalui S-box dan matriks MDS, kemudian kedua keluaran akan digabungkan oleh PHT.
e. Setelah melalui PHT, kedua bagian tersebut akan ditambah dengan bagian dari kunci sesuai dengan iterasi yang telah dilewati. Untuk keluaran dari fungsi f dengan *input* P_0 akan ditambah dengan K_{2r+8}. Untuk keluaran dari fungsi f dengan *input* P_1 akan ditambah dengan K_{2r+9}, dimana r adalah jumlah iterasi yang telah dilewati. Masing-masing ditambah delapan dan sembilan karena delapan urutan awal sudah digunakan untuk *whitening input* dan *output*.
f. Keluaran dari fungsi f dengan input P0 akan di-XORdengan P_2, kemudian hasil XOR tersebut akan di-*rotate* 1-bit.
g. Keluaran dari fungsi f dengan input P_1 akan di-XOR dengan P_3, namun P_3 sebelumnya di-*rotate* 1-bit terlebih dahulu.
h. Setelah perhitungan bit selesai, bagian kanan yang telah dihitung tadi akan menjadi bagian kiri dan bagian kiri yang belum dihitung akan menjadi bagian kanan.
i. Kemudian setelah 16 iterasi, akan dilakukan *whitening* terhadap keluarannya. *Whitening* pada *output* akan mengundo pertukaran bagian kanan dan bagian kiri pada iterasi terakhir, dan melakukan XOR data dengan 4 bagian kunci. $C_i = R_{16,(i+2)} \bmod 4\ K_{i+4}$ di mana i = 0, ..., 3 Bagian kunci yang digunakan disini berbeda dengan bagian kunci yang digunakan saat *whitening* pada *input*. Oleh karena itu urutan bagian kunci yang dipakai ditambah empat, karena empat urutan bagian kunci satu sampai empat sudah terlebih dahulu digunakan untuk *whitening* pada *input.*
j. Keempat bagian cipherteks tersebut kemudian ditulis menjadi 16 byte C_0,...,C_{15} menggunakan konversi *little-endian* seperti pada plainteks.

3.2 Pengujian *Black Box*

Pada tabel 1 bagian ini akan ditampilkan hasil pengujian *black box testing* pada menu enkripsi, dekripsi dan *about*. Dalam pengujian ini akan mengambil contoh kasus dari tahap pengujian program terhadap kesesuaian dengan kebutuhan aplikasi.

Tabel 1. Prngujian *Black Box* Aplikasi Enkripsi dan Dekripsi Twofish

No.	Spesifikasi	Status	Hasil Pengujian
1	Memilih data file asli	Bekerja	Dapat memilih data file asli dari *memory server* web dan bisa *open*.
2	Mengenkripsi data file asli	Bekerja	Fungsi enkripsi dapat beroperasi membentuk data *file cipher*.
3	Buka data *file cipher* yang telah dienkripsi	Bekerja	Data *file cipher* tidak dapat dibuka, dengan tampilan pesan data file telah teremkripsi.
4	Memilih data *file cipher*	Bekerja	Dapat memilih data *file cipher* dari *memory server* web dan bisa *open*.
5	Mengdekripsi data *file cipher*	Bekerja	Fungsi dekripsi dapat beroperasi membentuk data file asli.
6	Buka file yang telah didekripsi	Bekerja	File dapat dibuka
7	Masukkan Kunci/*password* salah/tidak sesuai pada proses enkripsi/dekripsi	Tidak Bekerja	Proses enkripsi/dekripsi tidak jalan muncul pesan "kunci/password salah/tidak sesuai"
8	Masukkan Kunci/password benar/sesuai pada proses enkripsi/dekripsi	Bekerja	Proses enkripsi/dekripsi jalan muncul hasil proses berupa nama file hasil proses, ukuran file dalam *byte* dan lama waktu proses dalam milidetik.

3.3 Pengujian Enkripsi

Tabel 2 merupakan tabel pengujian enkripsi.

Pada *gambar* 10. Menggambarkan rata-rata hasil pengujian enkripsi data file cabang perusahaan dari aplikasi penerapan algoritma kriptografi *twofish*

Tabel 2. Pengujian Enkripsi

Hasil Uji (Data Normal)			
Data Masukan	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
Pilih File *Plaintext* aelain berjenis ems	File *Plaintext* yang selain berjenis ems dapat masuk	File *Plaintext* yang selain berjenis ems dapat masuk ke dalam form enkripsi	[X] Diterima [ ] Ditolak
Hasil Uji (Data Salah)			
Data Masukan	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
File *Plaintext* yang selain berjenis ems tidak dapat diinput	*Plaintext* tidak dapat masuk ke inputan form enkripsi	Tampil pesan error	[X] Diterima [ ] Ditolak

Nama File	Ukuran File	Ukuran File Enkrip	Waktu Enkrip (ms)	Nilai Akhir - Nilai awal	Nilai akhir * 100 %	(Nilai Akhir - Nilai Awal) / (Nilai Akhir * 100 %)
Mei	231,83	231,915	6,730187	0,085	23,1915	0,36651%
Juni	225,136	225,211	4,937188	0,075	22,5211	0,33302%
Juli	226,447	226,523	5,779125	0,076	22,6523	0,33551%
November	185,594	185,675	4,129562	0,081	18,5675	0,43625%
ALPHA jakarta	461,000	471,206	8,240313	10,206	47,1206	21,65932%
Data sp karyawan	12,000	122,61	8,192813	110,610	12,261	902,128705%
SO,PO	85,000	864,41	3,465	779,410	86,441	901,667016%
Gaji karyawan	26,000	256,69	3,623094	230,690	25,669	898,710511%
Biaya mes	185,000	188,721	4,633438	3,721	18,8721	19,716945%
Cos report AP	294,000	300,774	5,91225	6,774	30,0774	22,521899%
ALPHA bali	396,000	404,621	9,368188	8,621	40,4621	21,306365%
ALPHA medan	391,000	399,399	6,551125	8,399	39,9399	21,029107%
ALPHA sidoarjo	434,000	444,392	7,46675	10,392	44,4392	23,384765%
MX-Resita	173,9000	178,0128	13,7635	4,113	17,80128	23,103965%
QS- modul	243,2000	248,996	2,560069	5,796	24,8996	23,277681%
Total	3570,107	4749,1558	95,352602	1179,049	474,91558	248,264929%

Gambar 10. Rata-Rata Hasil Pengujian Enkripsi

3.4 Pengujian Dekripsi

Tabel 3 di bawah ini merupakan tabel pengujian dekripsi**.**

Tabel 3..Pengujian Dekripsi

Hasil Uji (Data Normal)			
Data Masukan	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
Pilih File *ciphertext* yang berjenis ems	ile *ciphertext* yang berjenis ems dapat masuk	ile *ciphertext* yang berjenis ems ke dalam form dekripsi	[X] Diterima [ ] Ditolak
Hasil Uji (Data Salah)			
Data Masukan	**Yang Diharapkan**	**Pengamatan**	**Kesimpulan**
File *ciphertext* yang selain berjenis ems tidak dapat diinput	*Ciphertext* tidak dapat masuk ke inputan form dekripsi	Tampil pesan error	[X] Diterima [ ] Ditolak

Pada Gambar 11. Rata-rata hasil Pengujian Dekripsi data *file cipher* cabang perusahaan dari aplikasi penerapan algoritma kriptografi *twofish.*

Nama File	Ukuran File	Ukuran File dekrip	Waktu dekrip (ms)	Nilai Akhir - Nilai awal	Nilai akhir * 100 %	(Nilai Akhir - Nilai Awal) / (Nilai Akhir * 100 %)
Mei	231,915	231,915	6,730187	0,000	23,1915	0,00000%
Juni	225,211	225,211	4,937188	0,000	22,5211	0,00000%
Juli	226,523	226,523	5,779125	0,000	22,6523	0,00000%
November	185,675	185,675	4,129562	0,000	18,5675	0,00000%
ALPHA Jakarta	471,206	471,232	6,1825	0,026	47,1232	0,05517%
Data sp karyawan	122,610	122,61	8,192813	0,000	12,261	0,00000%
SO,PO	864,410	864,41	3,465	0,000	86,441	0,00000%
Gaji karyawan	256,690	256,96	3,623094	0,270	25,696	1,05075%
Biaya mes	188,721	188,721	4,633438	0,000	18,8721	0,00000%
Cos report AP	300,774	300,8	5,91225	0,026	30,08	0,08644%
ALPHA bali	404,621	404,621	9,368188	0,000	40,4621	0,00000%
ALPHA medan	399,399	399,399	6,551125	0,000	39,9399	0,00000%
ALPHA sidoarjo	444,392	444,41	7,46675	0,018	44,441	0,04050%
MX-Resita	178,0128	178,0144	13,7635	0,002	17,80144	0,00899%
QS- modul	248,9960	248,9984	2,560069	0,002	24,89984	0,00964%
Total	4749,1558	4749,4998	93,294789	0,344	474,94998	0,07243%

Gambar 11. Rata-Rata Hasil Pengujian Dekripsi

Hasil uji coba yang dilakukan sebanyak 15 buah file yang dienkripsi, maka rata-rata file yang dienkripsi ukurannya menjadi besar sebesar 0.11%, lama waktu proses enkripsi sebesar 9,5352 milidetik dan lama waktu proses dekripsi sebesar 9,3294 milidetik.

3.5 Pengujian *User Acceptance Test* (UAT)

Pengujian UAT melibatkan 25 responden pengguna aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data file. Para responden menjawab kuesioner setelah menggunakan aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data *file.* Pada Tabel 4 mempresentasikan daftar pertanyaan survei kuesioner yang terdiri dari 4 bagian: *setting* fungsi; *system metric; user satisfaction;* dan *usability.*

Tabel 4. Daftar Pertanyaan Survei Kuesioner

No	Daftar Pertanyaan
1.	Apakah tampilan aplikasi penerapan algoritma kriptografi *twofish* menarik?
2.	Apakah Menu-menu aplikasi penerapan algoritma kriptografi *twofish* ini mudah dipahami?
3.	Apakah aplikasi penerapan algoritma kriptografi *twofish* ini mudah dioperasikan?
4.	Apakah aplikasi penerapan algoritma kriptografi *twofish* ini *Responsive*?
5.	Apakah Performa aplikasi penerapan algoritma kriptografi *twofish* ini baik?
6.	Apakah aplikasi penerapan algoritma kriptografi *twofish* dapat mengamankan data file?
7.	Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *twofish application* ini sudah cukup baik?
8.	Apakah keluaran dari aplikasi penerapan algoritma kriptografi *twofish* sudah sesuai dengan hasil untuk mengamankan data file.yang melakukannya?

Pertanyaan 1 dan 2 merupakan fokus *setting* fungsi yang meliputi pertanyaan Apakah tampilan aplikasi penerapan algoritma kriptografi *twofish* menarik dan Apakah Menu-menu aplikasi penerapan algoritma kriptografi *twofish* ini mudah dipahami bagi pengguna aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data *file* berbasis *web.*

Pertanyaan 3 sampai dengan 5 merupakan fokus *system metric* yang meliputi pertanyaan Apakah aplikasi penerapan algoritma kriptografi *twofish* ini mudah dioperasikan, Apakah aplikasi penerapan algoritma kriptografi *twofish* ini *Responsive* dan Apakah Performa aplikasi penerapan algoritma kriptografi *twofish* ini baik bagi pengguna aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data *file* berbasis *web.*

.Pertanyaan 6 merupakan fokus *user satisfaction* yang *meliputi pertanyaan* Apakah aplikasi penerapan algoritma kriptografi *twofish* dapat mengamankan data file bagi pengguna aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data file berbasis *web.*

Pertanyaan 7 dan 8 merupakan fokus *usability* yang meliputi pertanyaan Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *twofish* ini sudah cukup baik dan Apakah keluaran dari aplikasi penerapan algoritma kriptografi *twofish* sudah sesuai hasil untuk mengamankan data *file*.yang melakukannya bagi pengguna aplikasi penerapan

algoritma kriptografi *twofish* untuk mengamankan data file berbasis *web*.

Aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data file berbasis *web* yang akan diimplementasikan untuk mengetahui tanggapan responden (*user*), maka dilakukan pengujian dengan memberikan pertanyaan kepada 25 responden di mana jawaban dari pertanyaan tersebut terdiri dari tingkatan yang dapat dipilih, seperti Tabel 5.

Tabel 5. Tabel Pilihan Jawaban UAT

Pilihan	Keterangan Jawaban UAT
A	**Sangat**: Mudah/Baik/Sesuai/Jelas/Menarik/Paham/Setuju
B	Mudah/Baik/Sesuai/Jelas/Menarik/Paham/Setuju
C	**Netral**
D	**Cukup**: Sulit/Cukup Baik/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju
E	**Sangat**: Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju

Tabel Bobot Nilai Jawaban UAT dapat dilihat Tabel 6.

Tabel 6. Tabel Bobot Nilai Jawaban UAT

Jawaban UAT	Bobot
A **Sangat**: Mudah/Baik/Sesuai/Jelas/Menarik/Paham	**5**
B **Mudah**/Baik/Sesuai/Jelas/Menarik/Paham	**4**
C **Netral**	**3**
D **Cukup Sulit**/Cukup Baik/Tidak Sesuai/Tidak Jelas/ Tidak Menarik/Tidak Paham/Tidak Setuju	**2**
E **Sangat:** Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju	**1**

Tabel 7 merupakan hasil UAT yang melibatkan pengguna aplikasi penerapan algoritma kriptografi *twofish* untuk mengamankan data file berbasis *web*. Sebanyak 25 responden melakukan evaluasi dalam pengisian kuesioner. Diperoleh hasil kuesioner dalam bentuk *likert scale* yang akan dianalisis.

Tabel 8 merupakan hasil perkalian masing-masing jawaban UAT dikalikan dengan masing-masing bobot nilai jawaban UAT

1. Analisa pertanyaan pertama Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan pertama adalah 107. Nilai rata-ratanya adalah 107/25= 4,28. Prosentase nilainya adalah 4,28/5 x 100 %= 85,6%.
2. Analisa pertanyaan kedua
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan kedua adalah 109. Nilai rata-ratanya adalah 109/25 = 4,36. Prosentase nilainya adalah 4,36/5 x 100% = 87,2%.
3. Analisa pertanyaan ketiga
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan ketiga adalah 109. Nilai rata-ratanya adalah 109/25 = 4,36 Prosentase nilainya adalah 4,36/5 x 100% = 87,2%.

Tabel 7. Hasil UAT

Pertanyaan	**Pilihan Jawaban**				
***Setting* Fungsi**	**A**	**B**	**C**	**D**	**E**
Apakah Tampilan aplikasi penerapan algoritma kriptografi *twofish* menarik?	10	13	1	1	0
Apakah Menu-menu aplikasi penerapan algoritma kriptografi *twofish* ini mudah dipahami?	14	8	1	2	0
System Metric	**A**	**B**	**C**	**D**	**E**
Apakah aplikasi penerapan algoritma kriptografi *twofish* ini mudah dioperasikan?	13	9	2	1	0
Apakah aplikasi penerapan algoritma kriptografi *twofish* ini *Responsive*?	18	6	1	1	0
Apakah Performa aplikasi penerapan algoritma kriptografi *twofish* ini baik?	19	5	1	0	0
User Satisfaction	**A**	**B**	**C**	**D**	**E**
Apakah aplikasi penerapan algoritma kriptografi *twofish* dapat mengamankan data file?	20	2	3	0	0
Usability	**A**	**B**	**C**	**D**	**E**
Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *twofish* ini sudah cukup baik?	19	4	1	1	0
Apakah keluaran dari aplikasi *penerapan* algoritma kriptografi *twofish* sudah sesuai hasil mengamankan data file .yang melakukannya?	18	6	1	0	0

4. Analisa pertanyaan keempat
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan keempat adalah 117. Nilai rata-ratanya adalah 117/25 = 4,68. Prosentase nilainya adalah 4,68/5 x 100% = 93,6%.
5. Analisa pertanyaan kelima
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan kelima adalah 118. Nilai rata-ratanya adalah 118/25 = 4,72. Prosentase nilainya adalah 4,72/5 x 100% = 94,4%.
6. Analisa pertanyaan keenam
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan keenam adalah 117 Nilai rata-ratanya adalah 117/25 = 4,68. Prosentase nilainya adalah 4,68/5 x 100% = 93,6%.
7. Analisa pertanyaan ketujuh
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan ketujuh adalah 116. Nilai rata-ratanya adalah 116/25 = 4,64. Prosentase nilainya adalah 4,64/5 x 100% = 92,8%.
8. Analisa pertanyaan kedelapan
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan keedelapan adalah 117. Nilai rata-ratanya adalah 117/25 = 4,68. Prosentase nilainya adalah 4,68/5 x 100% = 93,6%.

Tabel 8. Hasil UAT x Bobot Nilai

Pertanyaan	Pilihan Jawaban					Jumlah
***Setting* Fungsi**	**A**	**B**	**C**	**D**	**E**	
Apakah Tampilan aplikasi penerapan algoritma kriptografi *twofish* menarik?	50	52	3	2	0	107
Apakah Menu-menu Sistem pakar berbasis *client-server* ini mudah dipahami?	70	32	3	4	0	109
System Metric	**A**	**B**	**C**	**D**	**E**	
Apakah aplikasi penerapan algoritma kriptografi *twofish* ini mudah dioperasikan?	65	36	6	2	0	109
Apakah aplikasi penerapan algoritma kriptografi *twofish* ini Responsive?	90	24	3	0	0	117
Apakah Performa aplikasi penerapan algoritma kriptografi *twofish* ini baik?	95	20	3	0	0	118
User Satisfaction	**A**	**B**	**C**	**D**	**E**	
Apakah aplikasi penerapan algoritma kriptografi *twofish* dapat mengamankan data file?	100	8	9	0	0	117
Usability	**A**	**B**	**C**	**D**	**E**	
Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *twofish* ini sudah cukup baik?	95	16	3	2	0	116
Apakah keluaran dari aplikasi penerapan algoritma kriptografi *twofish* sudah sesuai hasil mengamankan data file yang melakukannya?	90	24	3	0	0	117

Dari data di atas dapat disimpulkan bahwa prosentase dari ***setting* fungsi sebesar 86,4% setuju** aplikasi penerapan algoritma *twofish* untuk mengamankan data *file* berbasis web tersebut mempunyai tampilan aplikasi penerapan algoritma *twofish* menarik dan menu-menu aplikasi penerapan algoritma *twofish* ini mudah dipahami, dan prosentase dari ***system metric* sebesar 91,73% setuju** aplikasi penerapan algoritma *twofish* ini mudah dioperasikan, aplikasi penerapan algoritma kriptografi *twofish* ini *responsive* dan performa aplikasi penerapan algoritma *twofish* ini baik serta prosentase dari ***User Satisfaction* sebesar 93,6% setuju** aplikasi penerapan algoritma *twofish* dapat mengamankan data file dan prosentase dari ***Usability* sebesar 93,2% setuju** fitur-fitur aplikasi penerapan algoritma *twofish* ini sudah cukup baik dan keluaran dari aplikasi penerapan algoritma *twofish* sudah sesuai hasil mengamankan data file yang melakukannya. Hasil proses pengujian dengan UAT, **para responden setuju (di atas 91,23%)** bahwa secara keseluruhan aplikasi penerapan algoritma *twofish* untuk mengamankan data *file* dapat terjaga kerahasiannya.

4. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah 8 spesifikasi hasil pengujian *blackbox*, keempat fungsi dapat berfungsi sesuai dengan spesifikasi yang dinginkan. Hasil uji coba yang dilakukan sebanyak 15 buah *file* yang dienkripsi, maka rata-rata *file* yang dienkripsi ukurannya menjadi besar sebesar 0.11%, lama waktu proses enkripsi sebesar 9,5352 milidetik dan lama waktu proses dekripsi sebesar 9,3294 milidetik. Hasil proses pengujian dengan UAT, para responden setuju (di atas 91,23%) bahwa secara keseluruhan aplikasi penerapan algoritma *twofish* untuk mengamankan data file cabang perusahaan dapat terjaga kerahasiannya.

Saran untuk pengembangan aplikasi ini ke depannya agar dibuat berbasis *mobile* android dan ditambah metode kompesi data *file*, agar data *file cipher* ukurannya tidak menjadi lebih besar.

5. Daftar Pustaka

[1] Erfan H;, 2019**,** Implementasi Algoritma Twofish Pada Keamanan Data Berbasis Aplikasi Android, Proseding Sensitif, pp 407-414, Tersedia di: https://ejurnal.dipanegara.ac.id/index.php/sensitif/article/view/564, [Accessed 10 Maret 2021].

[2] Christy A. S., dkk, 2016. Optimasi Metode Twofish Untuk Mengamankan Password Pada Kriptografi, Prosiding Seminar Nasional Multi Disiplin Ilmu & Call For Papers Unisbank (SENDI_U), pp. 199 - 208.

[3] Chandra S. P. dan Banni S. A., 2016. Sistem Informasi Manajemen Pengarsipan Dengan Menggunakan Algoritma Twofish. Jurnal Informatika Polinema. Vol.2(2), pp. 50 -58.

[4] Endang C. P., 2017. Pengujian UAT (User Acceptance Test). Tersedia di: https://endangcahyapermana.wordpress.com/2017/03/14/pengujian-uat-user-acceptance-test/, [Accessed 12 Maret 2021].

[5] C. S. Theng, 2017. "Leisure Technology for the Elderly : A Survey , User Acceptance Testing and Conceptual Design," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 12, pp. 100–115, 2017.

[6] Danang W. U., Defri K. dan Yani P. A.. 2018. Teknik Pengujian Perangkat Lunak Dalam Evaluasi Sistem Layanan Mandiri Pemantauan Haji Pada Kementerian Agama Provinsi Jawa Tengah. Jurnal SIMETRIS, Vol. 9 No. 2 November 2018, P-ISSN: 2252-4983, E-ISSN: 2549-3108, pp.731–746.

[7] Herbert A. T., Jimmi H. P. S., 2017, Enkripsi Dan Dekripsi Dalam Proses Pengiriman Data Dengan Menggunakan Algoritma Twofish, Vol. 1 No. 1 (2017): Jurnal Bisantara Informatika (JBI), ISSN 2686–6455, pp. 1-17, Tersedia di: http://bisantara.amikparbinanusantara.ac.id/index.php/bisantara/article/view/11, [Accessed 12 Maret 2021].

[8] Muhathir, 2018, Perbandingan Algoritma Blowfish Dan Twofish Untuk Kriptografi File Gambar, JITE, 2 (1) Juli 2018, ISSN 2549-6255 (Print), ISSN 2549-6247 (Online), pp. 23-32, Tersedia di: https://ojs.uma.ac.id/index.php/jite/article/view/1673/1601, [Accessed 13 Maret 2021].

[9] Fathonah K.K., 2014, Implementasi Keamanan Pengiriman Pesan Suara dengan Enkripsi dan Dekripsi Menggunakan Algoritma Twofish, *Journal of Informatics and Technology*, vol. 1, no. 3, pp. 84-89, Sep. 2014, Tersedia di:

https://ejournal3.undip.ac.id/index.php/joint/article/view/6323, [Accessed 13 Maret 2021].

[10] Imelda, Ega P., 2018, Pengamanan Disposisi Dokumen secara online menggunakan Kriptografi Twofish dan Kompresi Huffman pada CV. TMU, Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri 2018, ISSN 2085-4218, ITN Malang, 3 Pebruari 2018, pp, 363-369, Tersedia di: https://ejournal.itn.ac.id/index.php/seniati/article/view/1914/1659, [Accessed 14 Maret 2021].

[11] Arif N., Vivi S. dan Baibul T., 2019,. Penerapan Metode Pengamanan Data Enkripsi Dan Deskripsi Menggunakan Metode Twofish Pada PT. Gaya Makmur Tractor, Tersedia di:http://eprints.binadarma.ac.id/288/1/JURNAL%20PENERAPANMETODE%20PENGAMANAN%20DATA%20ENSKRIPSI%20DAN.pdf, [Accessed 14 Maret 2021].

[12] Ibrahim M. S., Anggi P. S. dan Wawan G., 2019, Aplikasi Enkripsi dan Dekripsi untuk Keamanan Komunikasi Data pada SMS (Short Message Service) Berbasis Android Menggunakan Algoritma Blowfish, Jurnal FORMAT, Volume 8, Nomor 1, Tahun 2019, ISSN : 2089–5615 , pp. 34-41, Tersedia di: https://publikasi.mercubuana.ac.id/index.php/format/article/view/5716/2761, [Accessed 15 Maret 2021].

[13] Dimas A. T. dan Herlina L. S., 2016, Analisis Perbandingan Kinerja Algoritma Blowfish Dan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi, ,Jurnal Pseudocode, Volume 2 Nomor 1, Februari 2015, ISSN 2355 – 5920, pp. 37-44, Tersedia di: https://ejournal.unib.ac.id/index.php/pseudocode/article/view/424/368, [Accessed 15 Maret 2021], DOI: https://doi.org/10.33369/pseudocode.2.1.37-44,

[14] Siswo W., Zaldi I, Rian F, Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android, Jurnal Nasional Teknik Elektro, Vol: 5, No. 1, Maret 2016, ISSN: 2302 – 2949, pp. 36-44, Tersedia di: http://jnte.ft.unand.ac.id/index.php/jnte/article/view/199/209, [Accessed 25 Maret 2021], DOI : 10.20449/jnte.v5i1.199.2016..

[15] Mujito, Anugrah, 2016. Aplikasi Kriptografi File Menggunakan Metode Blowfish dan Metode Base64 pada Dinas Kependudukan dan Pencatatan Sipil Kota Tangerang Selatan, Jurnal SISFOKOM, Volume 05, Nomor 01, September 2016, pp. 54-60, Tersedia di: http://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/39/511., [Accessed 25 Maret 2021], DOI: https://doi.org/10.32736/sisfokom.v5i2.39.