BAB IV
PERENCANAAN

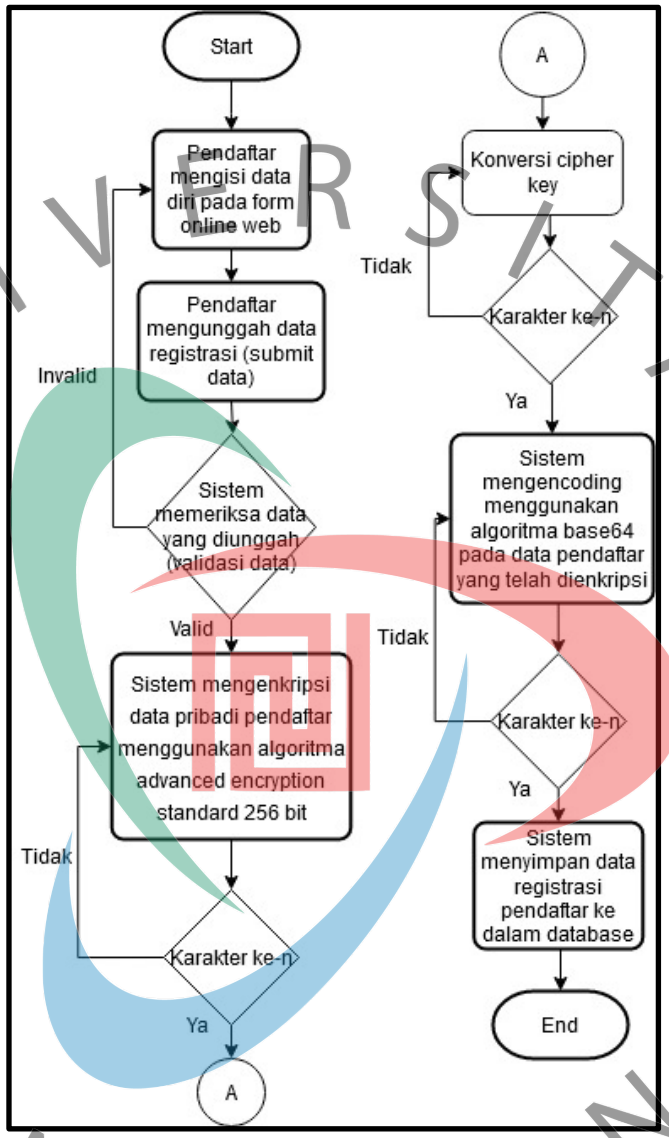
Pada bab ini, penulis akan membahas perencanaan yang menjadi upaya dalam merancang sistem pengamanan data hasil registrasi peserta pelatihan dan sertifikasi menggunakan algoritma *advanced encryption standard* dan algoritma *base64*.

4.1. Langkah-langkah Penelitian

Pada bagian ini, langkah-langkah penelitian bertujuan untuk menganalisa sistem yang akan dibuat, yang mana untuk memahami secara lebih *detail* masalah yang dihadapi sistem untuk selanjutnya dijadikan sebagai landasan rancangan penelitian, di mana dilakukan berdasarkan urutan kejadian yang ada, dan dari urutan kejadian tersebut dapat dibuat suatu sistem kriptografi untuk tujuan *data security system*. Sistem yang sedang berjalan pada saat ini secara keseluruhan dilakukan secara *manual*, yaitu pemasangan iklan di *media* sosial, proses pendaftaran menggunakan kertas pendaftaran, dan *form online* untuk pendataan.

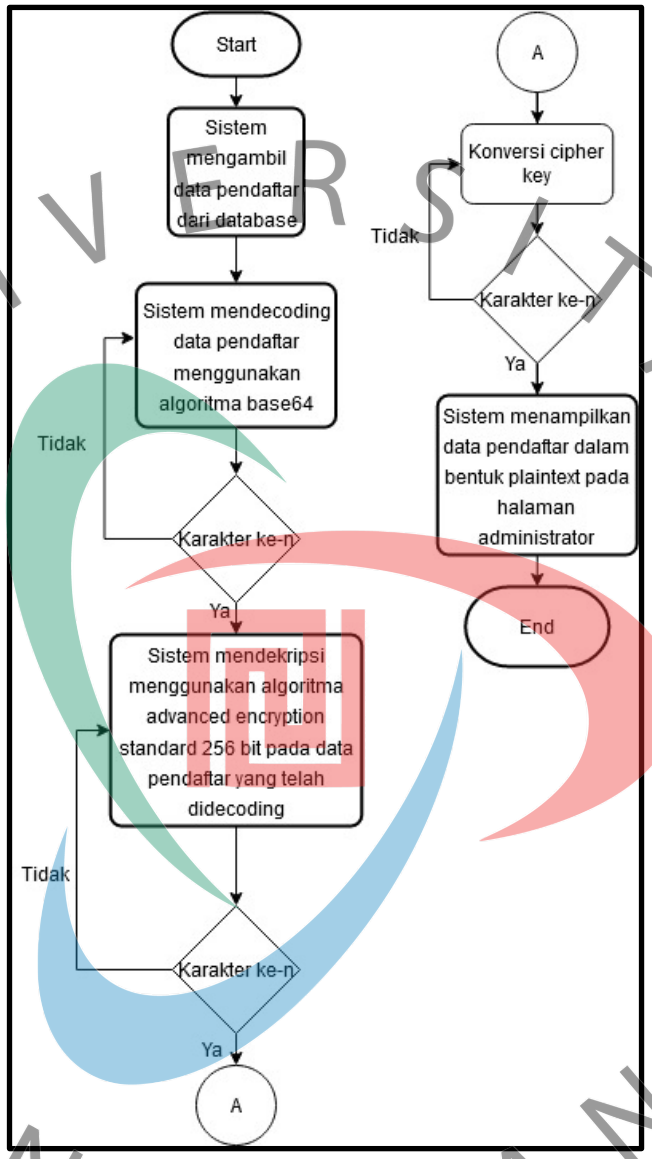
Pada tahap sebelumnya dari aplikasi yang dirancang dan dibangun oleh penulis, data hanya disimpan di dalam database tanpa ada fitur proteksi, sehingga hal tersebut yang mendasari penelitian ini, sistem yang dijadikan sebagai bahan penelitian lebih ditekankan pada kriptografi untuk tujuan *data security system*. Dengan demikian penelitian ini diharapkan dapat membantu mengatasi *cyberattack*, *data breaching*, dan *cyber extortion*, adapun hasil dari penelitian yang dilakukan merupakan langkah untuk lebih mengefektifkan dan mengefisienkan sistem yang ada atau terdahulu.

Untuk aliran langkah-langkah penelitian algoritma *AES* dan *Base64* yang diterapkan dalam sistem pada proses *encrypt* dan *encode* data dapat diperhatikan pada *flowchart diagram* di bawah ini.



Gambar 4.1. Implementasi Algoritma (1)

Untuk aliran langkah-langkah penelitian algoritma *AES* dan *Base64* yang diterapkan dalam sistem pada proses *decode* dan *decrypt* data dapat diperhatikan pada *flowchart diagram* di bawah ini.



Gambar 4.2. Implementasi Algoritma (2)

Hal-hal yang menjadi keutamaan dalam langkah-langkah penelitian sistem adalah sebagai berikut ini.

1. *User* mengisi data pribadi untuk melakukan registrasi secara *online* melalui *online form* yang terdapat pada aplikasi *web*, data tersebut yang telah *disubmit* akan dienkripsi menggunakan algoritma *advanced encryption*

standard 256 *bit* dan *diencode* menggunakan algoritma *base64 encoding*, untuk selanjutnya disimpan pada database *system*.

2. Data-data yang telah *disubmit* dapat diakses oleh *administrator* pada halaman *administrator*, di mana pada halaman tersebut data dari database yang ditampilkan merupakan *ciphertext* yang *didecode* menggunakan algoritma *base64* dan didekripsi menggunakan algoritma *advanced encryption standard* sehingga menjadi *plaintext*.

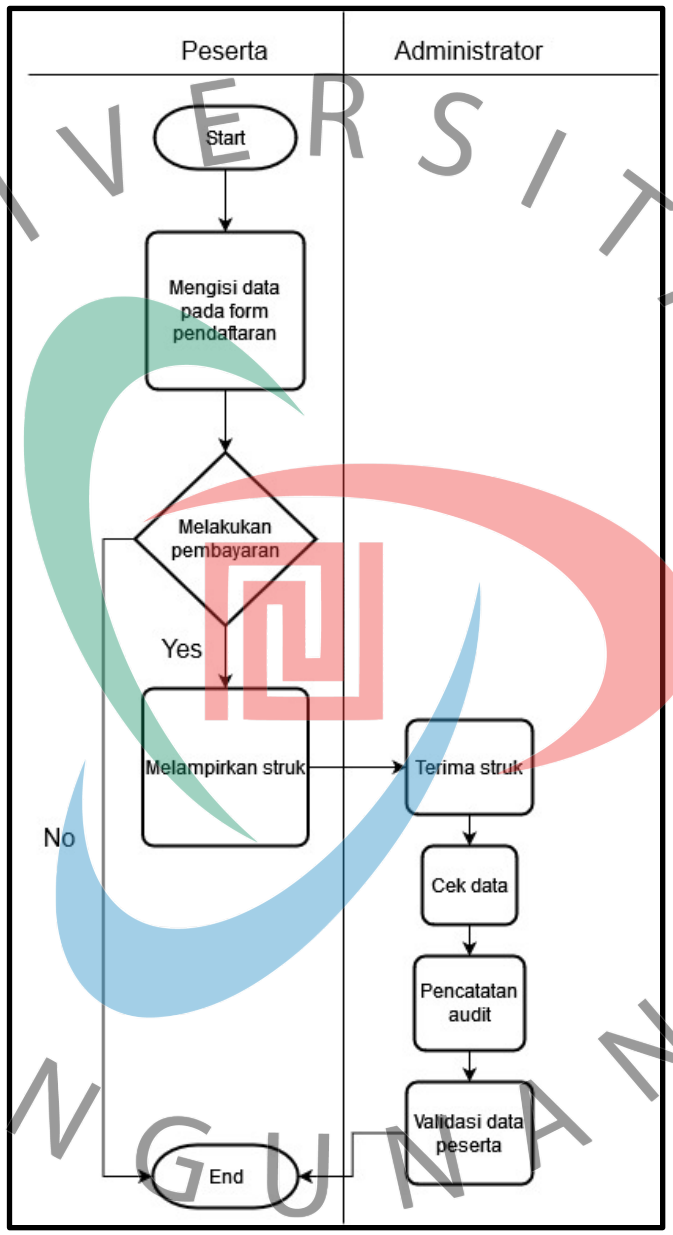
Berdasarkan pengumpulan data dan penelitian yang dilakukan oleh penulis terhadap sistem yang sedang berjalan, sistem masih memiliki kelemahan sebagai berikut ini.

1. Dalam penyimpanan data peserta beberapa kegiatan belum menggunakan sistem terkomputerisasi, masih menggunakan kertas dengan mengarsipkan data-data peserta pada *map* dan penyimpanan dilakukan secara manual.
2. Pada sisi waktu, sistem yang sedang berjalan tidak dapat menyediakan layanan 24 jam per hari baik kepada pendaftar maupun peserta.
3. Pelayanan yang dilakukan belum fleksibel. Hal ini karena banyaknya data yang masih disimpan dalam bentuk berkas kertas, dan pendataan yang disimpan dalam bentuk *file excel*, yang mana mengakibatkan peserta tidak dapat memperbaiki data yang salah input jika terjadi *human error*, dan data mudah untuk dicuri, dipalsukan, dan dimanipulasikan.
4. Tidak adanya sistem pengamanan data seperti enkripsi dan dekripsi, maka memiliki dampak negatif, karena maraknya kasus pembobolan data dan sistem yang terjadi belakangan ini, membuat pihak pengelola JCAL perlu berhati-hati dan melakukan pertimbangan.

Dari analisis dan evaluasi terhadap sistem yang berjalan pada JCAL secara keseluruhan, maka perlu dilakukan pengembangan terhadap *data security system*, dengan penerapan seni ilmu kriptografi menggunakan algoritma *advanced encryption standard* 256 *bit* dan algoritma *base64 encoding* terhadap sistem yang baru, di mana diharapkan dapat mengamankan informasi yang bersifat rahasia dan meningkatkan sistem keamanan data, serta mempercepat proses pendaftaran peserta pelatihan dan sertifikasi.

4.2. Rancangan Pengujian

Dalam rancangan pengujian, maka penulis menggunakan *swimlane diagram* untuk melakukan analisa pada sistem yang sedang berjalan, dapat diperhatikan pada gambar 4.3. aliran jalur proses pendaftaran.



Gambar 4.3. Aliran Jalur Proses Pendaftaran

Adapun alur pada proses pendaftaran yang berjalan adalah sebagai berikut ini.

1. Pendaftar melakukan pendaftaran melalui *form* yang disediakan untuk menjadi seorang peserta pelatihan atau sertifikasi.

2. Pendaftar melakukan pembayaran biaya pelatihan atau sertifikasi.
3. Pendaftar memberikan atau mengirimkan struk kepada *administrator*.
4. *Administrator* menerima struk pembayaran peserta.
5. *Administrator* memeriksa keaslian data pribadi peserta yang tertera pada *form*, dan data pembayaran.
6. *Administrator* melakukan pencatatan *audit*.
7. *Administrator* memvalidasi data peserta.

Untuk tahap rancangan pengujian, maka penulis membutuhkan beberapa alat dan bahan yang mana untuk mendukung kesuksesan terhadap pengujian algoritma *AES* dan *base64* pada objek yang sedang diteliti.

1. Alat dan Bahan

   Untuk dapat melakukan pengujian, maka penulis membutuhkan alat dan bahan berupa *Personal Computer* atau *laptop*, aplikasi *web* yang dibangun oleh penulis, *localhost* berupa *laragon*, *apache HTTP server*, *Open SSL*, *internet*, *PHP* v8, *codeigniter* v4, *bootstrap* v5, *MySQL* v8, *HeidiSQL*, *javascript*, algoritma *advanced encryption standard* 256 *bit*, algoritma *base64 encoding*, *PHPMailer*, dan *web browser*.
2. Objek

   Tujuan penggunaan algoritma *advanced encryption standard* dan algoritma *base64* untuk mengamankan data hasil registrasi peserta pelatihan dan sertifikasi, sehingga objek pada penelitian ini adalah data dari pendaftar pelatihan dan sertifikasi pada JCAL yang melakukan registrasi pada sistem.
3. Pengujian

   Untuk pengujian hanya dapat dilakukan pada *localhost* yang dimiliki oleh penulis, bersifat pribadi dan membutuhkan koneksi *internet*.

4.2.1. Tahapan Pengujian

Adapun tahapan pengujian yang dilakukan adalah sebagai berikut ini.

1. Pengujian algoritma *advanced encryption standard*
2. Pengujian algoritma *base64*
3. *Validation testing*

4.2.2. Pengujian Algoritma *Advanced Encryption Standard*

Pengujian algoritma *advanced encryption standard* memiliki tujuan untuk mengetahui fungsionalitas dari algoritma tersebut apabila dapat bekerja dengan baik. Adapun rencana pengujian algoritma *advanced encryption standard* pada sistem, dapat diperhatikan pada tabel 4.1. pengujian algoritma *AES*.

Tabel 4.1. Pengujian Algoritma *AES*

No.	Pengujian	Hasil yang Diharapkan
1	Data pribadi peserta *disubmit* dalam bentuk *plaintext*	Dapat dienkripsi (*encipher*) kemudian disimpan pada database
2	Data hasil enkripsi (*encipher*) diolah oleh sistem pada halaman *administrator*	Dapat didekripsi (*decipher*) sehingga data yang ditampilkan pada halaman *administrator* berupa *plaintext*
3	Data pribadi peserta diperbarui (*edit*) dalam bentuk *plaintext*	Dapat dienkripsi (*encipher*) kemudian disimpan pada database
4	Melakukan dekripsi (*decipher*) data pribadi peserta tanpa memiliki *cipher key* yang sesuai (*match*) pada proses enkripsi (*encipher*)	Tidak dapat melakukan dekripsi (*decipher*) data, sehingga data aman dari *data breaching* dan *data leakage*
5	Kode program *PHP* pada *codeigniter* v4 untuk *mengenerate random ciphertext characters*	Sistem dapat *mengenerate random ciphertext characters* yang mana untuk dijadikan sebagai *cipher key* pada proses enkripsi (*encipher*) dan dekripsi (*decipher*)

4.2.3. Pengujian Algoritma *Base64*

Pengujian algoritma *base64* memiliki tujuan untuk mengetahui fungsionalitas yang ada dari algoritma tersebut apabila dapat bekerja dengan baik. Adapun rencanan pengujian pada algoritma *base64* dapat diperhatikan pada tabel 4.2. pengujian algoritma *base64*.

Tabel 4.2. Pengujian Algoritma *Base64*

No.	Pengujian	Hasil yang Diharapkan
1	Data hasil enkripsi (*encipher*) *diencode* (*encoding*) menggunakan *base64 encoding*	Dapat *diencode* (*encoding*) dalam bentuk *index base64* kemudian hasil disimpan pada database
2	Data hasil *encoding base64 didecode* (*decoding*)	Dapat *didecode* (*decoding*) sehingga data yang ditampilkan berupa *plaintext*
3	Data diperbarui (*edit*) dalam bentuk *plaintext*	Dapat *diencode* (*encoding*) kemudian disimpan pada database
4	Hasil enkripsi (*encipher*) data pribadi peserta *diencode* (*encoding*) dalam bentuk *index base64*	Dapat *didecode* (*decoding*) dan didekripsi (*decipher*) oleh sistem sehingga data pribadi peserta yang ditampilkan berupa *plaintext* pada halaman *administrator*
5	Kode program *PHP* pada *codeigniter* v4 untuk *mengenerate random bytes* 32 *characters* dalam membuat *token* sebagai proses autentikasi	*Base64 encoding* dapat *mengenerate random bytes* 32 *characters* untuk membuat *token* pada proses autentikasi akun *user* dan *administrator*

4.2.4. *Validation Testing*

Validation testing dilakukan untuk mengetahui apabila validasi-validasi yang ada pada sistem dapat berjalan dengan baik ditujukan sebagai *web security*, dan untuk mengetahui hasil dari penerapan algoritma *AES* dan *base64* dalam mengamankan data peserta ditujukan untuk *data security system*. Adapun rencana pengujian dapat diperhatikan pada tabel 4.3. uji validasi.

Tabel 4.3. Uji Validasi

No.	Pengujian	Hasil yang Diharapkan
1	Membuat kode program untuk *SQL injection attack* pada *field* yang ada dan *submit data*	Sistem dapat melakukan validasi dan menolak data yang diisi pada *field* (*data invalid*)
2	Mengkosongkan setiap data pada *field* yang tertera pada *online form* dan *submit data*	Sistem dapat melakukan validasi dan memberikan *feedback data in these fields are required*
3	Mengisi *alphabet* pada *field* nomor telepon, nomor identitas, nominal *transfer* dan *submit data*	Sistem dapat melakukan validasi dan memberikan *feedback data in these fields must numeric*
4	Mengupload *file excel* pada *field browse a file* yang tertera pada *online form* dan *submit data*	Sistem dapat melakukan validasi dan memberikan *feedback data in these fields must jpg*, *jpeg*, *or png*
5	*Submit data* berupa *file* gambar dengan *format jpg*, *jpeg*, atau *png*	Sistem dapat *merename file* tersebut dengan *random name* untuk keamanan data kemudian menyimpannya pada database dan pada *folder directory* yang telah ditentukan