Implementasi Metode AES Dalam Pengamanan Data Soal Ujian Bimbingan Belajar Berbasis Web

IMPLEMENTATION OF AES METHOD IN SECURITY OF DATA BASED ON WEB-BASED TUTORING EXAM

M. Imam Hakiki[1], Muhammd Barka Akbar[2]
[1] Program Studi Teknik Informatika Universitas Potensi Utama
[2,]Dosen Program Studi Teknik Informatika Universitas Potensi Utama
[1,2] Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia – Medan
Email : [1]hakiki067@gmail.com, [2]Muhammad.barkah.akbar@gmail.com.

ABSTRAK

Kriptografi adalah merupakan langkah-langkah logis bagaimana cara menyembunyikan dan mengamankan informasi data yang di amankan dari yang tidak berhak atas data tersebut, Pelaksanaan ujian bimbingan belajar dimaksudkan untuk mengukur pengetahuan dan kepintaran seseorang atau peserta didik dalam mengingat pelajaran yang pernah di berikan, Selama ini soal ujian bimbingan belajar yang di buat oleh pembimbing atau guru hanya di berikan secara manual kepada bagian admin dalam bentuk dokumen kertas sehingga sering terjadi kebocoran data soal ujian bimbingan belajar, dari permasalahan tersebut peneliti termotivasi dan mencoba untuk memberikan pemecahan masalah tentang kebocoran data soal ujian bimbingan belajar yang dihadapi, yaitu dengan memberikan keamanan dengan menggunakan kriptografi AES (Advanced Encryption Standard), jadi kelebihan AES adalah dari segi ketahanannya dalam mengamankan data termasuk data soal ujian yang berbenruk file PDF. Penulis ingin mengembangkan keamanan data soal ujian bimbingan belajar dengan menggunakan metode AES dalam melakukan enkripsi dan deskripsi di pengamanan data soal ujian bimbingan belajar, ini akan di implementasikan di keamanan data soal ujian bimbingan belajar tersebut yang telah di tentukan dengan berbasis system Web.

Katakunci :Kriptografi, AES, Aplikasi.

ABSTRACT

Cryptography is logical steps on how to hide and secure data information that is safe from those who are not entitled to the data. The implementation of a tutoring test is intended to measure the knowledge and intelligence of a person or students in remembering lessons that have been given. tutoring exams made by supervisors or teachers are only given manually to the admin in the form of paper documents so that there is often a leak of data about tutoring exam questions, from these problems the researchers are motivated and try to provide solutions to the problem of data leakage of the tutoring exam questions faced, namely by providing security by using AES (Advanced Encryption Standard) cryptography, so the strength of AES is in terms of its durability in securing data including test question data in the form of PDF files. The author wants to develop the data security of tutoring exam questions by using the AES method in encrypting and encrypting the data security of the tutoring exam questions, this will be implemented in the data security of the tutoring exam questions that have been determined by Web-based systems.

Keywords : Cryptography, AES, Application

1. PENDAHULUAN

Selama ini Pembelajaran bimbingan merupakan salah satu tahap kegiatan sebagai sarana evaluasi yang dilakukan secara berkala untuk mengukur pengetahuan, untuk memenuhi syarat untuk kelulusan dan diterapkan antar pendidik (guru) dan peserta didik (siswa) dalam suatu lingkungan belajar[1]. dengan perkembangan teknologi saat ini khususnya perkembangan informasi dalam bentuk web telah banyak dikembangkan untuk menunjang efektifitas pertukaran informasi oleh beberapa pengembang aplikasi[2], Web adalah sebuah perangkat lunak untuk membantu manusia dengan mudah dalam memberikan informasi dan keamanan data, Salah satu teknik mengamankan data yaitu dengan teknik penyandian atau kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integrasi data, autentikasi data, serta untuk melakukan otentikasi data pada saat melakukan enkripsi dan depkripsi data Dengan adanya Kriptografi data atau informasi akan terjaga keamanannya dari pelaku kejahatan komputer[3]. AES (Advanced Encryption Standard) atau disebut Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu[4]. Selama ini soal ujian yang di buat oleh pembimbing di berikan secara manual kepada bagian admin dalam bentuk file sehingga sering terjadi kebocoran soal, dari permasalahan tersebut peneliti termotivasi dan mencoba memberikan pemecahan masalah tentang kebocoran soal yang dihadapi dengan kecurangan pada saat ujian maka peneliti merancang dan membangun aplikasi agar dapat mengamankan data dan menjaga kerahasiaan data soal ujian[5]. Dengan perkembangan teknologi saat ini yang menuntut suatu sistem pengujian yang efisien, efektif, dan mampu melaksanakan pengujian secara cepat dan tepat.

2. METODOLOGI PENELITIAN

Adapun Metodologi dalam Penelitian ini adalah :

2.1. Metode Pengumpulan Data

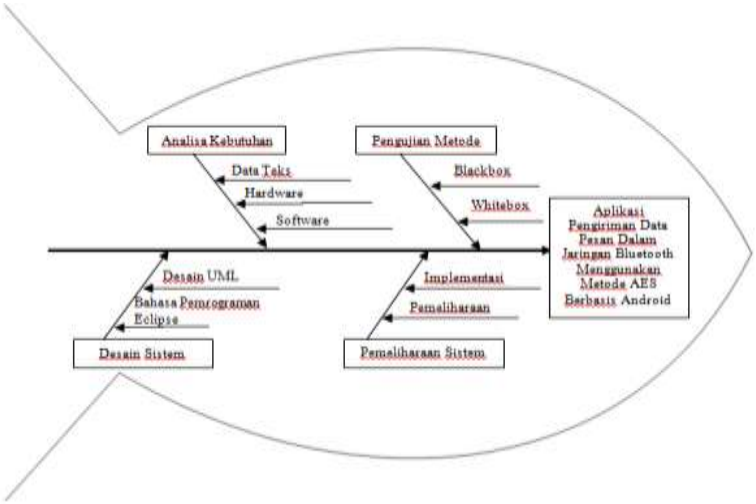
Di dalam melakukan penelitian diperlukan beberapa cara untuk mengumpulkan data yang diperlukan dalam kegiatan penelitian ini. Adapun teknik dalam pengumpulan data adalah :

1. Pengamatan (Observation)
   Dalam metode pengamatan ini peneliti melakukan pengamatan secara langsung pada objek pembahasan yang ingin diperoleh yaitu bagian-bagian terpenting dalam pengamanan data dengam menggunakan metode AES.
2. Wawancara (Interview)
   Pengumpulan data atau informasi pada metode ini dapat di lakukan dengan wawancara atau mengajukan pertanyaan-pertanyaan langsung pada sekolah atau tempat bimbingan belajar.
3. Sampel (Sampling)

Meneliti dan memilih data-data yang tersedia dan sesuai dengan bidang yang dipilih sebagai berkas lampiran.

2.2 Metode Penelitian

Merupakan cara pengumpulan data dengan mempelajari literatur, paket modul dan panduan, buku-buku pedoman, buku-buku perpustakaan dan segala kepustakaan lainnya yang dianggap perlu dan mendukung. Peneliti menggunakan Fishbone untuk menggambarkan alur kerja yang peneliti lakukan untuk menyelesaikan penelitian ini.



Gambar 1. Diagram Fishbone Proses Perancangan Sistem

Dalam pengembangannya metode kerangka fishbonememiliki beberapa tahapan yaitu : requirement (analisis kebutuhan), design sistem (system design), coding, pengujian program, pemeliharaan sistem:

2.2.1 Target/tujuan penelitian

Targe penelitian ini yaitu merancang dan membangun system keamanan data menggunakan metode aes pada soal ujian.

2.2.2 Tahap Identifikasi kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data teori yang terkait dengan data soal ujian bimbingan.

2.2.3 Pengujian Metode

Tujuan utama tahap pengujian metode untuk mengetahui syarat kemampuan yang harus dipenuhi oleh sistem agar keinginan pemakai sistem dapat terwujud. Tahap analisis ini terbagi menjadi dua, yaitu analisis kebutuhan sistem fungsional dan analisis kebutuhan sistem nonfungsional

2.2.3 Coding Sistem

Coding merupakan penerjemahan desain dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh programmer yang akan menterjemahkan transaksi yang diminta oleh user. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan dimaksimalkan dalam tahapan ini. Setelah pengkodean selesai maka akandilakukan testing terhadap sistem yang telah dibuat tadi. Tujuan testing adalah menemukan kesalahan-kesalahan terhadap system tersebut dan kemudian bisa diperbaiki.

2.2.4 Pengujian Program

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem.Pengujian yang dilakukan yaitu pengujian perangkat lunak yang tes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi/struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan, pengujian tersebut untuk masing-masing blok peralatan yang dirancang.

2.2.5 Pemeliharaan System

Perangkat lunak yang susah disampaikan kepada pelanggan pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan karena perangkat lunak harus menyesuaikan dengan lingkungan (periperal atau sistem operasi), atau karena pelanggan membutuhkan perkembangan fungsional.

2.3 Konribusi Penelitian

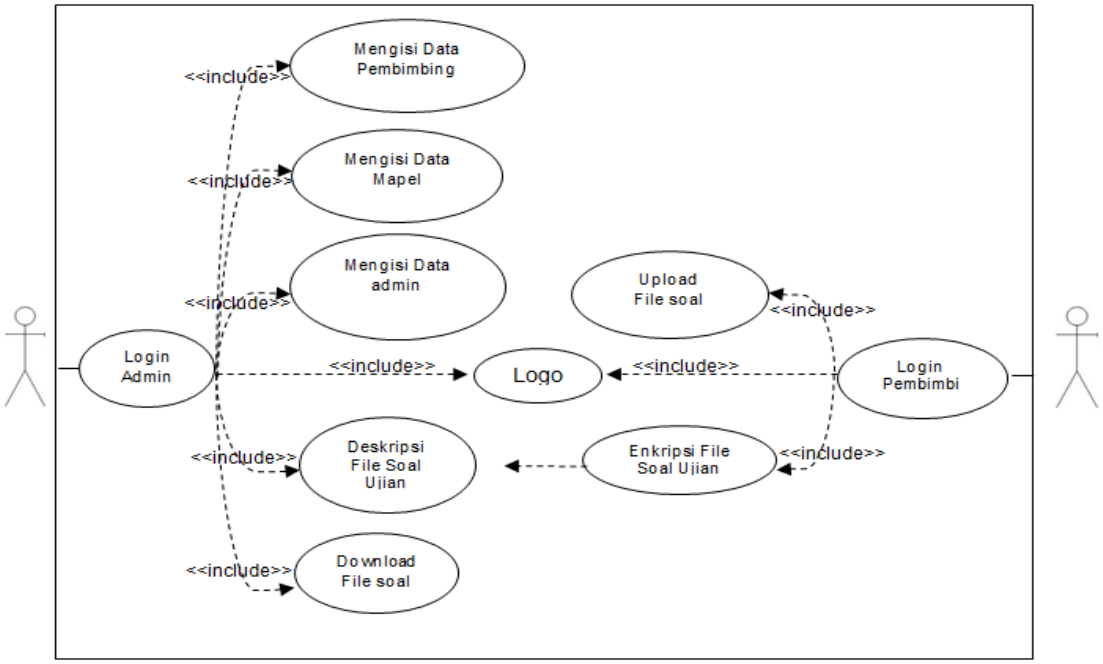
Konstribusi penelitian mengenai penelitian yang penulis buat yaitu tentang melindungi Data agar dapat meningkatkan keamanan data Soal ujian bimbingan.

3. HASIL DAN PEMBAHASAN

Sebelum melangkah ke dalam tahap perancangan aplikasi lebih lanjut, maka dilakukan perancangan pemodelan visual dari aplikasi yang akan dibangun dengan menggunakan pemodelan UML (Unified Modelling Language).

3.1 Usecase Diagram

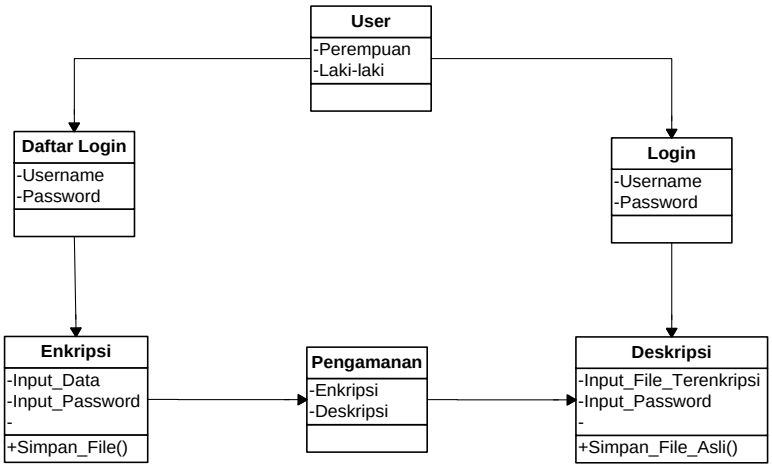
Berikut adalah usecase diagram dari aplikasi menu pencarian rute yang akan dirancang :



Gambar 2. Use Case Diagram

3.2 Class Diagram

Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar berikut :



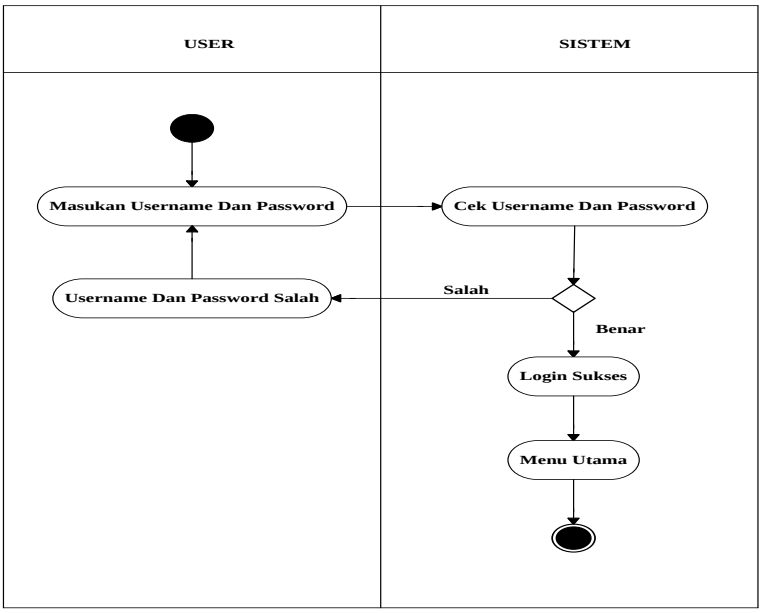
Gambar 3. Class Diagram

3.3 Activity Diagram

Proses yang telah digambarkan pada usecase diagram diatas dijabarkan dengan activity diagram:

3.3.1 Activity diagram login

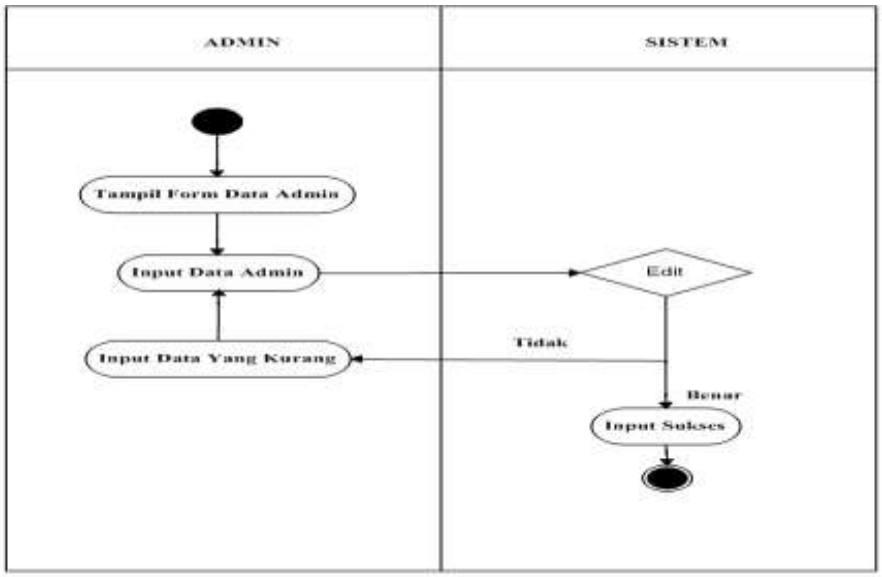
Aktivitas login yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah state yang ditunjukkan pada Gambar 4 sebagai berikut :



Gambar 4. activity diagram login.

3.3.2 Activity Diagram Data Admin

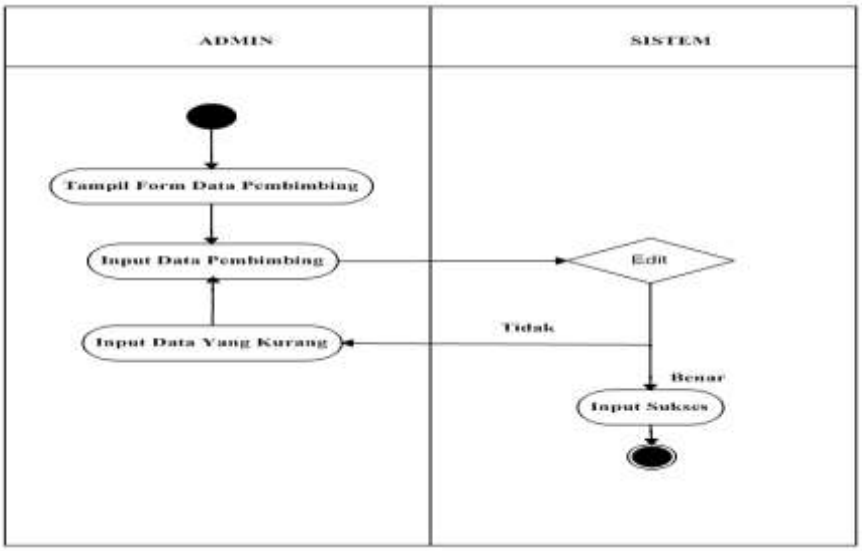
Aktivitas data admin yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah state yang ditunjukkan pada Gambar 5 sebagai berikut:



Gambar 5. activity diagram data admin

3.3.3 Activity Diagram data pembimbing

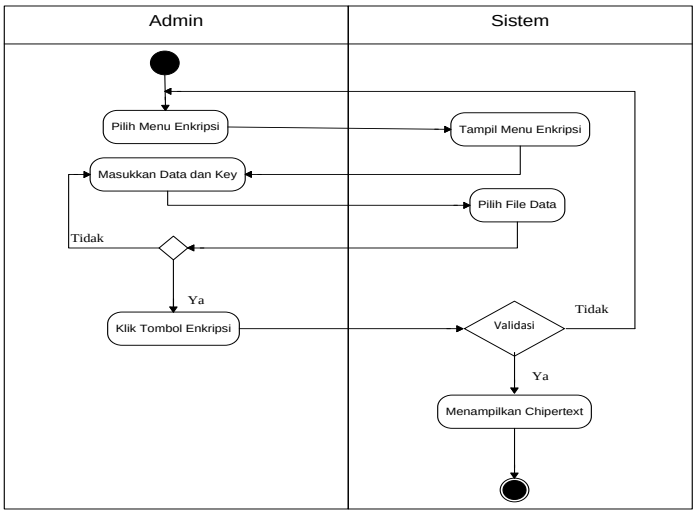
Aktivitas data Pembimbing yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah state yang ditunjukkan pada Gambar 6 sebagai berikut :



Gambar 6. Activity diagram data pembimbing

3.3.4 Activity diagram enkripsi

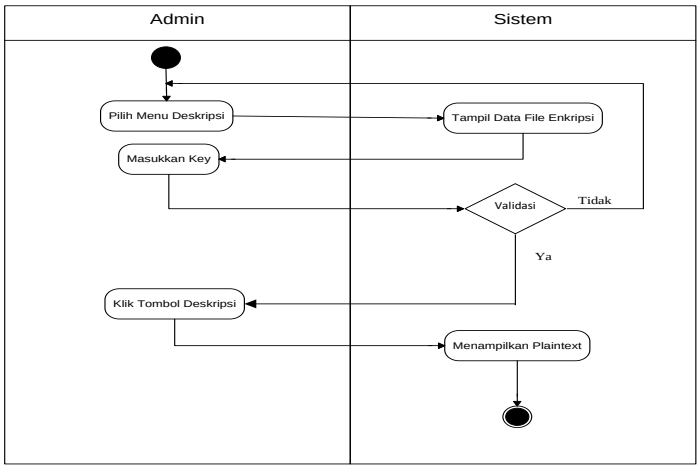
Aktivitas enkripsi yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah state yang ditunjukkan pada Gambar 7 sebagai berikut :



Gambar 7. Activity diagram enkripsi

3.3.5 Activity diagram deskripsi

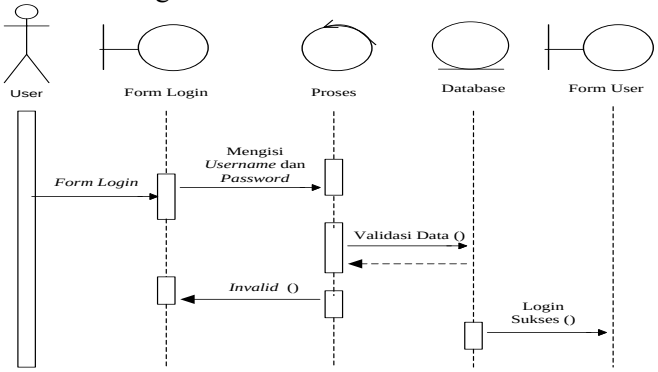
Aktivitas deskripsi yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah state yang ditunjukkan pada Gambar 8 sebagai berikut :



Gambar 8. activiti diagram deskripsi

3.3.6 *Sequence* Diagram *Login*

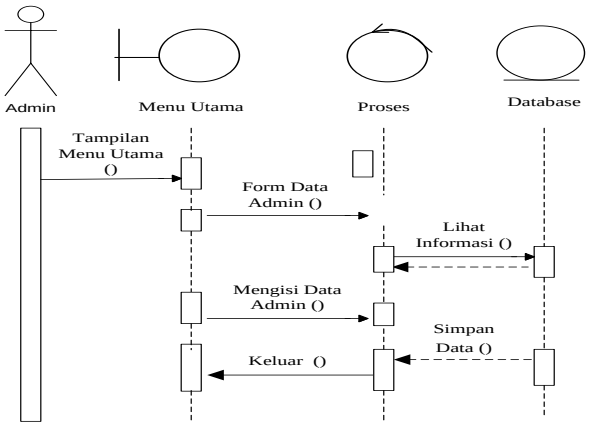
sequence diagram login dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar 9. *Sequence* Diagram *Login*

3.3.7 *Sequence* Diagram data admin

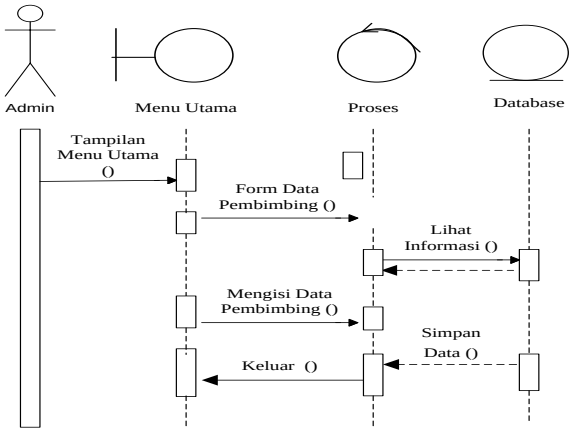
sequence diagram Data Admin dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar 10. *Sequence* Diagram data admin

3.3.8 *Sequence* Diagram Data pembimbing

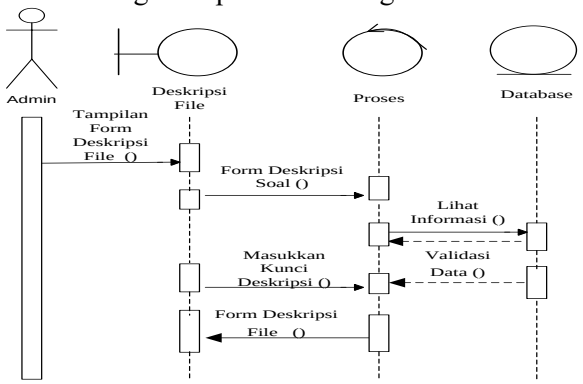
sequence diagram Data Pembimbing dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar 11 *Sequence* Diagram Data pembimbing

3.3.9 Sequence Diagram Deskripsi File Soal Ujian.

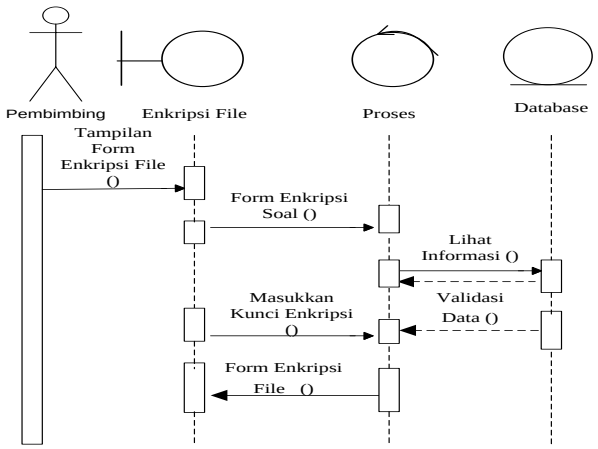
sequence diagram Deskripsi Soal File Ujian dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar 12. Sequence Diagram Deskripsi File Soal Ujian.

3.3.10 Sequence Diagram Enkripsi File Soal Ujian

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



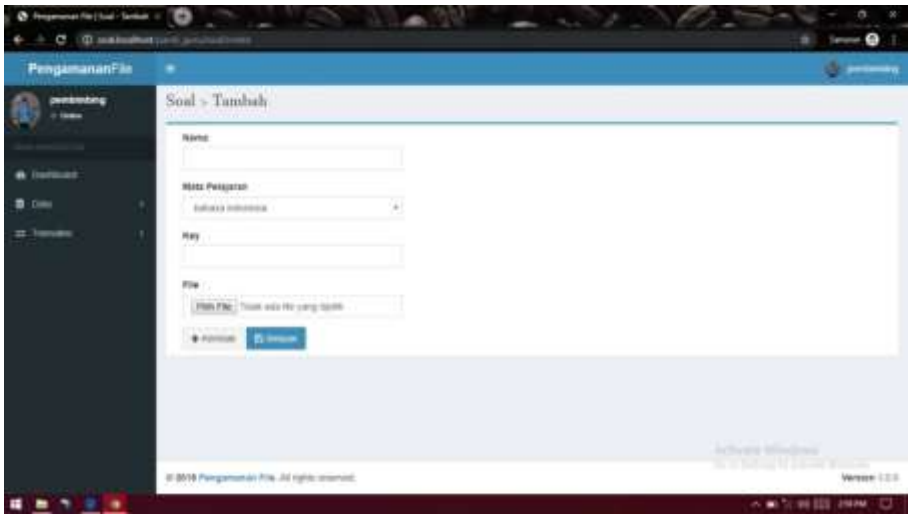
Gambar 13. Sequence Diagram Enkripsi File Soal Ujian.

Berikut ini dijelaskan tentang tampilan hasil dari aplikasi dalam implementasi metode aes dalam pengamanan data soal ujian bimbingan belajar berbasis web dapat dilihat sebagai berikut :

1. Tampilan *Form Login* Pengguna
   Hasil Tampilan *form* Login yang dapat dioperasikan oleh Pengguna dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada gambar 14. berikut :

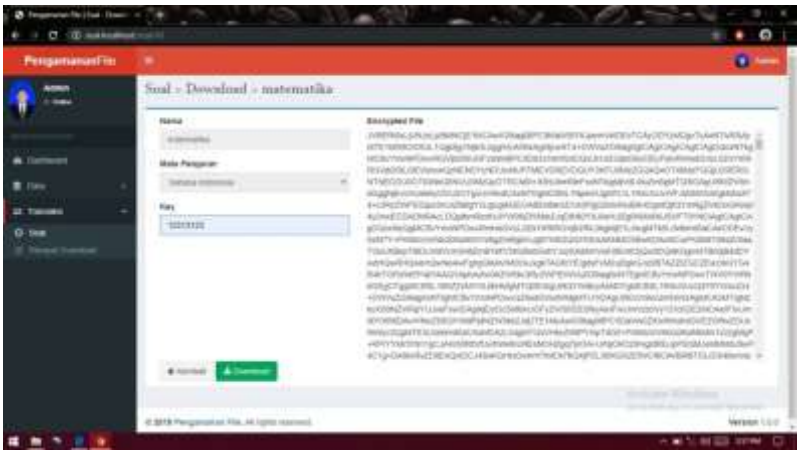
Gambar 14. Tampilan *Form Login* Pengguna

3. Tampilan *Form upload file soal*
   Hasil Tampilan *form* Edit Profil Umroh yang dilakukan oleh Pengguna dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada gambar 15. berikut :



Gambar 15. Tampilan *Form* upload soal

4. Tampilan *form* download file soal
   Tampilan menu download soal merupakan tampilan aktifitas yang dilakukan oleh admin. Dalam halaman menu download file soal yaitu halaman berisikan soal- soal dari mata pelajaran yang akan di upload dan akan di download berisikan enkripsi dari pembimbing. Tampilan pada Menu download File Soal dapat dilihat pada Gambar 16 berikut:



Gambar 16. Tampilan *Form* download file soal

4. KESIMPULAN

Dari hasil penelitian penulis, maka dapat diambil beberapa kesimpulan antara lain :

1. Aplikasi ini dirancang dengan menggunakan model prototype dalam bahasa pemrograman *Android Studio* untuk pengelolaan pemesanan paket umroh.
2. Pada aplikasi ini dapat mempermudah dan menghemat waktu dalam pengelolaan sebuah pesanan paket umroh.
3. Minim kesalahan yang terjadi dalam informasi pemesanan paket perjalanan umroh, sehingga tidak perlu lagi melakukan pemeriksaan pembayaran secara berulang – ulang.

5. SARAN

Adapun saran yang diberikan penulis untuk pengembangan dan perbaikan pada sistem ini selanjutnya adalah sebagai berikut :

1. Diharapkan kedepannya adanya pengembangan baik berupa penambahan fitur-fitur aplikasi yang sesuai dibutuhkan seperti fitur copy, cut, dan fitur tambahan lainnya.
2. Diharapkan pada penelitian selanjutnya dapat lebih menyederhanakan lagi bentuk tampilan pada aplikasi pengamanan soal ujian bimbingan agar lebih mudah digunakan oleh user (pengguna).
3. Diharapkan pada penelitian selanjutnya dapat menyediakan beberapa fitur yang lebih interaktif dalam hal desain dan tampilan aplikasi.
4. Diharapkan pada penelitian selanjutnya dapat menambahkan menu aplikasi yang dimana adanya fitur bagi siswa/I yang langsung dapat melakukan ujian pada aplikasi ini dan langsung adanya menu score dalam hasil ujian yang dilakukan oleh siswa/i.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah membantu penulis dalam menyelesaikan penelitian serta dukungan yang telah di berikan.

DAFTAR PUSTAKA

[1] Situmorang, R., Haryanto, E. V., & Akbar, M. B. (2020). Perancangan Media Pembelajaran Cara Memainkan Seruling 3 Dimensi Berbasis Multimedia. *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer*, *1*(1), 476-488.

[2] Juliawan, D., Puspasari, R., & Sianturi, C. J. M. (2018). Aplikasi Peminjaman dan Pengembalian Lcd Proyektor Berbasis Android dan Web Service. *IT (INFORMATIC TECHNIQUE) JOURNAL*, *5*(2), 162-171.

[3] Maulana, M. Y., Akbar, M. B., & Haryanto, E. V. (2020). PERANCANGAN APLIKASI MEDIA PEMBELARAN KRIPTOGRAFI PLAYFAIR CIPHER. *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer*, *1*(1), 357-367.

[4] FAHRIZAL, E. (2016). PERANCANGAN APLIKASI ENKRIPSI TEKS MENGGUNAKAN METODE AES BERBASIS ANDROID.

[5] Sadikin, M., & Gunawan, H. (2020). Peningkatan Sistem Seleksi Ujian Saring Masuk dengan Metode Linear Congruent Method Berbasis Mobile (Studi Kasus: Universitas Potensi Utama). Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer, 1(1), 1101-1112.

[6] Manurung, D. P., Puspasari, R., & Verina, W. (2020). Perbandingan Metode Stream Dengan Metode Caesar Cipher Terhadap Pengiriman Pesan Pada Jaringan Wireless LAN. *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer*, *1*(1), 332-342.