**BAB III**

**ANALISIS DAN PERANCANGAN**

* 1. **Analisis Masalah**

Kehalalan suatu produk baik itu makanan, minuman, obaat – obatan, kosmetik dan lalin sebagainya adalah hak konsumen. Indoenesia sebagai salah satu penganut agama islam terbesar tentunya mengkonsumsi barang – barang tersebut adalah suatu kewajiban, terlebih dijaman perdagangan bebas ini ratusan bahkan ribuan jenis produk telah masuk ke Indonesia, sehingga timbul masalah mengenai kehalalan produk tersebut.

Dalam kegiatan produksi dan perdagangan produk pangan di era globalisasi ini, masyarakat yang mengkonsumsi, khususnya umat islam perlu diberikan pengetahuan tentang kehalalan produk, informasi dan akses yang memadai agar memperoleh informasi yang benar tentang status kehalalan produk yang dibelinya, terlebih semakin banyaknya produk – produk asing yang masuk ke tanah air yang kehalalanya tentunya akan sangat sulit diketahui. Maka dari itu pemerintah saat ini dengan berdasarkan UU No 33 tahun 2014 (UU JPH) tentang jaminan produk halal melalui Kementrian Agama membentuk Badan Penyelenggara Jaminan Produk Halal (BPJPH) yang telah diresmikan pada tanggal 10 november 2017 yang tentunya akan menjadi lembaga yang mengelola sertifikasi kehalalan sebuah produk baik itu makanan, minuman, kosmetik dan obat – obatan dengan masa berlaku selama 2 tahun yang kemudian bisa di perpanjang kembali, dan pada awalnya semua proses tersebut yang sebelumnya oleh dikelola oleh Lembaga

Pengkajian Pangan, Obat-obatan, dan Kosmetika Majelis Ulama Indonesia ( **LPPOM MUI ).**

Maka dari permasalahan itu perlu perlunya pengembangan dari sistem yang ada dan penambahan platform baru atau sebuah media dimana kita sebagai konsumen dapat mengecek langsung ke validan sertifikasi kehalalan produk tersebut dengan praktis, mudah, relatime dan terpercaya berdasarkan data dari lembaga terkait.

* 1. **Analisis Sistem**

Pada sistem yang berjalan saat ini dalam proses penerbitan sertifikasi halal masih belum maksimal, terlebih sampai saat ini pemerintah melalui lembaga khusus yang bertugas dibawah naungan Kementrian Agama yaitu Badan Penyelenggara Jaminan Produk Halal (BPJPH) sampai saat ini masih dalam tahap proses persiapan baik itu secara kelembagaan dan sistem, fakta dilapangan yang penulis dapat adalah masih belum adanya sebuah sistem verifikasi keaslian sertifikasi kehalalan sebuah produk, selain itu kemungkinan pemalsuan pun tentunya masih mungkin dilakukan, dan faktanya banyak produk yang berlabel halal tanpa no sertifikasi halal resmi, selain itu belum adanya sebuah aplikasi khusus bagi masyarakat berbasis QR Code yang dapat mengetahui keaslian dan kehalalan suatu produk berdasarkan data dari server lembaga terkait sehingga masyarakat kesulitan untuk mengecek keaslian sebuah produk secara cepat.

1. Analisis Sistem yang sedang berjalan

Anslisis aplikasi didefinisikan sebagai penguraian dari suatu sistem yang utuh ke dalam bagian – bagian komponenya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan dan hambatan yang terjadi pada kebutuhan yang mana diharapkan dapat diusulkan, adapun sistem yang sedang berjalan sekarang sekarang untuk proses pengecekan keaslian produk halal yang dapat dilakukan masih menggunakan website halal MUI:



Gambar 3.1 *Rich Picture Diagram*  Sistem yang berjalan

1. Sistem yang ditawarkan

Sistem yang ditwarkan akan mempermudah kosumen dalam pengecekan keaslian data sertifikasi halal, selain itu proses nya cepat dikarnakan input data melaui teknologi Qr Code cukup akurat dan cepat dan bisa dilakukan dengan mudah dengan menggunakan smartphone android,berikut sistem yang ditwarkan dalam bentuk Rich Picture Diagram sistem yang akan ditawarkan :

Gambar 3.2 Rich Picture Diagram Sistem yang ditawarkan

* 1. **Analisis Kebutuhan Sistem**

Analisis kebutuhan sistem adalah analisis terhadap sistem yang akan diusulkan atau dikembangkan. Analisis ini meliputi analisis kebutuhan fungsional dan non fungsional yang disusulkan dapat sesuai dengan kebutuhan dan dapat menyelesaikan permasalahan yang ada berdasarkan hasil pengamatan.

* + 1. **Analisis kebutuhan Non Fungsional**

1. **Kebutuhan Perangkat Keras**

Spessifikasi perangkat keras yang digunakan penulis untuk membangun aplikasi adalah sebagai berikut :

1. Laptop dengan Spesifikasi
2. Processor : Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz (4 CPUs)
3. RAM : 6 GB
4. OS : Windows 10 Pro
5. Hardisk : 500 GB
6. Vga Card : NVIDIA GeForce 710 M

Selain itu untuk dibutuhkan juga sebuah perangkat pengujian aplikasi android dengan spesifikasi minimum sebagai berikut :

1. OS : Android Jelly Bean
2. API Level : 17
3. Kamera : 2 Mp
4. Ram : 512 Mb
5. Memori : 1 Gb
6. **Kebutuhan Perangkat Lunak**

Spesifikasi sistem operasi dan perangkat lunak yang digunakan penulis untuk membangun aplikasi ini adalah sebagai berikut :

1. Microsoft Windows 10 Pro
2. Xampp V 3.2.2
3. Android Studio V 3.1
4. Notepad ++
5. Browser Opera
6. **Kebutuhan Pengguna (User)**

Sebuah aplikasi dapat berjalan dengan baik ketika aplikasi tersebut digunakan dengan benar sesuai dengan fungsinya, aplikasi yang diusulkan dapat membantu masyarakat ataupun konsumen dalam melakukan validasi kehalalan sebuah produk berdasarkan data dari server Badan Penyelenggara Jaminan Produk Halal (BPJPH), bagi pemerintah pun ini adalah bentuk pelayanan yang baik bagi masyarakat maupun produsen. Dalam prosesnya dibutuhkan minimal seorang admin dalam mengelola data sertifikasi halal dan proses manajemen database serta generan kode QR yang nanti di tempe di produk, QR code yang dihasilkan adalah QR code yang sudah di enkripsi dengan algoritma Advance Encryption Standar (AES) 128 dan kode QR tersebut hanya bisa di baca dan di deskripsikan dengan aplikasi yang penulis buat.

* + 1. **Kebutuhan Fungsional** 
       1. **Perhitungan *Algoritma Advance Encryption Standar* (AES) 128**

1. **Enkripsi AES**

Pada dasarnya algoritma AES terdapat 4 proses tahapan dalam melakukan enkripsi yaitu *SubBytes*, ShiftRows, MixColumns, dan AddRoundKey, Berikut contoh perhitungan manual algoritma AES 128 :

**Langkah pertama** adalah menyiapkan plaintext dan sandi/kunci yang akan di terapkan :

Plaintext (Hexadesimal) = 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF

Kunci (Hexadecimal) = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Kemudia ubah dalam bentuk State baik plaintextnya ataupun kuncinya seperti berikut (Round 0) :

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 44 | 88 | CC |
| 11 | 55 | 99 | DD |
| 22 | 66 | AA | EE |
| 33 | 77 | BB | FF |

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 04 | 08 | 0C |
| 01 | 05 | 09 | 0D |
| 02 | 06 | 0A | 0E |
| 03 | 07 | 0B | 0F |

Langkah selanjutnya jika state telah terbentuk adalah melakukan opeasi XOR state plaintext dengan state kunci

00000000 = ‘00’ 00010001 = ‘11’ 00100010 = ‘22’ 00110011 = ‘33’

00000000 = ‘00’ 00000001 = ‘01’ 00000010 = ‘02’ 00000011 = ‘03’

00000000 = **‘00’** 00010000 = **‘10’** 00100000 = **‘20’** 00110000 = **‘30’**

01000100 = ‘44’ 01010101 = ‘55’ 01100110 = ‘66’ 01110111 = ‘77’

00000100 = ‘04’ 00000101 = ‘05’ 00000110 =’06’ 00000111 = ’07’

01000000 = **‘40’** 01010000 = **‘50’** 01100000 = **‘60’** 01110000 = **‘70’**

10001000 = ‘88’ 10011001 = ‘99’ 10101010 = ‘AA’ 10111011 = ‘BB’

00001000 = ‘08’ 00001001 = ‘09’ 00001010 = ‘0A’ 00001011 = ‘0B’

10000000 = **‘80’** 10010000 = **‘90’** 10100000 = **‘A0’** 10110000 = **‘B0’**

11001100 = ‘CC’ 11011101 = ‘DD’ 11101110 = ‘EE’ 11111111 = ‘FF’

00001100 = ‘0C’ 00001101 = ‘0D’ 00000111 = ‘0E’ 00001111 = ‘0F’

11000000 = **‘C0’** 11010000 = **‘D0’** 11101000 = **‘E0’** 11110000 = **‘F0’**

Maka dari hasil operasi XOR diatas adalah sebagai berikut :

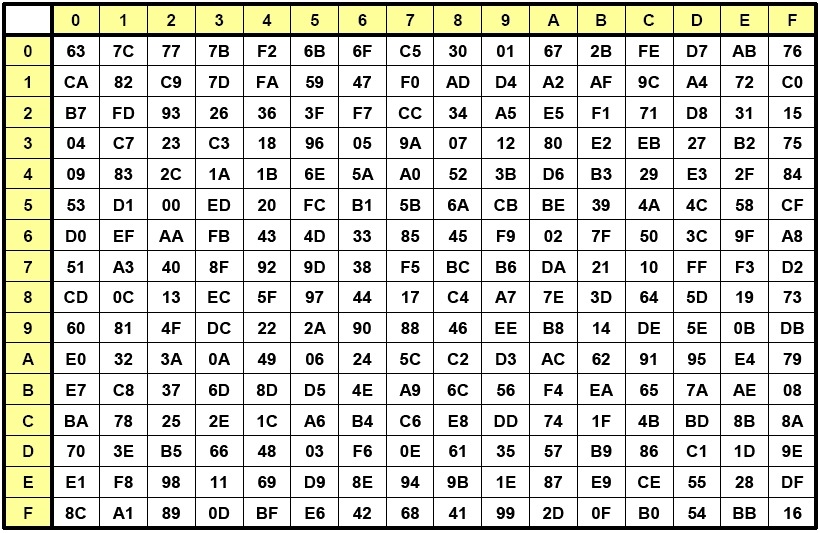
**{ 00, 20, 30, 40, 50, 60,70,80,90,A0,B0,C0,D0,E0,F0 }**

Kemudian masukan kedalam state

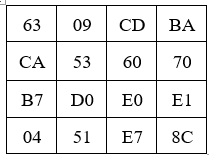
|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 10 | 50 | 90 | D0 |
| 20 | 60 | A0 | E0 |
| 30 | 70 | B0 | F0 |

Kemudian setelah didapatkan state baru yang dihasilkan pada *round* (0) kemudian selanjutnya masuk kepada proses round (1) dimana pada proses pertama ini dilakukan ***SubBytes*,** yaitu melakukan proses substitusi pada state diatas pada tabel S-Box , berikut proses dari subsitusi dari state pada round (1):

Cara Subsitusi nya sebagai berikut :

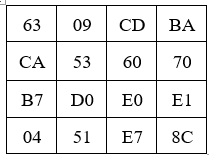


|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 10 | 50 | 90 | D0 |
| 20 | 60 | A0 | E0 |
| 30 | 70 | B0 | F0 |

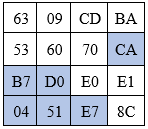


**S-Box**

Kemudian setelah mendapatkan state dari *SubByte*, langkah selanjutnya adalah dengan melakukan *ShifRows*, dengan menggeser beberapa blok byte yang ada pada state sebagai berikut :

State Awal

Lakukan Pergeseran pada baris ke dua sebanyak 1 byte, baris ke tiga sebanyak 2 byte, dan baris ke empat sebanyak 3 byte.

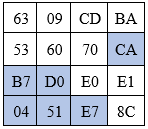
baris pertama tetap, baris kedua bergeser 1 byte :

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | 09 | CD | BA |
| CA | 53 | 60 | 70 |
| B7 | D0 | E0 | E1 |
| 04 | 51 | E7 | 8C |

1 byte

Baris ke tiga bergeser 2 byte :

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | 09 | CD | BA |
| 53 | 60 | 70 | CA |
| E0 | E1 | B7 | DO |
| 04 | 51 | E7 | 8C |



2 byte

Baris Ke empat Bergeser 3 byte : State Akhir

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | 09 | CD | BA |
| 53 | 60 | 70 | CA |
| E0 | E1 | B7 | DO |
| 04 | 51 | E7 | 8C |

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | 09 | CD | BA |
| 53 | 60 | 70 | CA |
| E0 | E1 | B7 | DO |
| 8C | 04 | 51 | E7 |

3 byte

Kemudian setelah didapat state akhir *shiftrows*, dilakukan proses *MixColumns* yaitu dengan melakukan perkalian dan penjumlahan menggunakan operator *irreducible polynomial*,berikut operasi perkalianya :

Lakukan perkalian blok pertama state dengan matriks a(x), untuk mempermudah perklaian maka kita lakukan satu persatu :

Pertama kita pecah menjadi 4 bagian dari state (array state) :

S0 = 63 53 E0

S1 = 09 60 E1 04

S2 = CD 70 B7 51

S3 = BA CA D0 E7

Kemudian masing masing bagian dari *array state* (Sx) kita kalikan dengan matrix a (x):

S’0,c =(63●[02])⊕(53●[03] ⊕ E0 ⊕8C)

S’1,c = 63 ⊕ (53 ● [02]) ⊕(E0 ● [03])⊕8C

S’2,c = 63 ⊕ 53 ⊕ (E0● [02]) ⊕(8C●[03])

S’3,c =(63 ● [02])⊕53 ⊕ E0 ⊕ (8C ● [02] )

Referesentasi Polinomial :

‘01’ = 00000001 = 1 (Elemen identitas)

‘02’ = 00000010 = 𝓍

’03’= 00000011= + 1

‘63’ = 01100011 = 𝓍6+ 𝓍5 + 𝓍 + 1

‘53’ = 01010011 = 6+ 𝓍4 + 𝓍 + 1

‘E0’ = 11100000 = 𝓍7+𝓍6+ 𝓍5

‘8C’= 10001100 = 𝓍7+𝓍3+ 𝓍2

Kemudian kita kalikan masing masing *array state* diatas dengan matriks a(x) :

1. S’0,c =(63●[02])⊕(53●[03] ⊕ E0 ⊕8C)

‘02’●’63’ = (𝓍).( 𝓍6+ 𝓍5 + 𝓍 + 1)

= 𝓍7+𝓍6+ 𝓍2 + 𝓍

=11000110

‘03’●’53’ = (𝓍+1).( 𝓍6+ 𝓍4 + 𝓍 + 1)

= ( 7+𝓍5+ 𝓍2 + 𝓍).( 𝓍6+ 𝓍4 + 𝓍 + 1)

= 𝓍7+𝓍6+ 𝓍5 + 𝓍4+𝓍2+ 1

= 11110101

‘01’ ● ‘E0’ = E0 = 11100000

‘01’ ● ‘8C’ = 8C = 10001100

1. S’1,c = 63 ⊕ (53 ● [02]) ⊕(E0 ● [03])⊕8C

‘01’ ● ‘63’ = 63 = 01100011

‘02’ ● ’53’ = (𝓍). ( 6+ 𝓍4 + 𝓍 + 1)

= 𝓍7+𝓍5+ 𝓍2 + 𝓍

= 10100110

‘03’ ● ‘E0’ = (𝓍+1).( 𝓍7+𝓍6+ 𝓍5)

= (𝓍8+𝓍7+ 𝓍6)+( 𝓍7+𝓍6+ 𝓍5)

= (𝓍8+𝓍5) mod (𝓍8+𝓍4+ 𝓍3 + 𝓍 + 1)

= 𝓍5+𝓍4+ 𝓍3 + 𝓍 + 1

= 00111011

‘01’ ● ‘8C’ = 8C = 10001100

1. S’2,c = 63 ⊕ 53 ⊕ (E0● [02]) ⊕(8C●[03])

‘01’ ● ‘63’ = 63 = 01100011

‘01’ ● ‘53’ = 53 = 01010011

‘02’ ● ‘E0’ = (𝓍).( 𝓍7+𝓍6+ 𝓍5)

= (𝓍8+𝓍7+ 𝓍6)

= (𝓍8+𝓍5) mod (𝓍8+𝓍4+ 𝓍3 + 𝓍 + 1)

= 𝓍7+𝓍6+ 𝓍4 + 𝓍3  + 𝓍 + 1

= 11011011

‘03’ ● ‘8C’ = (𝓍+1).( 𝓍7+𝓍3+ 𝓍2)

= (𝓍8+𝓍4+ 𝓍3)+( 𝓍7+𝓍3+ 𝓍2)

= 𝓍8+𝓍7+ 𝓍4 + 𝓍2

=(𝓍8+𝓍7+𝓍4+𝓍2) mod (𝓍8+𝓍4+ 𝓍3 + 𝓍 + 1)

= 𝓍7+𝓍3+ 𝓍2 + 𝓍+ 1

=10001111

1. S’3,c =(63 ● [02])⊕53 ⊕ E0 ⊕ (8C ● [02])

‘03’●’63’ = (𝓍+1). ( 6+ 𝓍4 + 𝓍 + 1)

= ( 7+𝓍6+ 𝓍2 + 𝓍).( 𝓍6+ 𝓍5 + 𝓍 + 1)

= 𝓍7+ 𝓍5 +𝓍2+ 1

= 10100101

‘01’ ● ‘53’ = 53 = 01010011

‘01’ ● ‘E0’ = E0 = 11100000

= 11011011

‘02’ ● ‘8C’ = (𝓍).( 𝓍7+𝓍3+ 𝓍2)

= (𝓍8+𝓍4+ 𝓍3)mod( 𝓍8+𝓍4+ 𝓍3+ 𝓍+1 )

= 𝓍+1 = 00000011

Setelah melakukan perkalian dari Sx dengan matriks polynomial tersebut semua hasilnya dijumlahkan dengan menggunakan operasi XOR (⊕)

Berikut operasi penjumlahanya (⊕)

Penjumlahan S0

11000110 01100011 01100011 10100101

11110101 10100110 01010011 01010011

11100000 00111011 11011011 11100000

10001100 10001100 10001111 00000011

01011111 = **5F** 01110010 = **72** 01100100 = **64** 00010101 = **15**

Lakukan hal yang sama seperti operasi diatas untuk S1,S2,S3 sehinggga akan didapat hasil state baru sebagai berikut :

|  |  |  |  |
| --- | --- | --- | --- |
| 5F | 57 | F7 | 1D |
| 72 | F5 | BE | B9 |
| 64 | BC | 3B | F9 |
| 15 | 92 | 29 | 1A |

State diatas adalah hasil dari operasi *SubByte, ShiftRows, MixColumns* dan *AddRoundKey* yang dilakukan satu kali, untuk mendapatkan state akhir maka perulangan tersebut dilakukan sebanyak 10 kali sesuai dengan panjang byte kunci yaitu 128 dengan catatan perulangan ke 10 tidak ditambahkan prosses *MixColumns* dan hasil akhirnya adalah berupa :

ChiperText = 69 C4 E0 D8 6A 7B 04 30 D8 CD B7 80 70 B4 C5 5A

1. **Deskripsi AES**

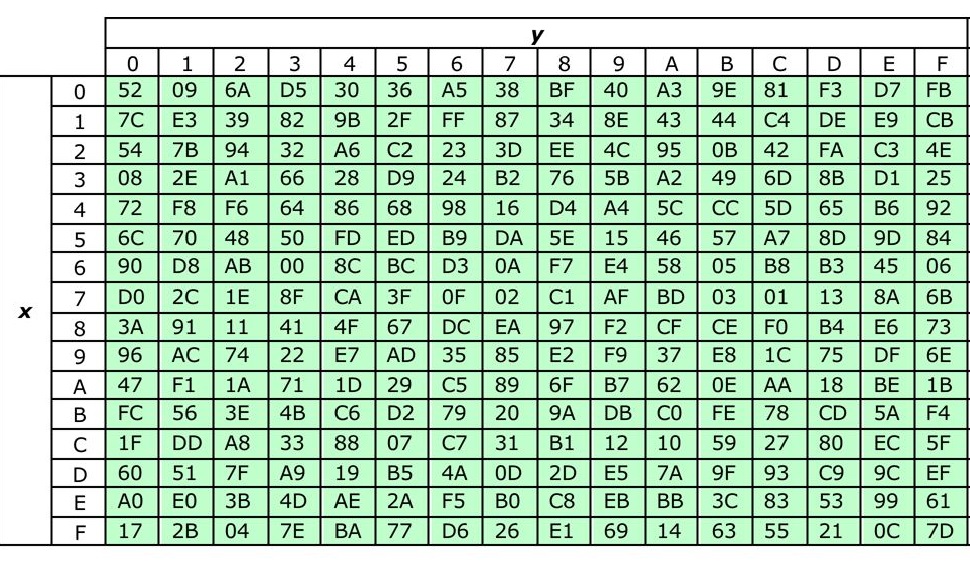
Deskripsi algoritma AES 128 mempunyai 4 proses, dimana semua proses itu adalah invers dari proses enkripsi AES 128, keempat proses itu adalah *InvSubByte, InvShiftRows, InvMixColumns* dan *AddRoundKey* :

Contoh kasus, kita ambil plaintext dari round 10=

Plaintext(hexadesimal) = 63 53 E0 8C 09 60 E1 04 CD 70 B7 51 BA CA D0 37

Kunci (hexadesimal) = 00 01 02 03 04 05 06 07 08 09 00 0A 0B 0C 0D 0E 0F

Operasi pertama yang dilakukan adalah proses *InvSubBytes* menggunakan tabel *InvSubytes* :



|  |  |  |  |
| --- | --- | --- | --- |
| 63 | 09 | CD | BA |
| 53 | 60 | 70 | CA |
| E0 | E1 | B7 | D0 |
| 8C | 04 | 51 | E7 |

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 50 | 90 | D0 | 10 |
| A0 | E0 | 20 | 60 |
| F0 | 30 | 70 | B0 |

S’-BOX

Kemudian langkah selanjutnya adalah dengan melakukan InvShiftRows dengan melakukan pergeseran seperti berikut :

State awal Setelah *InvShiftRows*

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 50 | 90 | D0 | 10 |
| A0 | E0 | 20 | 60 |
| F0 | 30 | 70 | B0 |

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 10 | 50 | 90 | D0 |
| 20 | 60 | A0 | E0 |
| 30 | 70 | B0 | F0 |

1 bit

2 bit

3 bit

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 10 | 50 | 90 | D0 |
| 20 | 60 | A0 | E0 |
| 30 | 70 | B0 | F0 |

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 40 | 80 | C0 |
| 10 | 50 | 90 | D0 |
| 20 | 60 | A0 | E0 |
| 30 | 70 | B0 | F0 |

Tahap selanjutnya adalah proses *AddRoundKey,* dari state hasil *InvShiftRows* dengan state kunci :

00000000 = ‘00’ 00010000 = ‘10’ 00100000 = ‘20’ 00110000 = ‘30’

00000000 = ‘00’ 00000001 = ‘01’ 00000010 = ‘02’ 00000011 = ‘03’

00000000 = **‘00’** 00010001 = **‘11’** 00100010 = **‘22’** 00110011 = **‘33’**

01000000 = ‘40’ 01010000 = ‘55’ 01100000 =‘66’ 01110000 = ‘77’

00000100 = ‘04’ 00000101 = ‘05’ 00000110 =’06’ 00000111 = ’07’

01000100 = **‘44’** 01010101 = **‘55’** 01100110 = **‘66’** 01110111 = **‘77’**

10000000 = ‘80’ 10010000 = ‘90’ 10100000 = ‘A0’ 10110000 = ‘B0’

00001000 = ‘08’ 00001001 = ‘09’ 00001010 = ‘0A’ 00001011 = ‘0B’

10001000 = **‘88’** 10011001= **‘99’** 10101010 = **‘AA’** 10111011 = **‘BB’**

11000000 = ‘C0’ 11010000 = ‘DD’ 11101000 = ‘E0’ 11110000 = ‘F0’

00001100 = ‘0C’ 00001101 = ‘0D’ 00000111 = ‘0E’ 00001111 = ‘0F’

11001100 = **‘CC’** 11011101 = **‘DD’** 11101110 = **‘EE’** 11111111 = **‘FF’**

Dari hasil proses operasi XOR didapatkan kembali plaintext awal yang artinya proses deskripsi berhasil berikut hasilnya : **{‘00’,’11’, ‘22’, ‘33’, ‘44’, ‘55’, ‘66’, ‘77’, ‘88’, ‘99’, ‘AA’, ‘BB’, ‘CC’, ‘EE’, ‘FF’}**

* 1. **Peracangan Sistem** 
     1. **Flowchart Algoritma Kriptografi**

1. **Flowchart Algoritma Enskripsi AES 128**

Proses enskripsi adalah proses pengacakan data dari data yang berbentuk plaintext kemudian dikombinasikan dengan kunci (*key*) yang nantinya akan menjadi data acak atau yang dalam istilah kriptografi di kenal dengan nama chipertext yang bertujuan untuk mengamankan data dari pihak yang tak berwenag.

Dalam aalgoritma kriptografi AES 128 terdapat beberapa langkah dalam proses enkripsi dan deskripsinya, hal pertama yang dilakukan dalam adalah dengan menentukan data awal berbentuk plaintext dan kunci yang akan di enkripsi selanjutnya adalah memproses plaintext dan kunci tersebut kedalam round (0) dan dengan melakukan proses *AddroundKey* selanjutnya adalah proses roud selanjutnya adalah proses *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey,* dan dilakukan proses perulagan sebanyak 9 kali, kemudian pada round (10) atau *final round* akan tetapi pada round akhir tidak dilakukan proses *MixColumns* dengan hasil akhir adalah data terenskripsi berupa Chipertext. Berikut flowchart algoritma AES :



Keterangan Variabel:

S’ = matrix polynomial

x = element matrix

w = *subword*

i = root subword

Gambar 3.3 Flowchart Enskripsi Algoritma AES 128

1. **Flowchart Algoritma Deskripsi AES 128**

Dalam ilmu kriptografi terdapat istilah deskripsi yaitu proses pengembalian data yang berupa chipertext ke data awal atau plaintext dengan maksud agar data tersebut dapat dibaca oleh user yang biasanya di kombinasikan dengan key, dalam proses deskripsi Algoritma AES 128 langkah – langkah nya hampir sama dengan proses enkripsi, yang membedakan adalah semua proses dilakukan kebalikanya (*invers*), proses tersebut adalah *InvSubByte, InvShiftRows, InvMixColumns* dan *AddRoundKey*

Berikut flowchart algoritma Deskripsi AES :

 Keterangan Variabel:

S’ = matrix polynomial

x = element matrix

w = subword

i = root subword

Gambar 3.4 Flowchart Deskripsi Algoritma AES 128

* + 1. **Use Case Diagram Aplikasi E- Halal**

Use case system adalah Deskripsi fungsi dari sebuah system dari perspektif pengguna yang bekerja dengan cara mendeskripsikan tipikal interaksi antara user (pengguna) sebuah system dengan systemnya sendiri melalui sebuah cerita bagaiman sistem itu di pakai.Dalam kasus ini terdapat 2 buah aktor yaitu konsumen dan admin, 3 use case utama, dan 2 extnd use case berikut use case diagramnya :



Gambar 3.5 Use Case Diagram Aplikasi E- Halal

* + 1. **Usecase Scenario**

1. Level Login

|  |  |
| --- | --- |
| **Identifikasi** | |
| **Ide Use Case** | E-Halal-01 |
| **Nama Use case** | Login |
| **Tujuan** | Pada level ini aktor mengakses sistem dengan memasukan username dan password |
| **Deskripsi** | |
| **Prioritas** | Primary |
| **Aktor** | Admin |
| **Skenario Utama** | |
| ***Precondition*** | Aktor berada pada form login |
| **Aksi aktor** | **Reaksi Sistem** |
| 1. Aktor Memasukan Username dan password | 1. Sistem melakukan validasi terhadap data username dan password ke database. 2. Sistem menampilkan pop up “Berhasil Login” yang menandakan bahwa data yang dimasukan adalah benar. 3. Sistem menampilkan halaman kelola data Sertifikasi E- Halal |
| **Post Condition** | Jika pada akhir interaksi semua data yang dimasukan user valid maka sistem secara default akan menampilkanform-form di layar yang dapat diakses oleh user dan Jika data username dan password yang dimasukan salah maka sistem akan memberitahukan dengan munculya pop up “username atau password anda salah” |

1. Level Mengelola Data user

|  |  |
| --- | --- |
| **Identifikasi** | |
| **Ide Use Case** | E-halal-02 |
| **Nama Use case** | Kelola Data User |
| **Tujuan** | Pada level ini aktor dapat melakukan pegelolaan data user |
| **Deskripsi** | |
| **Prioritas** | Primary |
| **Aktor** | admin |
| **Skenario Utama** | |
| ***Precondition*** | User telah mempunyai username dan password yang teregitrasi dan telah melakukan login pada sistem |
| **Aksi aktor** | **Reaksi Sistem** |
| 1. Memilih tombol tambah/edit user | 1. Sistem akan memunculkan form isian nama, *username*, email dan *password* |
| 1. Memasukan / mengupdate data pada form yang telah disediakan | 1. sistem akan melakukan validasi terhadap data yang dimasukan |
| 1. Admin melakukan konfirmasi pada data – data yang telah dimasukan dengan menekan tombol “OK” | 1. Sistem menyimpan data – data yang dimasukan kedalam database 2. Sistem menampilkan pop up “Data admin berhasil di simpan/update” |
| **Post Condition** | Jika pada akhir interaksi semua data yang di masukan aktor valid dan melakukan konfirmasi terhadap data yang akan dimasukkan, maka sistem akan menyimpan data kedalam *database,* atau data akan terhapus jika user menekan tombol hapus dan sistem akan menampilkan dialog konfirmasi sebelum proses eksekusi fungsi hapus.  Jika data yang dimasukan aktor tidak valid atau data yang diminta tidak dimasukan maka sistem akan menampilkan peringatan berupa pop up / alert dialog seperti “form harus diisi atau data tidak valid” |

1. Level mengelola Data Halal

|  |  |
| --- | --- |
| **Identifikasi** | |
| **Ide Use Case** | E-halal-03 |
| **Nama Use case** | Kelola Data Halal |
| **Tujuan** | Pada level ini aktor admin akan melakukan pengelolaan data dengan menambah, menghapus atau mengupdate data sertifikasi halal. |
| **Deskripsi** | |
| **Prioritas** | Primary |
| **Aktor** | Admin |
| **Skenario Utama** | |
| ***Precondition*** | Aktor telah mempunyai username dan password yang teregitrasi dan telah melakukan login pada sistem  Dan aktor telah berada pada form menu data sertifikasi |
| **Aksi aktor** | **Reaksi Sistem** |
| 1. Menekan tombol tambah/edit data | 1. Sistem akan menampilkan form inputan data no Sertifikasi halal, nama produk, nama, dan tanggal kaldaluarsa. |
| 1. Memasukan / mengupdate data pada form yang telah mdisediakan | 1. Sistem akan melakukan validasi terhadap data yang dimasukan dan menampilkan pesan konfirmasi data. |
| 1. Melakukan konfirmasi terhadap data yang dimasukan dengan menekan tombol simpan pada pop up konfirmasi | 1. Sistem akan menyimpan data – data kedalam database. 2. Sistem menampilkan pesan “data berhasil disimpan/di update/dihapus” |
| **Post Condition** | Jika pada akhir interaksi semua data yang di masukan aktor valid dan melakukan konfirmasi terhadap data yang akan dimasukkan, maka sistem akan menyimpan data kedalam *database.*  Jika data yang dimasukan aktor tidak valid atau data yang diminta tidak dimasukan maka sistem akan menampilkan peringatan berupa pop up / alert dialog seperti “form harus diisi ” |

1. Level Operasi Algoritma

|  |  |
| --- | --- |
| **Identifikasi** | |
| **Ide Use Case** | E-hala-04 |
| **Nama Use case** | Operasi Algoritma |
| **Tujuan** | Pada level ini aktor admin melakukan penambahan algoritma AES 128 pada no sertifikasi(primary key) data sertifikasi |
| **Deskripsi** | |
| **Prioritas** | Primary |
| **Aktor** | Admin |
| **Skenario Utama** | |
| ***Precondition*** | * Admin telah melakukan login * Admin telah berada di form input data |
| **Aksi aktor** | **Reaksi Sistem** |
| 1. Aktor Menginput data ke dalam data ke database melalui form input data dan telah menekan tombol simpan | 1. Sistem akan melakukan oprasi *Subyte* pada primary key (no\_sertifikasi). 2. Sistem akan melakukan oprasi *ShitRows* pada data hasil oprasi *subytes.* 3. Sistem akan melakukan operasi *MixColumns* pada data hasil operasi *ShiftRows*. 4. Sistem akan melakukan operasi *AddRoundKey* pada data hasil Operasi *MixColumns*, dalm proses ini data sudah terenkripsi berbentuk chipper text. 5. Sistem akan melakukan penyimpaan data ke database 6. Sistem akan menampilkan pesan “data berhasil disimpan” |
| **Post Condition** | Jika pada akhir interaksi semua data yang di masukan aktor valid dan melakukan konfirmasi terhadap data yang akan dimasukkan, maka sistem akan menyimpan data kedalam *database.*  Jika data yang dimasukan aktor tidak valid atau data yang diminta tidak dimasukan maka sistem akan menampilkan peringatan berupa pop up / alert dialog seperti “form harus diisi / data gagal disimpan” |
|  |  |

1. Level Mengecek Data Halal

|  |  |
| --- | --- |
| **Identifikasi** | |
| **Ide Use Case** | E-halal-05 |
| **Nama Use case** | Cek Data Halal |
| **Tujuan** | Pada level ini aktor admin dan user dapat melaukan pencarian data dengan menginput No Sertifikasi Halal / scan Qr Code |
| **Deskripsi** | |
| **Prioritas** | Primary |
| **Aktor** | Admin dan Konsumen |
| **Skenario Utama** | |
| ***Precondition*** | Aktor telah berada pada dashboard menu utama aplikasi |
| **Aksi aktor** | **Reaksi Sistem** |
| 1. Memasukan no sertifikat /scan pada Qr code | 1. Sistem melakukan pencarian data berdasarkan id 2. Sistem menampilkan data detail sesuai dengan id |
| **Post Condition** | Pada akhir interaksi data akan ditampilkan sesuai no sertifikasi, Jika data yang dimasukan aktor tidak valid atau data yang diminta tidak dimasukan maka sistem akan menampilkan peringatan berupa pop up / alert dialog seperti “ data tidak ditemukan / belum diregistrasi” |

1. Level Logout

|  |  |
| --- | --- |
| **Identifikasi** | |
| **Ide Use Case** | E-halal-06 |
| **Nama Use case** | Logout |
| **Tujuan** | Pada level ini aktor akan keluar dari sistem |
| **Deskripsi** | |
| **Prioritas** | Primary |
| **Aktor** | admin |
| **Skenario Utama** | |
| ***Precondition*** | Aktor berada didalam sistem |
| **Aksi aktor** | **Reaksi Sistem** |
| 1. Memilih tombol Logout | 1. Sistem akan keluar dan kembali kehalaman Login *username* dan *password.* |
| **Post Condition** | Jika pada akhir interaksi sistem keluar maka sistem akan mengarahkan ke halaman login dan proses logout berhasil. |

* + 1. **Activity Diagram**

Activity Diagram menggambarkan interasksi antara aktor dengan sistem yang berjalan, yang biasanya berupa *method*  yang ada pada sebuah usecase, berikut activity diagramnya

1. Activity Diagram Login



Gambar 3.6 Activity Diagram Login

1. Kelola data user



Gambar 3.7 Activity Diagram Kelola data User

1. Activity Diagram kelola Data Halal



Gambar 3.8 Diagram Activity kelola data Halal

1. Activity diagram Operasi Algoritma

Gambar 3.9 Activity Diagram Login

1. Activity Diagram Cek Data Halal



Gambar 3.10 Activity Diagram Cek Data halal

* + 1. **Class Diagram Aplikasi E-Halal**

****

Gambar 3.11 Class Diagram Aplikasi – E-halal

* + 1. **Sequence Diagram Aplikasi E-Halal**

1. Sequence Diagaram Login admin



Gambar 3.12 Sequence Diagam Login

1. Sequence diagram kelola data user



Gambar 3.13 Squence diagram kelola data user

1. Sequence diagram kelola data Sertikasi



Gambar 3.14 Sequence diagram Kelola data sertifikasi

1. Sequence diagram Oprasi algoritma

Gambar 3.15 Sequence diagram Oprasi Algoritma

1. Sequence diagram Cek data halal

Gambar 3.16 Sequence diagram Cek data halal

1. Sequence Diagram Logout



Gambar 3.16 diagram Logout

* + 1. Perancangan Database

Perancangan database pada apikasi E – Halal berfungsi sebagai tempat penyimpanan dan pengelolaan data sertifikasi halal ataupun user admin, yang nntinya akan dipakai baik dari sisi server web ataupun dari sisi client android. Dalam pembuatan aplikasi E-halal ini penulis membuat 2 buah tabel utama yaitu tabel admin dan tabel data sertifikasi, berikut perancangan tabelnya:

1. **Tabel User**

Tabel user disini terdapat beberapa field diantaranya, field id\_user, nama\_user, field password, field email.

Tabel 3.1 Tabel Admin

|  |  |  |
| --- | --- | --- |
| Nama Field | Type | Length |
| id\_admin | Varchar | 10 |
| nama\_user | Varchar | 30 |
| Password | Varchar | 50 |
| Email | Varchar | 50 |

1. Tabel Data Sertifikasi

Tabel data sertifikasi adalah tabel yang menapung data - data setifikasi terdapat beberapa field diantaranya field no\_sertifikat, field nama\_produk, field nama\_perusahaan, field tgl\_buat,field exp\_date.

Tabel 3.2 Tabel Data Sertifikasi

|  |  |  |
| --- | --- | --- |
| Nama Field | Type | Length |
| no\_sertifikat | varchar | 15 |
| nama\_produk | Varchar | 30 |
| nama\_perusahaan | Varchar | 50 |
| tgl\_buat | Date | 11 |
| exp\_date | date | 11 |

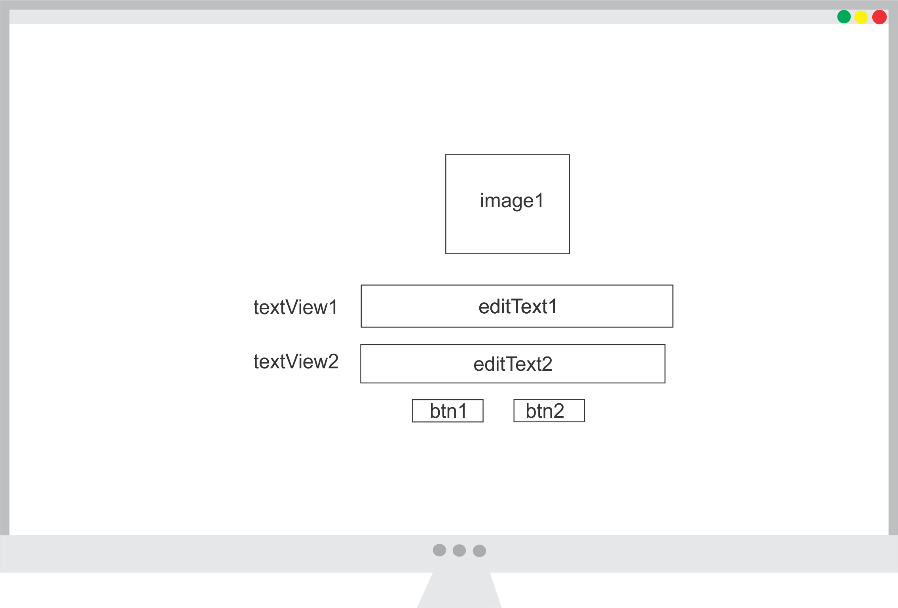
* 1. **Perancangan *Interface* / Antarmuka**

Perancangan *interface* merupakan slah satu langkah awal dalam membuat sebuah program aplikasi (*blueprint*), dimana perancangan *interface* dibuat senyaman mungkin ketika pengguna menggunakanya atau dengan kata lain harus *user friendly* bagi pemakai, pada penelitian ini penulis akan merancang *interface* dari sisi aplikasi (*client*) dan dari sisi web (*Server*) dan dalam sebuah program yang melibatkan CRUD data harus di rancang terlebih dahulu *interface* input dan outputnya.

* + 1. **Perancangan Input**

Perancangan input merupakan rancangan antar muka yang nantinya akan di gunakan untuk menerima masukan dari luar , berikut rancangan antar muka input dari aplikasi E – Halal dari sisi web server dan client.

1. Halaman Login



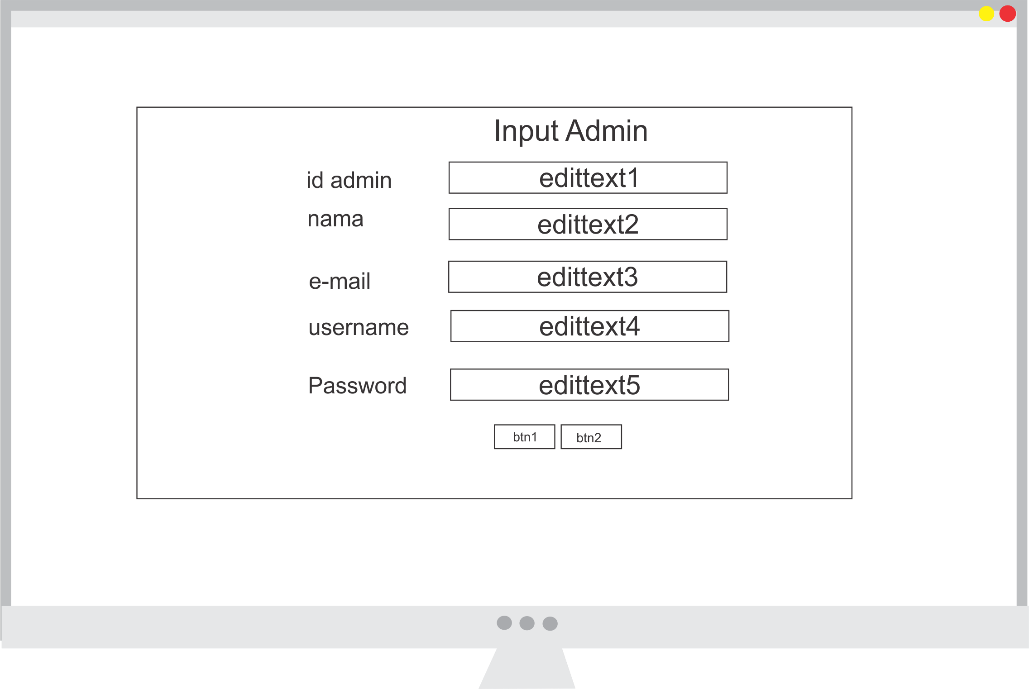
Gambar 3.18 Halaman Login

Keterangan komponen halaman login

Tabel 3. 3 Keterangan Kompoen Halaman Login

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | Image1 | Logo aplikasi E - Halal |
|  | Textview1 | Label username |
|  | Textview2 | Label password |
|  | editText1 | Kotak isian username |
|  | editText2 | Kotak isian password yang outputnya berupa simbol “\*\*\*\*” |
|  | Btn1 | Tombol login, yang berfungsi untuk masuk kedalam sistem. |
|  | Btn2 | Tombol reset, digunakan untuk menghapus inputan username dan password |

1. Halaman Kelola data admin

****

**Gambar 3.19** Halaman Input Admin

Keterangan Komponen Halaman input admin :

Tabel 3.4 Tabel Keterangan Komponen Halaman Input Admin

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | EditText1 | Digunakan utuk menginput id admin |
|  | EditText2 | Digunakan utuk menginput nama admin |
|  | EditText3 | Digunakan utuk menginput email admin |
|  | EditText4 | Digunakan utuk menginput username admin |
|  | EditText5 | Digunakan utuk menginput password admin |
|  | Btn1 | Tombol simpan digunakan untuk menyimpan data |
|  | Btn2 | Tombol reset digunakan untuk mereset kotak isian diatas. |

1. Halaman Input data sertifikasi



Gambar 3.20 Gambar halaman input data sertifikasi

Keterangan Komponen Halaman input data sertifikasi:

Tabel 3.5 Tabel Keterangan Komponen Halaman Input sertifikasi

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | EditText1 | Digunakan utuk menginput No Sertifikasi |
|  | EditText2 | Digunakan utuk menginput nama Produk |
|  | EditText3 | Digunakan utuk menginput nama perusahaan |
|  | EditText4 | Digunakan utuk menginput masa berlaku sertifikat |
|  | Btn1 | Tombol simpan digunakan untuk menyimpan data |
|  | Btn2 | Tombol reset digunakan untuk mereset kotak isian diatas. |

1. Update data admin



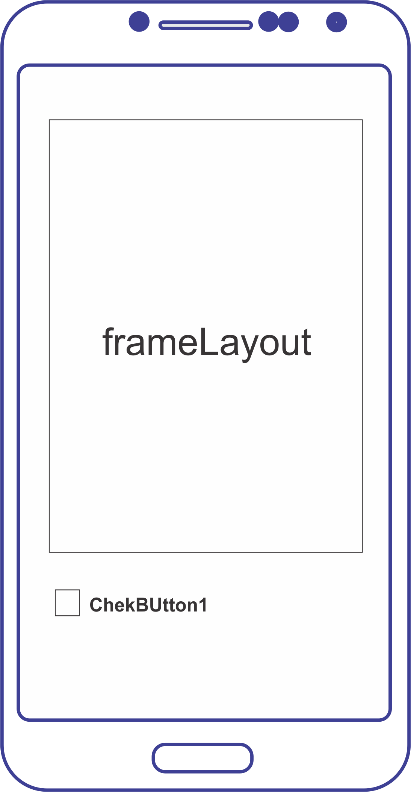
Gambar 3.21 Gambar halaman update data Admin

Keterangan Komponen Halaman Update data Admin:

Tabel 3.6 Tabel Keterangan Komponen Halaman Update data admin

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | EditText1 | Digunakan utuk menginput nama admin |
|  | EditText2 | Digunakan utuk menginput email admin |
|  | EditText3 | Digunakan utuk menginput username admin |
|  | EditText4 | Digunakan utuk menginput password admin |
|  | Btn1 | Tombol Update digunakan untuk mengupdate data |
|  | Btn2 | Tombol reset digunakan untuk mereset kotak isian diatas. |

1. Tampilan Input Scan Qr Code



Gambar 3.22 Tampilan input Scan Qr Code

Keterangan Komponen Tampilan Scan Qr Code:

Tabel 3.7 Tabel Keterangan Komponen Tampilan Scan Qr Code

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | Frame Layout | Adalah tampilan dari kamera android *smartphone* |
|  | Check Button | Digunakan untuk ceklis lampu Flash |

1. Tampilan input Pencarian No sertifikasi

Gambar 3.23 Tampilan input data Pencarian

Berikut keterangan komponen input pencarian datas sertifikasi berdasarkan no sertifkat:

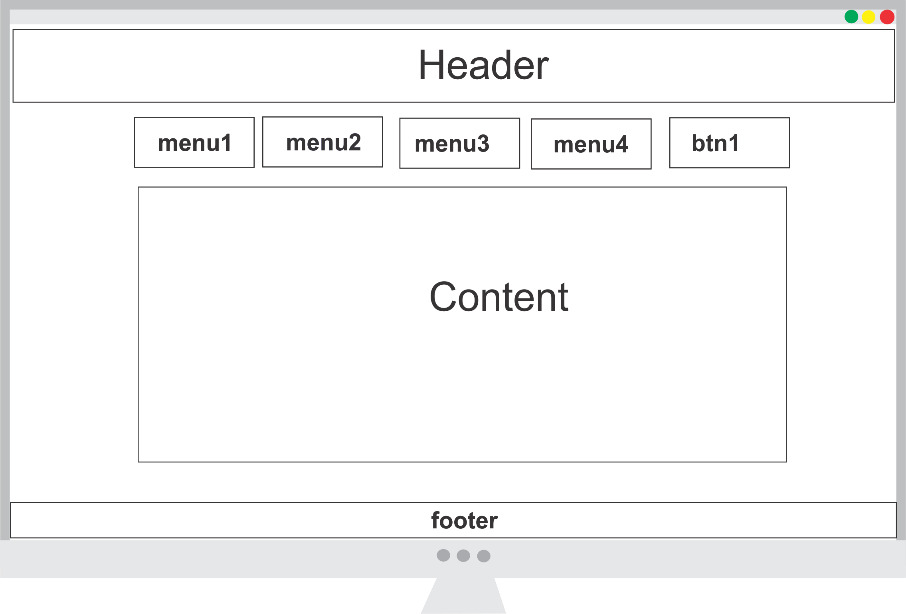
Tabel 3.8 Tabel Keterangan Komponen Tampilan pencarian data sertifikasi

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | EditText | Digunakan untuk menginput no sertifikat |
|  | Btn1 | Tombol cari yang berfungsi untuk mencari data |
|  | ListView | Digunakan untuk menampilkan data dalam bentuk list. |
|  | TextView 1 - 5 | Adalah data – data dalam bentuk list dari database |

* + 1. **Perancangan Output**

Perancangan output merupakan rancangan antarmuka keluaran data yang telah diperoses oleh aplikasi yang di dapat dari inputan ataupun dari database, berikut perancangan output tampilan aplikasi e-halal dari sisi aplikasi ataupun web server nya

1. Tampilan Menu Utama



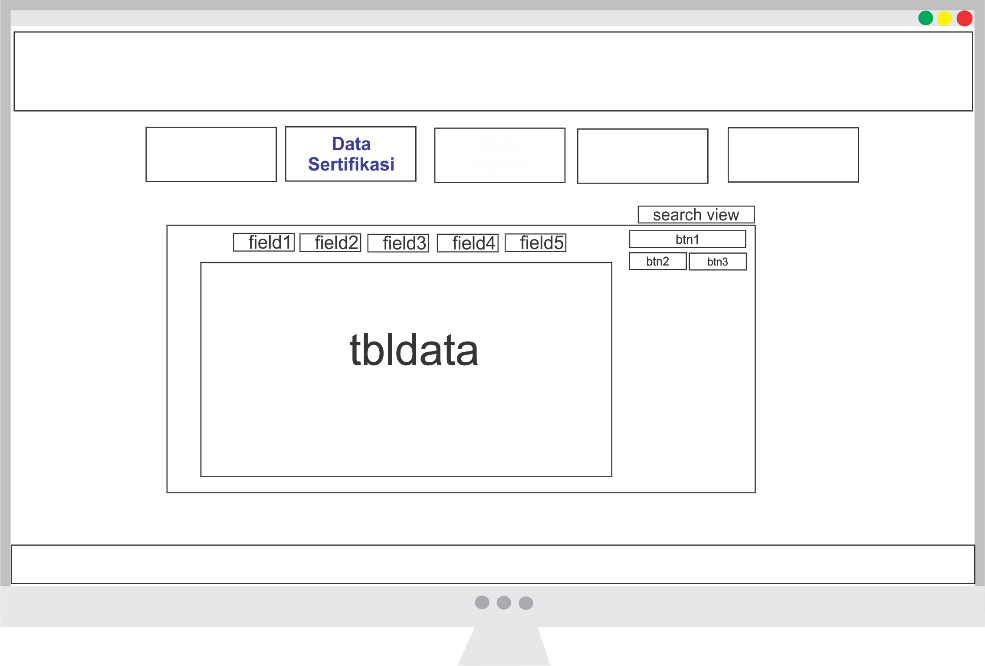
Gambar 3.24 Halaman Menu Utama

Berikut keterangan komponen halaman utama

Tabel 3.9 Tabel Keterangan Komponen Halaman Utama

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | Header | Digunakan untuk judul dari website dan logo |
|  | Footer | Berisi nama pegembang, tahun pembuatan, dan copyright |
|  | Menu1 | Menu Home, dashboard utama |
|  | Menu2 | Menu Data sertifikasi |
|  | Menu3 | Menu Data Admin |
|  | Menu4 | Menu info Pengembang |
|  | Btn1 | Tombol Logout untuk keluar |
|  | Content | Berisi informasi seputar badan pengelola jaminan produk halal dan informasi lainya. |

1. Menu Data Sertifikasi



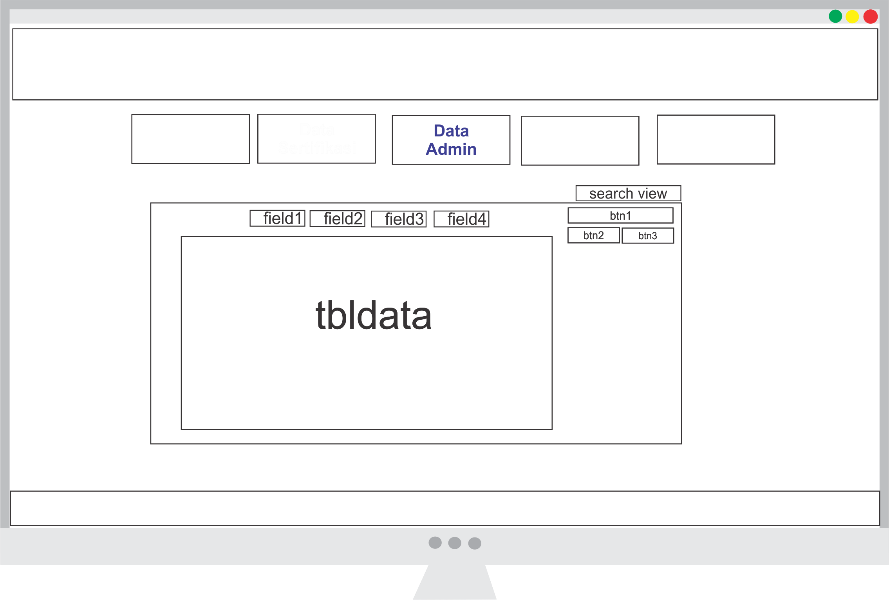
Gambar 3.25. Tampilan Halaman Data sertifikasi

Berikut keterangan komponen halaman Data sertifikasi

Tabel 3.10 Tabel Keterangan Komponen Halaman Data sertifikasi

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | Field1 | Digunakan untuk field no Sertifikat |
|  | Field2 | Digunakan untuk field nama Produk |
|  | Field3 | Digunakan untuk field nama perusahaan |
|  | Field4 | Digunakan untuk field tanggal kadaluarsa |
|  | Field5 | Digunakan untuk field gamba kode Qr |
|  | tblData | Berisi data – data sertifikasi yang diambil dari database |
|  | Btn1 | Dgunakan untuk tombol penambahan data |
|  | Btn2 | Dgunakan untuk tombol pengeditan data |
|  | Btn3 | Dgunakan untuk tombol penghapusan data |
|  | SearchView | Digunakan untuk melakukan pencarian data |

1. Menu Data Admin



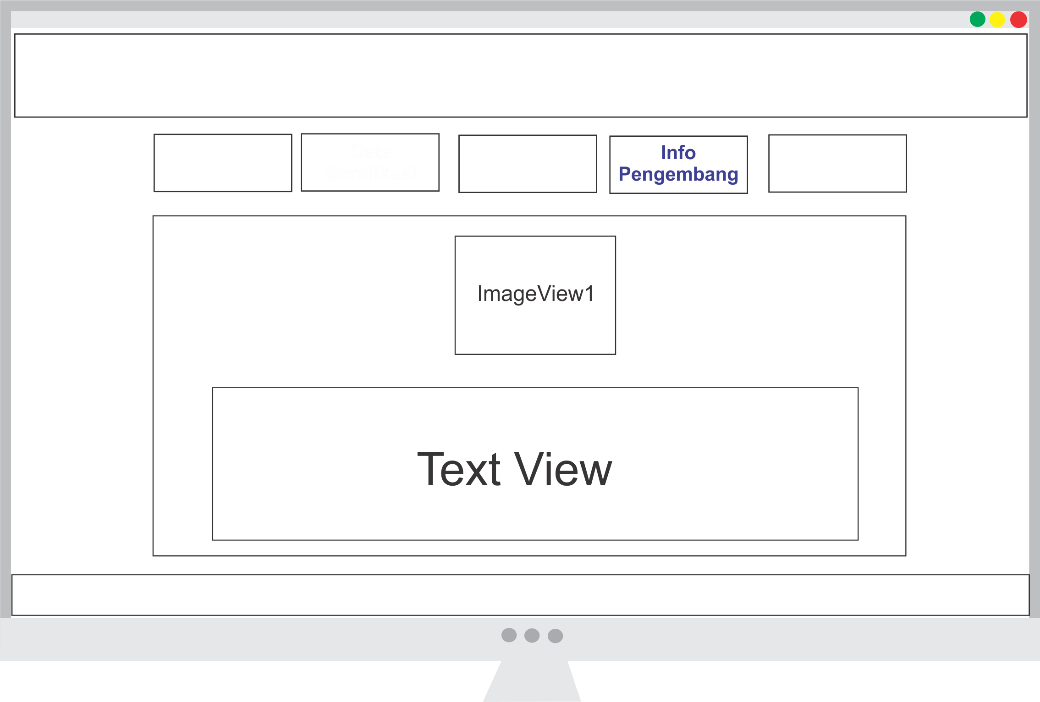
Gambar 3.26. Tampilan Halaman Data Admin

Berikut keterangan komponen halaman Data Admin

Tabel 3.11 Tabel Keterangan Komponen Halaman Data Admin

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | Field1 | Digunakan untuk field nama admin |
|  | Field2 | Digunakan untuk field Email admin |
|  | Field3 | Digunakan untuk field Username admin |
|  | Field4 | Digunakan untuk field password admin |
|  | tblData | Berisi data – data admin yang diambil dari database |
|  | Btn1 | Dgunakan untuk tombol penambahan data |
|  | Btn2 | Dgunakan untuk tombol pengeditan data |
|  | Btn3 | Dgunakan untuk tombol penghapusan data |
|  | SearchView | Digunakan untuk melakukan pencarian data |

1. Menu Info Pengembang



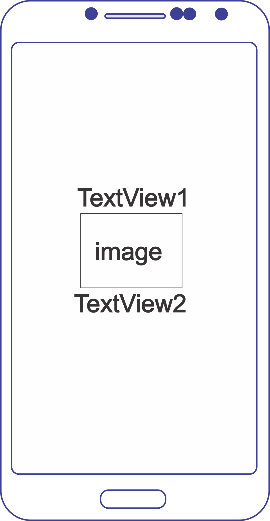
Gambar 3.27 Info Pengembang web

Berikut keterangan komponen halaman Info Pengembang

Tabel 3.12 Tabel Keterangan Komponen Info Pengembang

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Keterangan |
|  | ImageView1 | Digunakan untuk gambar pengembang |
|  | TextView | Digunakan untuk Biodata pengembang |

1. Splash Screen

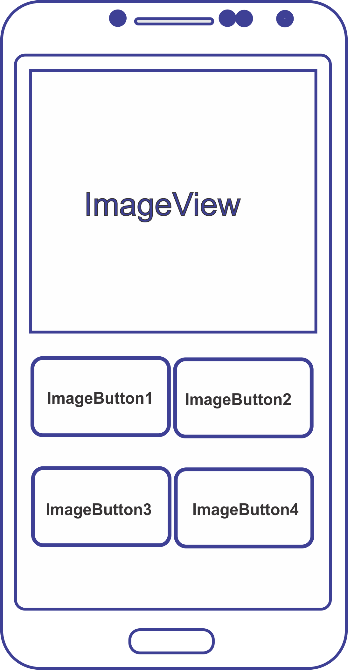


Gambar 3.28 Rancangan tampilan Splash Screen

Tabel 3.13 Tabel keterangan splash screen

|  |  |  |
| --- | --- | --- |
| No | Nama Item | Ketarangan |
|  | TextView1 | Nama Aplikasi |
|  | Image | Logo Aplikasi |
|  | TextView2 | Versi Aplikasi |

1. Menu Utama

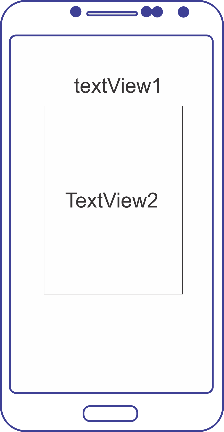


Gambar 3.29 Menu Utama Aplikasi

Berikut keterangan komponen menu utama

Tabel 3.14 Tabel keterangan Menu Utama

|  |  |  |  |
| --- | --- | --- | --- |
| No | | Nama Item | Keterangan |
|  | ImageView | | Gambar Slider View yang menampilkan cara pemakaian Aplikasi |
|  | ImageButton1 | | menu Scan Qr Code |
|  | ImageButton2 | | menu cari data berdasarkan id sertifikat |
|  | ImageButton3 | | Menu informasi seputar BPJPH / produk halal |
|  | ImageButton4 | | Menu tentang pegembang |

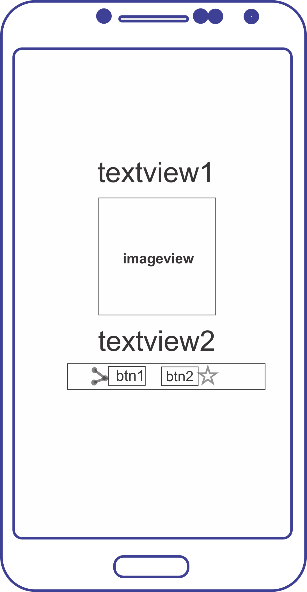
1. Hasil scan Qr Code

Gambar 3.30 Hasil Scan Qr Code

Berikut keterangan komponen menu utama

Tabel 3.15 Tabel keterangan Menu Utama

|  |  |  |  |
| --- | --- | --- | --- |
| No | | Nama Item | Keterangan |
|  | TextView1 | | Label “Hasil Scan Qr Code” |
|  | TextView2 | | Data hasil scan berupa keterangan nomor sertifikasi nama produk, nama perusahaan, masa berlaku |

1. Menu Info Pengembang

Gambar 3.31 Menu Info Pengembang

Berikut keterangan komponen menu info pengembang

Tabel 3.16 Tabel keterangan info Pengembang

|  |  |  |  |
| --- | --- | --- | --- |
| No | | Nama Item | Keterangan |
|  | TextView1 | | Digunakan untuk nama aplikasi “E - halal” |
|  | TextView2 | | Digunakan untuk informasi pengembang |
|  | ImageVIew | | Logo Aplikasi |
|  | Btn1 | | Tombol untuk berbagi aplikasi |
|  | Btn2 | | Tombol untuk memberi rate ke google playstore |