BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Berdasarkan analisis masalah, maka perangkat sistem keamanan data soal ujian bimbingan yang dikembangkan diharapkan dapat digunakan sebagai alternatif penyajian informasi keamanan data yang handal, sebagai aplikasi yang dapat mengklasifikasi berbagai soal ujian khususnya bimbingan belajar. Tahap analisis sistem yang berjalan ini bertujuan untuk menjaga keamanan data soal ujian guna mendapatkan bahan evaluasi untuk pengembangan pada sistem yang akan dirancang, Evaluasi pada sistem yang lama adalah sistem konvensional masih ujian dalam bentuk kertas. Hal ini dapat dilihat dari pelaksanaan ujian, pelaksanaan harus dibagi kertas ujiannya, harus mempersiapkan pinsil 2B, harus disiapkan papan ujiannya, harus di cek dulu siswa ujiannya, pelaksanaannya memakan waktu yang lebih lama dan keamanan ujiannya tidak terjamin. Adapun pemecahan masalah yang diusulkan oleh penulis adalah :

1. Siswa yang ujian mengalami kerepotan dalam menyiapkan peralatan untuk ujian.
2. Siswa pada saat ujian harus sangat berhati-hati sekali dalam menjawab ujiannya di kertas karena takut kertas koyak, remok dan rusak.
3. Belum ada sistem keamanan soal ujian bimbingan berbasiskan komputerisasi berbasiskan web.

III.2. Penerapan Metode

Untuk dapat membuktikan keamanan Soal ujian semester dan data nilai, maka diperlukan sebuah perhitungan. Adapun langkah enkripsi dan dekripsi metode AES adalah sebagai berikut :

III.2.1. Langkah Kerja Algoritma AES

Skema algoritma kriptografi kunci publik (asimetris) AES terdiri dari tiga proses yaitu pembentukan kunci, proses enkripsi, dan proses dekripsi.

III.2.1.1. Algoritma Pembangkit Kunci

Studi Kasus

Data yang ada di *field database* alamat yaitu :*data ini sangat penting*

1. Algoritma Key

Tahap pertama adalah pembentukan kunci internal, key yang di input adalah :0123456789ABCDEF

K[0] = 0	L[0] = 0000
K[1] = 1	L[1] = 1000
K[2] = 2	L[2] = 2000
K[3] = 3	L[3] = 3000
K[4] = 4	L[4] = 4000
K[5] = 5	L[5] = 5000
K[6] = 6	L[6] = 6000
K[7] = 7	L[7] = 7000
K[8] = 8	L[8] = 8000
K[9] = 9	L[9] = 9000

K[10] = A L[10] = A000

K[11] = B L[11] = B000

K[12] = C L[12] = C000

K[13] = D L[13] = D000

K[14] = E L[14] = E000

K[15] = F L[15] = F000

Psoucecode nya adalah sebagai berikut :

SimpleCrypto.encrypt("rahasia",editAlamat.getText().toString())

privatefinalstatic String *HEX* = "0123456789ABCDEF";

Keterangan:

sb.append(*HEX*.charAt((b>>4)&0x0f)).append(*HEX*.charAt(b&0x0f)); koding berikut ini melakukan addroundkey yaitu melakukan XOR antara state awal plainteks "rahasia" dengan cipherkey *HEX* = "0123456789ABCDEF".

2. Melakukan putaran

Tahap ke dua ini melakukan putaran Nr – 1x, Proses putaran pertama adalah :

a. SubBytes

Membuat tabel nilai S-box untuk menentukan nilai substitusi byte,

psoucode nya adalah :

publicstaticbyte[] toByte(String hexString) {

int len = hexString.length()/2;

byte[] result = newbyte[len];

for (int i = 0; i < len; i++)

```
result[i] = Integer.valueOf(hexString.substring(2*i, 2*i+2),
16).byteValue();
return result;
   }
```

b. ShiftRows

ShiftRows ini melakukan pergeseran baris=baris array state, adapun psoucode nya adalah :

```
sb.append(HEX.charAt((b>>4)&0x0f)).append(HEX.charAt(b&0x0f));
```

c. MixColumns

MixColumns ini untuk mengacak data di masing-masing kolom array state, psoucode adalah sebagai berikut :

```
privatestaticbyte[] getRawKey(byte[] seed) throws Exception {
      KeyGenerator kgen = KeyGenerator.getInstance("AES");
      SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");
sr.setSeed(seed);
kgen.init(128, sr);
      SecretKey skey = kgen.generateKey();
byte[] raw = skey.getEncoded();
return raw;
            }
```

d. AddRoundkey

AddRoundKey ini untuk melakukan XOR antara state sekarang Round Key,. Psoudecode nya adalah sebagai berikut :

```
publicstatic String toHex(byte[] buf) {
if (buf == null)
return "";
        StringBuffer result = newStringBuffer(2*buf.length);
for (int i = 0; i < buf.length; i++) {
appendHex(result, buf[i]);
        }
return result.toString();
                }
```

3. Hasil

```
byte[] rawKey = rawKey(kunci.getBytes(),tipe);
byte[] hasil = encrypt(rawKey,plaintext.getBytes());
returnk_hexa(hasil);
```

Data Asli

ID	NAMA	Soal
1	Wati	Bahasa Indonesia
2	Andi	Matematika
3	Susi	Bahasa Inggris

Hasil Enkripsi

ID	NAMA	Soal
1	Andi	587E6E8C9CE409A91158F8B7E14522AA
2	Budi	E34E6E8D9DE410A96658F7C7EER123BA
3	Siswo	F34A5A8D9DE410A93338A3B7BBA344BA

III.3. Desain Sistem

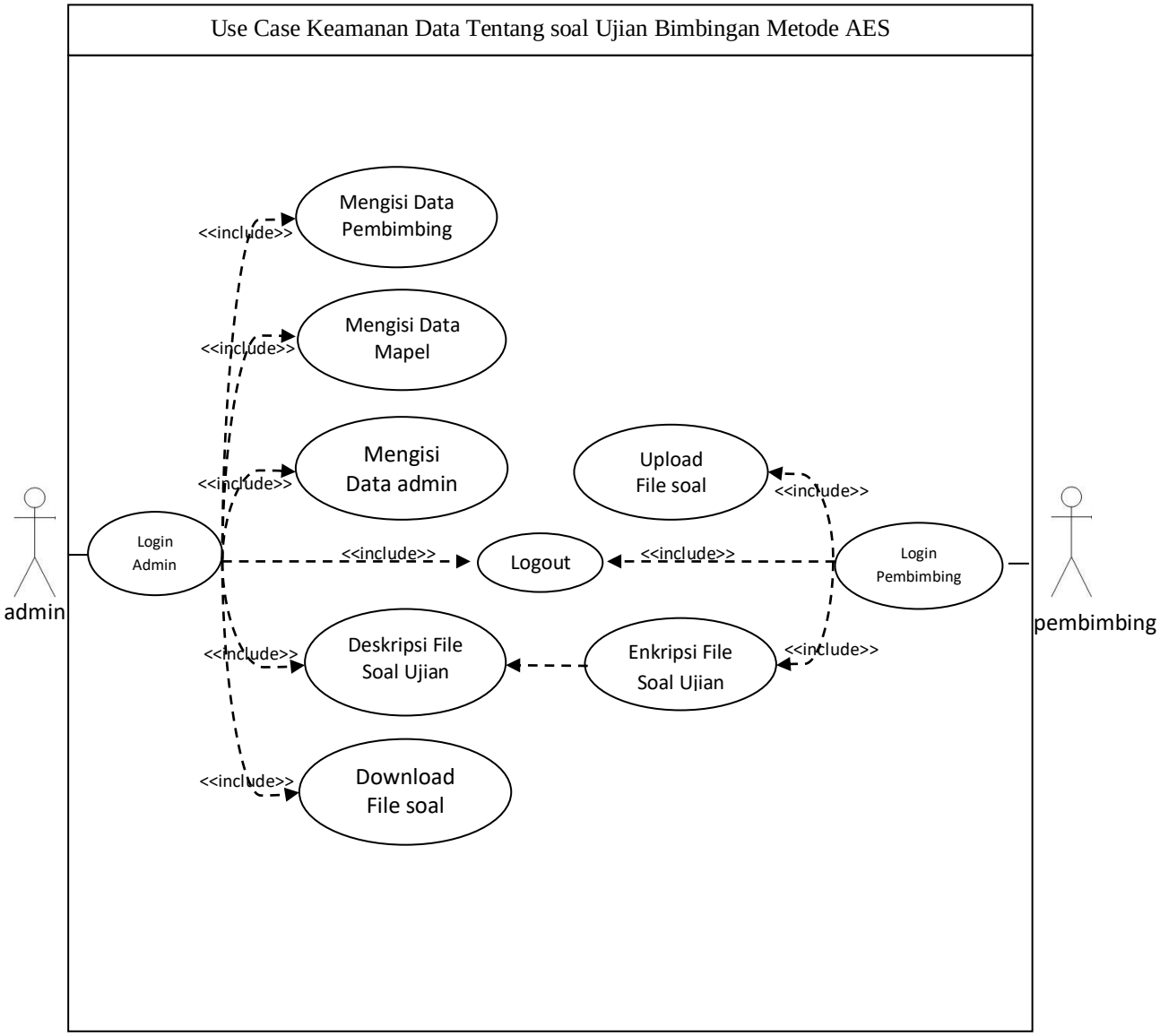
Adapun beberapa tahap yang dilakukan dalam membuat desain sistem adalah :

III.3.1. Desain Sistem Secara Global

Desain sistem atau perancangan sistem adalah proses pengembangan spesifikasi baru berdasarkan hasil *rekomendasi* analisis sistem. Dalam tahap perancangan, diharuskan merancang *spesifikasi* yang dibutuhkan. Bentuk rancangan sistem yang penulis buat menggunakan beberapa bentuk diagram dari *Unified Modeling Language* (UML) yaitu *Use Cace Diagram, Sequence Diagram, Activity Diagram, dan Class Diagram*.

III.3.1.1. *Use Case Diagram*

Perancangan dimulai dari *identifikasi* aktor dan bagaimana hubungan antara aktor dan *use case* didalam sistem. Perancangan *Use Case* Diagram dapat dilihat pada gambar III.1.



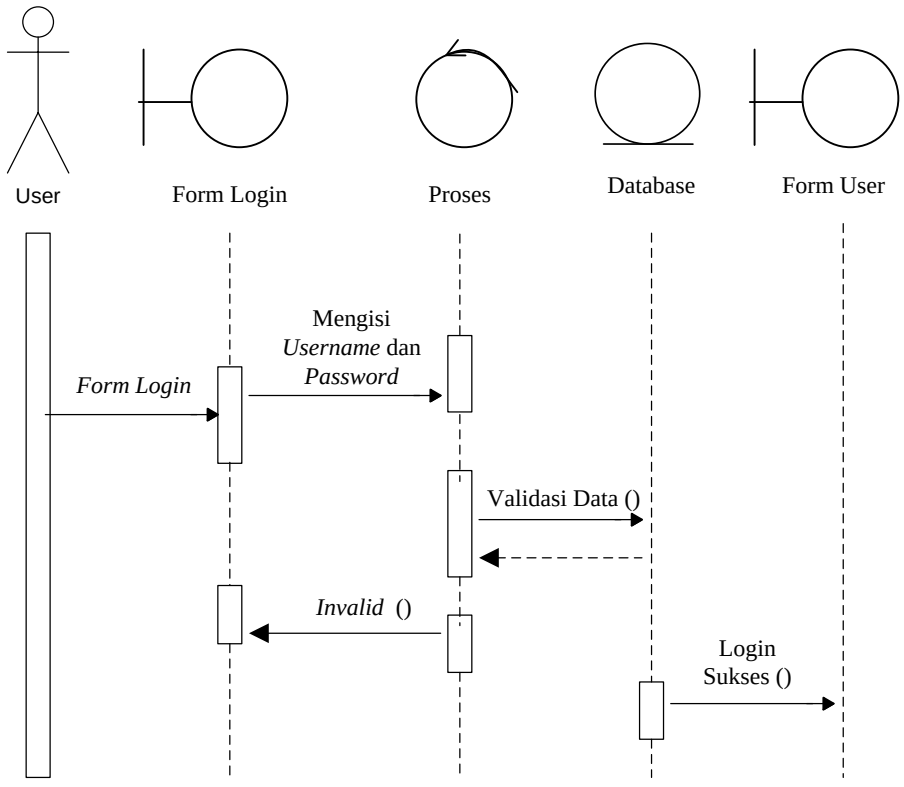
Gambar III.1. *Use Case Diagram* Ujian

III.3.1.2. *SequenceDiagram*

Rangkaian kerja melakukan pengamanan data nilai dan soal ujian semester dapat terlihat seperti pada Gambar III.2. berikut :

III.3.1.2.1. *Sequence Diagram Login*

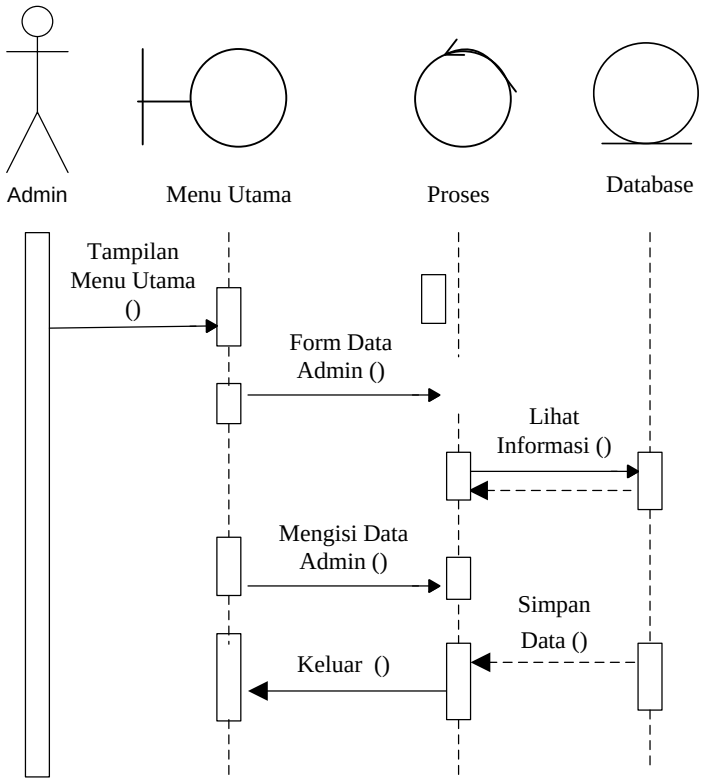
Gambar III.2. adalah *sequence* diagram login dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.2. *Sequence Diagram Login*

III.3.1.2.1. *Sequence Diagram* Data Admin

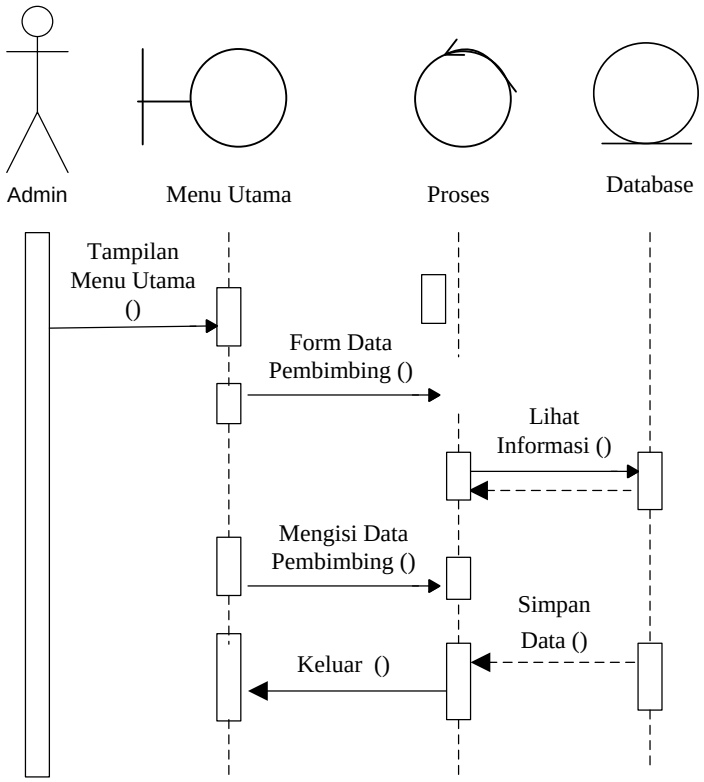
Gambar III.3. adalah *sequence diagram* Data Admin dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.3. *Sequence Diagram* Data Admin

III.3.1.2.1. *Sequence Diagram* Data Pembimbing

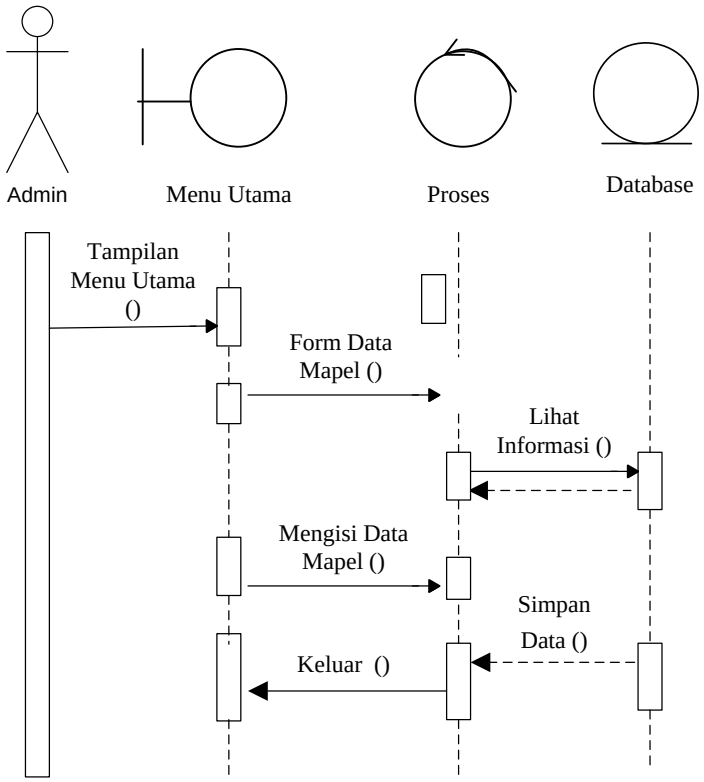
Gambar III.4. adalah *sequence diagram* Data Pembimbing dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.4. *Sequence Diagram* Pembimbing

III.3.1.2.1. *Sequence Diagram* Data Mapel

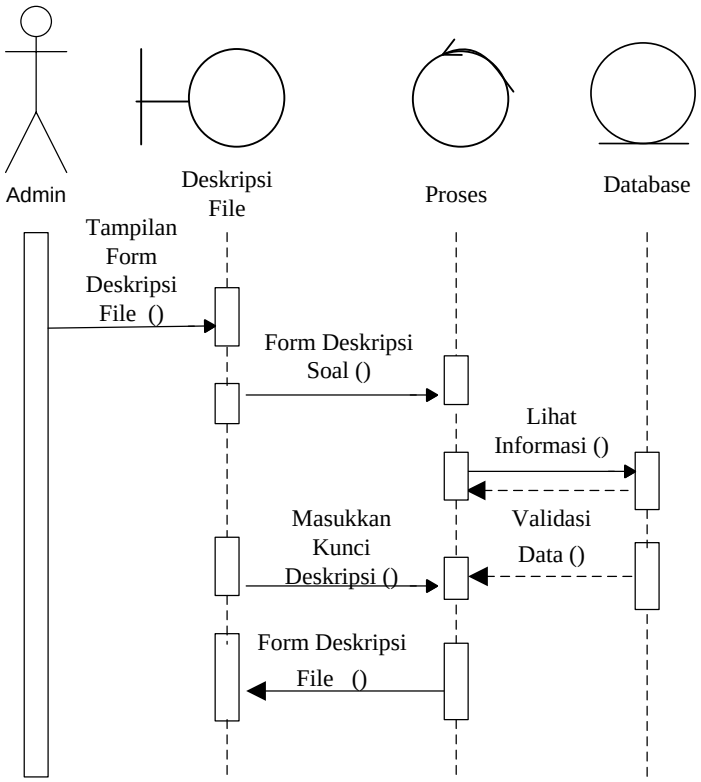
Gambar III.5. adalah *sequence diagram* Data Mapel dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.5. *Sequence Diagram* Data Mapel

III.3.1.2.1. *Sequence Diagram* Deskripsi File Soal Ujian

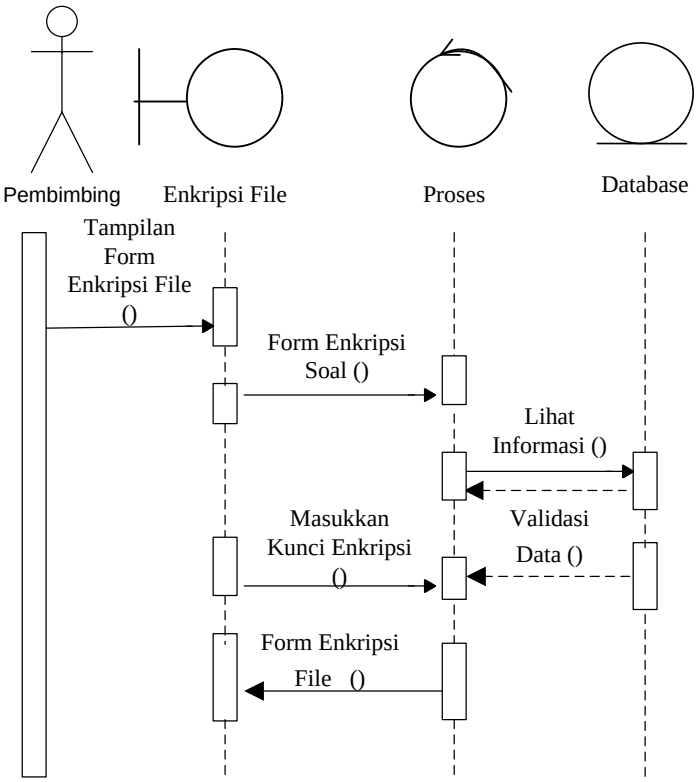
Gambar III.6. adalah *sequence diagram* Deskripsi Soal File Ujian dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.6. *Sequence Diagram* Deskripsi File Soal Ujian

III.3.1.2.1. *Sequence Diagram* Enkripsi File Soal Ujian

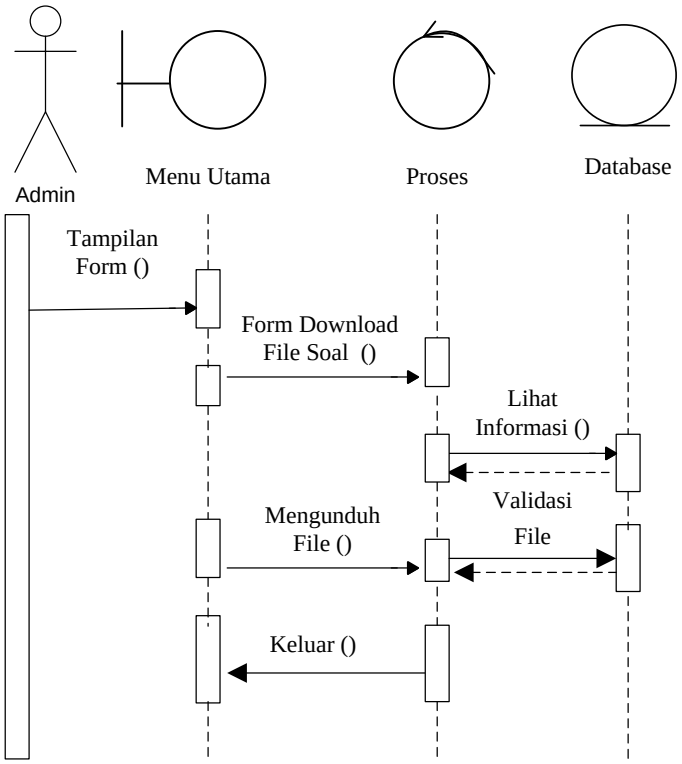
Gambar III.7. adalah *sequence diagram* Enkripsi File Soal Ujian dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.7. *Sequence Diagram* Enkripsi File Soal Ujian

III.3.1.2.1. *Sequence Diagram* Download File Soal

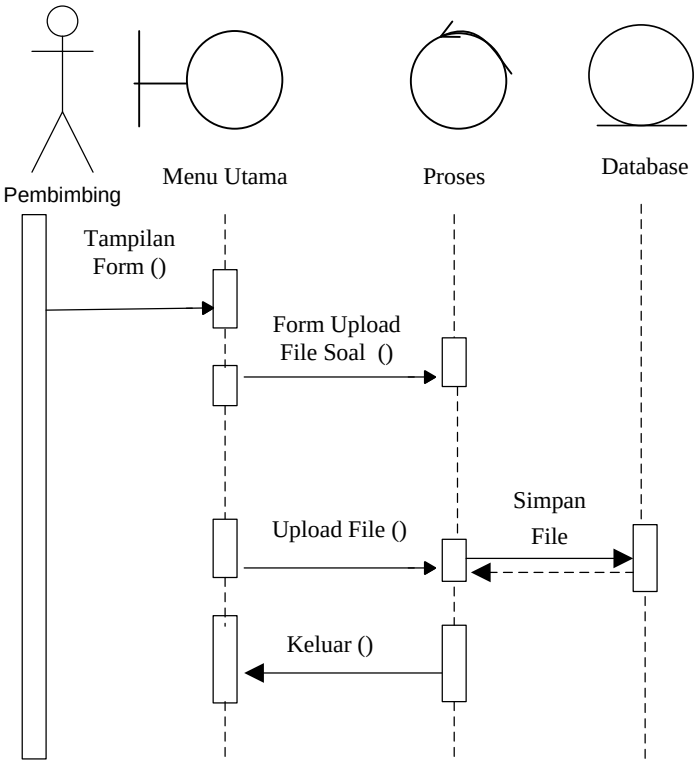
Gambar III.8. adalah *sequence diagram Download* File Soal dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar III.8. *Sequence Diagram* Download File Soal

III.3.1.2.1. *Sequence Diagram* Upload File Soal

Gambar III.9. adalah *sequence diagram Download* File Soal dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



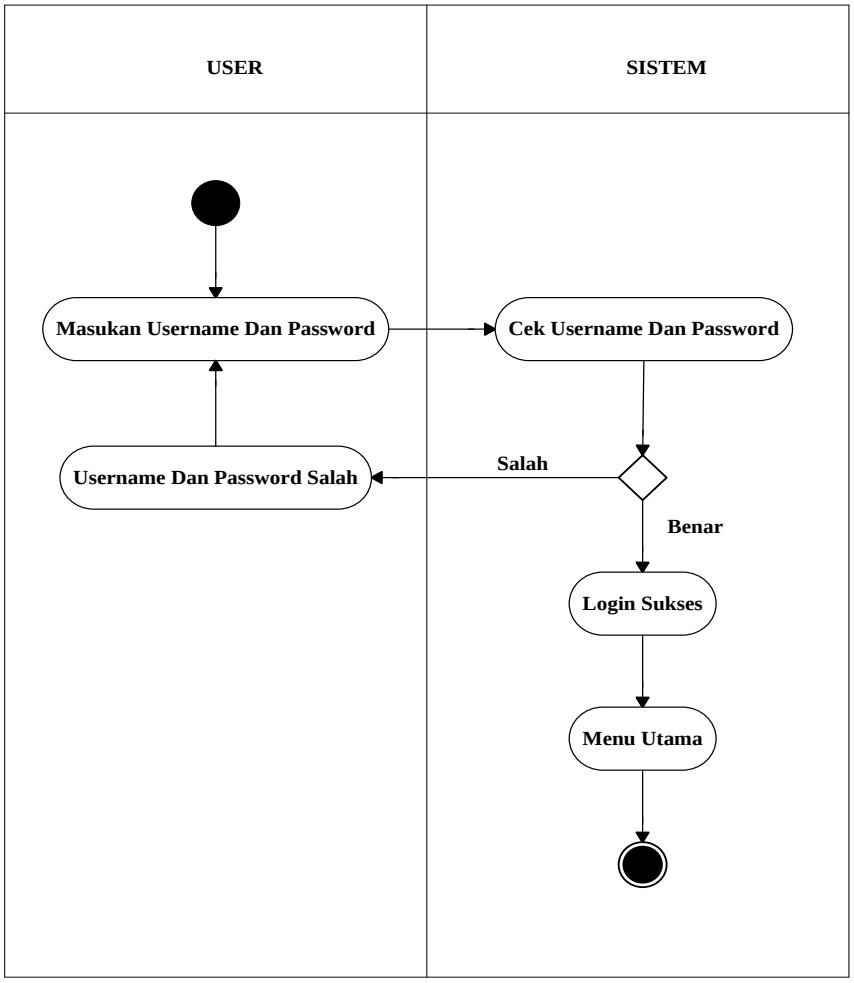
Gambar III.9. *Sequence Diagram* Upload File Soal

III.3.1.3. *Activity Diagram*

Proses yang digambarkan dalam *use case diagram* diatas dijabarkan dengan *activity diagram* :

III.3.1.3.1. *Activity Diagram Login*

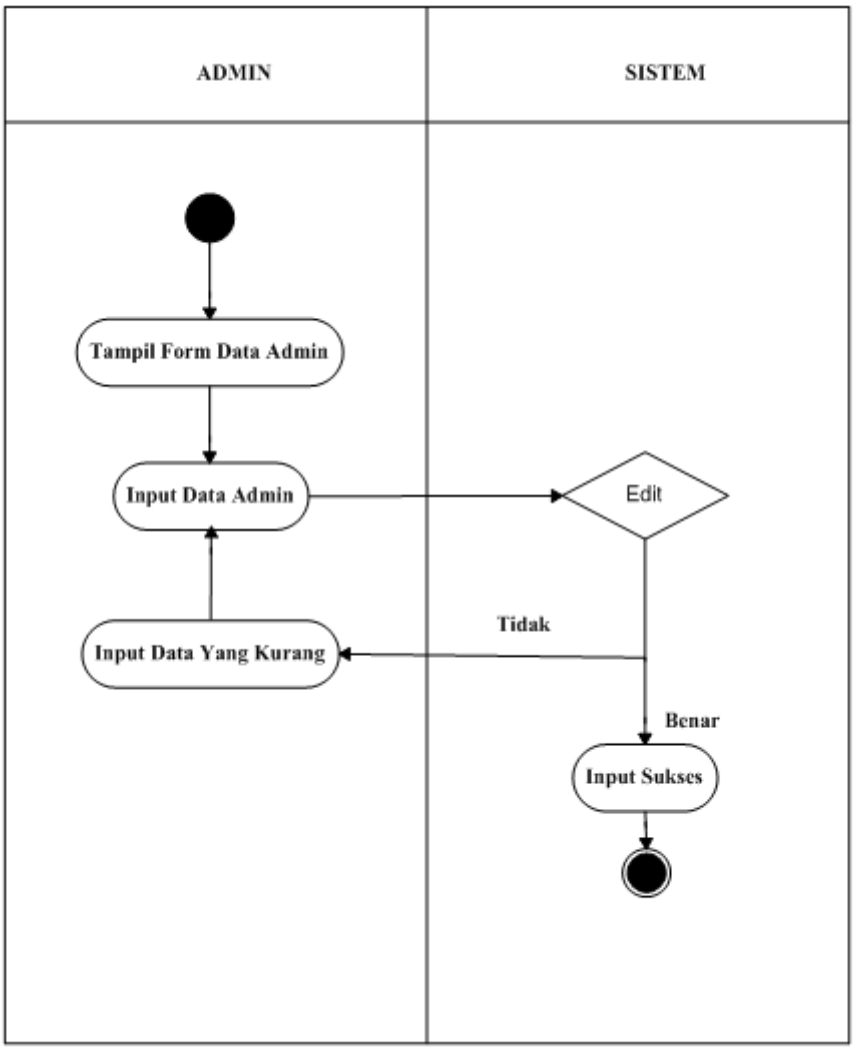
Aktivitas *login* yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada Gambar



Gambar III.10. *Activity Diagram Login*

III.3.1.3.1. *Activity Diagram* Data Admin

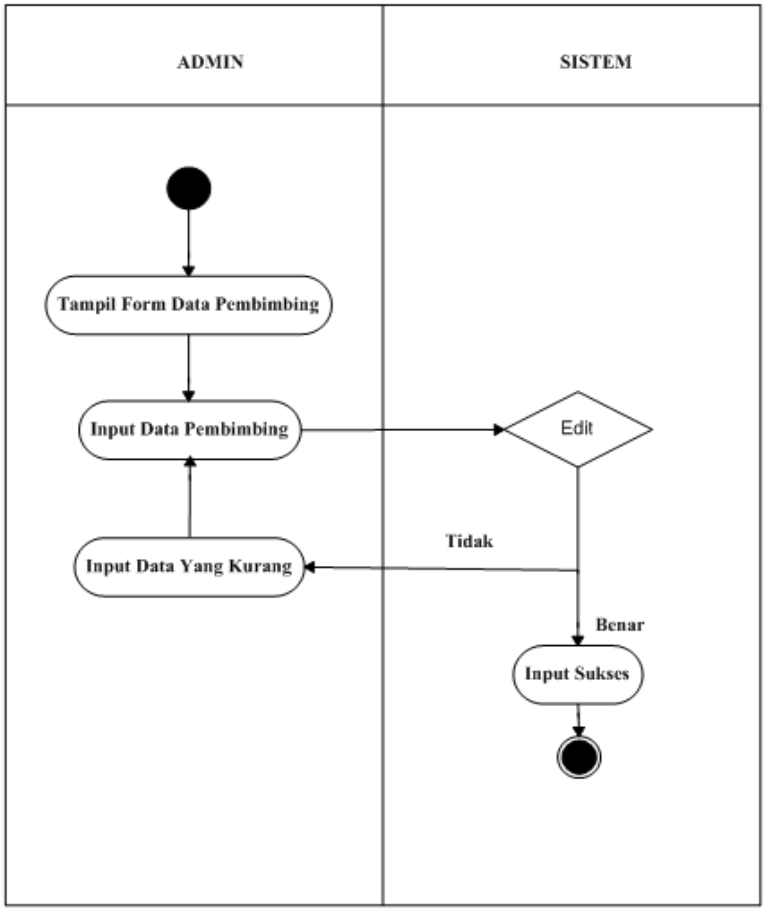
Aktivitas data admin yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada Gambar III.11. sebagai berikut :



Gambar III.11. *Activity Diagram* Data Admin

III.3.1.3.1. *Activity Diagram* Data Pembimbing

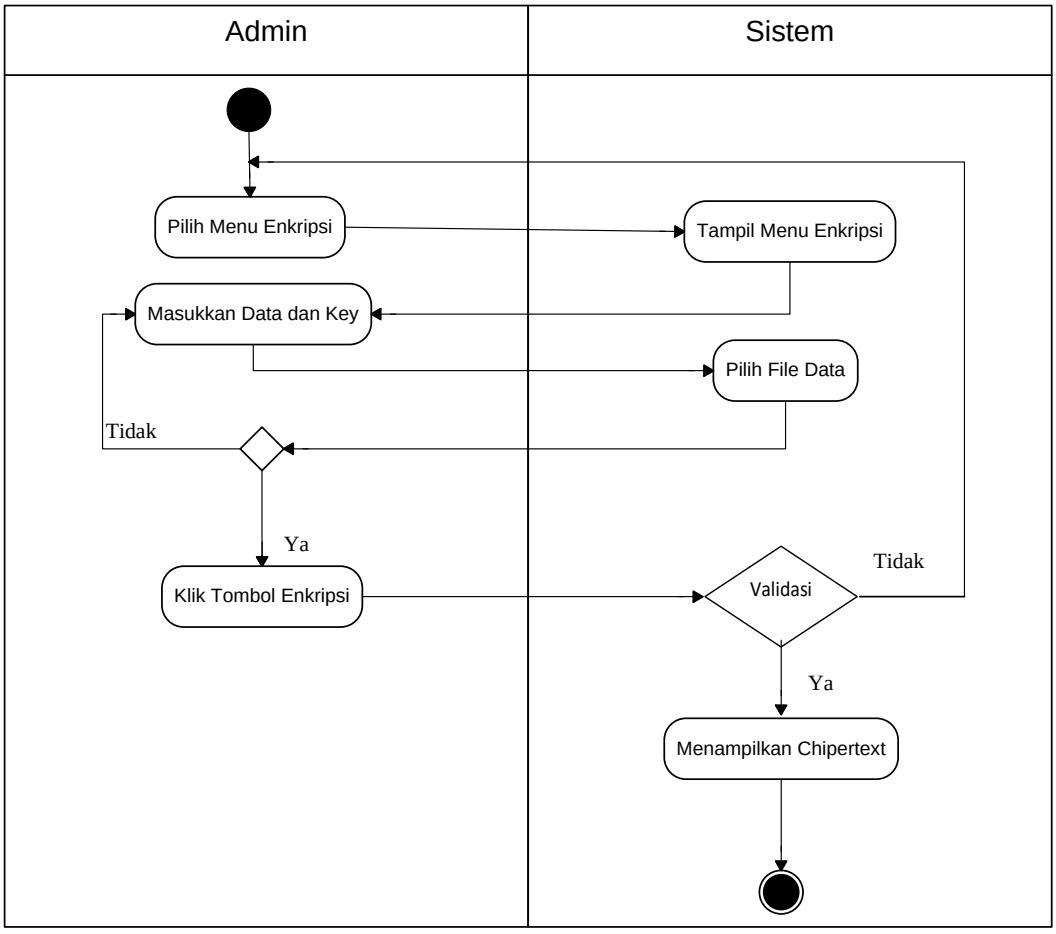
Aktivitas data Pembimbing yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada Gambar III.12 sebagai berikut :



Gambar III.12. *Activity Diagram* Data Pembimbing

III.3.1.3.1. *Activity Diagram* Enkripsi

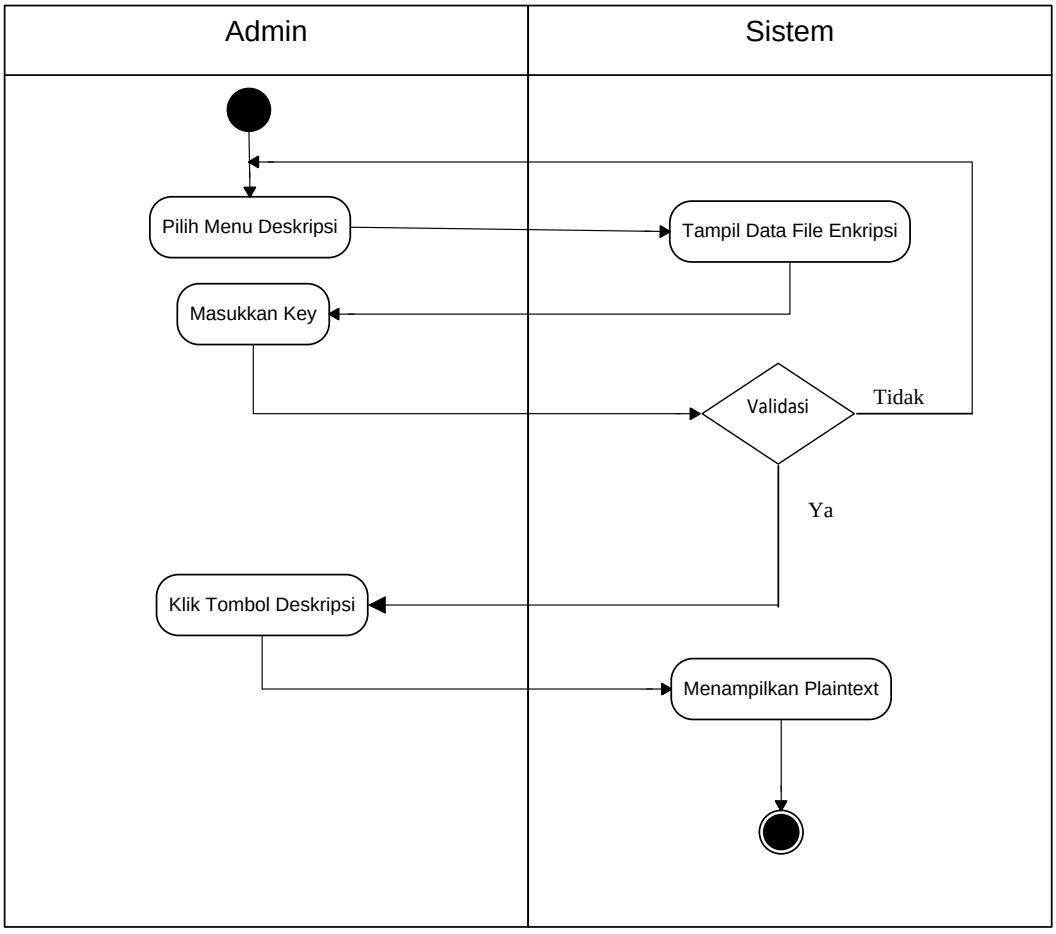
Aktivitas enkripsi yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada Gambar III.13. sebagai berikut :



Gambar III.13. *Activity Diagram* Enkripsi

III.3.1.3.1. *Activity Diagram* Deskripsi

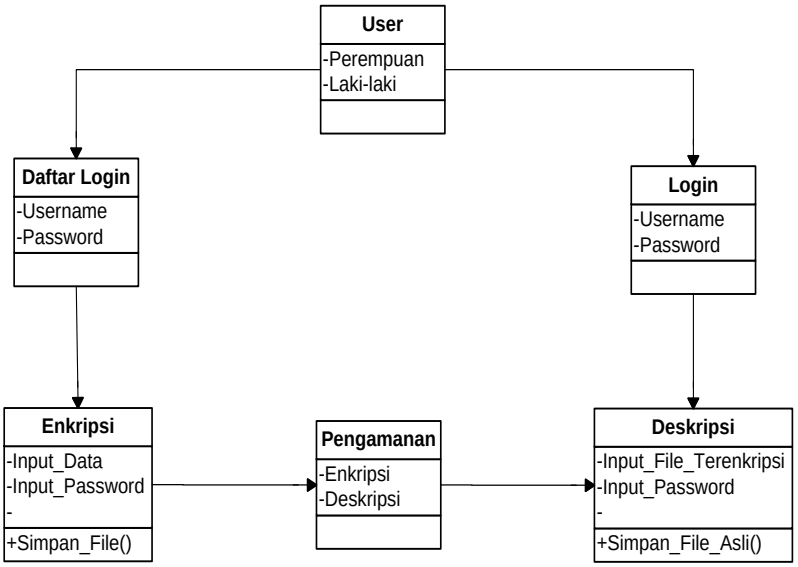
Aktivitas deskripsi yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada Gambar III.14. sebagai berikut :



Gambar III.14. *Activity Diagram* Deskripsi

III.3.2.*Class Diagram*

Perancangan dari *Class Diagram* di mulai dari *User*,dapat di lihat pada Gambar III.15. sebagai berikut.



Gambar III.15. *Class Diagram* Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES

III.4.2. Desain Tabel

Merancang struktur tabel pada *database* yang akan dibuat, berikut ini merupakan rancangan strukrut tabel tersebut :

1. Struktur Tabel *Login*

Tabel *login* digunakan untuk menyimpan data *username dan password* selengkapnya mengenai struktur tabel ini dapat dilihat pada tabel III.1berikut ini :

Tabel III.1. Rancangan Tabel *Login*

Nama Database		Dbbimbing	
Nama Tabel		Login	
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*username	Varchar	10	*Primary Key*
Password	int	11	-

2. Struktur Tabel Pembimbing

Tabel ini digunakan untuk menyimpan data dapat dilihat pada Tabel III.2 berikut ini :

Tabel III.2. Rancangan Tabel Pembimbing

Nama Database		Dbbimbing	
Nama Tabel		M_guru	
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Varchar	10	*Primary Key*
Nip	Varchar	30	-
Nama	Varchar	50	-

3. Struktur Tabel Mapel

Tabel ini digunakan untuk menyimpan data mapel dapat dilihat pada Tabel III.3 berikut ini :

Tabel III.3. Rancangan Tabel Mapel

Nama Database		Dbbimbing	
Nama Tabel		M_mapel	
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Int	5	*Primary Key*
Nama	Varchar	30	-

4. Struktur Tabel Soal

Tabel ini digunakan untuk menyimpan data soal dapat dilihat pada Tabel III.4. berikut ini :

Tabel III.4. Rancangan Tabel Soal

Nama Database		Dbbimbing	
Nama Tabel		M_soal	
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Int	6	*Primary Key*
Id_guru	Int	6	-

Id_mapel	Int	6	
Bobot	Int	2	
File	Varchar	150	
Tipe_file	Varchar	50	
Soal	longtext		
Opsi_a	longtext		
Opsi_b	longtext		
Opsi_c	longtext		
Opsi_d	longtext		
Opsi_e	longtext		
Jawaban	Varchar	5	
Tgl_input	datetime		
Jml_benar	int	6	
Jml_salah	int	6	

6. Struktur Tabel Ujian

Tabel ini digunakan untuk menyimpan data ikutujian dapat dilihat pada Tabel III.5 berikut ini :

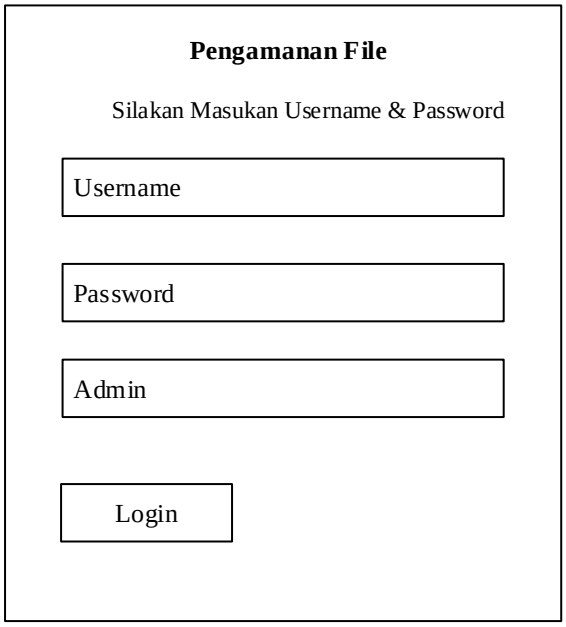
Tabel III.6. Rancangan Tabel Ikut Ujian

Nama Database	Dbbimbing		
Nama Tabel	M_ikut_ujian		
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Int	6	*Primary Key*
Id_tes	Int	6	-
Id_user	Int	6	
List_soal	longtext		
List_jawaban	longtext		
Jlh_benar	int	6	
Nilai	decimal	10,2	
Nilai_bobot	decimal	10,2	
Tgl_mulai	datetime		
Tgl_selesai	datetime		
Status	enum		

III.3.3. Perancangan Desain

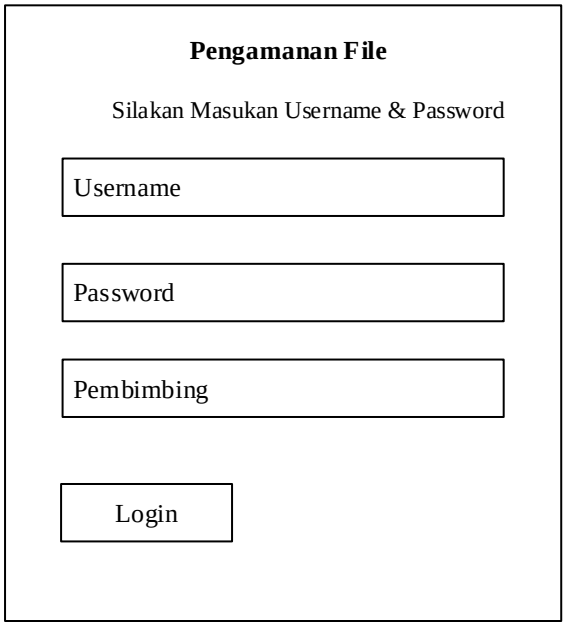
Perancangan tampilan awal berfungi untuk mengetahui beberapa sub menu masing-masing dari tombol pada tampilan menu awal dapat dilihat pada gambar III.16. sebagai berikut:

1. Tampilan Login Admin



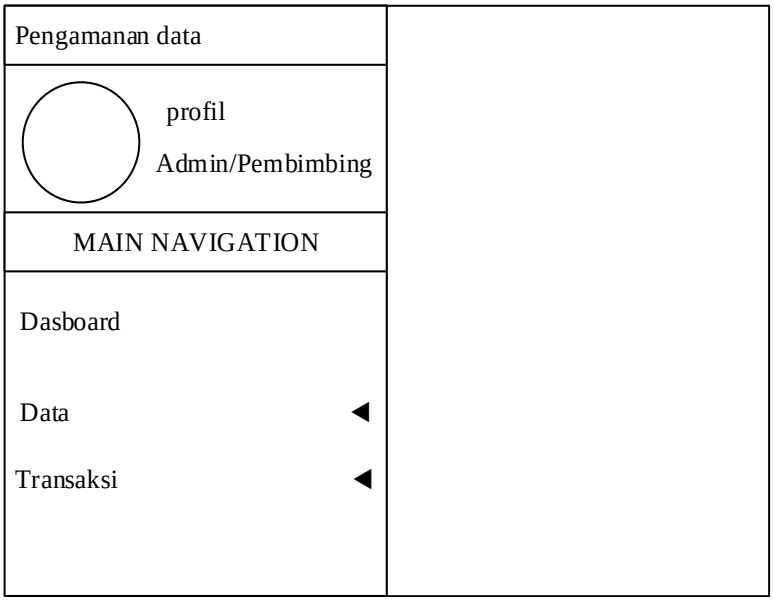
Gambar III.16. Tampilan Login Admin

2. Tampilan Login Pembimbing



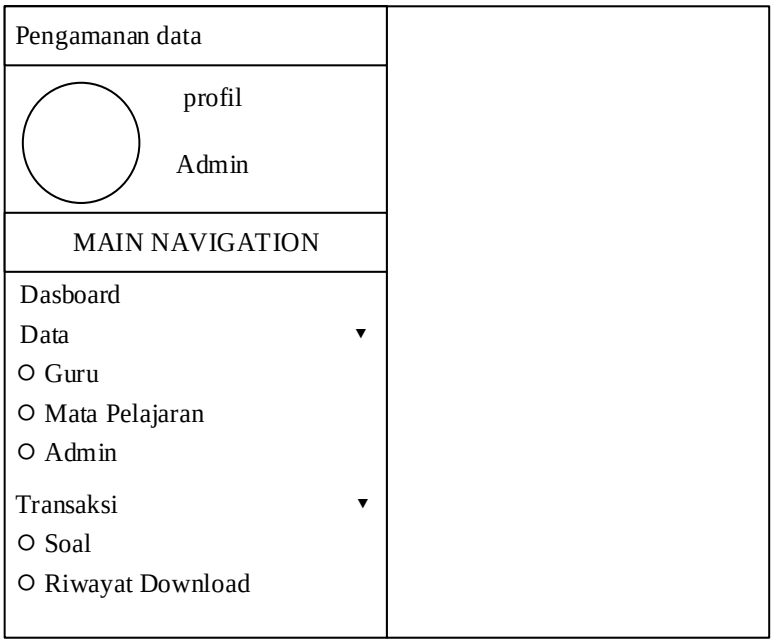
Gambar III.17. Tampilan Login Pembimbing

3. Tampilan Menu Utama



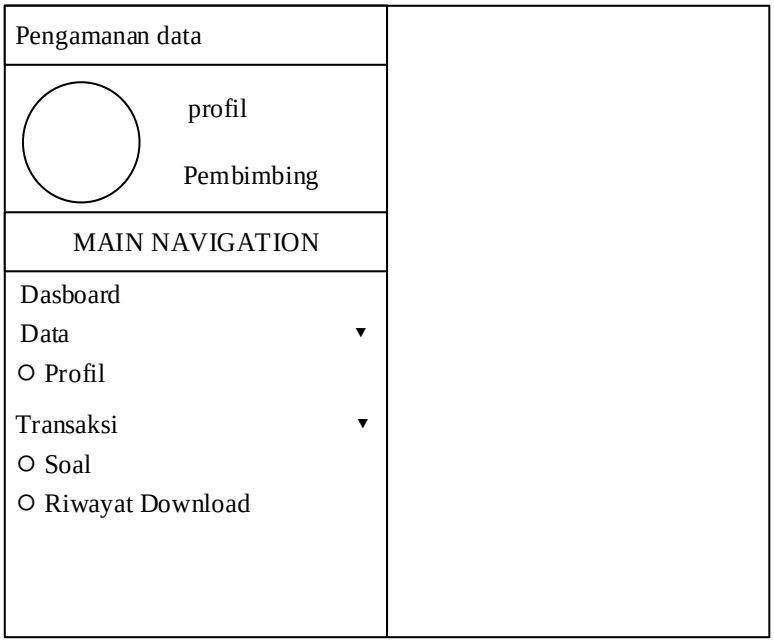
Gambar III.18. Halaman Menu Utama

4. Tampilan Menu Data Admin



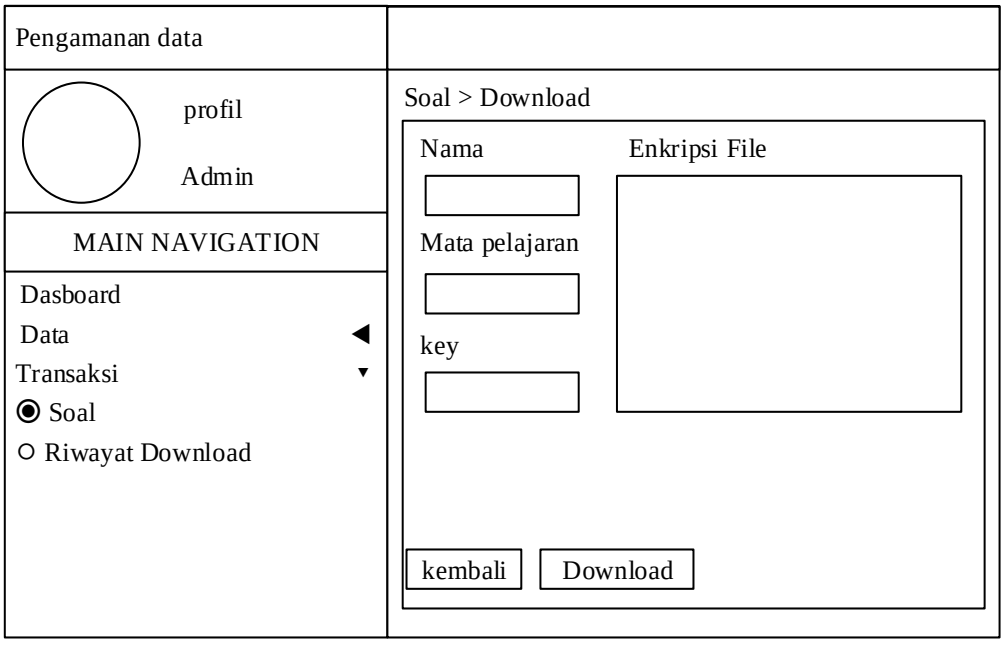
Gambar III.19. Halaman Data Admin

5. Tampilan Menu Data Pembimbing



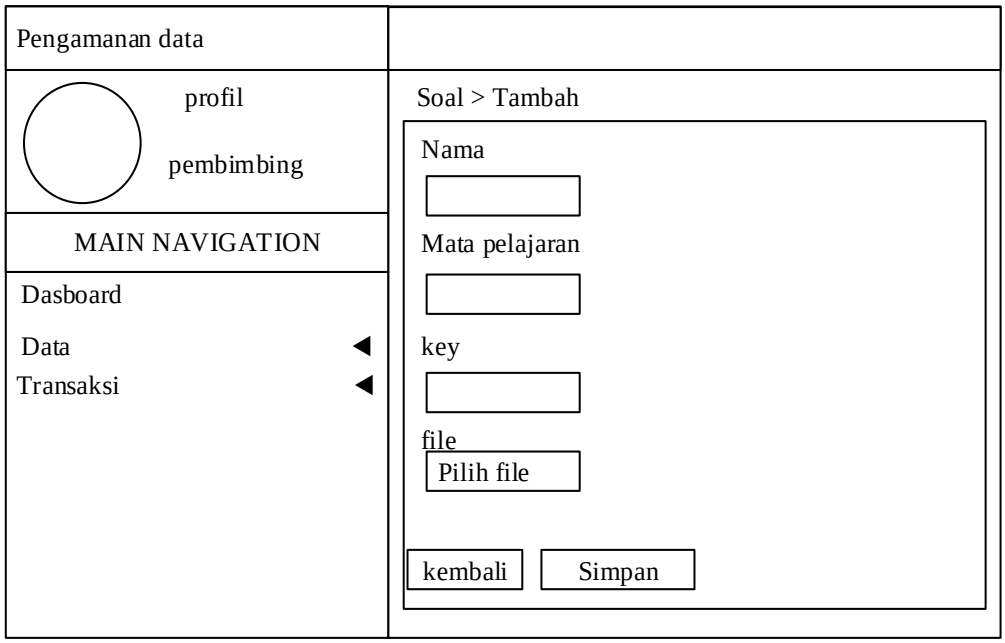
Gambar III.20. Halaman Data Pembimbing

6. Tampilan Menu halaman Download File Soal



Gambar III.21. Halaman Download File Soal

7. Tampilan Menu Halaman Upload File Soal



Gambar III.22. Halaman Upload File Soal