Pengamanan Data pada Aplikasi Android dengan Algoritma Blowfish dan AES-128 (Studi Kasus pada Fitur BluCareer Aplikasi BluCampus Universitas Budi Luhur)

Khaeri Diniari[1)], **Achmad Solichin**[2)]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : [1)]dinikhaeridiniari@gmail.com , [2)]achmad.solichin@budiluhur.ac.id

Abstrak

Pengembangan fitur BluCareer pada aplikasi BluCampus yang dimiliki Universitas Budi Luhur bertujuan untuk mempermudah pengguna yang memiliki kemampuan tertentu dan ingin membuka sebuah kelas belajar serta mempermudah pengguna lain dalam mencari kelas belajar untuk mengasah kemampuan dan pengetahuan yang mereka miliki. BluCareer juga sangat memperhatikan keamanan data, bagi penulis hal ini sangat dianggap penting untuk menghidari pemalsuan data. Penulis menerapkan algoritma kriptografi Blowfish dan AES-128 yang diharapkan dapat menjaga kerahasiaan dan keaslian data, sehingga pihak yang tidak bertanggung jawab tidak dapat memanipulasi data pada fitur BluCareer pada aplikasi BluCampus. Hasil dari penelitian ini diimplementasikan dalam program aplikasi BluCampus yang dapat memberikan kemudahan pada kebutuhan berbagi kelas bagi setiap pengguna BluCampus. Di dalam implementasi fitur Blu Career mampu memiliki fungsi yang sesuai untuk mempermudah kebutuhan pengguna dalam memproses berbagi kelas serta memiliki User Interface dan User Experience yang cukup memuaskan dalam pengalaman pemakaian aplikasi oleh pengguna. Kelemahan dari aplikasi yang dikembangkan adalah masih sering terjadi error, hang, bahkan crash pada beberapa perangkat sehingga masih terus dikembangkan.

Kata kunci: Kriptografi, Blowfish, AES-128.

1. PENDAHULUAN

Blu Campus pada fitur Blu Career bertujuan untuk mempermudah pengguna yang memiliki kemampuan tertentu dan ingin membuka sebuah kelas belajar serta mempermudah pengguna lain dalam mencari kelas belajar untuk mengasah kemampuan dan pengetahuan yang mereka miliki. Dalam fitur Blu Career terdapat menu *Profile* yang di dalamnya menyimpan kegiatan pengguna seperti pengguna pernah mengikuti acara seminar, workshop, open class (pada fitur Blu Career), dan my experience (pengalaman pengguna mengajar pada fitur Blu Career).

Menu *Profile* pada fitur Blu Career masih terbatas karena tujuan penggunanya tidak lain adalah seorang mahasiswa. Sedangkan Blu Campus merupakan aplikasi yang memiliki tujuan agar mahasiswa Kampus Budi Luhur yang mudah dalam mengetahui *event* dan pengumuman penting yang berada di kampus. Serta mempermudah organisasi kampus yang ingin melakukan upaya penyebaran *event* yang dibuatnya. Tidak sampai disitu pada aplikasi Blu Campus fitur Blu Career pengamanan data turut menjadi hal yang tidak dapat diabaikan, data pada Blu Career dinilai penting bagi pembuat aplikasi. Untuk pengamanan data dapat digunakan metode kriptografi yang diterapkan pada Android.

c. Bagaimana tingkat fungsionalitas, reliability, usability dan efficiency menurut pengguna aplikasi.

Algoritma kriptografi yang digunakan oleh penulis adalah Blowfish dan AES-128. Penulis menggunakan 2 metode ini agar data pada aplikasi Blu Career memiliki tingkat keamanan yang tinggi. Alasan penulis menggunakan metode Blowfish adalah karena keamanan Blowfish telah terbukti dengan diadopsinya sebagai Open Cryptography Interface (OCI) pada kenel linux versi 2.5 keatas. Dengan itu dunia *open source* menyatakan blowfish adalah salah satu algoritma kriptografi terbaik. Dan alasan penulis menggunakan metode AES-128 adalah karena AES ini merupakan standard algoritma kriptografi yang baru dan lebih baik dibandingkan dengan pendahulunya (DES) yang sudah dianggap tidak aman karena panjang kunci yang relatif pendek sehingga mudah dipecahkan menggunakan teknologi saat ini. Dari Penjelasan ini, maka dapat dirumuskan sebagai masalah berikut:

a. Bagaimana mengamankan data pada aplikasi Android dari pencurian dengan cara mengimplementasikan kriptografi menggunakan algoritma Blowfish dan AES-128.
b. Bagaimana mengembalikan data terenkripsi menjadi data asli sehingga tidak mengubah data.

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma Blowfish dan AES-128. Secara umum tujuan dari penelitian ini adalah untuk membuat suatu inovasi baru dalam

Android diiringi oleh pengamanan data agar pihak ketiga tidak mengetahui jalur data yang digunakan oleh pengguna.

2. LANDASAN TEORI

2.1. Algoritma Blowfish

Enkripsi Blowfish merupakan golongan Enkripsi Simetrik diciptakan oleh Bruce Schneier, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan pada tahun 1994. Enkripsi blowfish dibuat untuk digunakan komputer dengan mikroprsesor besar (32-bit keatas dengan cache data yang besar). Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 clock cycle per Byte, kompak dimana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya dan keamanan yang variabel dimana panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, multiple 8 bit, default 128 bit) [1]. Algoritma Blowfish terdiri dari dua bagian yaitu, key expansion dan enkripsi data.

Referensi [2] menunjukan cara perhitungan manual pada algoritma Blowfish untuk itu penulis akan memberikan contoh perhitungan manual pada Algoritma Blowfish, sebagai berikut:

Inisialisasi P-Array (P0, P1, ..., P17) masing-masing 32 bit, seperti tabel berikut :

Tabel 1: Index P ke Biner.

Index P	Hex	Bin
P0	243F6A88	0010 0100 0011 1111 0110 1010 1000 1000
P1	85A308D3	1000 0101 1010 0011 0000 1000 1101 0011
...	...	...
P16	9216D5D9	1001 0010 0001 0110 1101 0101 1101 1001
P17	8979FB1B	1000 1001 0111 1001 1111 1011 0001 1011

Inisialisasi S-Array yang berjumlah masing-masing 255 dalam bentuk hexadecimal yang kemudian di konversi ke biner, seperti table berikut:

Tabel 2: Index S-Box

Index S-Box	Index	Hex	Bin
$S\text{-}BOX_0$	0	D131 0BA6	1101 0001 0011 0001 0000 1011 1010 0110
	1	98DF B5A C	1001 1000 1101 1111 1011 0101 1010 1100
	...	...	...
	254	08BA 4799	0000 1000 1011 1010 0100 0111 1001 1001
	255	6E85 076A	0110 1110 1000 0101 0000 0111 0110 1010
...	...	....	...
$S\text{-}BOX_3$	0	3A39 CE37	0011 1010 0011 1001 1100 1110 0011 0111
	1	D3F AF5C F	1101 0011 1111 1010 1111 0101 1100 1111
	..	...	...
	254	578F DFE3	0101 0111 1000 1111 1101 1111 1110 0011
	255	3AC3 72E6	0011 1010 1100 0011 0111 0010 1110 0110

Plaintext = “UBLFTITI”.

Tabel 3: Karakter ke Biner

CHR	ASCII	BIN
U	85	1000 0101
B	42	0100 0010
L	4C	0100 1100
F	46	0100 0110
T	53	0101 0011
I	49	0100 1001
T	53	0101 0011
I	49	0100 1001

Kemudian plaintext dibagi menjadi 2 bagian XL dan XR menjadi :

XL = 10000101 01000010 01001100 01000110

XR = 01010011 01001001 01010011 01001001

Pembagian sub kunci

Key = 2322

Tabel.4: Key ke Biner

CHR	ASCII	BIN
2	32	0011 0010
3	33	0011 0011
2	32	0011 0010
2	32	0011 0010

Biner = 00110010 00110011 00110010 00110010

Sub kunci iterasi pertama

P0 = P0 XOR Key

P0 = 0001 0110 0000 1100 0101 1000 1011 1010

Sub kunci iterasi kedua

P1 = P1 XOR Key

P1 = 1011 0111 1001 0000 0011 1010 1110 0001

Dan seterusnya hingga iterasi ke-18.

Dalam hal ini penulis hanya melakukan satu iterasi, disebabkan total iterasi enkripsi adalah sebanyak 16 putaran.

Untuk putara pertama i = 0 ;

XL = XL XOR P0

XL = 1001 0011 0100 1110 0001 0100 1111 1100

Lalu masukan fungsi F, fungsi F didapat dari XL dibagi menjadi 4 (a,b,c,d) masing-masing 8 bit, berikut adalah hasilnya :

a = 1001 0011 c = 0001 0100

b = 0100 1110 d = 1111 1100

$F(xL) = ((S_{0,a} + S_{1,b} \bmod 2^{32}) \oplus S_{2,c}) + S_{3,d} \bmod 2^{32}$

F(XL) = 11010011100000101011001110010010

XR = F(XL) XOR XR

XR = 1000 0000 1100 1011 1110 0000 1101 1011

Menukar nilai XR dan XL

XR = 1001 0011 0100 1110 0001 0100 1111 1100

XL = 1000 0000 1100 1011 1110 0000 1101 1011

Setelah melakukan iterasi ke 16, maka akan menghasilkan nilai baru XL dan XR masing-masing 32 bit. Tukar kembali XL dan XR setelah itu XOR kan nilai XL dan XR : XR = XR XOR P16 dan XL = XL XOR P17

Kemudian XL dan XR digabugangkan sehingga membentuk 64 bit. Contoh hasil chipertext:

01011011	01000010	01000000	00110010
91	66	64	50
00110000	00110011	00110001	00110011
48	51	49	51

Hasil Biner di masukan ke dalam model ASCII sehingga terbentuk ciphertext "[B@20313"

2.2. Algoritma AES-128

Advanced Encryption Standard (AES) 128 memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan [3].

Referensi [4] menunjukan bahwa ekspansi kunci menghasilkan total Nb (Nr+1) *word*. Algoritma ini membutuhkan set awal *key* yang terdiri dari Nb *word*, dan setiap round Nr membutuhkan data kunci sebanyak Nb *word*. Hasil key schedule terdiri dari array 4 byte word linear yang dinotasikan dengan (Li).

SubWord adalah fungsi yang mengambil 4 byte *word input* dan mengaplikasikan S-Box untuk menghasilkan *word output*. Fungsi RotWord adalah melakukan pergeseran sebanyak 1 byte. Rcon[i] terdiri dar nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x.

2.3. Studi Literatur

Tabel 5: Referensi Ilmiah

Penulis	Judul	Implikasi Penelitian
Siswo Wardoyo, Rian Fahrizal, dan Zaldi Imanullah [1]	Aplikasi Teknik Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android	Menjadi referensi penulis mencari kriptografi yang sesuai untuk perangkat mobile berbasis android.
Mochammad Aminudin [2]	Implementasi Kriptografi Pada Aplikasi Teks Editor Menggunakan Algoritma Blowfish dan DES (Data Encryption Standard) Berbasis WEB Pada PT.Kargo Lintas Angkasa	Pada skripsi ini penulis sangat terbantu dalam mempelajari perhitungan manual Blowfish.
Didi Surian [3]	Algoritma Kriptografi AES Rijndael	Membantu penulis menemukan algoritma kriptografi yang akan disandingkan oleh Blowfish. Dan memberikan informasi bahwa AES termasuk salah satu kriptografi yang baik dalam pengamanan data.
Rifkie Primartha [4]	Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Advanced Encryption Standard (AES)	Membantu penulis dalam pengertian key expansion pada AES dan alur AES menggunakan key expansion
Amish Umar dan Namita Tiwari [5]	Effective Implementation and Evaluation of AES in Matlab	Dari sumber ini penulis dapat mengetahui perhitungan manual dari setiap sub rumus pada AES

3. METODE PENELITIAN

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Untuk mendapatkan informasi dari berbagai sumber ilmiah, dilakukan studi pustaka baik dari referensi yang tersedia di perpustakaan maupun dari sumber lain.

Sementara itu, metode enkripsi yang digunakan adalah algoritma Blowfish dan AES-128 dan pengembangan aplikasi berbasis Android. Pengujian aplikasi ini menggunakan ISO 9126 untuk mengukur kualitas aplikasi yang dihasilkan.

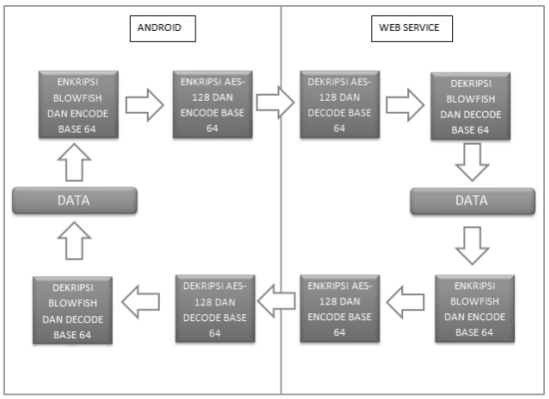
3.1. Arsitektur dan Rancangan Aplikasi

Di era yang serba canggih ini masih sulitnya bagi seseorang untuk mencari kelas terbuka yang dibutuhkan dan seseorang masih sulit untuk mempromosikan kemampuan yang dimiliki. Tidak hanya itu, di era yang serba canggih ini pun masih banyak yang mengabaikan keamanan pada data. Padahal keamanan data sangatlah dirasa penting dan tidak dapat diabaikan, karena jika kita lengah keamanan akan data akan diketahui bahkan dimanipulasi oleh pihak yang tidak bertanggung jawab dan berakibat merugikan bagi pengguna. Dari masalah yang ada, maka dibuatlah suatu aplikasi yang mempermudah pengguna untuk mencari kelas terbuka yang dibutuhkan dan mempromosikan kemampuan yang dimiliki dengan memperhatikan keamanan data dalam aplikasi, sehingga tidak ada pihak yang dapat dengan mudah mengubah bahkan merusak data yang sudah dibuat sebelumnya.

Aplikasi ini dibuat berbasis Android agar pengguna lebih mudah mengakses aplikasi, karena di era yang serba canggih ini lebih banyak pengguna

menggunakan *smartphone* dikehidupan sehari-harinya dari pada benda elektronik lainnya. Keamanan aplikasi berbasis Android ini menggunakan kriptografi dengan algoritma Blowfish dan AES-128. Dengan sistem keamanan ini diharapkan mampu menjaga data pada pengguna agar tidak dimanipulasi oleh pihak yang tidak bertanggung jawab.

Pada Gambar 1 penulis hanya akan mengoperasikan alur kriptografi di dalam Android saja, berikut Gambar 1 alur kriptografi android dengan web service.



Gambar 1: Alur Kriptografi Android dengan Web Service

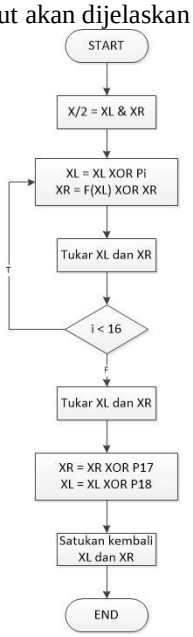
Algoritma dibawah ini menjelaskan bagaimana proses pengguna mengisi field pada Create Class serta penjelasan tentang proses enkripsi program.

```
1.  Tampilkan semua field create class
2.  Masukan field pada create class
3.  If action = finish then
4.      If semua field != kosong then
5.          Proses enkripsi
6.          Tersimpan dalam web service
7.      Else
8.          Alert field tidak boleh kosong
9.      End If
10. Else If action = back then
11.     Kembali ke form Open Class then
12. End If
```

Algoritma dibawah ini menjelaskan bagaimana proses mengambil data pada web service lalu memunculkan pada form Open Class hingga fungsi yang ditampilkan pada Open Class.

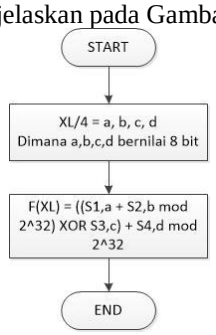
```
1.  Proses Dekripsi data
2.  Tampilkan isi form Open Class
3.  If pemilik = 1
4.      If Action = absen then
5.          Masuk ke form absen
6.      Else If Action = edit then
7.          Masuk ke fotm edit
8.      Else If Action = delete then
9.          Hapus data kelas dari Open Class
10.     Else If Action = Create Class than
11.         Masuk ke form Create Class
12.     End If
13. Else
14.     If Action = Create Class then
15.         Masuk ke form Create Class
16. End If
```

Flowchart proses Enkripsi adalah gambaran bagaimana proses enkripsi blowfish pada program dijalankan. Berikut akan dijelaskan pada Gambar 2.



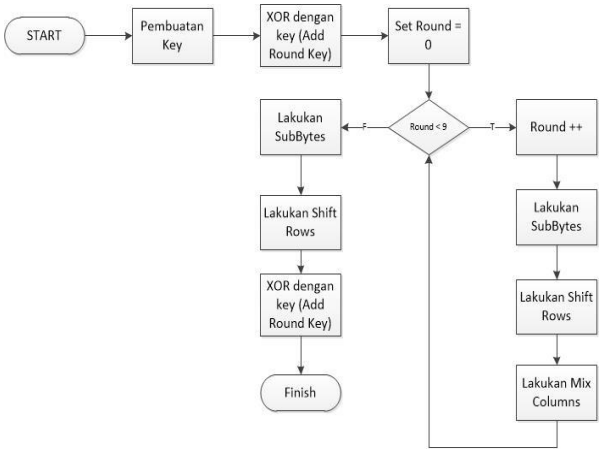
Gambar 2: Flowchart Enkripsi Blowfish

Flowchart proses pembentukan fungsi F adalah gambaran bagaimana fungsi F terbentuk dari kunci. Berikut akan dijelaskan pada Gambar 3.



Gambar 3: *Flowchart* Proses Pembentukan Fungsi F

Flowchart proses ekripsi AES merupakan gambaran alur data yang telah terenkripsi dengan blowfish lalu di enkripsi lagi dengan menggunakan algoritma AES. Berikut akan dijelaskan pada Gambar 4.

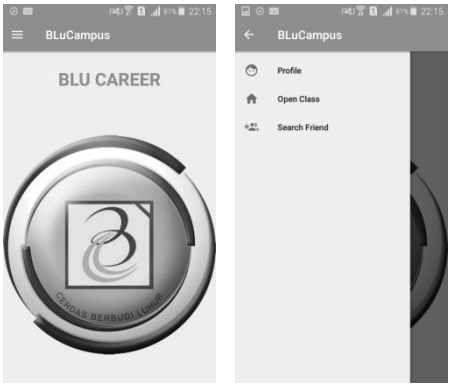


Gambar 4: Flowchart Proses Enkripsi AES

4. HASIL DAN PEMBAHASAN

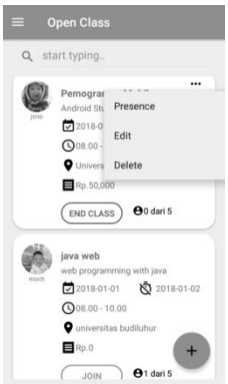
4.1. Tampilan Aplikasi

Tampilan layar dari *form* Menu Utama pada Gambar 5 ini muncul pada pertama kali aplikasi dijalankan dan terlihat ada sidebar yang menampilkan beberapa pilihan menu yaitu, Profile, Open Class, dan Search Friend.



Gambar 5: Tampilan Form Menu Utama

Tampilan layar pada *Form Open Class* pada gambar 6 ini muncul pada saat pertama kali program dijalankan ketika pengguna memilih menu Open Class pada gambar sebelumnya. Jika pengguna memiliki kelas maka pengguna dapat mengakses menu option yang terdapat pilihan menu Precense, Edit, dan Delete.



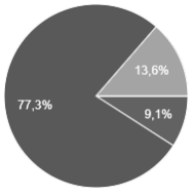
Gambar 6: Tampilan Form Open Class

4.2. Pengujian Program

Dalam pengujian kali ini penulis meminta 22 responden yang akan mencoba aplikasi dan mengisi kuesioner yang mencangkup pertanyaan-pertanyaan yang bersangkutan. Berikut pertanyaan dan hasil dari kuisioner.

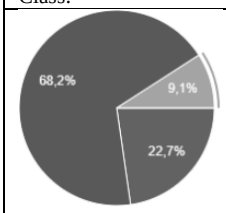
Tabel 6: Hasil Pertanyaan Fungsional

1. Aplikasi ini sudah sesuai dengan kebutuhan dan harapan



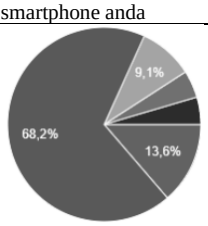
Respond en	Keterangan
2	Sangat Setuju
17	Setuju
3	Ragu-Ragu

2. Data masih akurat setelah proses enkripsi di Menu Create Class.



Respon den	Keterangan
5	Sangat Setuju
15	Setuju
2	Ragu-Ragu

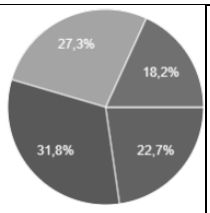
3. Aplikasi ini dapat berjalan sesuai standar spesifikasi perangkat smartphone anda



Responde n	Keterangan
3	Sangat Setuju
15	Setuju
2	Ragu-Ragu
1	Tidak Setuju
1	Sangat Tidak Setuju

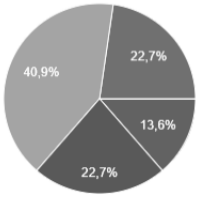
Tabel 7: Hasil Pertanyaan Reliability

1. Aplikasi ini tidak membuat perangkat smartphone anda hang atau melambat



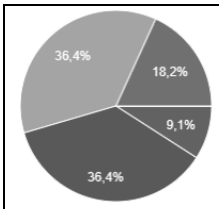
Respon den	Keterangan
5	Sangat Setuju
7	Setuju
6	Ragu-Ragu
4	Tidak Setuju

2. Aplikasi ini tidak pernah crash



Respon den	Keterangan
3	Sangat Setuju
5	Setuju
9	Ragu-Ragu
5	Tidak Setuju

3. Aplikasi ini tidak pernah muncul error



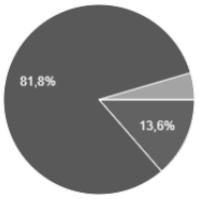
Responden	Keterangan
2	Sangat Setuju
8	Setuju
8	Ragu-Ragu
4	Tidak Setuju

Tabel 8: Hasil Pertanyaan Usability

1. Aplikasi ini memiliki tampilan yang mudah dipahami

Responden	Keterangan
2	Sangat Setuju
20	Setuju

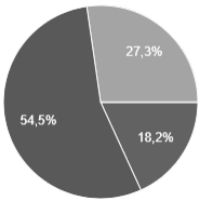
2. Aplikasi ini sangat mudah dioperasikan



Responden	Keterangan
1	Sangat Setuju
3	Setuju
18	Ragu-Ragu

Tabel 9: Hasil Pertanyaan Efficiency

1. Data pada menu Blu Career tampil dengan cepat



Responden	Keterangan
4	Sangat Setuju
12	Setuju
6	Ragu-Ragu

4.3. Kelebihan dan Kekurangan Program

Berdasarkan pengujian data pada tabel 1, tabel 2, tabel 3, dan tabel 4. Penulis menyimpulkan kelebihan dan kekurangan program yang telah diuji oleh 22 responden dengan 22 jenis perangkat.

Apliksai sesuai kebutuhan dan harapan pengguna dalam tujuan dari Blu Career itu sendiri. Data yang terkirim pada menu Create Class dengan data yang diterima pada menu Open Class masih akurat atau sama. Memiliki tampilan yang mudah dipahami. Sangat mudah dioperasikan oleh pengguna. Memiliki *Effeciency* yang cukup bagus.

Ketika menggunakan aplikasi ini masih banyak perangkat yang mengalami hang atau melambat. Beberapa smartphone mengalami crash saat menjalani aplikasi ini. Aplikasi ini masih sering mengalami eror dibeberapa smartphone.

5. KESIMPULAN

Berdasarkan perancangan, pembuatan, serangkaian uji coba dan analisa program dari aplikasi kriptografi ini, maka dapat diambil suatu kesimpulan yaitu, dengan adanya kriptografi, proses pembuatan, penyimpanan, dan pengambilan data menjadi lebih aman dan terpercaya. Kunci pada program hanya diketahui oleh penulis dan partner penulis sebagai pembuat web service sehingga kunci dapat di update berulang kali demi keamanan data. Proses dekripsi mengembalikan data seperti data asli tanpa mengalami perubahan sedikit pun. Terlepas dari kriptografi, aplikasi masih sering mengalami hang, error dan membuat dibeberapa perangkat smartphone crash sehingga terjadi ketidaknyamanan bagi pengguna. Apliksai sesuai kebutuhan dan harapan pengguna dalam tujuan dari Blu Career itu sendiri. Data yang terkirim pada menu Create Class dengan data yang diterima pada menu Open Class masih akurat atau sama. Memiliki tampilan yang mudah dipahami. Sangat mudah dioperasikan oleh pengguna. Memiliki *Effeciency* yang cukup bagus.

DAFTAR PUSTAKA

[1] Siswo Wardoyo, Rian Fahrizal, Zaldi Imanullah. (2014). *Aplikasi Teknik Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android*. 3 (1), 1-11.

[2] Mochammad Aminudin (2016). *Implementasi Kriptografi Pada Aplikasi Teks Editor Menggunakan Algoritma Blowfish dan DES (Data Encryption Standard) Berbasis WEB Pada PT.Kargo Lintas Angkasa*. Jakarta: Universitas Budi Luhur. p4-12.

[3] Surian Didi . (2006). ALGORITMA KRIPTOGRAFI AES RIJNDAEL. *Jurnal Teknik Elektro*. 8 (2), 97-101.

[4] Rifkie Primartha. (2013). -. *Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Advanced Encryption Standard (AES)*. 2 (1), 13-18.

[5] Amish Umar, Namita Tiwari . (2013). *Effective Implementation and Evaluation of AES in Matlab*, 95-99.