JISTech (Journal of Islamic Science and Technology)
JISTech, 7(1), 1-14, Januari-Juni 2022
ISSN: 2528-5718
http://jurnal.uinsu.ac.id/index.php/jistech

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) E-ASPIRASI MAHASISWA PADA FAKULTAS SAINS DAN TEKNOLOGI BERBASIS WEB

Mayasari[1], Suendri[2], M. Fakhriza[3]

[1,2,3] Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
E-mail: mayasari0916@gmail.com

ABSTRACT

Student aspirations are various demands that are packaged in students' creative ideas that propose a process of changing something. There is no aspiration complaint service system at the Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara. So that students do not have a place to express their aspirations. Along with the development of technology, a web-based student complaint application was made which is equipped with the AES (Advanced Encryption Standard) algorithm which is able to secure student aspiration messages so that the aspiration messages conveyed by students cannot be read by other students, so that student aspiration messages are more confidential. The design and manufacture of this web-based public complaint application uses the waterfall model. The waterfall model begins with the analysis stage, namely by analyzing and collecting data through interviews with students and the Administration of the Faculty of Science and Technology, the system design stage, namely by designing the system interface, the system coding stage, and this stage ends with the system testing stage. Carried out to determine the feasibility of the system.

Keywords: *Student Aspiration, AES, Web.*

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat dalam berbagai bidang kehidupan seperti dalam bidang politik, sosial dan budaya, pendidikan, ekonomi dan bisnis. Semua bidang tersebut telah mengaplikasikan teknologi informasi dan komunikasi untuk mempermudah kinerja instansi di masyarakat. Pada bidang pendidikan,

khususnya pihak universitas sudah banyak menerapkan teknologi ini sebagai proses pembelajaran melalui *website* Depdiknas, *e-learning*, beasiswa dan kotak saran *online*.

Fakultas Sains dan Teknologi merupakan salah satu Fakultas di Universitas Islam Negeri Sumatera Utara yang memiliki 2.800 mahasiswa yang terdiri dari 5 program studi. Penyampaian aspirasi yang dilakukan mahasiswa saat ini kebanyakan melalui demonstrasi, karena tidak adanya wadah yang disediakan Fakultas Sains dan Teknologi untuk menampung aspirasi mahasiswa tersebut. sehingga dibutuhkan sistem untuk menyalurkan aspirasi yang mudah dan cepat. Di mana sistem ini juga mampu mengamankan pesan aspirasi mahasiswa agar pesan aspirasi yang disampaikan oleh mahasiswa tidak dapat dibaca oleh mahasiswa lain, sehingga pesan aspirasi mahasiswa lebih bersifat rahasia.

Untuk mengamankan pesan tersebut, diperlukan suatu sistem keamanan yang kuat. Pesan harus diproses dan diubah dalam bentuk kode sebelum dikirimkan, ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan istilah kriptografi. Salah satu algoritma kriptografi yang bisa digunakan dalam sistem ini adalah algoritma enkripsi AES.

LANDASAN TEORI

1. Algoritma *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (*AES*) merupakan sistem penyandian blok yang bersifat *non-Feistel* karena AES menggunakan komponen yang selalu memiliki *invers* dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde. Proses di dalam AES merupakan transformasi terhadap *state*. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai *state*. Enkripsi AES adalah transformasi terhadap *state* secara berulang dalam beberapa ronde. *State* yang menjadi keluaran ronde k menjadi masukan untuk ronde ke-k +1 [1].

2. Enkripsi AES

Pada awal proses enkripsi, input yang telah di*copy*kan ke dalam *state*

akan mengalami transformasi *byte AddRoundKey*. Setelah itu, *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya, dimana pada *round* terakhir state tidak mengalami transformasi *MixColumns* [2].

3. Dekripsi AES

Transformasi *chipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* [2].

4. Web

World wide web atau sering dikenal sebagai *web* adalah suatu layanan sajian informasi yang menggunakan konsep *hyperlink* (tautan), yang memudahkan surfer (sebutan para pemakai komputer yang melakukan *browsing* atau penelusuran informasi melalui internet). Keistimewaan inilah yang telah menjadikan *web* sebagai *service* yang paling cepat pertubuhannya [3].

5. Aspirasi

Aspirasi merupakan salah satu faktor yang sangat mempengaruhi motivasi belajar. Motivasi seorang pembelajar menjadi begitu tinggi ketika ia sebelumnya sudah memiliki cita-cita. Aspirasi memberikan dorongan bagi siswa untuk meraih keberhasilan. Menurut Departemen Pendidikan Nasional bahwa aspirasi merupakan harapan dan tujuan untuk keberhasilan pada masa yang akan datang. Beraspirasi berarti bercita-cita, berkeinginan, berhasrat.

METODE PENELITIAN

Model pengembangan dalam penelitian ini menggunakan metode

penelitian dan pengembangan (*Research and Development/R&D*). Menurut Sukmadinata penelitian pengembangan merupakan pendekatan penelitian untuk menghasilkan suatu produk baru atau menyempurnakan produk yang telah ada [4]. Adapun tahap penelitian ini sebagai berikut:

1. Pengumpulan Data

Pengumpulan data merupakan suatu cara memperoleh data-data yang diperlukan dalam penelitian dengan melakukan survei lapangan yang ada hubungannya dengan masalah yang diteliti. Jenis penelitian ini dilakukan untuk mendapatkan data primer.

a. Observasi

   Observasi yaitu pengumpulan data yang dilakukan dengan cara meninjau atau mengunjungi perusahaan yang bersangkutan secara langsung, untuk mencatat informasi yang berkaitan dengan masalah yang akan diteliti.

b. Wawancara

   Wawancara dilakukan dengan tanya jawab kepada Bapak Munawir S.E selaku Bendahara Pengeluaran Pembantu di Administrasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.

c. Studi Kepustakaan

   Studi Kepustakaan (*Library Research*) yaitu pengumpulan data atau informasi yang dilakukan dengan cara membaca dan mempelajari *literature* atau sumber yang berkaitan dengan masalah yang diteliti. Studi perpustakaan dapat diperoleh dari data sekunder yaitu *literature-literature*, buku-buku, yang berkaitan dengan objek yang diteliti dan bertujuan mengetahui teori yang ada kaitannya dengan masalah yang diteliti.

2. Metode Pengembangan Sistem

Metode yang digunakan pada pengembangan perangkat lunak perancangan sistem informasi ujian berbasis *web* menggunakan model *Waterfall*, alasan menggunakan metode *Waterfall* adalah karena Metode ini tahapan dan juga urutan dari metode yang dilakukan berurutan dan

berkelanjutan, seperti layaknya sebuah air terjun. Tahapan-tahapan model *Waterfall* [5] adalah:

a. Analisis

   Dalam analisa kebutuhan ini bertujuan untuk menganalisis kebutuhan yang dibutuhkan dalam perancangan baik berupa dokumen maupun sumber lain yang dapat membantu dalam menentukan solusi permasalahan yang ada baik dari sisi *user* maupun admin.

b. Perancangan (*Desain*)

   Dalam Desain perangkat lunak menggunakan permodelan basis data dengan menggunakan diagram konteks, dan *UML* (*unifed Modelling Language*).

c. Pemrograman (*Coding*)

   Dalam tahap ini peneliti mulai membangun aplikasi sesuai dengan analisis kebutuhan untuk membuat *form input* dan *output* dengan aplikasi berbasis *web* dengan bahasa pemrograman PHP.

d. Pengujian (*Testing*)

   Pada tahapan akhir dimana sistem yang baru diuji kemampuan dan keefektifannya sehingga didapatkan kekurangan dan kelemahan sistem yang kemudian dilakukan pengkajian ulang dan perbaikan terhadap aplikasi menjadi lebih baik dan sempurna.

e. Operasi dan Perawatan

   Dalam proses pemeliharaan ini penulis mengupayakan pengembangan sistem yang telah dirancang terkait *software* dan *hardware* dapat dibuat maksimal agar aplikasi dapat berjalan dengan baik.

HASIL DAN PEMBAHASAN

1. Algoritma AES

Aspirasi mahasiswa memiliki nilai yang sangat berarti dan merupakan suatu data yang bersifat rahasia atau tidak untuk diketahui orang banyak. Karena hal ini dibutuhkannya metode keamanan data atau biasa disebut enkripsi data. Algoritma AES ini memiliki 3 langkah atau proses yaitu: Ekspansi Kunci, Enkripsi dan Dekripsi. Penyandian algoritma AES

(*Advanced Encryption Standard*) menggunakan proses berulang yang disebut ronde baik pada proses enkripsi maupun dekripsi. Jumlah ronde yang digunakan yaitu sebanyak 10 ronde karena panjang kunci yang digun akan 128 bit. Di mana setiap ronde menggunakan *roundkey* yang berbeda yang diperoleh dari ekspansi kunci.

Di bawah ini akan dijelaskan bagaimana ekspansi kunci untuk mendapatkan *round key*, proses enkripsi dan dekripsi terhadap contoh kasus:

1. Ekspansi Kunci

Kunci ronde (*round key*) diperlukan untuk proses enkripsi dan dekripsi pada algoritma AES (*Advanced Encryption Standard*). Panjang kunci yang digunakan sebanyak 16 digit. Pada contoh kasus ini, kunci yang digunakan yaitu "sistem_informasi".

a. Urutkan kunci kedalam blok berukuran 128 bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk *hexadecimal*.

s	i	s	t	e	m	_	i	n	f	o	r	m	a	s	i
73	69	73	74	65	6D	5F	69	6E	66	6F	72	6D	61	73	69

b. Langkah selanjutnya yaitu, susun kunci yang telah diubah ke dalam *state* berukuran 4 x 4 seperti berikut :

Cipherkey/kunci ronde ke-0

73	65	6E	6D
69	6D	66	61
73	5F	6F	73
74	69	72	69

c. Setelah itu, untuk mendapatkan hasil kolom pertama pada sub kunci, langkah pertama yaitu dilakukan fungsi *RotWord* yaitu dengan menggeser setiap bit pada kolom ke-4 ke atas 1 kali dari kunci ronde ke-0.

d. Perhitungan Rk1

Tahap akhir untuk mendapatkan kolom pertama yaitu proses XOR

antara kolom pertama dari kunci ronde ke-0 dan hasil dari *SubBytes* lalu di XOR kan lagi dengan RCon. Untuk mendapatkan kolom kedua, diperoleh dengan XOR antara *wi* dengan kolom kedua dari kunci ronde ke-0. Untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua.

Tabel 1. Kolom 1 Rk1

Kolom 1			
73 XOR EF 73 = 0111 0011 EF = 1110 1111 X1 = 1001 1100 01 = 0000 0001 X1 = 1001 1101 = 9D = 9 D	69 XOR 8F 69 = 0110 1001 8F = 1000 1111 X1 = 1110 0110 00 = 0000 0000 X1 = 1110 0110 = E6 = E 6	73 XOR F9 73 = 0111 0011 F9 = 1111 1001 X1 = 1000 1010 00 = 0000 0000 X1 = 1000 1010 = 8A = 8 A	74 XOR 3C 74 = 0111 0100 3C = 0011 1100 X1 = 0100 1000 00 = 0000 0000 X1 = 0100 1000 = 48 = 4 8

Hasil keseluruhan:

73	65	6E	6D	9D	F8	96	FB	FB	03	95	6E	C1	C2	57	39
69	6D	66	61	E6	8B	ED	8C	3B	B0	5D	D1	AA	1A	47	96
73	5F	6F	73	8A	D5	BA	C9	0A	DF	65	AC	7C	A3	C6	6A
74	69	72	69	48	21	53	3A	47	66	35	0F	D8	BE	8B	84
0				Rk1				Rk2					Rk3		

59	9A	CD	F4	B3	29	E4	DD	A3	8A	6E	B3	59	D3	BD	0E
A8	B2	F5	63	D9	6B	9E	08	3D	56	C8	C0	39	6F	A7	67
23	80	46	2C	02	82	C4	AE	D8	5A	9E	30	1F	45	DB	EB

CA	74	FF	7B	75	01	F E	7A	B4	B5	4 B	31	D 9	6C	27	16
			Rk4				Rk5				Rk6				Rk7

5C	8F	32	3C	95	1A	28	14	2E	70	8B	16
D0	BF	18	7F	08	B7	AF	D0	88	E8	40	84
58	1D	C6	2D	4D	50	96	BB	41	74	52	41
72	1E	39	2F	99	87	BE	91	7C	B9	FE	E3
		Rk8				Rk9				Rk10	

2. Tahap Enkripsi

Berikut adalah proses enkripsi dari *plaintext* tersebut.

a. Urutkan *plaintext* kedalam blok dan ubah ke bilangan *hexadecimal*.

k	e	a	M	a	n	a	n		r	a	h	a	s	i	a
6 B	6 5	61	6 D	61	6 E	61	6 E	2 0	7 2	61	6 8	61	7 3	6 9	61

b. *Plaintext* di XOR kan dengan *cipherkey* atau kunci ronde ke-0. Proses ini dinamakan *AddroundKey*.

c. Tahap *SubBytes*

18	04	4E	0 C
0 C	03	14	12
12	3E	0 E	1A
19	07	1A	08

AF	F2	2F	F E
FE	7B	FA	C9
C9	B2	AB	A 2
D 4	C5	A2	30

Hasil didapat dari *s-box table*

d. Tahap *ShifRows*

Tahap selanjutnya adalah *ShifRows* yaitu hasil *SubBytes* digeser ke kiri mulai dari baris ke 1 dilakukan 0 pergeseran, baris ke 2 dilakukan

1 pergeseran, baris ke 3 dilakukan 2 pergeseran, dan baris ke 4 dilakukan 3 pergeseran.

e. Tahap *MixColumns*

Pada transformasi *MixColumns*, melakukan proses perkalian antara suatu matriks polinominal tetap dengan *state* hasil *ShiftRows*.

Hasil keseluruhan *mixcolumn*

53	8C	D2	16
8D	34	23	14
C9	31	3B	B3
C0	E6	E0	88

f. Proses *MixColumns* di XOR kan dengan kunci ronde ke-1. Berikut adalah proses *AddRoundKey* ronde ke-1.

Hasil dari proses AddRoundKey pada ronde ke-10 merupakan hasil akhir proses enkripsi yaitu: a7936ea308519658461256e3ee3d94c3

3. Dekripsi

a. Melakukan proses *AddRoundKey,* antara *ciphertext* yang telah diperoleh dari proses enkripsi dengan *roundkey* ke-10.

A7	08	46	EE
93	51	12	3D
6E	96	56	94
A3	58	E3	C3

2E	70	8B	16
88	E8	40	84
41	74	52	41
7C	B9	FE	E3

89	78	CD	F8
1B	B9	52	B9
2F	E2	04	D5
DF	E1	1D	20

b. Melakukan transformasi *InvShiftRows*, karena pada ronde ke-1 dalam proses dekripsi tidak dilakukan proses *InvMixColumns*.

c. Melakukan proses transformasi *InvSubBytes*,

d. Kemudian melakukan operasi XOR antara hasil *InvSubBytes* dengan *RoundKey 9* untuk melakukan transformasi putaran ke 2.

e. Kemudian hasil *AddRoundKey* tersebut akan melakukan proses transformasi *InvMixColumn s* dengan aturan *irreducible polynominal*.

Setelah proses ronde ke-10 selesai, hasil dari *InvSubBytes* ronde ke-10 di XOR dengan *cipherkey* atau *key* ke-0.

18	04	4E	0C
0C	03	14	10
12	3F	0E	1A
19	07	1A	08

73	65	6E	6D
69	6D	66	61
73	5F	6F	73
74	69	72	69

=

6B	61	20	61
65	6E	72	73
61	61	61	69
6D	6E	68	61

Hexadecimal

6B	65	61	6D	61	6E	61	6E	20	72	61	68	61	73	69	61

Plaintext

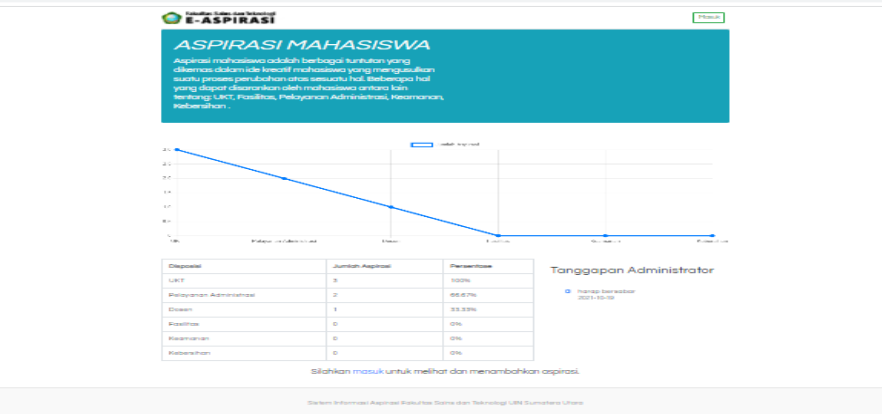
k	e	a	m	a	n	a	n		r	a	h	a	s	I	a

Implementasi Sistem

Tahap ini adalah tahap dimana rancangan yang sudah dibuat akan diterapkan menjadi sebuah sistem yang akan dapat membantu mahasiswa dalam memberikan aspirasinya terhadap Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.

1. Halaman Utama *User*

Pada halaman ini menampilkan halaman utama *user*. Berikut gambar halaman utama user di bawah ini:



Gambar 1. Halaman Utama *User*

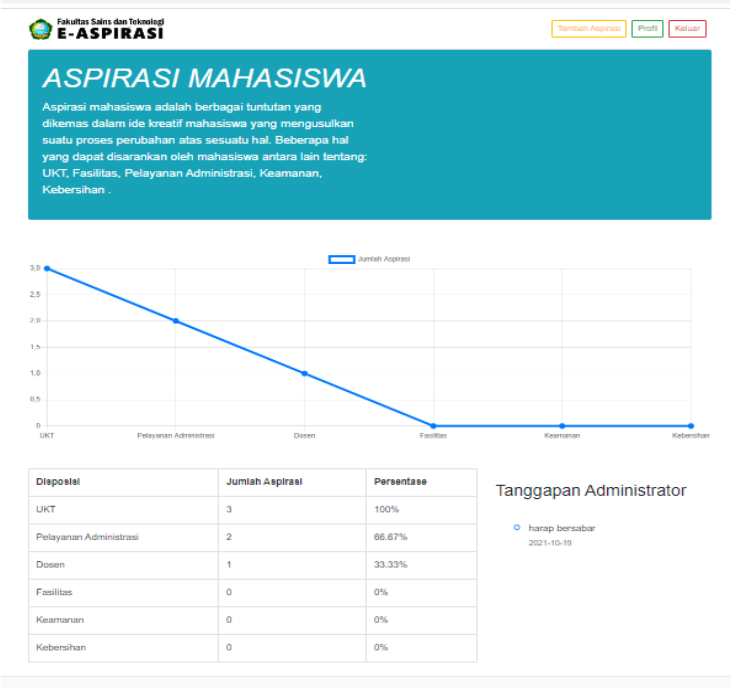
2. Halaman *Login* Mahasiswa

Halaman ini merupakan halaman mahasiswa untuk masuk ke sistem. Berikut gambar *login* mahasiswa di bawah ini:

Gambar 2. Halaman *Login* Mahasiswa

3. Halaman Utama Mahasiswa

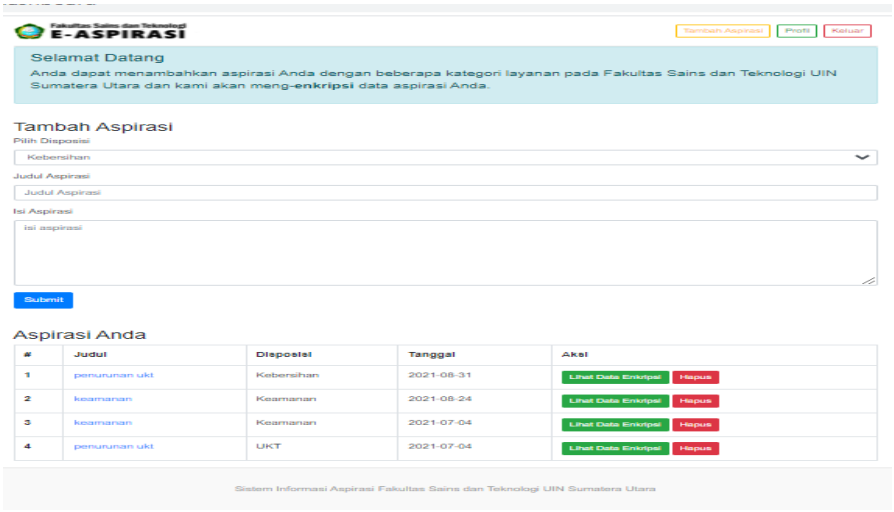
Halaman ini merupakan halaman utama mahasiswa. Berikut gambar halaman utama mahasiswa di bawah ini:



Gambar 3. Halaman Utama Mahasiswa

4. Halaman Tambah Aspirasi

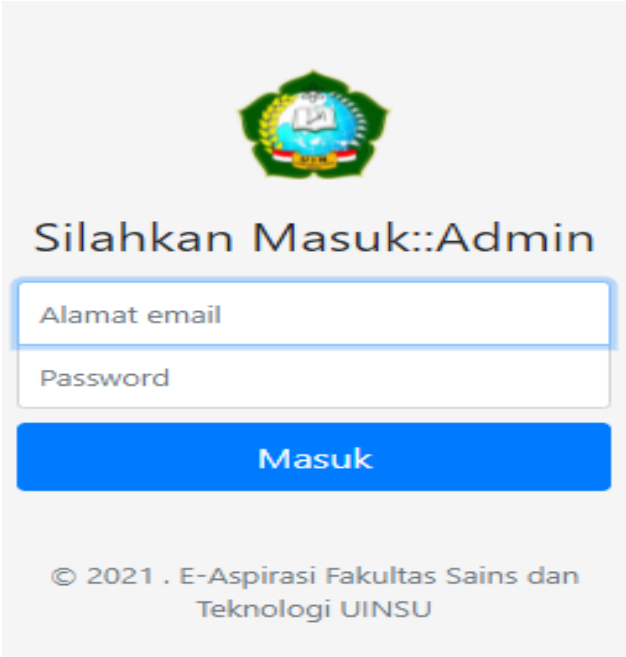
Halaman ini adalah halaman mahasiswa untuk menambahkan aspirasinya. Berikut gambar halaman tambah aspirasi di bawah ini:



Gambar 4. Halaman Tambah Aspirasi

5. Halaman *Login* Admin

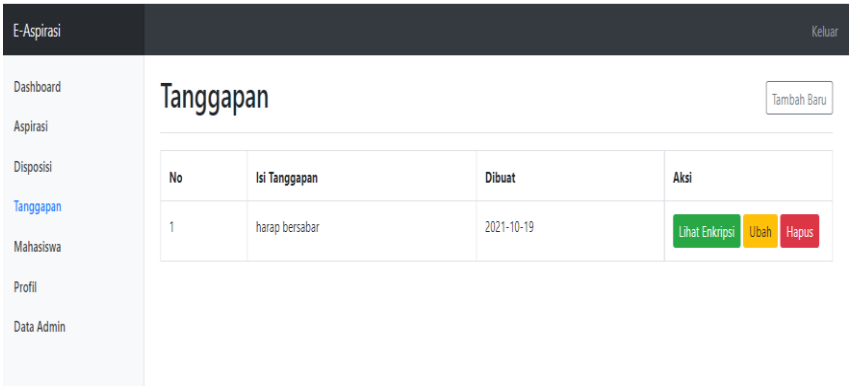
Halaman ini merupakan halaman admin untuk masuk ke sistem. Berikut gambar *login* admin di bawah ini:



Gambar 5. Halaman *Login* Admin

6. Halaman Data Tanggapan

Halaman ini adalah halaman untuk memberi tanggapan. Berikut gambar halaman data tanggapan di bawah ini:



Gambar 6. Halaman Data Tanggapan

KESIMPULAN

Perancangan E-aspirasi berbasis web dengan menggunakan *security* algoritma *Advanced Encryption Standard* (AES) ini dibangun agar dapat memberikan kemudahan mahasiswa Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara dalam memberikan aspirasi atau sarannya yang bersifat rahasia. Berdasarkan penelitian di atas dapat diperoleh kesimpulan sebagai berikut:

1. Perancangan E-aspirasi berbasis *web* ini dirancang dengan menggunakan bahasa pemrograman PHP dan dilengkapi menggunakan *security* algoritma *Advanced Encryption Standard* (AES).
2. Perancangan E-aspirasi berbasis *web* ini dapat menampung semua aspirasi mahasiswa Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara.
3. Perancangan E-aspirasi berbasis *web* ini dapat menampilkan persentase atau *tranding* dari semua aspirasi.

DAFTAR PUSTAKA

[1] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 2, no. 1, pp. 118–125, 2016.

[2] G. G. P. U. K and A. Erlanshari, "IMPLEMENTASI METODE A DVANCED ENCRYPTION STANDARD (AES) DAN MESSAGE DIGEST 5 (MD5) PADA ENKRIPSI DOKUMEN (STUDI KASUS

LPSE UNIB)," vol. 4, no. 3, pp. 277–287, 2016.

[3] R. V Palit, Y. D. Y. Rindengan, and A. S. M. Lumenta, "Rancangan Sistem Informasi Keuangan Gereja Berbasis Web Di Jemaat Gmim Bukit Moria Malalayang," *J. Tek. Elektro dan Komput.*, vol. 4, no. 7, pp. 1–7, 2015, doi: 10.35793/jtek.4.7.2015.10458.

[4] I. A. Wynarti, "Pengembangan Permainan Charades Sebagai Media Pembelajaran Materi Jenis-jenis Bisnis Ritel Kelas XI Pemasaran Di SMK Negeri 2 Buduran," *J. Pendidik. Tata Niaga*, vol. 6, no. 3, pp. 63–70, 2018.

[5] D. S. Purnia, A. Rifai, and S. Rahmatullah, "Penerapan Metode Waterfall dalam Perancangan Sistem Informasi Aplikasi Bantuan Sosial Berbasis Android," *Semin. Nas. Sains dan Teknol. 2019*, pp. 1–7, 2019.