# PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES-128) PADA SISTEM PENGAMANAN DOKUMEN DINAS PENDIDIKAN DAN KEBUDAYAAN KABUPATEN BONDOWOSO

**SKRIPSI**

oleh

**Aji Mukti Rizkio Pratama**
**122410101085**

**PROGRAM STUDI SISTEM INFORMASI**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS JEMBER**
**2019**

# PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES-128) PADA SISTEM PENGAMANAN DOKUMEN DINAS PENDIDIKAN DAN KEBUDAYAAN KABUPATEN BONDOWOSO

**SKRIPSI**

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan Pendidikan Sarjana (S1) Program Studi Sistem Informasi dan mencapai gelar Sarjana Komputer

oleh

**Aji Mukti Rizkio Pratama**
**122410101085**

**PROGRAM STUDI SISTEM INFORMASI**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS JEMBER**
**2019**

**PERNYATAAN**

Saya yang bertanda tangan dibawah ini:

Nama : Aji Mukti Rizkio Pratama

NIM : 122410101085

menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul "Penerapan Algoritma Kriptografi *Advanced Encryption Standard* (AES-128) Pada Sistem Manajemen Arsip Dinas Pendidikan Dan Kebudayaan Kabupaten Bondowoso", adalah benar-benar hasil karya sendiri, kecuali jika dalam pengutipan substansi disebutkan sumbernya, belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika di kemudian hari pernyataan ini tidak benar.

Jember, Juli 2019

Yang menyatakan,

Aji Mukti Rizkio Pratama

NIM 122410101085

**SKRIPSI**

**PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES-128) PADA SISTEM PENGAMANAN DOKUMEN DINAS PENDIDIKAN DAN KEBUDAYAAN KABUPATEN BONDOWOSO**

Oleh

Aji Mukti Rizkio Pratama

122410101085

**PEMBIMBING**

| | |
|---|---|
| Dosen Pembimbing Utama | : Drs.Antonius Cahya Prihandoko, M.App.Sc., Ph.D. |
| Dosen Pembimbing Pendamping | : Yanuar Nurdiansyah ST,.M.Cs. |

**PENGESAHAN PEMBIMBING**

Skripsi berjudul "Penerapan Algoritma Kriptografi *Advanced Encryption Standard* (AES-128) Pada Sistem Manajemen Arsip Dinas Pendidikan Dan Kebudayaan Kabupaten Bondowoso", telah diuji dan disahkan pada,

hari, tanggal :

tempat : Fakultas Ilmu Komputer Universitas Jember

Disetujui oleh:

| Pembimbing I, | Pembimbing II, |
|---|---|
| Drs.Antonius Cahya Prihandoko, M.App.Sc., Ph.D. | Yanuar Nurdiansyah ST,.M.Cs. |
| NIP 196909281993021001 | NIP 198201012010121004 |

**PENGESAHAN**

Skripsi berjudul "Penerapan Algoritma Kriptografi *Advanced Encryption Standard* (AES-128) Pada Sistem Manajemen Arsip Dinas Pendidikan Dan Kebudayaan Kabupaten Bondowoso", telah diuji dan disahkan pada,

hari, tanggal :

tempat : Program Studi Sistem Informasi Universitas Jember

Tim Penguji:

| Penguji I, | Penguji II, |
|---|---|
| Nelly Oktavia Adiwijaya S.Si.,MT. | Diksy Media Firmansyah S.Kom., M.Kom |
| NIP 198410242009122008 | NIP 760016853 |

Mengesahkan

a.n Dekan

Wakil Dekan I Fakultas Ilmu Komputer,

Drs.Antonius Cahya Prihandoko, M.App.Sc., Ph.D.

NIP 196909281993021001

# DAFTAR ISI

## DAFTAR GAMBAR

# DAFTAR TABEL

# BAB 1. PENDAHULUAN

Bab ini merupakan langkah awal dari penulisan tugas akhir. Bab ini berisi latar belakang, rumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan.

## 1.1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi saat ini sangat pesat. Pengolahan informasi dan pendistribusiannya melalui jaringan telekomunikasi membuka banyak peluang untuk dimanfaatkan di berbagai bidang kehidupan manusia. Salah satunya adalah penggunaan jaringan internet yang sangat memungkinan orang saling bertukar data atau dokumen. Seiring dengan berkembangnya teknologi tersebut, maka banyak orang yang sering menyalah gunakan teknologi informasi untuk mengakses data atau dokumen tanpa ijin pada pihak terkait. Orang-orang yang mengakses data atau dokumen tanpa ijin dapat disebut dengan *hacker*, *cracker*, *carder*, dan lain sebagainya. Sehingga perlu adanya pengaman data atau dokumen tersebut.

Dinas Pendidikan dan Kebudayaan Kabupaten Bondowoso adalah institusi dibawah Pemerintah Kabupaten Bondowoso, salah satu divisi yang terdapat di dalam Dinas Pendidikan dan Kebudayaan adalah divisi pengarsipan, yang memiliki tugas utama yaitu mengelola surat dan dokumen yang keluar dan masuk institusi. Selama ini pengelolaan surat dan dokumen masih menggunakan sistem manual berbasis *spreadsheet* excel, dalam perjalanannya, terdapat masalah yang sering dihadapi, seperti: redundansi, kesulitan dalam pemilahan jenis surat dan yang paling krusial adalah kebocoran dokumen dan data.

Untuk menjaga keamanan dokumen dan surat tugas, diperlukan suatu metode untuk menjaga keamanan informasi yang terdapat dalam kriptografi. Dalam kriptografi proses untuk menyamarkan data atau mengubah *plaintext* menjadi *ciphertext* disebut enkripsi, sedangkan untuk mengubah *chipertext* menjadi *plaintext* disebut dekripsi.

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan dan atau alat khusus (Anwar, 2015). Enkripsi memungkinkan merubah kode-kode yang dapat dimengerti diubah kedalam kode-kode yang tidak dimengerti dengan menggunakan algoritma khusus. Untuk memecahkan kode yang telah dienkripsi dibutuhkan sebuah proses dekripsi.

Pada pengembangan sistem ini akan menggunakan metode enkripsi dengan menggunakan algoritma AES-128. Algoritma AES digunakan pada pengembangan sistem dalam proses enkripsi dan dekripsi. Algoritma AES ini memiliki 3 faktor penilaian yang lebih unggul daripada versi pendahulunya *Data Encryption Standard* (DES) yaitu: keamanan, harga dan karakteristik algoritma. Dalam segi keamanan, metode ini tahan terhadap serangan konvensional (*linear* dan *differential attack*), dan dalam segi ekonomis, metode ini dapat digunakan secara bebas tanpa harus membayar lisensi atau *royalty* (Franc¸ois Dassance, 2007). Penggunaan algoritma AES-128 akan diimplementasikan untuk mengamakan surat dan dokumen pada divisi perngarsipan Dinas Pendidikan dan Kebudayaan Kabupaten Bondowoso. Dengan dikembangkannya sistem ini, diharapkan pengelolaan arsip surat dan pembuatan surat dan dokumen menjadi lebih efektif dan aman.

## 1.2. Rumusan Masalah

Berdasarkan masalah yang telah diuraikan diatas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi algoritma AES-128 dalam mengamankan dokumen dan surat tugas dalam Dinas Pendidikan dan Kebudayaan Kabupaten Bondowoso?
2. Bagaimana tingkat keamanan AES-128 yang diterapkan pada surat masuk dan surat keluar dalam sistem informasi manajemen di Dinas Pendidikan dan Kebudayaan Kabupaten Bondowoso?

## 1.3. Tujuan

Tujuan dari penelitian yang dilakukan dalam skripsi ini adalah sebagai berikut:

1. Mengetahui proses implementasi AES-128 dalam mengamankan dokumen berupa surat keluar dan surat masuk dalam Dinas Pendidikan dan Kebudayaan Kabupaten Bondowoso.
2. Menguji tingkat keamanan algoritma AES-128 dalam sistem informasi manajemen yang dibangun.

## 1.4. Batasan Masalah

Pembahasan yang dilakukan dalam skripsi ini memiliki batasan masalah sebagai berikut:

1. Lingkup penelitian adalah Dinas Pendidikan dan Kebudayaan Bondowoso.
2. Sistem ini digunakan untuk menunjang keamanan pengarsipan Dinas Pendidikan dan Kebudayaan Bondowoso.
3. Sistem menggunakan algoritma kriptografi AES-128.

## 1.5. Sistematika Penulisan

Sistematika penulisan dan urutan skripsi ini disusun sebagai berikut:

1. Pendahuluan

Bab ini menjelaskan tentang latar belakang, perumusan masalah, tujuan dan manfaat, ruang lingkup studi dan sistematika penulisan.

2. Tinjauan Pustaka

   Bab ini menjelaskan tentang materi, informasi, tinjauan pustaka, dan studi terdahulu yang menjadi kerangka pemikiran dalam penelitian.

3. Metodologi Penelitian

   Bab ini menjelaskan tentang metode penelitian yang digunakan dalam penelitian.

4. Pengembangan Sistem

   Bab ini menjelaskan tentang gambaran umum pengembangan sistem, pengujian kinerja, pemeliharaan operasi sistem informasi.

5. Hasil dan Pembahasan

   Bab ini menjelaskan tentang hasil dan pembahasan dari penelitian yang dilakukan.

6. Penutup

   Bab ini berisi tentang kesimpulan dari penelitian dan saran untuk penelitian selanjutnya.

# BAB 2. TINJAUAN PUSTAKA

Pada bagian ini dipaparkan teori-teori dan pustaka yang akan dipakai dalam penelitian. Teori-teori ini berupa teori dari buku literatur dan jurnal. Berikut merupakan teori-teori yang dibahas dalam penelitian.

## 2.1. Penelitian Terdahulu

Penelitian terdahulu yang dilakukan oleh Asri Prameshwari, dan Nyoman Putra Sastra (2008) menyebutkan penelitian tersebut penerapan algoritma ini akan dilakukan pada pengamanan jenis data berjenis dokumen dengan tipe *pdf*, *doc*, *txt*. Hasil yang telah didapat dalam penelitian ini adalah algoritma AES-128 dapat dijadikan salah satu alternatif untuk proses keamanan data dalam hal ini enkripsi dan dekripsi file dokumen, dan hasil dari enkripsi ini bisa dijamin keamanannya selama *symmetry key encryption* tidak bocor ke pihak yang tidak bertanggung jawab.

Penelitian oleh Prastyo (2014) menyebutkan untuk membangun enkripsi file dengan mengkombinasikan kriptografi dengan metode AES dan steganografi dengan metode *Least Significant Bit*. Hasil yang didapat dalam penelitian ini bahwa aplikasi dapat melindungi file dengan membuatnya tidak dapat dibuka secara normal walaupun membuka dengan *open with*, menyisipkan *file* kedalam gambar tidak merusak kualitas gambar secara signifikan, dan *file* dapat terlindungi dengan aman dan tidak rusak, dengan catatan tidak dilakukan *cropping*, penambahan kontras, dan pengurangan kontras.

Penelitian oleh Imron, dkk (2016) menyebutkan metode yang diterapkan pada rancangan program kriptografi implementasi *Advanced Encryption Standard*, dimana program ini dirancang untuk dapat mengenkripsikan dan mendekripsikan data di koperasi NASARI Purwokerto. Dan yang menjadi masukkan program tersebut adalah data digital, sedangkan keluaran dari data tersebut berupa enkripsi/dekripsi. Hasil yang didapatkan dalam penelitian ini adalah algoritma AES

jumlah panjang 256 bit dapat mengamankan data koperasi dengan menghasilkan *cipher* 16 bit, pada *client* dan *server*.

## 2.2. Dokumen

Optimasi berasal dari kata dasar optimal yang berarti terbaik, tertinggi, paling menguntungkan, menjadikan paling baik, dan perbuatan mengoptimalkan (menjadikan paling baik, paling tinggi, dan sebagainya). Secara istilah optimasi adalah proses untuk mencapai hasil ideal atau optimal (Departemen Pendidikan Indonesia, 2008).

Optimasi distribusi cabai merupakan sebuah proses untuk mengoptimalkan pengiriman produksi cabai ke seluruh area yang menjadi cakupan distribusi di Jawa Timur. Optimasi distribusi cabai juga dapat diartikan sebagai suatu bentuk mengoptimalkan perencanaan distribusi dan menjadikannya lebih efektif.

## 2.3. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "gráphein" artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" atau tulisan rahasia (Munir, 2006). Dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Menurut Menezes, kriptografi adalah ilmu yang mempelajari teknik - teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Menurut Schneier, kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan (Munir, 2006).

## 2.4. Pesan, *Plaintext*, dan *Ciphertext*

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Dalam ilmu kriptografi, pesan dapat disebut sebagai *plaintext*. Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi

data, dsb) atau yang disimpan di dalam media perekaman (kertas, *storage*, dsb). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain,maka pesan disandikan ke bentuk lain. Bentuk pesan yang tersandi disebut 17 *ciphertext* atau *histogram* (*cryptogram*). *Ciphertext* harus dapat ditransformasi kembali menjadi *plaintext*.

## 2.5. Enkripsi dan Dekripsi

Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering* (standar nama menurut ISO 7498-2). Proses mengembalikan *ciphertext* menjadi *plaintext*-nya disebut dekripsi (*decryption*) atau deciphering (standard nama menurut ISO 7498-2) (Munir, 2006). Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca).

Proses yang dilakukan untuk mengamankan pesan (yang disebut plainteks) menjadi pesan yang tersembunyi (disebut chiperteks) adalah enkripsi (encryption). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext* disebut deskripsi (*decryption*) (Rahardjo, 1998).

## 2.6. Konsep Algoritma Kriptografi

Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yaitu himpunan yang berisi elemen-elemen *plaintext* dan himpunan yang berisi *ciphertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut.

Misalkan P menyatakan *plaintext* dan C menyatakan *ciphertext*, maka fungsi enkripsi E memetakan P ke C, dan fungsi dekripsi D memetakan C ke P,

$D(C) = P$ ..... Persamaan (1)

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal maka persamaan berikut harus benar,

$D(E(P)) = P$ ..... Persamaan (2)

Dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi menjadi,

$EK(P) = C$ ..... Persamaan (3)

$DK(C) = P$ ..... Persamaan (4)

dan kedua fungsi ini memenuhi:

$DK\big(EK(P)\big) = P$ ..... Persamaan (5)

## 2.7. *Advanced Encryption Standard* (AES)

AES (*Advanced Encryption Standard*) merupakan standar enkripsi yang diperkenalkan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001 sebagai pengganti dari algoritma DES. Algoritma AES yang disebut juga dengan algoritma Rijndael menggunakan teknik enkripsi *block cipher* dengan menggunakan subtitusi terhadap tabel *S-Box* secara langsung terdhadap naskah (*plaintext*).

1. *Key Schedule*

Proses *key schedule* diperlukan untuk mendapatkan subkey-subkey dari kunci utama agar cukup untuk melakukan enkripsi dan dekripsi. Proses ini terdiri dari beberapa operasi, yaitu:

a. Operasi *Rotate*, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
b. Operasi *SubBytes*, pada operasi ini 8 bit dari *subkey* disubstitusikan dengan nilai dari S-Box.
c. Operasi Rcon, operasi ini dapat diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari *user*. Operasi ini menggunakan nilai-nilai dalam Galois *field*. Nilai-nilai dari Rcon kemudian akan di-XOR dengan hasil operasi *SubBytes*.
d. Operasi XOR dengan w[i-Nk] yaitu *word* yang berada pada Nk sebelumnya.

2. *AddRoundKey*

Pada proses ini *subkey* digabungkan dengan *state*. Proses penggabungan ini menggunakan operasi XOR untuk setiap *byte* dari *subkey* dengan *byte* yang bersangkutan dari *state*. Untuk setiap tahap, *subkey* dibangkitkan dari kunci utama

dengan menggunakan proses *key schedule*. Setiap *subkey* berukuran sama dengan *state* yang bersangkutan. Proses *AddRoundKey* diperlihatkan pada gambar 2.1

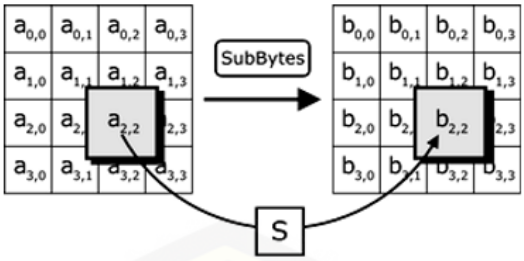

Gambar 2. 1 Proses *AddRoundKey*

*3. SubByte*

Proses *SubBytes* adalah operasi yang akan melakukan substitusi tidak linear dengan cara mengganti setiap *byte state* dengan *byte* pada sebuah tabel yang dinamakan tabel SBox. Sebuah tabel S-Box terdiri dari 16x16 baris dan kolom dengan masing-masing berukuran 1 byte. Tabel S-Box diperlihatkan pada Gambar 2 sedangkan proses *SubBytes* diperlihatkan pada gambar 2.2.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 10 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 20 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 30 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 40 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 50 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 60 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 70 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 80 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 90 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a0 | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b0 | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c0 | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d0 | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e0 | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f0 | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

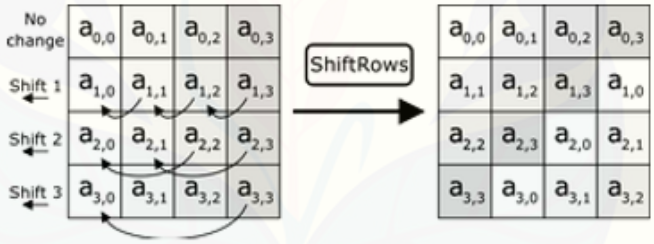
Gambar 2. 2 Tabel *SBox*




Gambar 2. 3 Proses *SubBytes*

4. *ShiftRows*

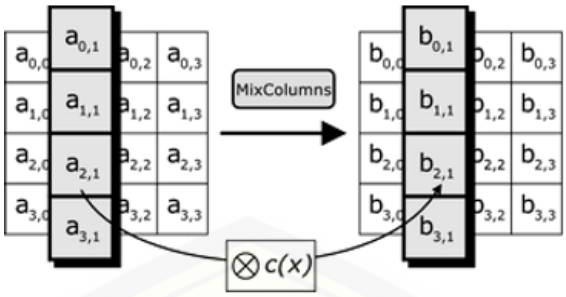
Proses *Shift Rows* akan beroperasi pada tiap baris dari tabel *state*. Proses ini akan bekerja dengan cara memutar *byte-byte* pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbeda-beda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris 3 akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar. Proses *Shift Rows* dapat dilihat pada gambar 4.




Gambar 2. 4 Proses *ShiftRows*

5. *MixColumns*

Proses *Mix Columns* akan beroperasi pada tiap kolom dari tabel *state*. Operasi ini menggabungkan 4 *bytes* dari setiap kolom tabel state dan menggunakan transformasi linier Operasi *Mix Columns* memperlakukan setiap kolom sebagai polinomial 4 suku dalam dan kemudian dikalikan dengan c(*x*) modulo (*x*4+1), dimana c(*x*)=3x3+*x*2+*x*+2. Kebalikkan dari polinomial ini adalah c(*x*)=11x3+13x2+9*x*+14. Operasi *Mix Columns* juga dapat dipandang sebagai perkalian matriks.




Gambar 2. 5 Proses *MixColumns*

# BAB 3. METODE PENELITIAN

Pada bab ini akan dibahas mengenai metodologi penelitian, yaitu tahapan-tahapan yang dilalui oleh peneliti mulai dari analisa kebutuhan data untuk pengembangan sistem.

## 3.1. Jenis Penelitian

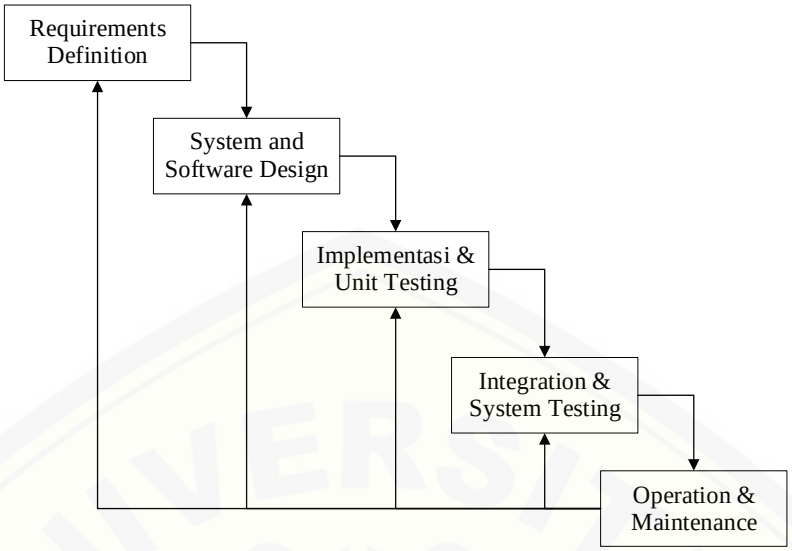
Jenis penelitian yang digunakan dalam membangun sistem keamanan manajemen arsip merupakan penelitian pengembangan, karena tujuan penelitian adalah untuk membangun sebuah sistem manajemen arsip. Penelitian ini bukan jenis penelitian yang ditujukan untuk menemukan teori atau menguji kebenaran dari suatu teori dalam bentuk eksperimentasi. Sedangkan model yang digunakan dalam pengembangannya adalah model *waterfall*.

## 3.2. Tempat dan Waktu Penelitian

Tempat penelitian dilakukan di Dinas Pendidikan dan Kebudayaan Kabupaten Bondowoso bagian pengarsipan. Objek penelitian adalah arsip surat masuk dan surat keluar, serta beberapa kebijakan operasional yang berlaku. Waktu penelitian dilakukan pada bulan Agustus 2016.

## 3.3. Tahapan Penelitian

Tahapan penelitian pengembangan sistem menggunakan model implementasi sistem *waterfall*. Model *waterfall* merupakan model pengembangan sistem yang dilakukan terutur mulai dari mengumpulkan kebutuhan, mendisain sistem, mengimplementasikan sistem, *testing*, dan *maintenance*. Model *waterfall* menurut Pressman (2001) tahapan-tahapan seperti pada Gambar 6.




Gambar 3. 1 Model *Waterfall* (Pressman, 2001)

### 3.3.1. Analisis Kebutuhan *(Requirements Definition)*

Analisis kebutuhan merupakan tahap untuk mengumpulkan data dan informasi yang dibutuhkan untuk membangun sistem. Hasil analisa pembuatan sistem akan dituangkan dalam bentuk SOP (*Statement of Purpose*). Data tersebut dikelompokkan menjadi kebutuhan fungsional dan kebutuhan non fungsional. Untuk memahami sifat program yang akan dibangun, maka harus memahami informasi yang dibutuhkan untuk perangkat lunak, fungsi yang diperlukan, alur, kinerja dan *interface* dari program yang akan dibangun (Pressman, 2001).

1. Tahap Pengumpulan Data

Tahap pengumpulan data bertujuan untuk memperoleh data atau informasi yang dibutuhkan dalam mencapai tujuan penelitian. Pengumpulan data pada penelitian ini dilakukan melalui beberapa cara yaitu:

a. Studi Literatur

Studi literatur berisi uraian tentang teori, temuan dan bahan penelitian lain yang diperoleh dari bahan acuan untuk dijadikan landasan kegiatan penelitian. Studi literatur berisi ulasan, rangkuman data pemikiran penulisan tentang beberapa sumber pustaka (dapat berupa artikel, buku, *slide*, informasi

internet dan lain-lain) tentang topik yang dibahas dan biasanya ditempatkan pada bab awal (Hasibuan, 2007).

b. Wawancara

Wawancara merupakan teknik pengumpulan data survei berupa tanya jawab peneliti dengan narasumber. Wawancara tersebut berupa percakapan langsung antar dua pihak atau lebih untuk mendapatkan informasi secara lisan dengan tujuan untuk memperoleh data yang dapat menjelaskan ataupun menjawab suatu permasalahan penelitian (Hasibuan, 2007).

Peneliti melakukan wawancara kepada pengawas sekolah, dan kepala divisi pengarsipan di dinas pendidikan dan kebudayaan kabupaten Bondowoso. Data yang didapatkan dalam wawancara berupa alur kerja dari divisi pengarsipan.

2. Tahap Pengolahan Data

Alur kerja yang didapat dari wawancara selanjutnya dikembangkan menjadi sistem informasi, celah keamanan yang telah di analisa dari alur kerja tersebut dapat diatasi dengan menggunakan algoritma AES-128, yang terdapat pada keluar dan masuknya surat atau dokumen.

### 3.3.2. Sistem dan Desain Software *(System and Software Design)*

Tahapan berikutnya adalah desain sistem menggunakan *Unified Modeling Languange (UML)* yang dirancang menggunakan konsep *Object-Oriented Programming (OOP).* Berikut pemodelan UML yang digunakan antara lain:

1. *Business Process*

*Business process* merupakan diagram yang menggambarkan proses dari sebuah sistem yang meliputi data apa yang diperlukan lalu data diolah untuk menghasilkan output yang diinginkan.

2. *Usecase Diagram*

Menggambarkan fitur-fitur yang tersedia pada aplikasi yang dibangun dan hak akses setiap actor yang terlibat.

3. *Scenario*

   *Scenario* digunakan untuk menjelaskan cara kerja sistem berdasarkan tugas user yang terdapat pada *usecase diagram*. *Scenario* terdiri dari nama *usecase*, aksi aktor dan reaksi sistem.

4. *Sequence Diagram*

   *Sequence Diagram* digunakan untuk menunjukkan interaksi antar objek pada sebuah sistem berupa pesan yang digambarkan terhadap waktu. *Sequence* merupakan *blueprint* bagi programmer.

5. *Activity Diagram*

   *Activity Diagram* digunakan untuk menggambarkan urutan aktivitas dalam sebuah proses. Aktivitas tersebut sesuai dengan *scenario* yang berisi tugas user dan reaksi sistem dan digambarkan dalam bentuk diagram.

6. *Class Diagram*

   *Class Diagram* menggambarkan struktur dan deskripsi class, package dan objek beserta hubungan satu sama lain seperti pewarisan, asosiasi, dependensi dan lain-lain.

7. *Entity Relationship Diagram*

   *Entity Relationship Diagram* menggambarkan struktur database yang akan dibangun pada sistem.

### 3.3.3. Implementasi Sistem *(Implementation and Unit Testing)*

Tahap implementasi dilakukan berdasarkan desain system yang selanjutnya diubah dalam bentuk pogram, yaitu:

1. Penulisan program menggunakan bahasa pemrograman *Page Hyper Text Processor (PHP)* dengan framework *Codeigniter (CI).*
2. *Database Management System (DBMS)* yang digunakan adalah *MySQL* dengan menggunakan jaringan lokal aplikasi *XAMPP*.

### 3.3.4. Pengujian Sistem *(Integration and System Testing)*

Tahap pengujian sistem bertujuan untuk mengetahui sejauh mana sistem ini dapat berjalan. *Integration Testing* berfungsi untuk mengetahui apakah sistem ini dapat berfungsi dengan baik sesuai dengan yang diharapkan, serta untuk mengetahui letak kekurangan pada sistem. Penelitian ini melakukan pengujian sistem dengan cara sebagai berikut:

1. *Black Box Testing*

   *Black box testing* merupakan metode pengujian perangkat lunak yang memeriksa fungsional dari aplikasi yang berkaitan dengan struktur internal atau kerja. Metode ini memfokuskan pada keperluan fungsional dari software (Pressman, 2001).

2. Uji Keamanan Sistem Informasi

   Uji keamanan sistem informasi digunakan untuk mengetahui celah keamanan apa saja yang terdeteksi pada sistem informasi, celah keamanan ini dapat menjadi kelemahan sistem dan dapat mudah diserang atau diretas oleh *hacker*. Beberapa metode sederhana untuk menguji keamanan sistem adalah sebagai berikut:

   *a. SQL Injection*

   *SQL injection* merupakan aksi *hacking* pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem. SQL injection yaitu serangan yang mirip dengan serangan XSS dalam bahwa penyerang memanfaatkan aplikasi vektor dan juga dengan *Common* dalam serangan XSS.

   *b. Cross-site Scripting*

   XSS merupakan kode HTML atau *Client Script* yang diinjeksikan penyerang pada suatu website. Akibatnya penyerang dapat melewati keamanan di sisi klien, mendapatkan informasi sensitif, dan bahkan menyisipkan aplikasi berbahaya.

3.3.5. Pemeliharaan *(Operation and Maintenance)*

Tahap pemeliharaan dilakukan ketika sistem memiliki kesalahan yang belum terdeteksi sebelumnya, sehingga kesalahan-kesalahan sistem perlu diperbaiki. Pemeliharaan juga dilakukan apabila ssitem mengalami perubahan-perubahan karena permintaan baru dari *user*.

# BAB 4. PENGEMBANGAN SISTEM

Pengembangan sistem ini dilakukan dengan menggunakan menggunakan model *waterfall*. Model ini merupakan metodologi pengembangan perangkat lunak yang mengusulkan pendekatan kepada perangkat lunak sistematik dan sekuensial yang mulai pada tingkat kemajuan sistem pada seluruh analisis, desain, kode, pengujian dan pemeliharaan.

## 4.1. Analisis Kebutuhan

Analisis kebutuhan perangkat lunak dalam penelitian ini yaitu dengan cara mengidentifikasi permasalahan dan dijadikan bahan untuk mulai membangun sistem informasi manajemen arsip menggunakan algoritma AES-128 untuk mengamankan dokumen. Analisis kebutuhan yang dilakukan meliputi proses pengumpulan data kebutuhan fungsional dan kebutuhan non-fungsional. Hasil analisa berpengaruh pada fungsionalitas sistem yang sesuai dengan kebutuhan pengguna.

### 4.1.1. SOP (*Standart Operating Procedure*)

Sistem informasi manajemen arsip pada dinas pendidikan dan kebudayaan kabupaten Bondowoso menggunakan algoritma AES-128 untuk mengamankan dokumen berupa surat masuk dan surat keluar. Tujuan pengembangan sistem untuk membantu divisi pengarsipan di dinas pendidikan dan kebudayaan kabupaten Bondowoso dalam mengamankan dokumen berupa surat masuk dan surat keluar, dengan mengenkripsi dokumen yang akan diunggah.

### 4.1.2. Kebutuhan Fungsional

Berdasarkan data yang terkumpul dalam tahapan analisa, maka diperoleh kebutuhan fungsional dan non fungsional yang dibutuhkan untuk membangun aplikasi optimalisasi distribusi cabai. Kebutuhan fungsional dan non fungsional merupakan hal pokok yang harus dilakukan oleh sistem dalam menerima masukan

untuk diproses sehingga menghasilkan keluaran. Kebutuhan fungsional berisi proses-proses apa saja yang nantinya dibutuhkan oleh sistem informasi manajemen arsip.

1. Sistem mampu mengelola data surat masuk meliputi menambah, mengubah dan menghapus.
2. Sistem mampu mengelola data surat keluar meliputi menambah, mengubah dan menghapus.
3. Sistem mampu mengelola data arsip meliputi menambah, mengubah dan menghapus.
4. Sistem mampu mengajukan peminjaman arsip meliputi menambah, dan mengubah.
5. Sistem mampu mengelola data pegawai meliputi menambah, mengubah dan menghapus.
6. Sistem mampu mengelola data unit kerja meliputi menambah, mengubah dan menghapus.
7. Sistem mampu menampilkan hasil data surat masuk.
8. Sistem mampu menampilkan hasil data surat keluar.
9. Sistem mampu menampilkan data peminjaman arsip.
10. Sistem mampu menampilkan data pegawai.
11. Sistem mampu mengenkripsi dokumen surat masuk.
12. Sistem mampu mengenkripsi dokumen surat keluar.
13. Sistem mampu mendekripsi dokumen surat masuk.
14. Sistem mampu mendekripsi dokumen surat masuk.
15. Sistem mampu mengelola data masa inaktif meliputi menambah, mengubah dan menghapus.
16. Sistem mampu mengelola data retensi, dan unit kerja meliputi menambah, mengubah dan menghapus.
17. Sistem mampu mengelola akun pengguna sistem meliputi menambah, mengubah dan menghapus.

4.1.3. Kebutuhan Non-fungsional

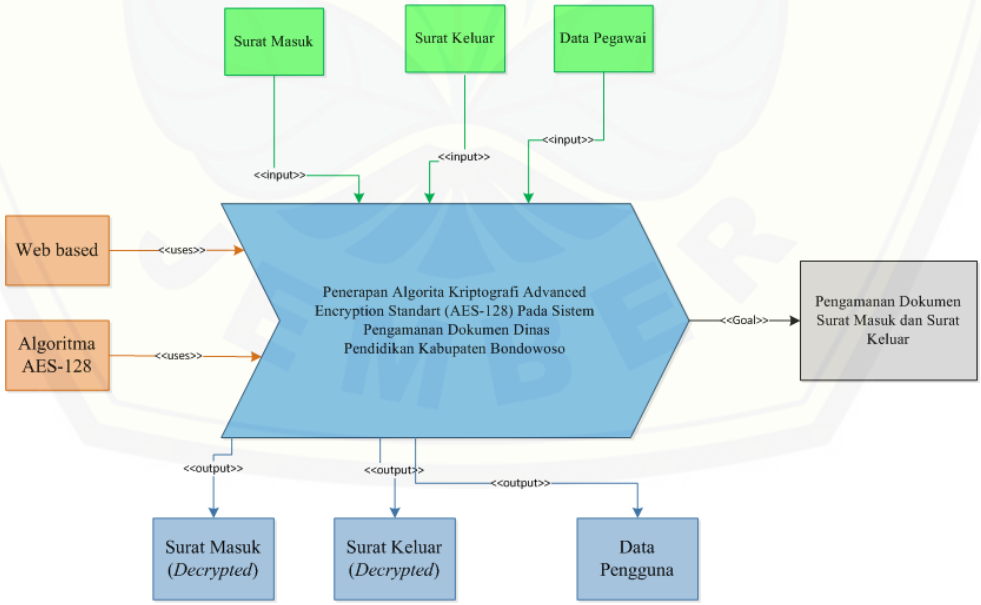
Sedangkan kebutuhan non-fungsional pada sistem ini adalah tampilan aplikasi yang *user friendly* dan aplikasi bisa diakses beberapa user/multi user.

## 4.2. Desain Sistem

Tahapan berikutnya adalah desain sistem menggunakan *Unified Modeling Languange (UML)* yang dirancang menggunakan konsep *Object-Oriented Programming (OOP).* Berikut pemodelan UML yang digunakan antara lain:

### 4.2.1. *Business Process*

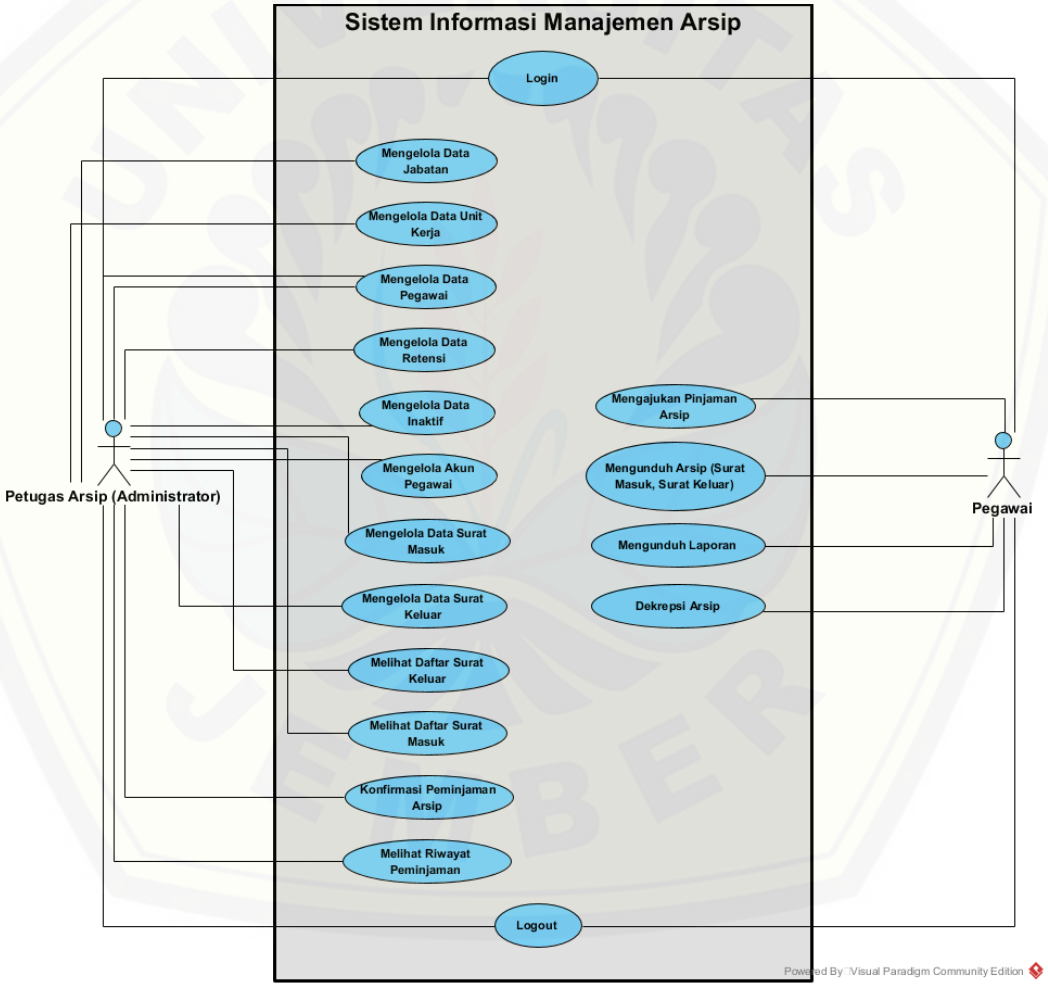
*Business Process* dalam sistem informasi manajemen arsip ini melibatkan petugas arsip dan pegawai. Petugas arsip (administrator) memiliki hak untuk mengelola data master, mengelola surat masuk, surat keluar, dan mengelola akun pengguna. Pegawai melakukan pinjaman arsip, mengunduh lapora, mengunduh arsip, dan mendekripsi arsip. *Business Process* dalam sistem informasi manajemen arsip dapat dilihat pada gambar 4.1.




Gambar 4. 1 Business Process Sistem Informasi Manajemen Arsip

### 4.2.2. *Usecase Diagram*

*Usecase Diagram* merupakan kumpulan dari serangkaian kegiatan yang dapat dilakukan oleh sebuah sistem. *Usecase* diagram berisi tentang fitur yang akan dikembangkan dalam sistem penunjang keputusan pembelian padi terbaik, selain hal diagram ini juga berisi hak akses yang diberikan untuk setiap pengguna dalam mengakses setiap fitur yang ada. Gambar *usecase diagram* ditunjukkan pada gambar 4.2 yang terdapat 2 aktor yang dapat mengakses sistem yaitu Petugas Arsip, dan Pegawai.




Gambar 4. 2 *Use Case Diagram*

Fitur-fitur yang terdapat pada sistem beserta aktor yang berhak mengakses fitur tersebut berdasarkan *usecase diagram* dijelaskan pada tabel 4.1.

Tabel 4. 1 Definisi Aktor

| No. | Aktor | Deskripsi |
|---|---|---|
| 1 | Petugas Arsip | Aktor petugas arsip bertugas sebagai *administrator* sistem informasi manajemen dengan mengelola hak akses, mengelola data master, mengelola surat masuk dan surat keluar. Aktor petugas arsip dapat melakukan *login* dan *logout*, mengelola data master (mengelola data jabatan, mengelola data unit kerja, mengelola data retensi, mengelola data inaktif, mengelola akun pegawai, konfirmasi peminjaman arsip, dan melihat riwayat peminjaman), mengelola data surat masuk, mengelola data surat keluar, melihat daftar surat masuk, dan melihat daftar surat keluar. |
| 2 | Pegawai | Aktor pegawai mempunyai hak akses normal, pegawai dapat melakukan *login* dan *logout* mengajukan pinjaman arsip, mengunduh arsip, mengunduh laporan, dekripsi arsip pada sistem informasi manajemen arsip. |

Tabel 4. 2 Definisi *Use Case Diagram*

| No. | *Use case* | Penjelasan |
|---|---|---|
| UC-01 | *Login* | Merupakan *use case* yang yang menggambarkan proses masuk dalam sistem. |
| UC-02 | Mengelola Data Surat Masuk | Merupakan *use case* yang menggambarkan proses menampilkan, menambah, dan mengubah data surat masuk dari dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |

| No. | *Use case* | Penjelasan |
|---|---|---|
| UC-03 | Mengelola Data Surat Keluar | Merupakan *use case* yang menggambarkan proses menampilkan, menambah, dan mengubah data surat keluar dari dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-04 | Melihat Daftar Surat Masuk | Merupakan *use case* yang menggambarkan proses menampilkan daftar surat masuk dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-05 | Melihat Daftar Surat Keluar | Merupakan *use case* yang menggambarkan proses menampilkan daftar surat keluar dari dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-06 | Mengelola Data Jabatan | Merupakan *use case* yang menggambarkan proses menampilkan, menambah, dan mengubah data jabatan dari dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-07 | Mengelola Data Unit Kerja | Merupakan *use case* yang menggambarkan proses menampilkan, menambah, dan mengubah data unit kerja dari dinas pendidikan dan |

| No. | *Use case* | Penjelasan |
|---|---|---|
| | | kebudayaan Bondowoso dalam sistem informasi manajemen arsip. |
| UC-08 | Mengelola Data Retensi | Merupakan *use case* yang menggambarkan proses menampilkan, menambahkan, mengubah, dan menghapus data retensi dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip. |
| UC-09 | Mengelola Data Inaktif | Merupakan *use case* yang menggambarkan proses menampilkan, menambahkan, mengubah, dan menghapus data inaktif dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip. |
| UC-10 | Mengelola Data Pegawai | Merupakan *use case* yang menggambarkan proses melihat, menambah, mengubah, dan menghapus akun pegawai dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip. |
| UC-11 | Mengelola Akun Pegawai | Merupakan *use case* yang menggambarkan proses melihat, menambah, mengubah, dan menghapus akun pegawai dinas pendidikan dan |

| No. | *Use case* | Penjelasan |
|---|---|---|
| | | kebudayaan Bondowoso dalam sistem informasi manajemen arsip. |
| UC-12 | Konfirmasi Peminjaman Arsip | Merupakan *use case* yang menggambarkan proses menampilkan, dan mengkonfirmasi data peminjaman arsip dari dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-13 | Melihat Riwayat Peminjaman | Merupakan *use case* yang menggambarkan proses menampilkan arsip yang terenkripsi dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-14 | Mengajukan Pinjaman Arsip | Merupakan *use case* yang menggambarkan proses menampilkan, mengubah, menambah, dan menghapus data kabupaten dan kota yang termasuk dalam wilayah provinsi Jawa Timur |
| UC-15 | Mengunduh Arsip | Merupakan *use case* yang menggambarkan proses menampilkan, mengunduh data dinas pendidikan dan kebudayaan Bondowoso dalam sistem informasi manajemen arsip |
| UC-16 | Mengunduh Laporan | Merupakan *use case* yang menggambarkan proses menampilkan, mengubah, menambah, dan menghapus |

| No. | *Use case* | Penjelasan |
|---|---|---|
| | | data kabupaten dan kota yang termasuk dalam wilayah provinsi Jawa Timur |
| UC-17 | Dekripsi Arsip | Merupakan *use case* yang menggambarkan proses keluar dari sistem |
| UC-18 | *Logout* | Merupakan *use case* yang menggambarkan proses keluar dari sistem |

4.2.3. *Scenario*

*Scenario* digunakan untuk menjelaskan cara kerja sistem berdasarkan tugas user yang terdapat pada *usecase diagram*. *Scenario* terdiri dari nama *usecase*, aksi aktor dan reaksi sistem.

1. *Scenario* Mengelola Data Surat Masuk

Pada *scenario* "Mengelola Data Surat Masuk" menjelaskan tentang alur dimana aktor petugas arsip memasukkan data surat masuk, dimana data berupa data pengajuan surat, dan mengunggah surat masuk yang akan di enkripsi. *Usecase scenario* dari *usecase* "Mengelola Data Surat Masuk" dapat dilihat di tabel 4.3.

Tabel 4. 3 *Scenario* Mengelola Data Surat Masuk

| **Nomor *Use case*** | **UC-02** |
|---|---|
| Nama | Mengelola Data Surat Masuk |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih fitur surat masuk pada menu arsip |

lanjut dilanjutkan

| | |
|---|---|
| *Postcondition* | Pegawai arsip berhasil mengisi *form* dan mengunggah dokumen surat masuk ke dalam sistem |

| ***SCENARIO* NORMAL**<br>**"Mengelola Data Surat Masuk"** | |
|---|---|
| **Aktor** | **Sistem** |
| 1. Memilih menu Arsip, dan memilih sub menu Surat Masuk | |
| | 2. Menampilkan formulir surat masuk, menampilkan kop surat yang terisi secara otomatis, dan jenis surat dengan nilai Penting,. Rahasia, dan Tidak Penting |
| 3. Mengisi formulir Surat Masuk | |
| | 4. Menampilkan atribut nomor surat, kop surat, judul, tanggal surat masuk, perihal, pengirim, penerima, jenis surat, tanggal retensi, tanggal inaktif, dokumen, password dan keterangan. |
| 5. Mengunggah dokumen dan mengisi *password* dokumen | |
| | 6. *Password* dokumen terisi 16 |

lanjut dilanjutkan

| | | | |
|---|---|---|---|
| | | | digit akan di *hash* dengan SHA-256 dan dokumen akan ter enkripsi dengan algoritma AES-128 |
| 7. | Memilih tombol simpan | | |
| | | 8. | Mengunggah formulir surat masuk, dan mengunggah dokumen yang terenkripsi ke dalam tabel *upload* |
| | ***SCENARIO* ALTERNATIF**<br>**"Melihat Data Surat Masuk"**<br>Jika aktor memilih daftar surat masuk pada halaman surat masuk | | |
| | **Aktor** | | **Sistem** |
| 7a. | Memilih "Daftar Surat Masuk" pada akhir formulir | | |
| | | 7b. | Menampilkan surat masuk yang dengan tabel berisi nomor surat, perihal, pengirim, dan keterangan. |
| | | 7c. | Menampilkan tombol Detail, Ubah, dan Hapus. |

2. *Usecase scenario* Mengelola Data Surat Keluar

Pada *usecase scenario* "Mengelola Data Surat Keluar" menjelaskan tentang alur dimana aktor petugas arsip memasukkan data surat keluar, dimana data berupa

data pengajuan surat, dan mengunggah surat keluar yang akan di enkripsi. *Usecase scenario* dari *usecase* "Mengelola Data Surat Keluar" dapat dilihat di tabel 4.

Tabel 4. 4 *Scenario* Mengelola Surat Keluar

| **Nomor *Use case*** | | **UC-03** |
|---|---|---|
| Nama | | Mengelola Data Surat Keluar |
| Aktor | | Petugas Arsip |
| *Precondition* | | Petugas arsip memilih fitur surat keluar pada menu arsip |
| *Postcondition* | | Pegawai arsip berhasil mengisi *form* dan mengunggah dokumen surat keluar ke dalam sistem |
| ***SCENARIO* NORMAL**<br>**"Mengelola Data Surat Keluar"** | | |
| **Aktor** | | **Sistem** |
| 1. | Memilih menu Arsip, dan memilih sub menu Surat Keluar | |
| | | 2. Menampilkan formulir surat keluar, menampilkan kop surat yang terisi secara otomatis, dan jenis surat dengan nilai Penting, Rahasia, dan Tidak Penting. |
| 3. | Mengisi formulir Surat Keluar | |

lanjut

dilanjutkan

| | | | |
|---|---|---|---|
| | | 4. | Menampilkan atribut nomor surat, kop surat, judul, tanggal surat masuk, perihal, pengirim, penerima, jenis surat, tanggal retensi, tanggal inaktif, dokumen, password dan keterangan. |
| 5. | Mengunggah dokumen dan mengisi *password* dokumen | | |
| | | 6. | *Password* dokumen terisi 16 digit akan di *hash* dengan SHA-256 dan dokumen akan terenkripsi dengan algoritma AES-128 |
| 7. | Memilih tombol simpan | | |
| | | 8. | Mengunggah formulir surat keluar, dan mengunggah dokumen yang terenkripsi ke dalam tabel *upload* |
| **_SCENARIO_ ALTERNATIF** | | | |
| **“Melihat Data Surat Keluar”** | | | |
| Jika aktor memilih daftar surat masuk pada halaman surat keluar | | | |
| **Aktor** | | **Sistem** | |
| 7a. | Memilih “Daftar Surat Keluar” pada akhir formulir | | |

lanjut

dilanjutkan

| | | |
|---|---|---|
| | 7b. | Menampilkan surat keluar dengan tabel atribut berisi nomor surat, perihal, pengirim, dan keterangan. |
| | 7c. | Menampilkan tombol Detail, Ubah, dan Hapus. |

3. *Scenario* Mengunduh Arsip

Pada *scenario* "Mengunduh Arsip" menjelaskan tentang alur dimana aktor petugas arsip dan pegawai mengunduh arsip, dimana data berupa data surat masuk atau keluar. Dokumen yang terunduh akan terdekripsi oleh sistem. Illustrasi *scenario* dari *usecase* "Mengunduh Arsip" dapat dilihat di Lampiran A (Gambar A1).

4. *Scenario* Mengajukan Pinjaman Arsip

Pada *scenario* "Mengajukan Pinjaman Arsip" menjelaskan tentang alur aktor pegawai melakukan peminjaman arsip, data arsip berupa surat keluar atau surat masuk sesuai dengan permintaan aktor. Illustrasi *scenario* dari *usecase* "Pinjaman Arsip" dapat dilihat di Lampiran A (Gambar A2).

5. *Scenario* Konfirmasi Peminjaman Arsip

Pada *scenario* "Konfirmasi Pinjaman Arsip" menjelaskan tentang alur aktor petugas arsip mengelola peminjaman arsip, petugas arsip melakukan konfirmasi peminjaman arsip dari aktor pegawai. Illustrasi *scenario* dari *usecase* "Mengelola Pinjaman Arsip" dapat dilihat di Lampiran A (Gambar A3).

6. *Scenario* Mengelola Data Unit Kerja

Pada *scenario* "Mengelola Data Unit Kerja" menjelaskan tentang alur aktor petugas arsip mengelola data unit kerja, petugas arsip memasukkan data unit kerja dari pegawai, data unit kerja berguna untuk mengetahui unit kerja dari pegawai yang mengajukan pinjaman. Illustrasi *scenario* dari *usecase* "Mengelola Data Unit Kerja" dapat dilihat di Lampiran A (Gambar A4).

7. *Scenario* Mengelola Data Jabatan

Pada *scenario* "Mengelola Data Jabatan" menjelaskan tentang alur dimana aktor petugas arsip mengelola data jabatan, dimana petugas arsip memasukkan data unit kerja dari pegawai, data jabatn berguna untuk mengetahui jabatan dari pegawai yang mengajukan pinjaman. Illustrasi *scenario* dari *usecase* "Mengelola Data Jabatan" dapat dilihat di Lampiran A (Gambar A5).

8. *Scenario* Mengelola Data Pegawai

Pada *scenario* "Mengelola Akun Pegawai" menjelaskan tentang alur dimana aktor petugas arsip mengelola data pegawai, dimana petugas arsip memasukkan data dari pegawai, data unit kerja berguna untuk mengetahui pegawai yang mengajukan pinjaman. Illustrasi *scenario* dari *usecase* "Mengelola Data Pegawai" dapat dilihat di Lampiran A (Gambar A6).

9. *Scenario* Mengelola Data Retensi

Pada *scenario* "Mengelola Data Retensi" menjelaskan tentang alur dimana aktor petugas arsip mengelola data retensi, dimana petugas arsip memasukkan data retensi atau tingkat kepentingan dari arsip. Illustrasi *scenario* dari *usecase* "Mengelola Data Retensi" dapat dilihat di Lampiran A (Gambar A7).

10. *Scenario* Mengelola Data Inaktif

Pada *scenario* "Mengelola Data Inaktif" menjelaskan tentang alur aktor petugas arsip mengelola data inaktif, dimana petugas arsip memasukkan data inaktif atau tingkat kepentingan dari arsip sebelum arsip masuk dalam pemberkasan dan tidak dapat dilihat lagi. Illustrasi *scenario* dari *usecase* "Mengelola Data Inaktif" dapat dilihat di Lampiran A (Gambar A8).

11. *Scenario* Mengelola Akun Pegawai

Pada *usecase scenario* "Mengelola Data Akun Pegawai" menjelaskan tentang alur aktor petugas arsip mengelola data akun pegawai, dimana petugas arsip menambah, mengubah dan menghapus akun pegawai untuk mendapatkan akses masuk pada sistem. Illustrasi *scenario* dari *usecase* "Mengelola Data Akun Pegawai" dapat dilihat di Lampiran A (Gambar A9).

12. *Scenario* Mengunduh Laporan

Pada *usecase scenario* "Mengelola Data Akun Pegawai" menjelaskan tentang alur aktor petugas arsip mengelola data akun pegawai, dimana petugas arsip menambah, mengubah dan menghapus akun pegawai untuk mendapatkan akses masuk pada sistem. Illustrasi *scenario* dari *usecase* "Mengelola Data Akun Pegawai" dapat dilihat di Lampiran A (Gambar A10).

13. *Scenario* Dekripsi Arsip

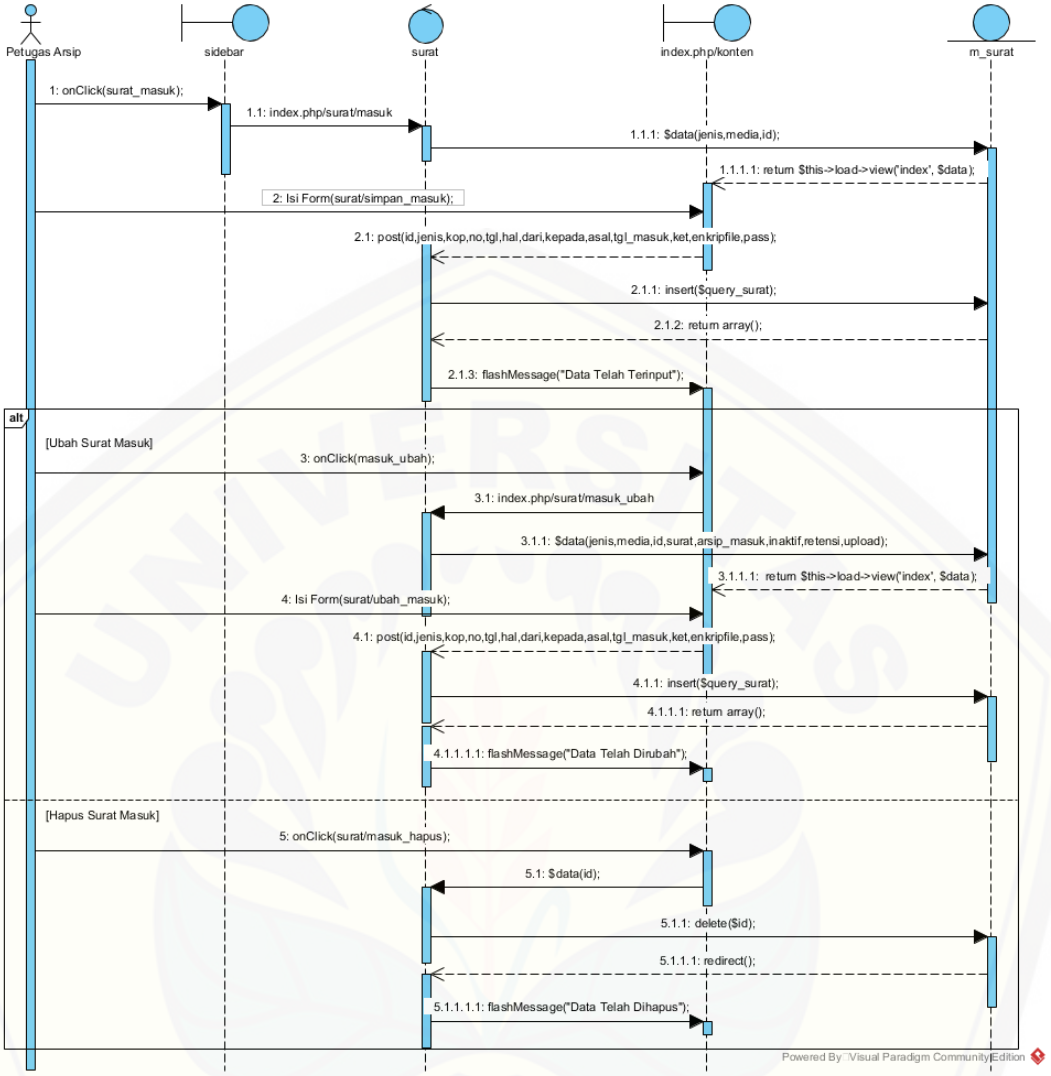
Pada *usecase scenario* "Mengelola Data Akun Pegawai" menjelaskan tentang alur aktor petugas arsip mengelola data akun pegawai, dimana petugas arsip menambah, mengubah dan menghapus akun pegawai untuk mendapatkan akses masuk pada sistem. Illustrasi *scenario* dari *usecase* "Mengelola Data Akun Pegawai" dapat dilihat di Lampiran A (Gambar A11).

### 4.2.4. *Sequence Diagram*

*Sequence Diagram* digunakan untuk menunjukkan interaksi antar objek pada sebuah sistem berupa pesan yang digambarkan terhadap waktu. *Sequence* merupakan *blueprint* bagi *programmer*.

1. *Sequence* Mengelola Data Surat Masuk

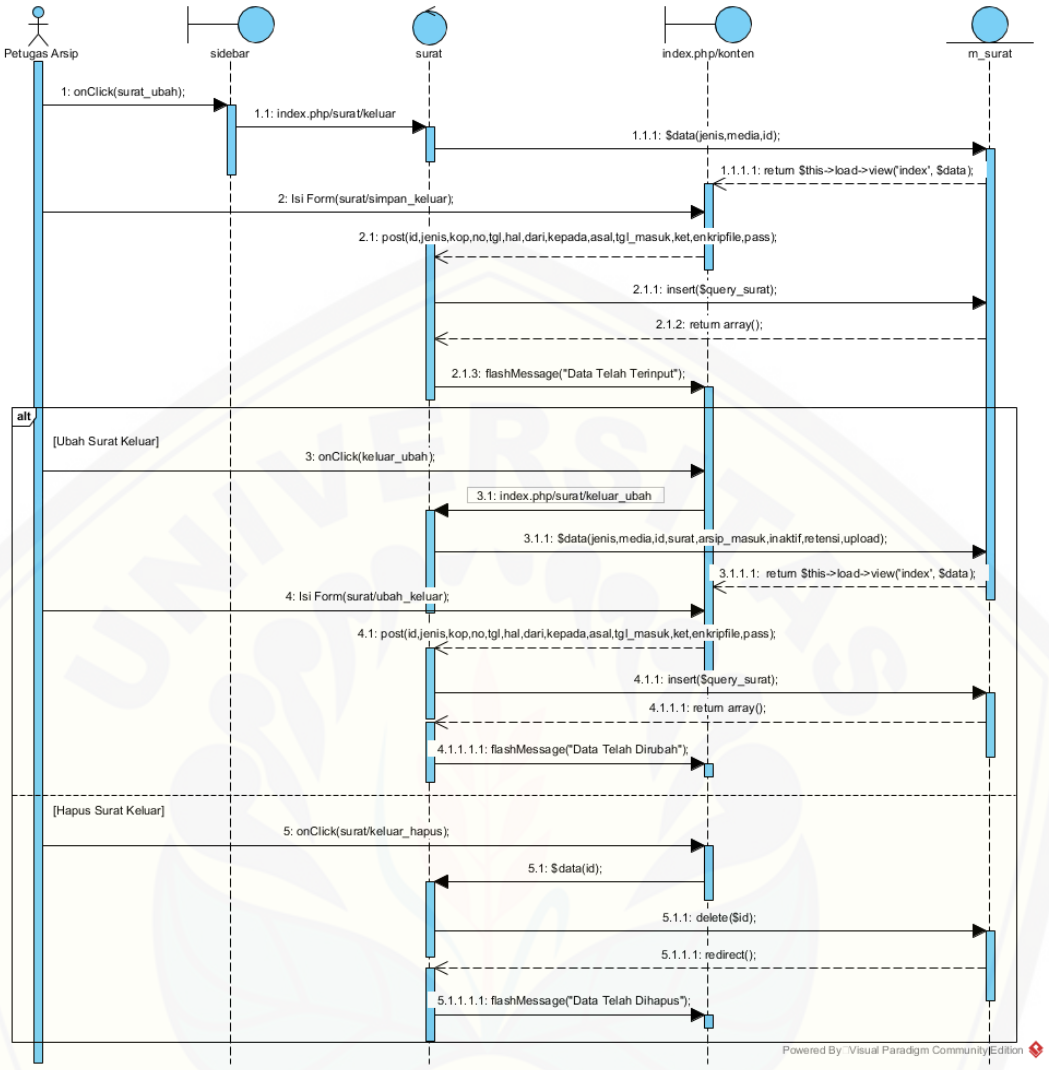
Penjelasan urutan reaksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengelola data surat masuk, aktor petugas arsip dapat mengisi formulir dan mengunggah dokumen pada fitur ini. Dalam fitur ini dokumen yang diunggah akan terenkripsi dengan AES-128 dan *password* akan di *hash* dengan metode SHA-256, data formulir surat masuk akan masuk dalam tabel surat_masuk sedangkan dokumen yang terenkripsi dan *password* masuk dalam tabel *upload* dalam *database*. Proses dari fitur ini dapat dilihat pada gambar 4.3.




Gambar 4. 3 *Sequence Diagram* Mengelola Surat Masuk

2. *Sequence* Mengelola Data Surat Keluar

Penjelasan urutan reaksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengelola data surat keluar, aktor petugas arsip dapat mengisi formulir dan mengunggah dokumen pada fitur ini. Dalam fitur ini dokumen yang diunggah akan terenkripsi dengan AES-128 dan *password* akan di *hash* dengan metode SHA-256, data formulir surat keluar akan masuk dalam tabel surat_keluar sedangkan dokumen yang terenkripsi dan *password* masuk dalam tabel upload dalam *database*. Proses dari fitur ini dapat dilihat pada gambar 4.4.




Gambar 4. 4 Sequence Diagram Mengelola Surat Keluar

3. *Sequence* Mengunduh Arsip

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* mengunduh data arsip, aktor petugas arsip dan pegawai yang dituju dapat mengisi megunduh dan mengunggah dokumen pada fitur ini. Dalam fitur ini dokumen yang diunduh telah terenkripsi dengan AES-128 dan *password* telah di *hash* dengan metode SHA-256, untuk melihat dokumen kedalam bentuk utuh, aktor perlu mendekripsi dokumen yang telah terenkripsi sebelumnya. Aktor mengunggah dokumen yang telah terunduh sebelumnya, dan diproses untuk dapat melihat dokumen kedalam bentuk semula. Proses dari fitur ini dapat dilihat pada gambar 10 berikut.

4. *Sequence* Mengajukan Pinjaman Arsip

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor pegawai. Dalam fitur ini pegawai mengajukan pinjaman arsip dengan mengisi formulir ke di fitur Pinjam Arsip. *Diagram sequence* mengajukan pinjaman arsip dapat dilihat pada Lampiran B (Gambar B1).

5. *Sequence* Mengelola Peminjaman Arsip

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor petugas arsip. Dalam fitur ini petugas arsip, mengelola peminjaman arsip dengan mengkonfirmasi berkas apa saja yang akan dipinjam oleh *user* pegawai di fitur Kelola Arsip. *Diagram sequence* mengajukan kelola arsip dapat dilihat pada Lampiran B (Gambar B2)

6. *Sequence* Mengunduh Laporan

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor petugas arsip. Dalam fitur ini petugas arsip mengunduh laporan di fitur Unduh Laporan, dengan mengisi jenis laporan apa saja yang ingin di unduh dalam rentang waktu tertentu. *Diagram sequence* mengajukan unduh laporan dapat dilihat pada Lampiran B (Gambar B3).

7. *Sequence* Mengelola Data Unit Kerja

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data unit kerja di fitur Data Unit Kerja, aktor dapat menambahkan, mengubah, dan mengahapus data unit kerja. *Diagram sequence* mengajukan mengelola data unit kerja dapat dilihat pada Lampiran B (Gambar B4).

8. *Sequence* Mengelola Data Jabatan

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data jabatan di fitur Data Jabatan, aktor dapat menambahkan, mengubah, dan mengahapus data jabatan. *Diagram sequence*

mengajukan mengelola data unit jabatan dapat dilihat pada Lampiran B (Gambar B5).

9. *Sequence* Mengelola Data Pegawai

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data pegawai di fitur Data Pegawai, aktor dapat menambahkan, mengubah, dan mengahapus data pegawai. *Diagram sequence* mengajukan mengelola data pegawai dapat dilihat pada Lampiran B (Gambar B6).

10. *Sequence* Mengelola Data Retensi

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data retensi di fitur Data Retensi, aktor dapat menambahkan, mengubah, dan mengahapus data retensi. *Diagram sequence* mengajukan mengelola data retensi dapat dilihat pada Lampiran B (Gambar B7).

11. *Sequence* Mengelola Data Inaktif

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data inaktif di fitur Data Inaktif, aktor dapat menambahkan, mengubah, dan mengahapus data inaktif. *Diagram sequence* mengajukan mengelola data inaktif dapat dilihat pada Lampiran B (Gambar B8).

12. *Sequence* Mengelola Akun Pegawai

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data akun pegawai di fitur Akun Pegawai, aktor dapat menambahkan, mengubah, dan mengahapus data akun pegawai. *Diagram sequence* mengajukan mengelola data akun pegawai dapat dilihat pada Lampiran B (Gambar B.9).

13. *Sequence* Mengelola Data Jabatan

Penjelasan urutan aksi aktor dan reaksi sistem pada diagram *sequence* pada fitur mengajukan pinjaman arsip yang dilakukan oleh aktor *administrator*. Dalam fitur ini *administrator* mengelola data jabatan di fitur Data jabatan, aktor dapat menambahkan, mengubah, dan mengahapus data jabatan. *Diagram sequence* mengajukan mengelola data jabatan dapat dilihat pada Lampiran B (Gambar B.10).

### 4.2.5. *Activity Diagram*

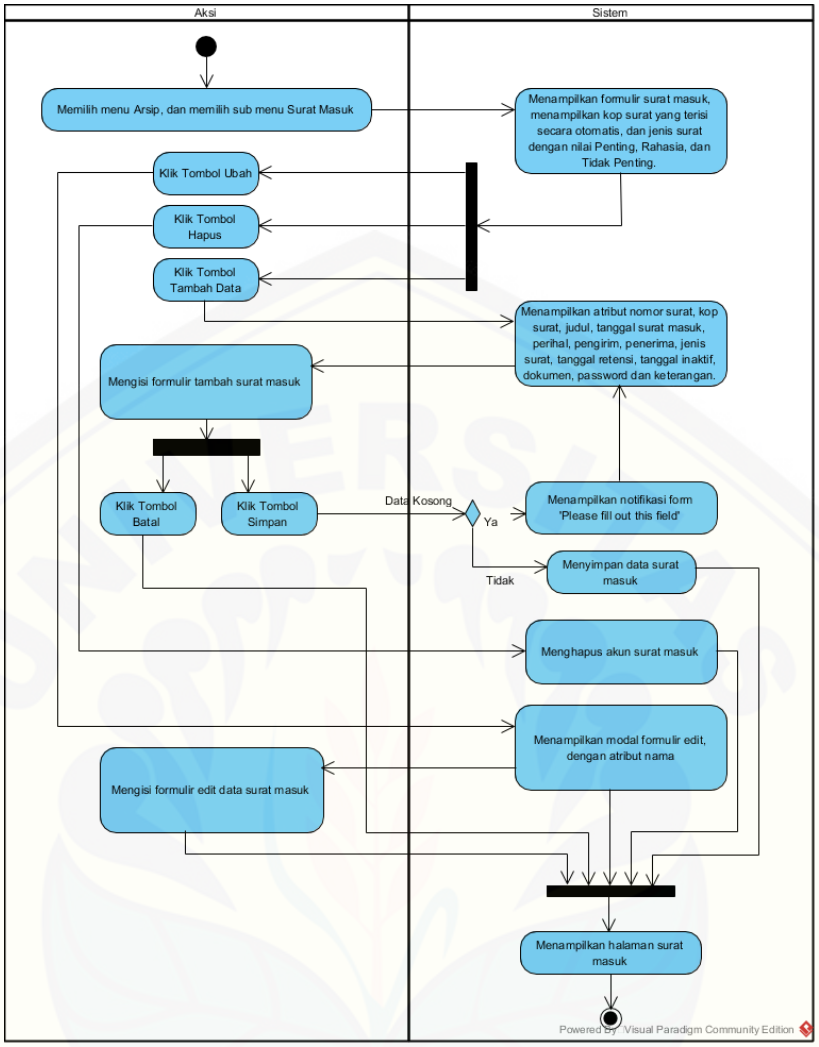
*Activity Diagram* digunakan untuk menggambarkan urutan aktivitas dalam sebuah proses. Aktivitas tersebut sesuai dengan *scenario* yang berisi tugas aktor dan reaksi sistem dan digambarkan dalam bentuk diagram.

1. *Activity Diagram* Mengelola Data Surat Masuk.

*Activity diagram* mengelola data surat masuk menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data surat masuk diuraikan sebagai berikut:

a. Petugas arsip memilih menu surat masuk, dan reaksi sistem menampilkan halaman surat masuk.
b. Petugas arsip mengisi *form* yang tersedia di halaman surat masuk, dengan atribut nomor kop surat, tanggal surat masuk, tanggal surat diterima, perihal, pengirim, penerima, unggah surat, *password* surat, tanggal inaktif, tanggal retensi, dan keterangan.
c. Petugas arsip memilih tombol simpan dan reaksi sistem menyimpan, menggungah, dan mengenkripsi surat. Setelah surat tersimpan sistem mengalihkan ke halaman utama halaman surat masuk.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat di gambar 4.5.




Gambar 4. 5 *Activity Diagram* Mengelola Data Surat Masuk

2. *Activity Diagram* Mengelola Data Surat Keluar.

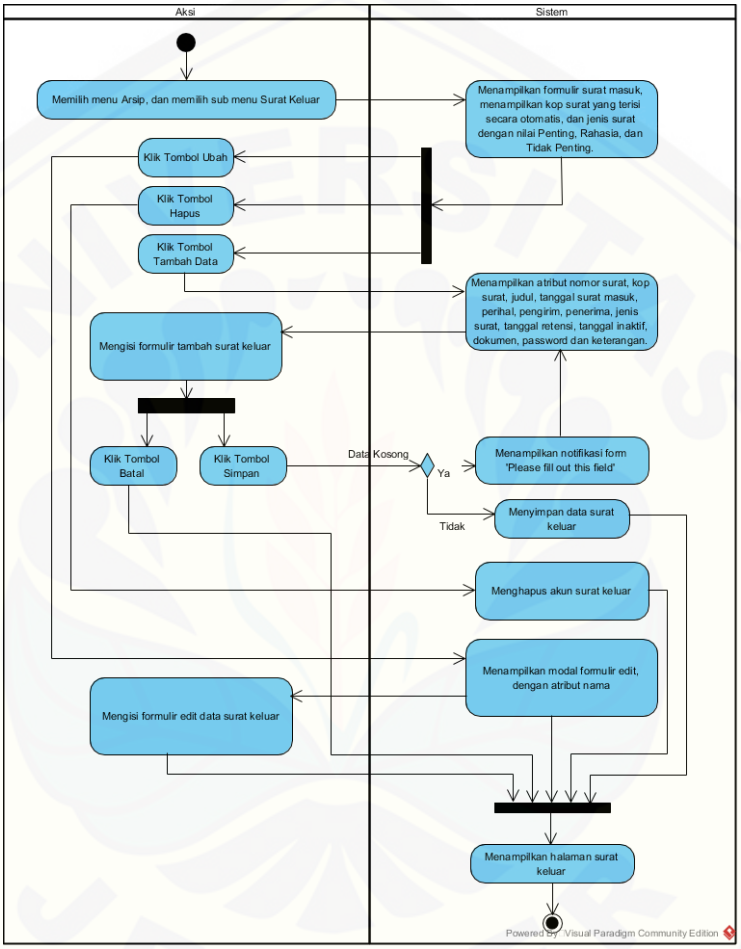
*Activity diagram* mengelola data surat keluar menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data surat masuk diuraikan sebagai berikut:

a. Petugas arsip memilih menu surat keluar, dan reaksi sistem menampilkan halaman surat masuk.

b. Petugas arsip mengisi *form* yang tersedia di halaman surat keluar, dengan atribut nomor kop surat, tanggal surat masuk, tanggal surat diterima, perihal, pengirim, penerima, unggah surat, *password* surat, tanggal inaktif, tanggal retensi, dan keterangan.

c. Petugas arsip memilih tombol simpan dan reaksi sistem menyimpan, menggungah, dan mengenkripsi surat. Setelah surat tersimpan sistem mengalihkan ke halaman utama halaman surat keluar.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat di gambar 4.6.




Gambar 4. 6 Activity Diagram Mengelola Data Surat Keluar

3. *Activity Diagram* Mengunduh Arsip.

*Activity diagram* mengunduh arsip menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh pegawai. Aliran aktivitas pegawai saat mengunduh data arsip diuraikan sebagai berikut:

a. Pegawai memilih menu arsip, dan reaksi sistem menampilkan halaman data arsip.

b. Pegawai dapat melihat daftar arsip yang berupa surat keluar dan surat masuk yang telah diajukan untuk peminjaman.
c. Pegawai dapat mengunduh arsip yang terenkripsi, dan reaksi sistem menampilkan dialog unduh pada *browser*.
d. Pegawai mendekrip arsip yang telah terunduh, dengan masuk pada halaman enkrip file, dan reaksi sistem menampilkan halaman enkrip file dengan atribut *form* unggah arsip, dan *password* arsip.
e. Pegawai mengunggah arsip yang telah terenkrip, dan memasukkan password arsip yang telah disediakan, dan reaksi sistem menampilkan dialog unduh arsip pada *browser*.

Ilustrasi aktivitas pegawai dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C1).

4. *Activity Diagram* Mengajukan Pinjaman Arsip.

*Activity diagram* mengajukan pinjam arsip menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh pegawai. Aliran aktivitas pegawai saat mengajukan pinjaman arsip diuraikan sebagai berikut:

a. Pegawai memilih submenu pinjaman arsip pada menu arsip, dan reaksi sistem menampilkan halaman pinjaman arsip dengan tabel yang memiliki atribut nama arsip, jenis arsip, tanggal peminjaman, status pinjam, tombol edit, tombol hapus, dan tombol tambah data.
b. Pegawai memilih tombol tambah data dan reaksi sistem menampilkan form halaman tambah pinjam arsip dengan atribut *form* nama peminjam, tanggal peminjaman, jenis surat, surat yang dipinjam, dan tombol simpan.
c. Pegawai memilih tombol simpan dan reaksi sistem mengalihkan halaman pinjaman arsip.

Ilustrasi aktivitas pegawai dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C2).

5. *Activity Diagram* Mengelola Peminjaman Arsip.

*Activity diagram* mengelola pinjam arsip menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola pinjaman arsip diuraikan sebagai berikut:

a. Petugas arsip memilih menu peminjaman arsip, dan reaksi sistem menampilkan halaman mengelola pinjaman arsip dengan tabel yang memiliki atribut nama pegawai, nama arsip, jenis arsip, tanggal peminjaman, status pinjam, dan tombol tolak, tombol konfirmasi.
b. Petugas arsip memilih konfirmasi, dan reaksi sistem menampilkan dialog konfirmasi.
c. Petugas arsip memilih tombol oke, dan reaksi sistem akan mengalihkan ke halaman peminjaman arsip, peminjaman disetujui oleh petugas arsip.
d. Petugas arsip memilih tolak, dan reaksi sistem menampilkan dialog konfirmasi.
e. Petugas arsip memilih tombol oke, dan reaksi sistem akan mengalihkan ke halaman peminjaman arsip, peminjaman ditolak oleh petugas arsip.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C3).

6. *Activity Diagram* Mengelola Data Unit Kerja.

*Activity diagram* mengelola data unit kerja menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data unit kerja diuraikan sebagai berikut:

a. Petugas arsip memilih submenu data unit kerja pada menu master data, dan reaksi sistem menampilkan halaman mengelola data unit kerja dengan tabel yang memiliki atribut nama unit kerja, tombol edit, tombol hapus, dan menampilkan form dengan atribut nama unit kerja, id unit kerja, dan tombol simpan
b. Petugas arsip mengisi form dengan atribut nama unit kerja.
c. Petugas arsip memilih simpan, dan reaksi sistem akan mengalihkan ke halaman data unit kerja arsip.
d. Petugas arsip dapat melihat data unit kerja pada tabel daftar unit kerja.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C4).

7. *Activity Diagram* Mengelola Data Jabatan.

*Activity diagram* mengelola data jabatan menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data jabatan diuraikan sebagai berikut:

a. Petugas arsip memilih submenu data jabatan pada menu master data, dan reaksi sistem menampilkan halaman mengelola data jabatan dengan tabel yang memiliki atribut nama jabatan, tombol edit, tombol hapus, dan menampilkan form dengan atribut nama jabatan, id jabatan, dan tombol simpan
b. Petugas arsip mengisi form dengan atribut nama jabatan.
c. Petugas arsip memilih simpan, dan reaksi sistem akan mengalihkan ke halaman data jabatan.
d. Petugas arsip dapat melihat data unit kerja pada tabel daftar jabatan.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C5).

8. *Activity Diagram* Mengelola Data Pegawai.

*Activity diagram* mengelola data pegawai menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data pegawai diuraikan sebagai berikut:

a. Petugas arsip memilih submenu data pegawai pada menu master data, dan reaksi sistem menampilkan halaman mengelola data jabatan dengan tabel yang memiliki atribut nama jabatan, tombol edit, tombol hapus, dan menampilkan form dengan atribut nama jabatan, id pegawai, unit kerja, jabatan, nip, dan tombol simpan
b. Petugas arsip mengisi form dengan atribut nama jabatan, id pegawai, unit kerja, jabatan, dan nip.
c. Petugas arsip memilih simpan, dan reaksi sistem akan mengalihkan ke halaman data pegawai.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C6).

9. *Activity Diagram* Mengelola Data Retensi.

*Activity diagram* mengelola data retensi menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data retensi diuraikan sebagai berikut:

a. Petugas arsip memilih submenu data retensi pada menu master data, dan reaksi sistem menampilkan halaman mengelola data inaktif dengan tabel yang memiliki atribut jenis retensi, batas waktu, tombol edit, tombol hapus, dan menampilkan form dengan atribut id retensi, retensi, batas waktu, dan tombol simpan
b. Petugas arsip mengisi form dengan id retensi, retensi, dan batas waktu.
c. Petugas arsip memilih simpan, dan reaksi sistem akan mengalihkan ke halaman data retensi.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C7).

10. *Activity Diagram* Mengelola Data Inaktif.

*Activity diagram* mengelola data inaktif menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data inaktif diuraikan sebagai berikut:

a. Petugas arsip memilih submenu data inaktif pada menu master data, dan reaksi sistem menampilkan halaman mengelola data inaktif dengan tabel yang memiliki atribut jenis inaktif, batas waktu, tombol edit, tombol hapus, dan menampilkan form dengan atribut id inaktif, inaktif, batas waktu, dan tombol simpan
b. Petugas arsip mengisi form dengan id inaktif, inaktif, dan batas waktu.
c. Petugas arsip memilih simpan, dan reaksi sistem akan mengalihkan ke halaman data inaktif.

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C8).

11. *Activity Diagram* Mengelola Akun Pegawai.

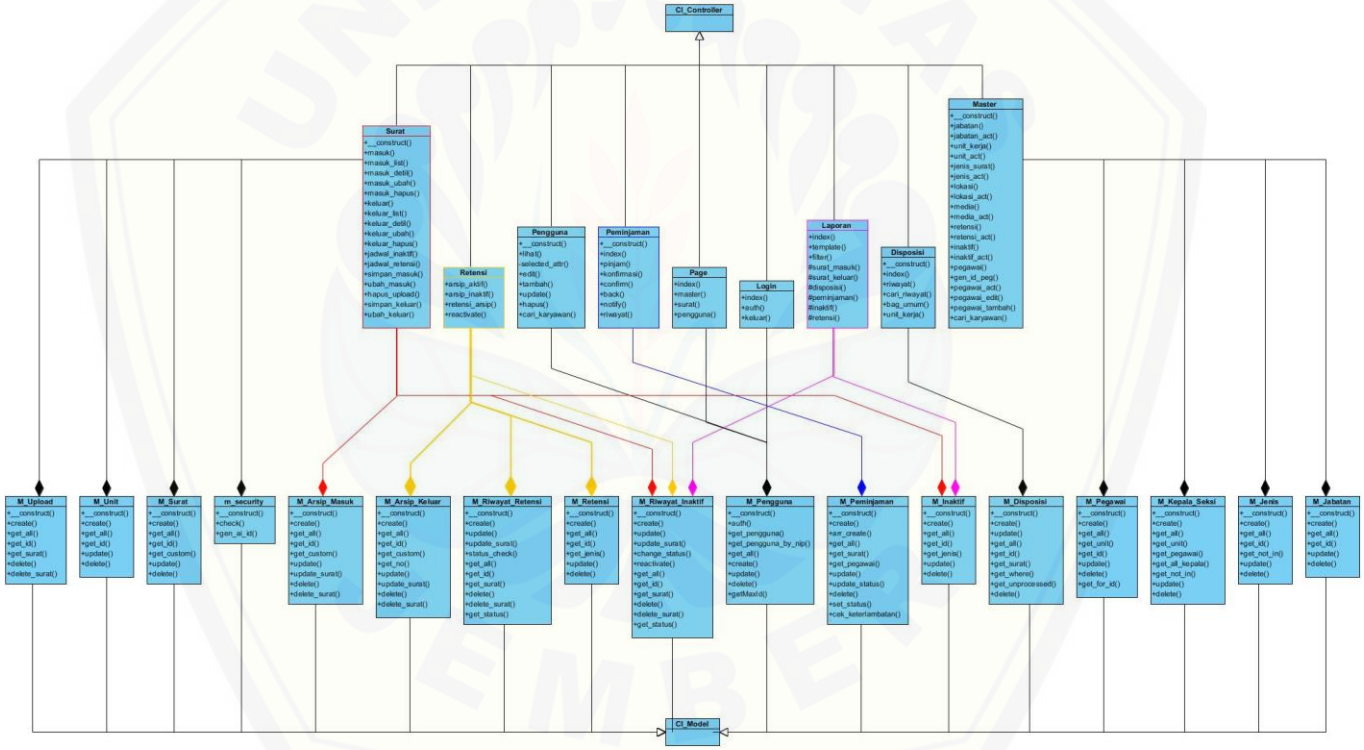
*Activity diagram* mengelola data akun pegawai menggambarkan alur aktivitas dan proses yang terjadi dalam sistem yang dilakukan oleh petugas arsip. Aliran aktivitas petugas arsip saat mengelola data akun pegawai diuraikan sebagai berikut:

a. Petugas arsip memilih submenu data akun pegawai pada menu master data, dan reaksi sistem menampilkan halaman mengelola data akun pegawai dengan tabel yang memiliki atribut jenis inaktif, batas waktu, tombol edit, tombol tambah data, dan tombol hapus.
b. Petugas memilih tombol tambah data, dan reaksi sistem akan menampilkan halaman tambah data pegawai.
c. Petugas arsip mengisi form dengan atribut nip, nama pegawai, dan password.
d. Petugas memilih tombol simpan, dan reaksi sistem akan menampilkan halaman akun pegawai

Ilustrasi aktivitas petugas arsip dan proses yang terjadi dalam sistem dapat dilihat pada lampiran C (Gambar C9).

### 4.2.6. *Class Diagram*

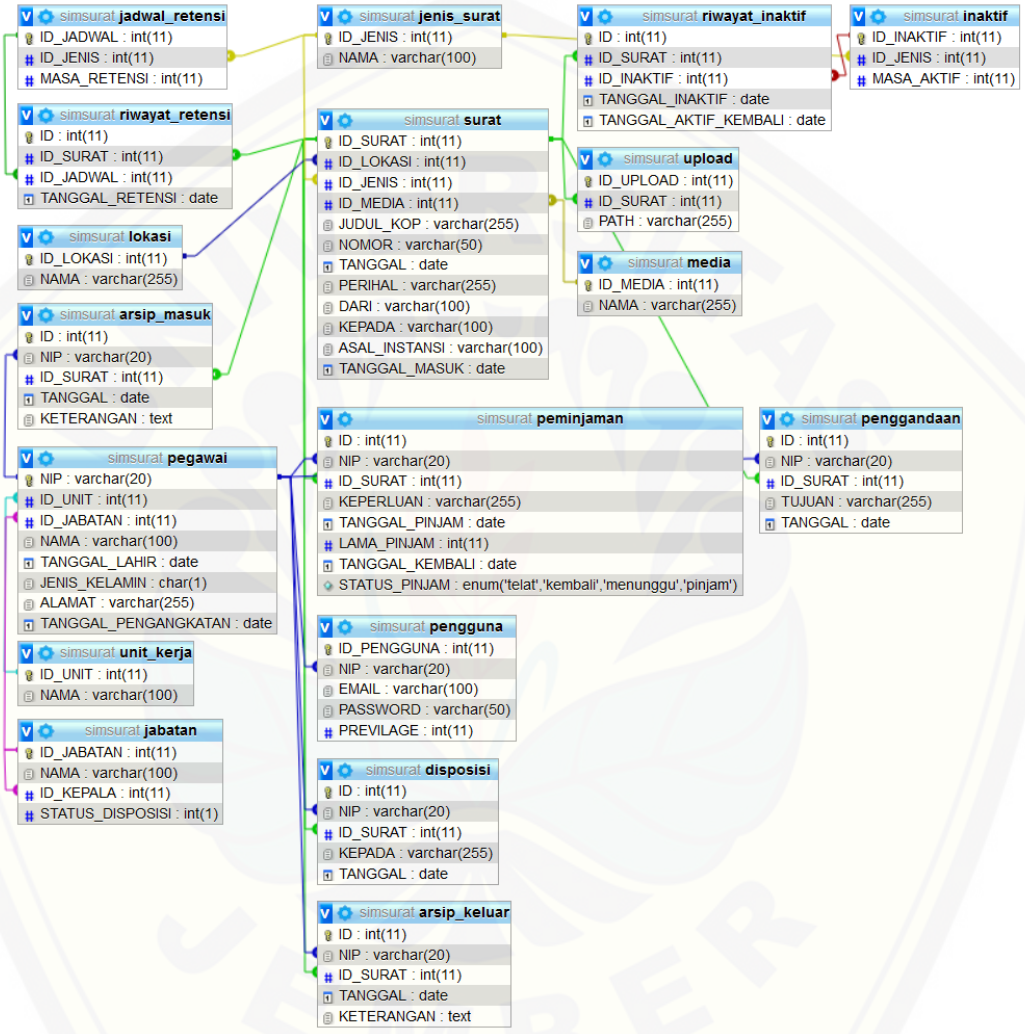
*Class Diagram* pada sistem informasi manejemen arsip ini mengambarkan struktur dan deskripsi *class*, *package* dan objek beserta hubungan satu sama lain seperti pewarisan, asosiasi, dependensi dan lain-lain. *Class diagram* pada sistem informasi manajemen arsip ditunjukkan pada gambar 13 berikut.




Gambar 4. 7 *Class Diagram* Sistem Informasi Manajemen Arsip

### 4.2.7. *Entity Relationship Diagram*

*Entity Relationship Diagram* menggambarkan struktur database yang akan dibangun pada sistem. *Entity Relationship Diagram* dijelaskan pada gambar 14 berikut.




Gambar 4. 8 Entity Relationship Diagram Sistem Informasi Manajemen

# BAB 6. PENUTUP

Pada bab ini merupakan bagian terakhir dari penulisan skripsi yang berisi tentang kesimpulan dan saran yang didapat selama proses penelitian ini berlangsung. Kesimpulan yang telah didapat diharapkan dapat menjadi acuan dalam pengembangan lebih lanjut dari sistem infomasi manajemen arsip dinas pendidikan kebudayaan Bondowoso.

## 6.1. Kesimpulan

Berdasarkan pada hasil penelitian ini, diperoleh beberapa analisis yang didapat selama berlangsungnya penelitian ini. Kesimpulan dari penelitian yang telah dilakukan adalah sebagai berikut:

1. Implementasi algoritma kriptografi AES-128 dalam mengamankan dokumen pada sistem informasi manajemen yaitu dengan menggunakan *library* AES yang di implementasikan pada *framework codeigniter*, dengan menggunakan AES-128 dengan mode enkripsi CTR. *Library* aes disisipkan pada proses unggah *file* dengan melakukan operasi perhitungan XOR antara *cipher key* (kunci) dengan *plain text* (dokumen), dimana kunci sudah dikonversi terlebih dahulu ke dalam bilangan hexadecimal dan sudah melakukan operasi perputaran 10 kali, operasi perputaran ini dikenal dengan sebutan add*RoundKey*. Lalu proses perhitungan dilakukan terhadap isi dokumen (*plain text*) yang juga telah dikonversi ke dalam bilangan *hexadecimal* diterapkan operasi penjumlahan XOR terhadap hasil *addRoundKey* (menyesuaikan dengan perputaran yang dilakukan). Password atau *key* melalui proses *hashing* dengan menggunakan SHA-256.
2. AES-128 yang digunakan untuk mengamankan surat masuk dan surat tugas, aman di implementasikan, dari percobaan *bruteforce* yang dilakukan oleh penulis membutuhkan waktu yang lama dengan rentang waktu 1-2 hari untuk mendekripsi 1 baris kalimat. Sedangkan implementasi AES-128 yang

digunakan pada sistem informasi manajemen arsip diterapkan pada keseluruhan *file*.

## 6.2. Saran

Pengembangan lebih lanjut dari sistem informmasi manajemen ini diharapkan dapat memberikan kemudahan dalam mengelola dan mengamankan berkas dan dokumen dalam divisi pengarsipan di dinas kebudayaan dan pendidikan bondowoso yang lebih aman lagi, dengan menggunakan kombinasi algoritma kriptografi modern dalam mengamankan dokumen yang berupa surat masuk dan surat keluar.

# DAFTAR PUSTAKA


Andri, Y. M. (2009). Implementasi Algoritma DES,RSA dan Algoritma Kompresi LZQ pada berkas digital. *Skripsi*.

Asri Prameshwari, N. P. (2008). Implementasi Algoritma Advanced Encryption Standart (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Jurnal Eksplora Informatika*, 1-7.

Barbosa, L. S. (2015, September 21). *POWER8 in-core cryptography*. Dipetik Mei 25, 2019, dari www.ibm.com: https://www.ibm.com/developerworks/library/se-power8-in-core-cryptography/index.html

Departemen Pendidikan Indonesia. (2008). *Kamus Besar Bahasa Indonesia.* Jakarta: Balai Pustaka.

Dony, A. (2008). *Pengantar ilmu kriptografi, teori, analisis, dan implementasi.* Yogyakarta: Penerbit Andi.

Franc¸ois Dassance, A. V. (2007). Combined Attacks on the AES Key Schedule. *Inside Secure*, 3-7.

Hasibuan, M. S. (2007). *Manajemen Sumber Daya Manusia Perusahaan.* Bandung: PT. Bumi Aksa.

Kersting, W. H. (2017). *Distribution System Modeling and Analysis.* Florida, United States: CRC Press.

Mohammad Imron, I. A. (2016). Implementasi Pengamanan Data Koperasi Menggunakan Algoritma Advanced Encryption Standard (AES). *Jurnal STMIK AMIKOM Purwokerto*, 1-8.

Munir, R. (2008). *Belajar Ilmu Kriptografi*. Yogyakarta: Penerbit Andi.

Prastyo, A. K. (2014). Pengamanan Data Dengan Metode Advanced Encryption Standard dan Metode Least Significant Bit. *Skripsi*, 1-9.

Pressman, R. S. (2001). *Software Engineering: A Practitioner's Approach, Fifth Edition.* New York: McGraw-Hill Higher Education ©2001.

Schneir, B. (2008). *Applied Cryptography : Protocols, Algorithm, and Source Code in C.* New Jersey: Wiley.

# LAMPIRAN

## A. Lampiran *Scenario*

A1. Lampiran *Scenario* Mengunduh Arsip

| **Nomor *Use case*** | **UC-15** |
|---|---|
| Nama | Mengunduh Arsip |
| Aktor | Pegawai |
| *Precondition* | Pegawai memilih menu dokumen dan memilih menu arsip |
| *Postcondition* | Pegawai berhasil mengunduh arsip |
| ***SCENARIO* NORMAL**<br>**"Mengunduh Arsip"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Dokumen, dan memilih sub menu Arsip | |
| | 2. Menampilkan tabel arsip dengan atribut sebagai berikut:<br>- Nama Arsip<br>- Instansi<br>- Jenis Surat<br>- Tanggal Pinjam<br>- Aksi unduh |
| 3. Memilih tombol unduh pada kolom aksi | |

| | | | |
|---|---|---|---|
| | | 4. | Menampilkan jendela unduh pada *browser* |
| 5. | Memilih *save* dan tombol oke | | |
| | | 6. | Arsip terunduh dalam computer, dengan ekstensi dokumen ".enc" |

A2. Lampiran *Scenario* Mengajukan Pinjaman Arsip

| **Nomor *Use case*** | **UC-14** |
|---|---|
| Nama | Mengajukan Pinjaman Arsip |
| Aktor | Pegawai |
| *Precondition* | Pegawai memilih menu peminjaman dan memilih sub menu peminjaman arsip |
| *Postcondition* | Pegawai berhasil mengajukan pinjaman arsip |
| ***SCENARIO* NORMAL**<br>**"Mengajukan Pinjaman Arsip"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Peminjaman, dan memilih sub menu Peminjaman Arsip | |
| | 2. Menampilkan tabel daftar arsip dengan atribut sebagai berikut:<br>- Nomer Surat<br>- Asal Instansi |

| | | |
|---|---|---|
| | | - Jenis Surat<br>- Tanggal Masuk<br>- Perihal<br>- Pilih |
| | | 3. Menampilkan formulir peminjaman arsip dengan atribut sebagai berikut:<br>- NIP Peminjam<br>- Tanggal Kembali<br>- Keterangan |
| 4. | Memilih *checkbox* pilih pada arsip yang dipinjam | |
| 5. | Mengisi formulir dengan kondisi sebagai berikut:<br>- NIP peminjam sesuai dengan *session login*<br>- Tanggal kembali telah ditentukan oleh sistem<br>- Keterangan pinjam disertai dengan alasan yang jelas | |
| 6. | Memilih tombol simpan | |
| | | 7. Menyimpan data pengajuan pinjaman arsip. |
| **_SCENARIO_ ALTERNATIF**<br>**"Mengajukan Pinjaman Arsip"** | | |

| Jika aktor tidak memilih arsip dan mengisi formulir | |
|---|---|
| **Aktor** | **Sistem** |
| 7a. Memilih tombol simpan | |
| | 7b. Menampilkan peringatan "r*equired to fill*" pada formulir yang belum terisi |

A3. Lampiran *Scenario* Konfirmasi Pinjaman Arsip

| **Nomor *Use case*** | **UC-12** |
|---|---|
| Nama | Konfirmasi Pinjaman Arsip |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu peminjaman dan memilih sub menu konfirmasi peminjaman |
| *Postcondition* | Petugas arsip berhasil mengkonfirmasi peminjaman |
| ***SCENARIO* NORMAL**<br>**"Konfirmasi Peminjaman"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Peminjaman, dan memilih sub menu Konfirmasi Peminjaman | |
| | 2. Menampilkan tabel konfirmasi peminjaman dengan atribut sebagai berikut: |

| | | | |
|---|---|---|---|
| | | | - Nomer Surat<br>- Peminjam<br>- Surat<br>- Keperluan<br>- Tanggal Pinjam<br>- Tanggal Kembali<br>- Status<br>- Opsi |
| 3. | Memilih opsi konfirmasi kepada peminjam dengan status menunggu | | |
| | | 4. | Peminjam dengan status menunggu menjadi telah dikonfirmasi. |
| **_SCENARIO_ ALTERNATIF**<br>**"Konfirmasi Peminjaman"**<br>Jika aktor tidak menyetujui peminjam | | | |
| **Aktor** | | **Sistem** | |
| 7a. | Memilih opsi tolak kepada peminjam dengan status menunggu | | |
| | | 7b. | Peminjam dengan status menunggu menjadi ditolak |

A4. Lampiran *Scenario* Mengelola Data Unit Kerja

| | |
|---|---|
| **Nomor *Use case*** | **UC-07** |

| | |
|---|---|
| Nama | Mengelola Data Unit Kerja |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu data master dan memilih sub menu unit kerja |
| *Postcondition* | Petugas arsip berhasil mengelola data unit kerja |

**_SCENARIO_ NORMAL**

**"Mengelola Data Unit Kerja"**

| | **Aktor** | | **Sistem** |
|---|---|---|---|
| 1. | Memilih menu Data Master, dan memilih sub menu Unit Kerja | | |
| | | 2. | Menampilkan tabel daftar unit kerja dengan atribut sebagai berikut:<br>- Nomer<br>- Unit Kerja<br>- Opsi |
| | | 3. | Menampilkan formulir dengan atribut sebagai berikut:<br>- Nama unit kerja |
| 4. | Mengisi formulir tambah data unit kerja | | |
| 5. | Memilih tombol simpan | | |
| | | 6. | Menyimpan data unit kerja |

| | | | |
|---|---|---|---|
| 7. | Memilih tombol edit` | | |
| | | 8. | Menampilkan *modal* formulir edit, dengan atribut nama |
| 9. | Mengisi formulir edit data unit kerja pada modal | | |
| 10. | Memilih tombol simpan | | |
| | | 11. | Menyimpan data edit unit kerja |
| 12. | Memilih tombol hapus | | |
| | | 13. | Menampilkan dialog konfirmasi, dengan opsi Ya dan Tidak |
| 14. | Memilih opsi Ya | | |
| | | 15. | Menghapus data unit kerja |

A5. Lampiran *Scenario* Mengelola Data Jabatan

| **Nomor *Use case*** | **UC-06** |
|---|---|
| Nama | Mengelola Data Jabatan |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu data master dan memilih sub menu jabatan |
| *Postcondition* | Petugas arsip berhasil mengelola data jabatan |
| ***SCENARIO* NORMAL**<br>**"Mengelola Data Jabatan"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Data Master, dan memilih sub menu Jabatan | |
| | 2. Menampilkan tabel daftar jabatan dengan atribut sebagai berikut:<br>- Nomer<br>- Jabatan<br>- Kepala<br>- Disposisi<br>- Opsi |
| | 3. Menampilkan formulir dengan atribut sebagai berikut:<br>- Nama jabatan<br>- Kepala<br>- Disposisi |

| | | | |
|---|---|---|---|
| 4. | Mengisi formulir tambah data jabatan | | |
| 5. | Memilih tombol simpan | | |
| | | 6. | Menyimpan data jabatan |
| 7. | Memilih tombol edit` | | |
| | | 8. | Menampilkan *modal* formulir edit, dengan atribut sebagai berikut:<br>- Nama jabatan<br>- Kepala<br>- Disposisi |
| 9. | Mengisi formulir edit data jabatan pada *modal* | | |
| 10. | Memilih tombol simpan | | |
| | | 11. | Menyimpan data edit jabatan |
| 12. | Memilih tombol hapus | | |
| | | 13. | Menampilkan dialog konfirmasi, dengan opsi Ya dan Tidak |
| 14. | Memilih opsi Ya | | |
| | | 15. | Menghapus data jabatan |

A6. Lampiran *Scenario* Mengelola Data Pegawai

| **Nomor *Use case*** | **UC-10** |
|---|---|
| Nama | Mengelola Data Pegawai |

| | |
|---|---|
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu data master dan memilih sub menu pegawai |
| *Postcondition* | Petugas arsip berhasil mengelola data pegawai |

| ***SCENARIO* NORMAL**<br>**"Mengelola Data Pegawai"** | |
|---|---|
| **Aktor** | **Sistem** |
| 1. Memilih menu Data Master, dan memilih sub menu Pegawai | |
| | 2. Menampilkan tabel daftar jabatan dengan atribut sebagai berikut:<br>- NIP<br>- Nama<br>- Jenis Kelamin<br>- Jabatan<br>- Unit Kerja<br>- Alamat<br>- Opsi |
| 3. Memilih tombol tambah pegawai | |
| | 4. Menampilkan halaman forumlir data pegawai dengan atribut sebagai berikut:<br>- NIP<br>- Nama |

| | | |
|---|---|---|
| | | - Tanggal Lahir<br>- Tanggal Pengangkatan<br>- Jenis Kelamin<br>- Jabatan<br>- Unit Kerja<br>- Alamat |
| 5. | Mengisi formulir tambah data pegawai dengan kondisi sebagai berikut:<br>- NIP secara otomatis terisi jika tanggal lahir dan tanggal pengangkatan telah terisi | |
| 6. | Memilih tombol simpan | |
| | | 7. Menyimpan data pegawai |
| 8. | Memilih tombol edit | |
| | | 9. Menampilkan halaman edit data pegawai dengan atribut sebagai berikut:<br>- NIP<br>- Nama<br>- Tanggal Lahir<br>- Tanggal Pengangkatan<br>- Jenis Kelamin<br>- Jabatan<br>- Unit Kerja<br>- Alamat |

| | |
|---|---|
| 10. Mengisi formulir tambah data pegawai dengan kondisi sebagai berikut:<br>- NIP secara otomatis terisi jika tanggal lahir dan tanggal pengangkatan telah terisi | |
| 11. Memilih tombol simpan | |
| | 12. Menyimpan edit data pegawai |
| 13. Memilih tombol hapus | |
| | 14. Menampilkan dialog konfirmasi dengan opsi Ya dan Tidak |
| 15. Memilih opsi Ya | |
| | 16. Menghapus data pegawai |

A7. Lampiran *Scenario* Mengelola Data Retensi

| **Nomor *Use case*** | **UC-08** |
|---|---|
| Nama | Mengelola Data Retensi |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu data master dan memilih sub menu retensi |
| *Postcondition* | Petugas arsip berhasil mengelola data retensi |
| ***SCENARIO* NORMAL**<br>**"Mengelola Data Retensi"** | |

| Aktor | Sistem |
|---|---|
| 1. Memilih menu Data Master, dan memilih sub menu Retensi | |
| | 2. Menampilkan tabel daftar jadwal retensi dengan atribut sebagai berikut:<br>- Nomer<br>- Jenis Surat<br>- Masa Retensi<br>- Opsi |
| | 3. Menampilkan formulir dengan atribut sebagai berikut:<br>- Jenis Surat<br>- Masa Retensi |
| 4. Mengisi formulir tambah data jadwal retensi | |
| 5. Memilih tombol simpan | |
| | 6. Menyimpan data jadwal retensi |
| 7. Memilih tombol edit | |
| | 8. Menampilkan *modal* formulir edit, dengan atribut sebagai berikut:<br>- Jenis Surat<br>- Masa Retensi |
| 9. Mengisi formulir edit data jadwal retensi pada *modal* | |

| | | | |
|---|---|---|---|
| 10. | Memilih tombol simpan | | |
| | | 11. | Menyimpan data edit jadwal retensi |
| 12. | Memilih tombol hapus | | |
| | | 13. | Menampilkan dialog konfirmasi, dengan opsi Ya dan Tidak |
| 14. | Memilih opsi Ya | | |
| | | 15. | Menghapus data jadwal retensi |

A8. Lampiran *Scenario* Mengelola Data Inaktif

| **Nomor *Use case*** | **UC-09** |
|---|---|
| Nama | Mengelola Data Inaktif |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu data master dan memilih sub menu inaktif |
| *Postcondition* | Petugas arsip berhasil mengelola data inaktif |

| | | | |
|---|---|---|---|
| ***SCENARIO* NORMAL**<br>**"Mengelola Data Inaktif"** | | | |
| **Aktor** | | **Sistem** | |
| 1. | Memilih menu Data Master, dan memilih sub menu Inaktif | | |

| | | | |
|---|---|---|---|
| | | 2. | Menampilkan tabel daftar jadwal inaktif dengan atribut sebagai berikut:<br>- Nomer<br>- Jenis Surat<br>- Masa Inaktif<br>- Opsi |
| | | 3. | Menampilkan formulir dengan atribut sebagai berikut:<br>- Jenis Surat<br>- Masa Inaktif |
| 4. | Mengisi formulir tambah data jadwal inaktif | | |
| 5. | Memilih tombol simpan | | |
| | | 6. | Menyimpan data jadwal inaktif |
| 7. | Memilih tombol edit | | |
| | | 8. | Menampilkan *modal* formulir edit, dengan atribut sebagai berikut:<br>- Jenis Surat<br>- Masa Retensi |
| 9. | Mengisi formulir edit data jadwal inaktif pada *modal* | | |
| 10. | Memilih tombol simpan | | |
| | | 11. | Menyimpan data edit jadwal inaktif |

| | | | |
|---|---|---|---|
| 12. | Memilih tombol hapus | | |
| | | 13. | Menampilkan dialog konfirmasi, dengan opsi Ya dan Tidak |
| 14. | Memilih opsi Ya | | |
| | | 15. | Menghapus data jadwal inaktif |

A9. Lampiran *Scenario* Mengelola Akun Pegawai

| **Nomor *Use case*** | **UC-09** |
|---|---|
| Nama | Mengelola Akun Pegawai |
| Aktor | Petugas Arsip |
| *Precondition* | Petugas arsip memilih menu atur pengguna |
| *Postcondition* | Petugas arsip berhasil mengelola akun pegawai |
| ***SCENARIO* NORMAL**<br>**"Mengelola Akun Pegawai"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Atur Pengguna | |
| | 2. Menampilkan tabel daftar pengguna aplikasi dengan atribut sebagai berikut:<br>- NIP<br>- Nama<br>- Email |

| | | |
|---|---|---|
| | | - Hak Akses<br>- Opsi |
| 3. | Memilih tombol tambah pengguna | |
| | | 4. Menampilkan *modal* formulir tambah pengguna dengan atribut sebagai berikut:<br>- NIP<br>- Nama<br>- Password<br>- Email<br>- Hak Akses |
| 5. | Mengisi formulir pada modal tambah pengguna | |
| 6. | Memilih tombol edit | |
| | | 7. Menampilkan *modal* formulir edit pengguna dengan atribut sebagai berikut:<br>- NIP<br>- Nama<br>- Email<br>- Hak Akses |
| 8. | Mengisi formulir pada modal edit pengguna | |
| 9. | Memilih tombol simpan | |
| | | 10. Menyimpan data edit pengguna |
| 11. | Memilih tombol hapus | |

| | | | |
|---|---|---|---|
| | | 12. | Menampilkan dialog konfirmasi, dengan opsi Ya dan Tidak |
| 13. | Memilih opsi Ya | | |
| | | 14. | Menghapus data pengguna aplikasi |

A10. Lampiran *Scenario* Menguduh Laporan

| **Nomor *Use case*** | **UC-16** |
|---|---|
| Nama | Mengunduh Laporan |
| Aktor | Pegawai |
| *Precondition* | Pegawai memilih menu laporan |
| *Postcondition* | Pegawai berhasil mengunduh laporan |
| ***SCENARIO* NORMAL**<br>**"Mengunduh Laporan"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Laporan | |
| | 2. Menampilkan formulir unduh laporan dengan atribut sebagai berikut:<br>- Laporan<br>- Tanggal Mulai<br>- Tanggal Sampai |
| 3. Mengisi formulir unduh, dan memilih jenis laporan | |

| | | | |
|---|---|---|---|
| 4. | Memilih tombol unduh | | |
| | | 5. | Menampilkan dialog unduh |
| 6. | Memilih tombol oke | | |
| | | 7. | Laporan terunduh ke dalam komputer |

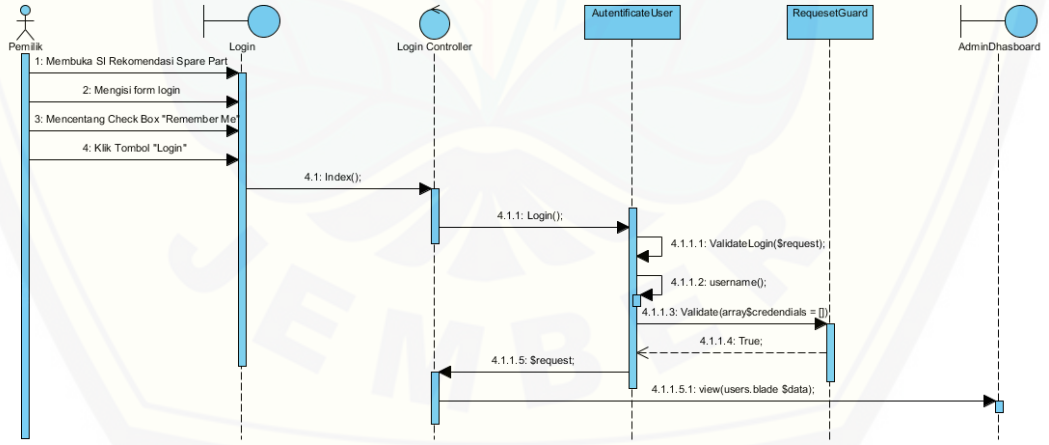
A11. Lampiran *Scenario* Dekripsi Arsip

| **Nomor *Use case*** | **UC-17** |
|---|---|
| Nama | Dekripsi Arsip |
| Aktor | Pegawai |
| *Precondition* | Pegawai memilih menu dokumen arsip dan sub menu dekripsi arsip |
| *Postcondition* | Petugas arsip berhasil mendekripsi arsip |
| ***SCENARIO* NORMAL**<br>**"Dekripsi Arsip"** | |
| **Aktor** | **Sistem** |
| 1. Memilih menu Dokumen Arsip dan sub menu Dekripsi Arsip | |
| | 2. Menampilkan formulir dekripsi arsip dengan atribut:<br>- Unggah arsip<br>- Password |
| 3. Mengunggah arsip terenkripsi | |

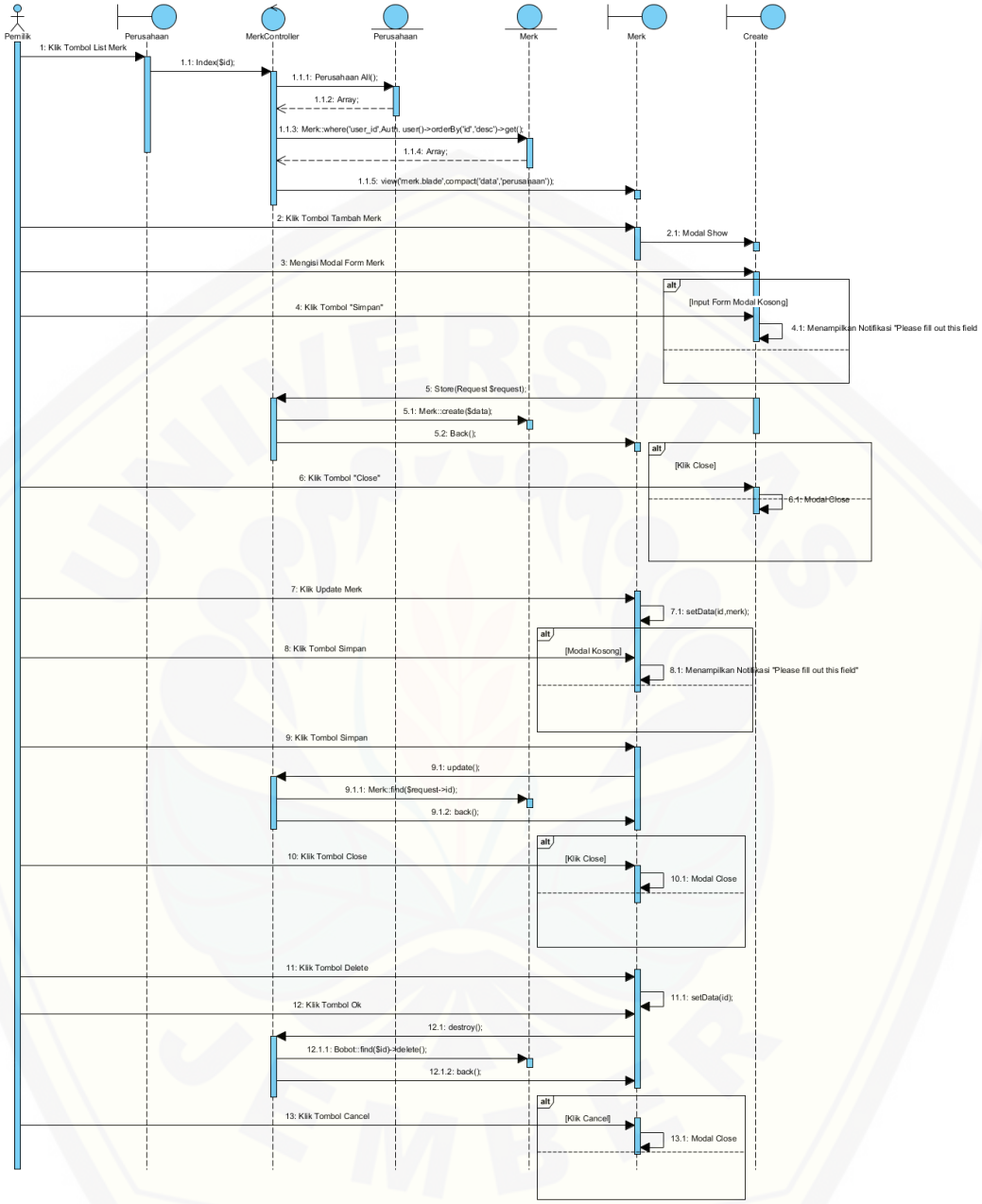
| | | | |
|---|---|---|---|
| 4. | Mengisi password arsip terenkripsi | | |
| 5. | Memilih tombol dekrip arsip | | |
| | | 6. | Arsip menyocokkan *password* dan mendekripsi arsip dengan metode AES-128 yang di *inverse* |
| | | 7. | Menampilkan dialog unduh |
| 8. | Memilih tombol *save* | | |
| | | 9. | Arsip yang terdekripsi telah terunduh dalam komputer |

## *B.* Lampiran *Sequence Diagram*

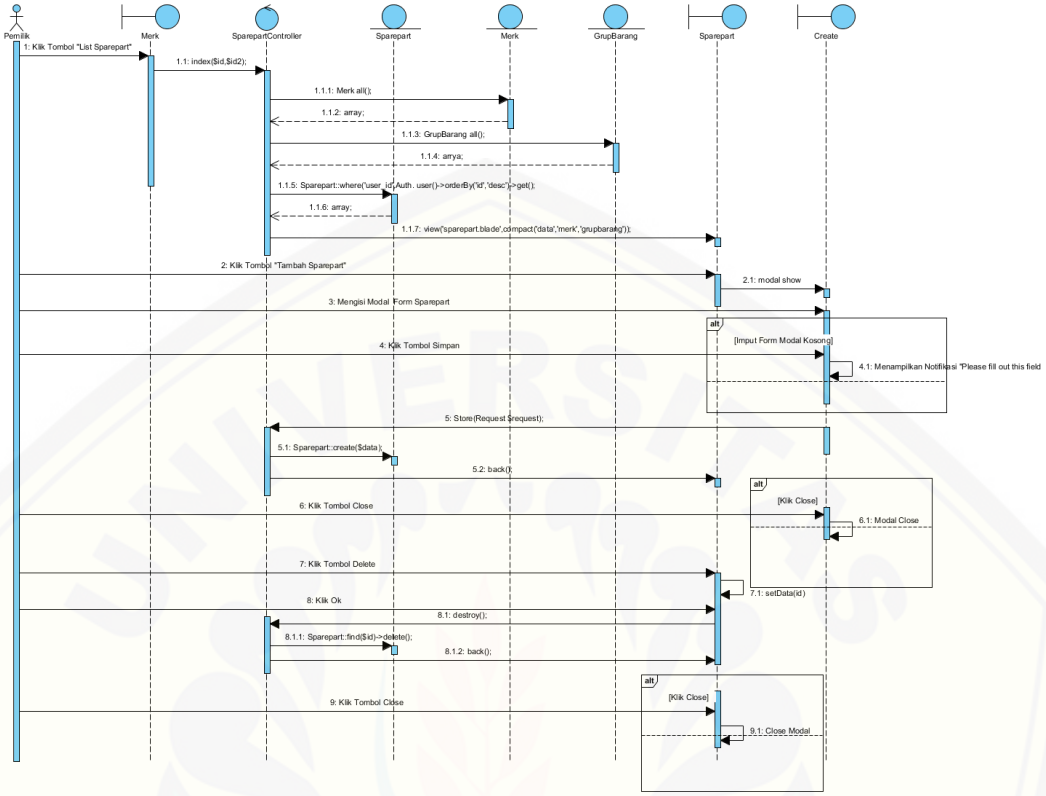
B1. Lampiran *Sequence Diagram* Mengunduh Arsip



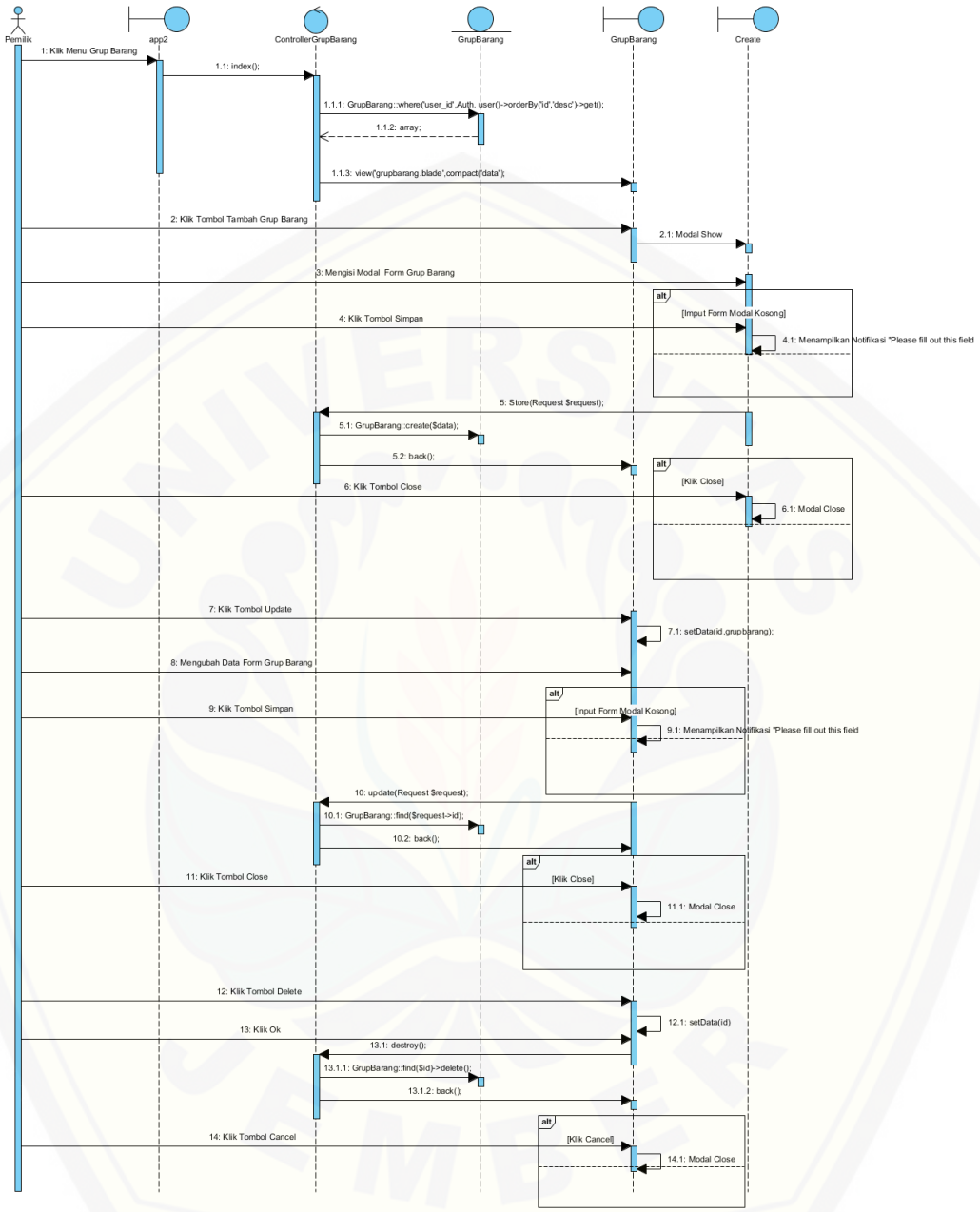
B2. Lampiran *Sequence Diagram* Mengajukan Pinjaman Arsip



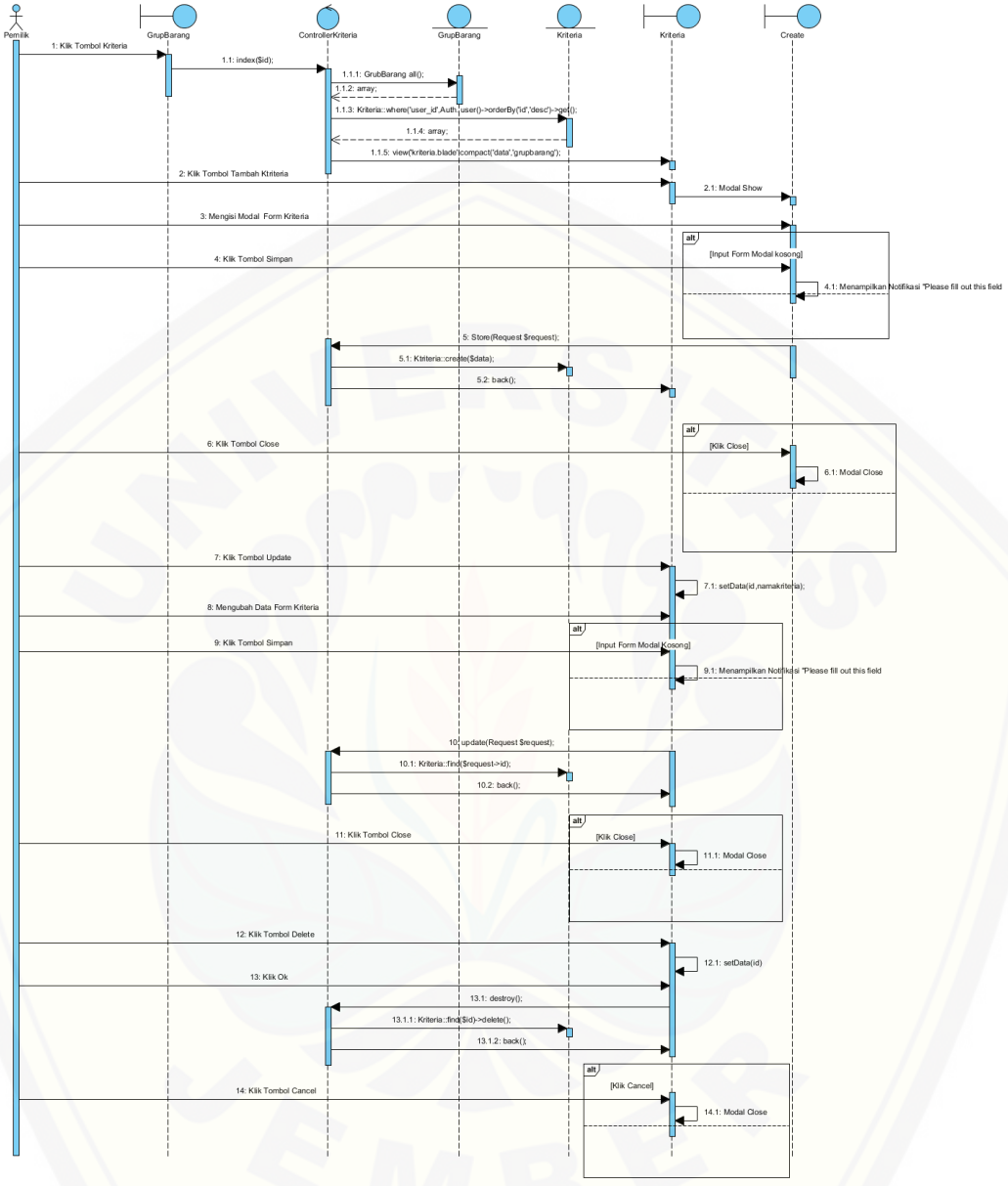
B3. Lampiran *Sequence Diagram* Konfirmasi Pinjaman Arsip



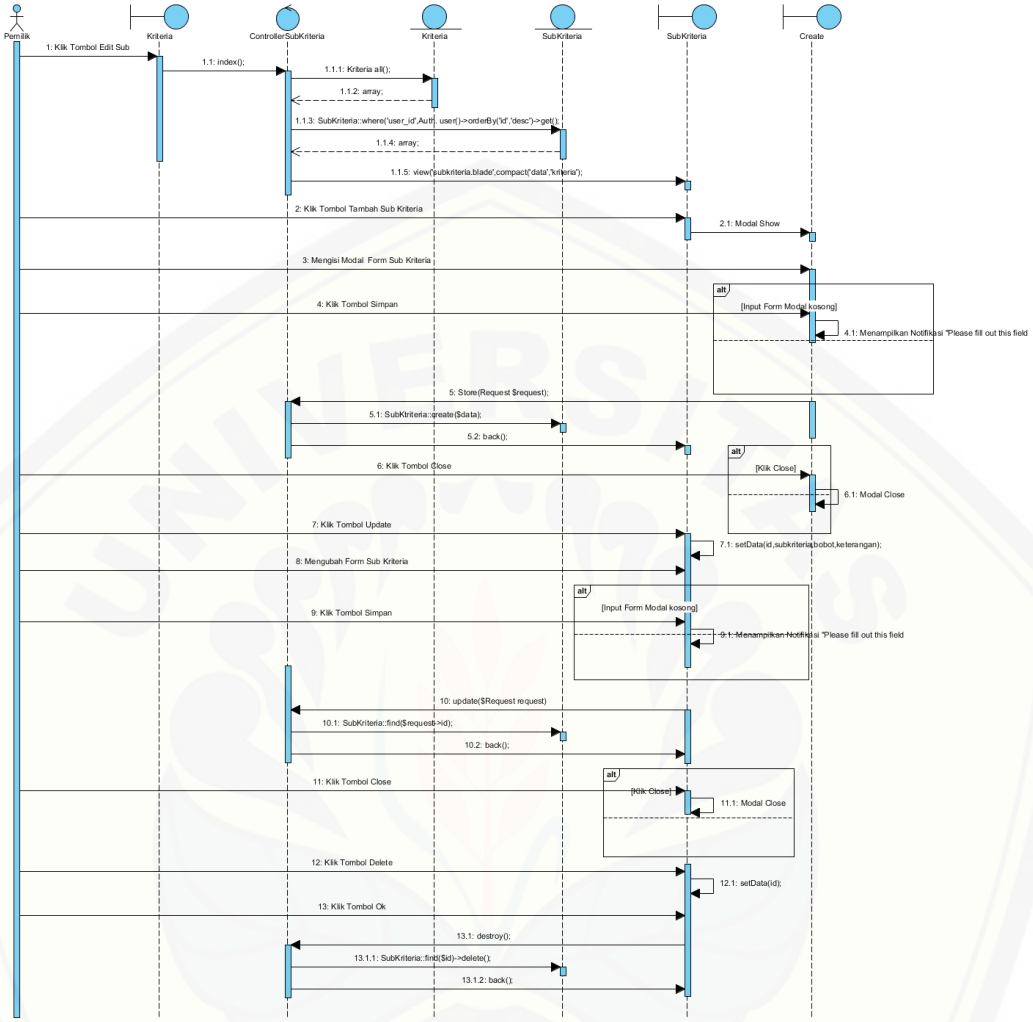
B4. Lampiran *Sequence Diagram* Mengelola Data Unit Kerja



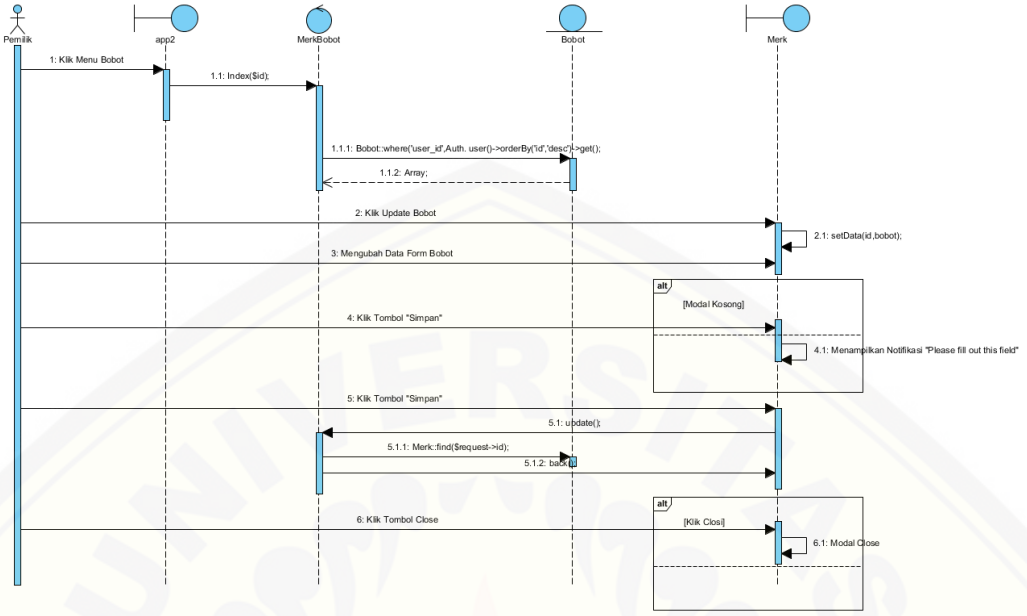
B5. Lampiran *Sequence Diagram* Mengelola Data Jabatan



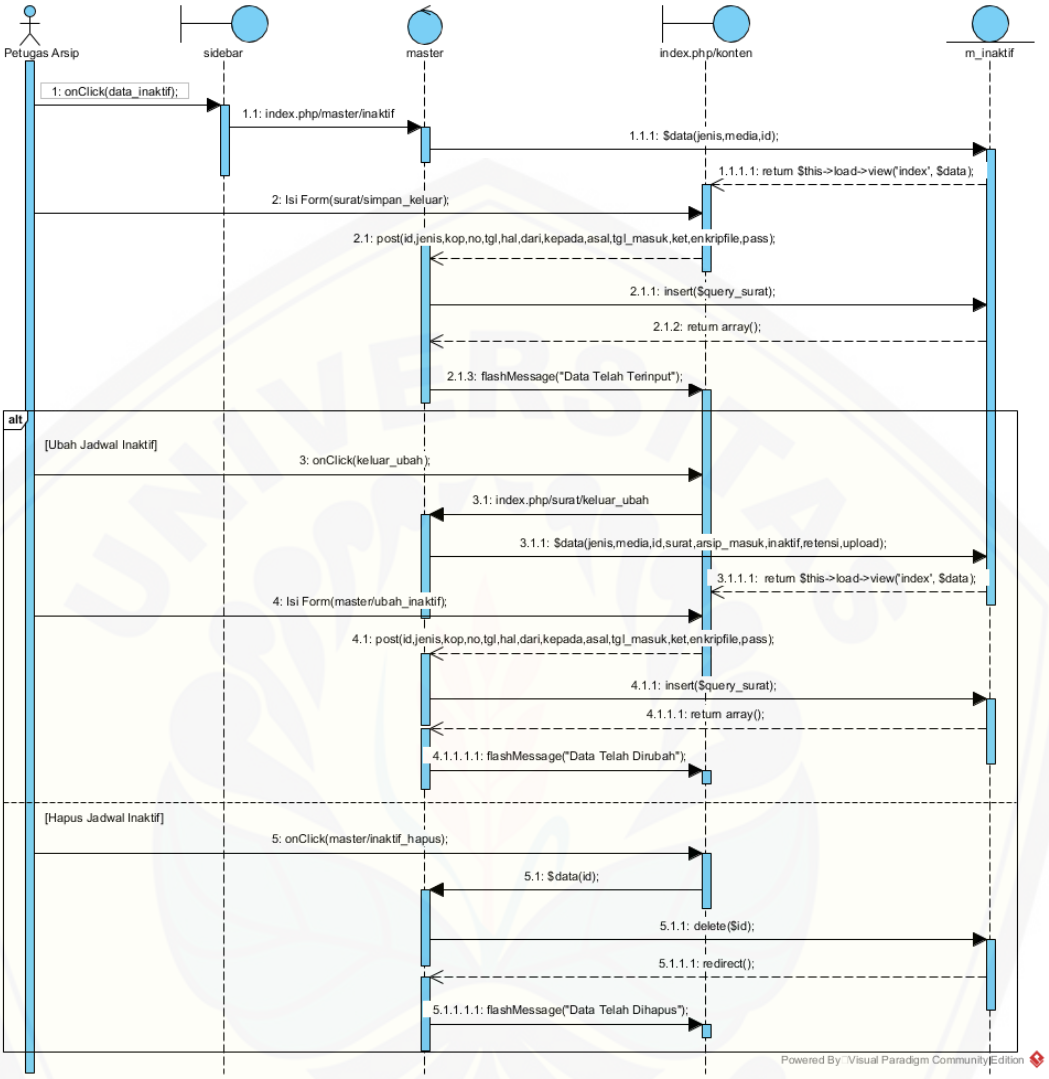
B6. Lampiran *Sequence Diagram* Mengelola Data Pegawai



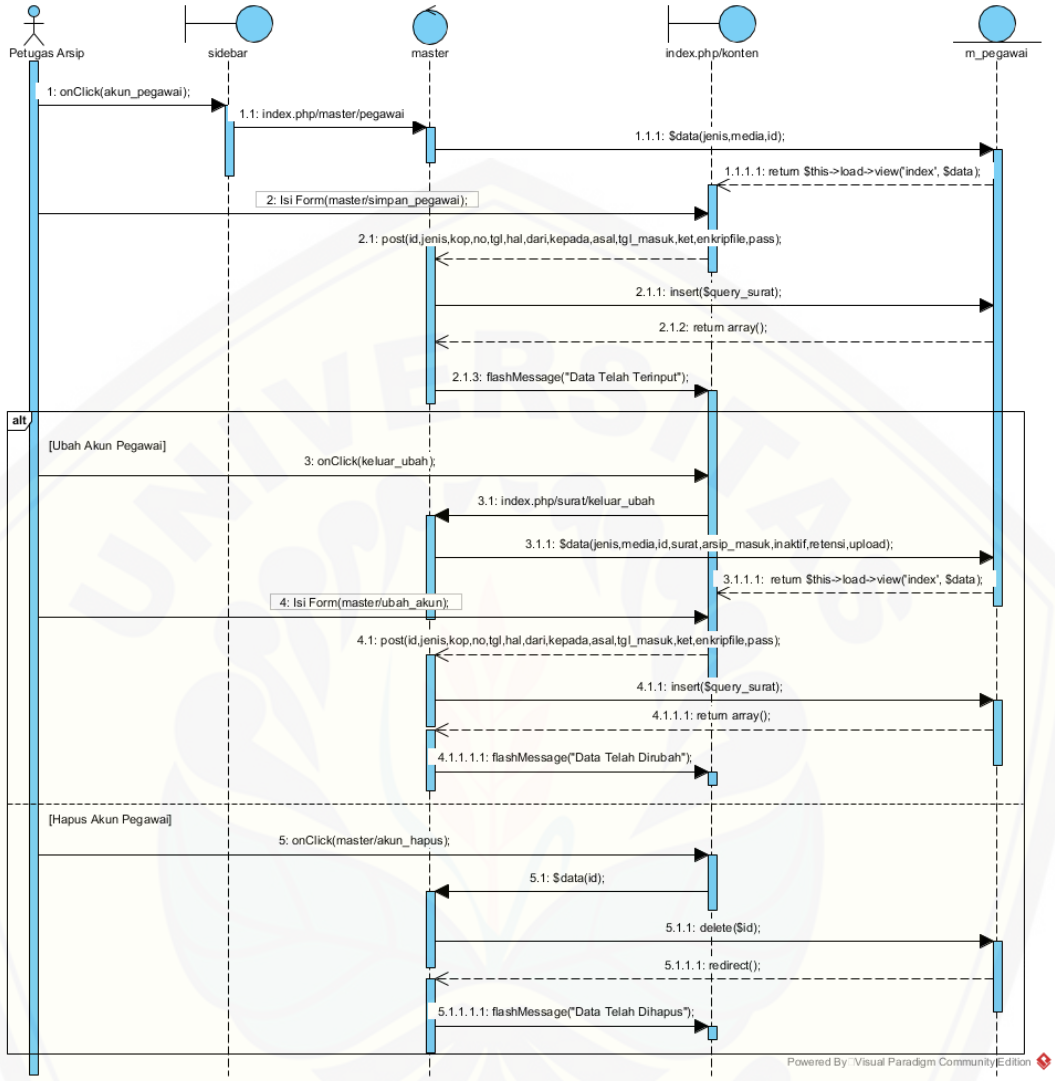
B7. Lampiran *Sequence Diagram* Mengelola Data Retensi



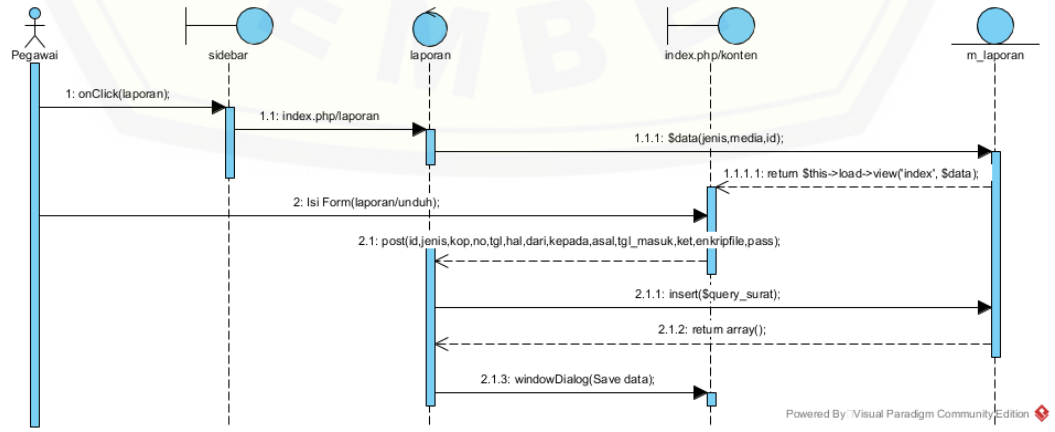
B8. Lampiran *Sequence Diagram* Mengelola Data Inaktif



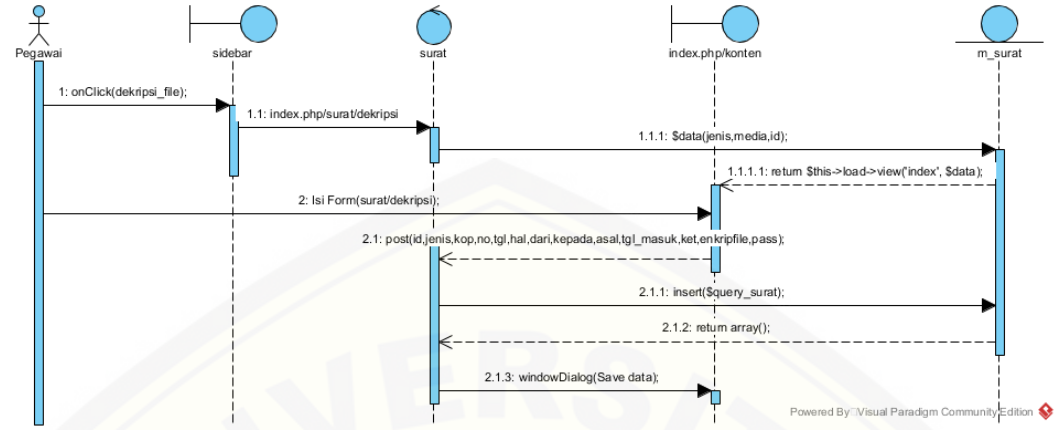
B9. Lampiran *Sequence Diagram* Mengelola Akun Pegawai




B10. Lampiran *Sequence Diagram* Mengunduh Laporan

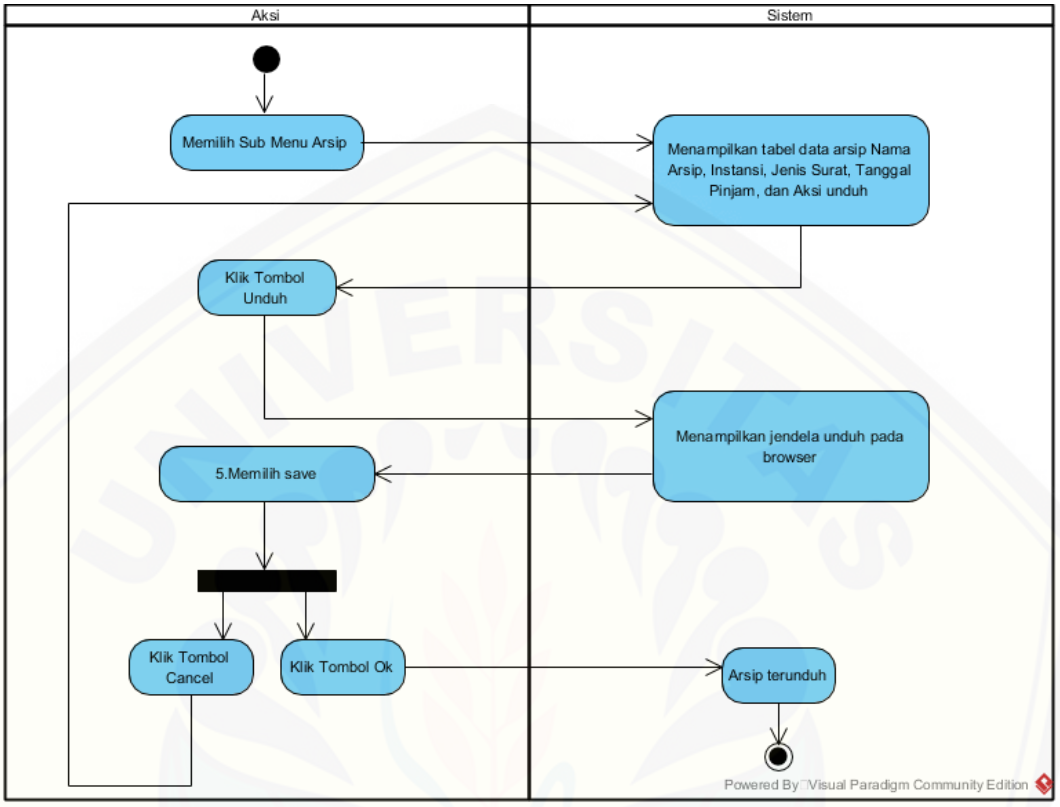


B11. Lampiran *Sequence Diagram* Dekripsi Arsip

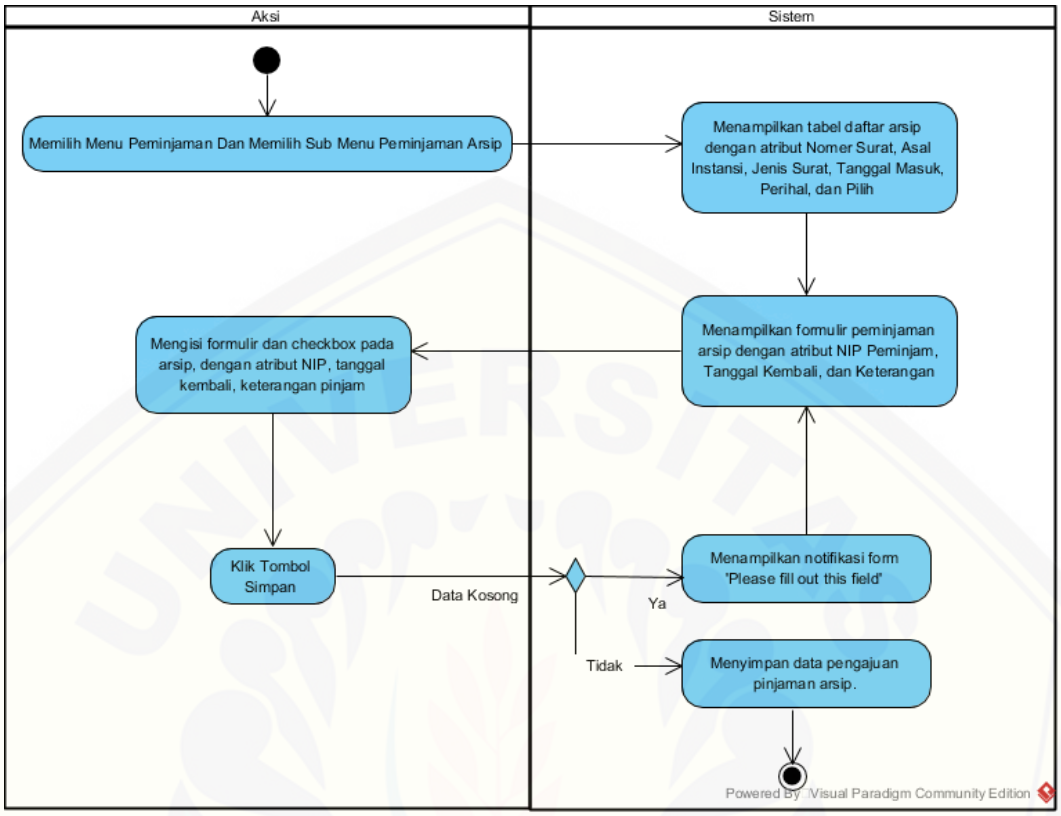


## *C.* Lampiran *Sequence Diagram*

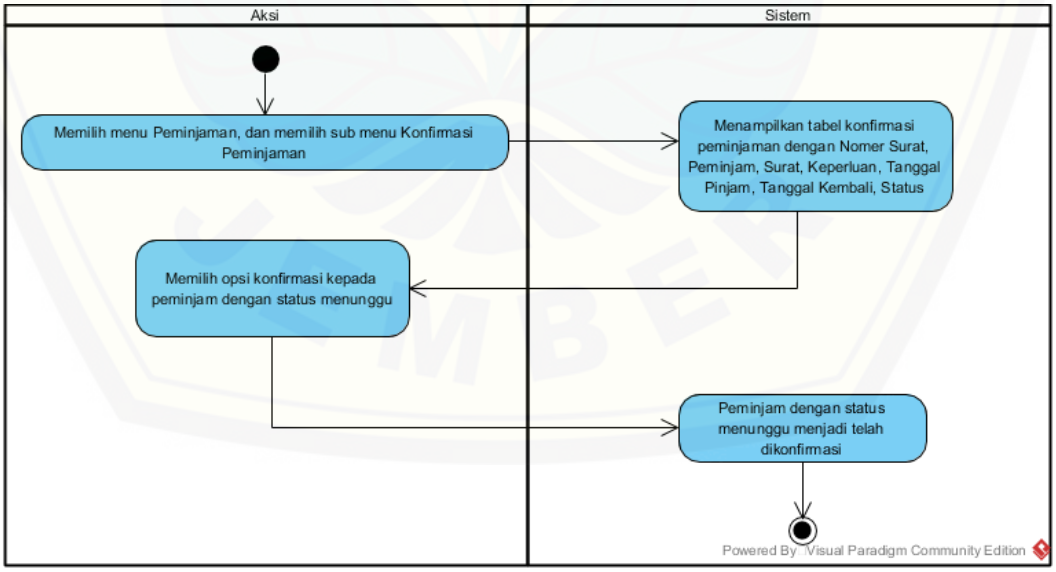
C1. *Activity Diagram* Mengunduh Arsip



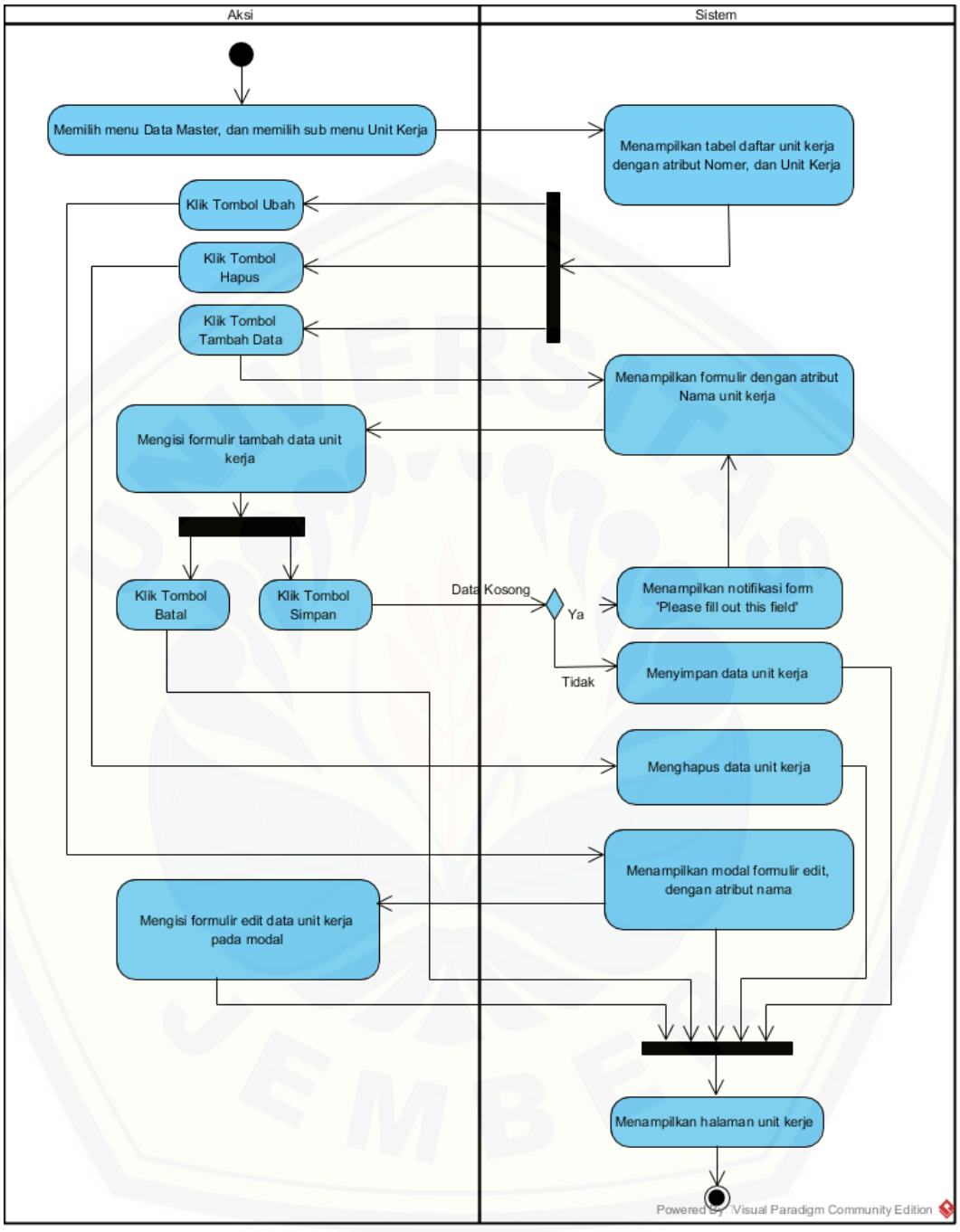
C2. *Activity Diagram* Mengajukan Pinjaman Arsip



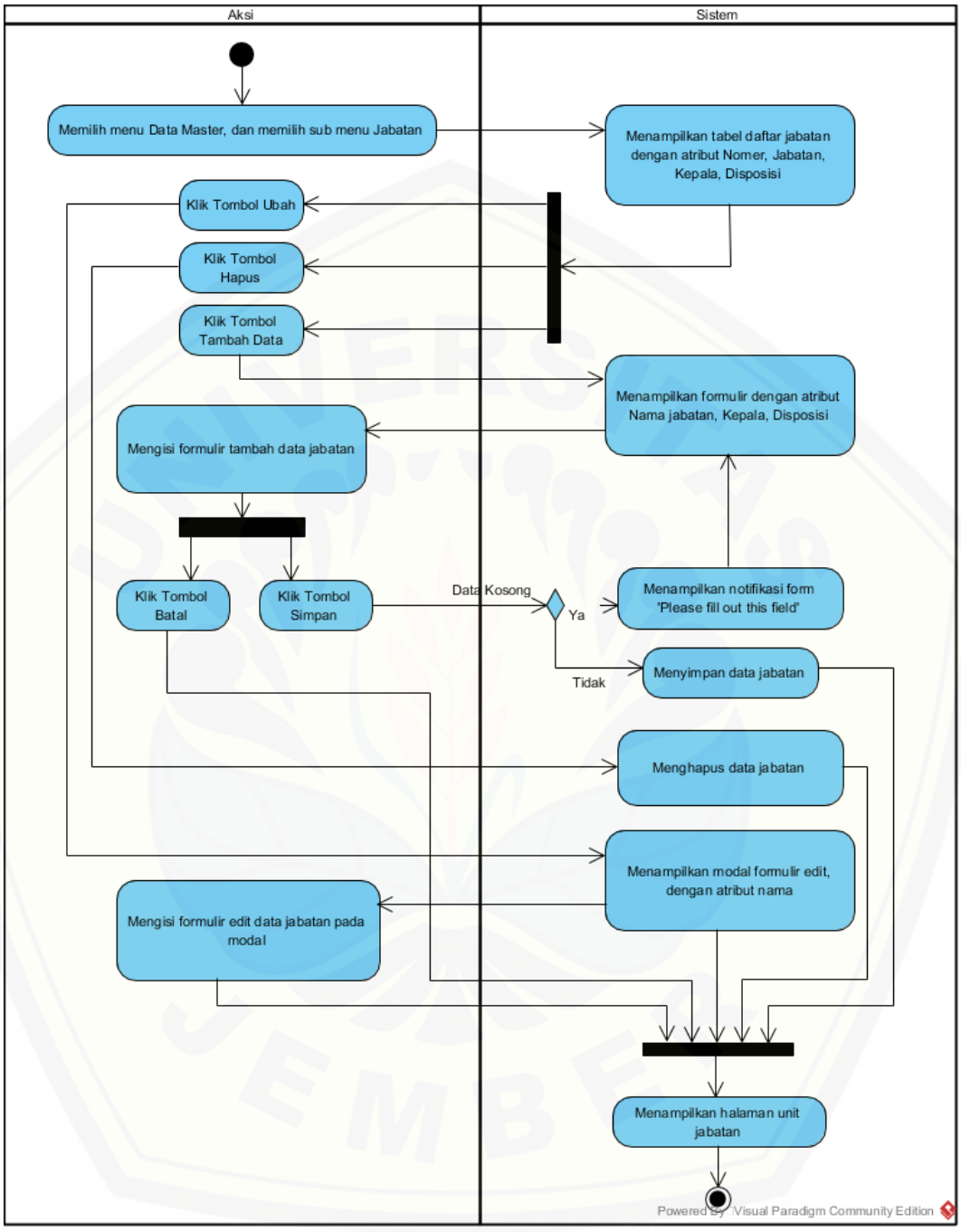

C3. *Activity Diagram* Konfirmasi Pinjaman Arsip



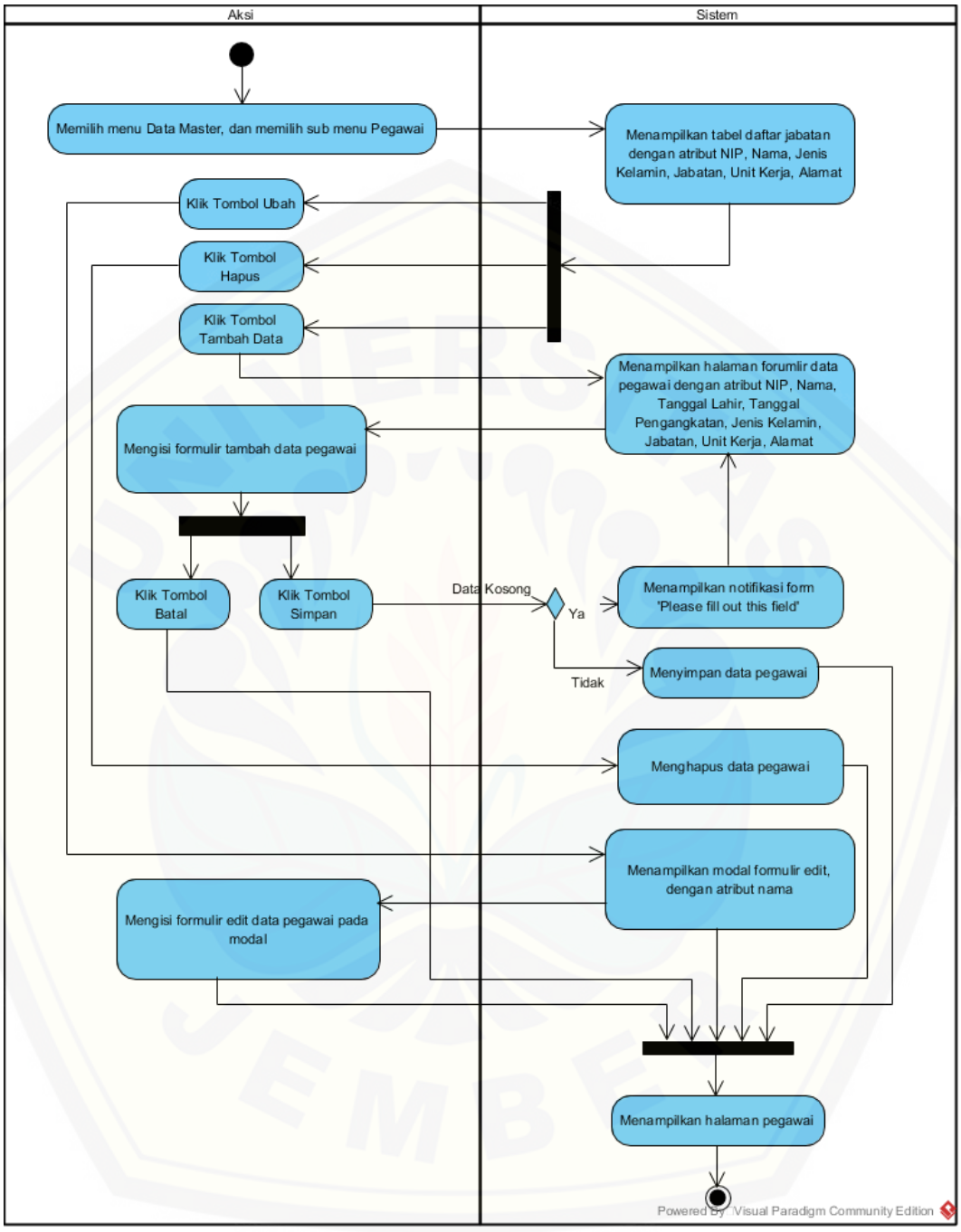
C4. *Activity Diagram* Mengelola Data Unit Kerja



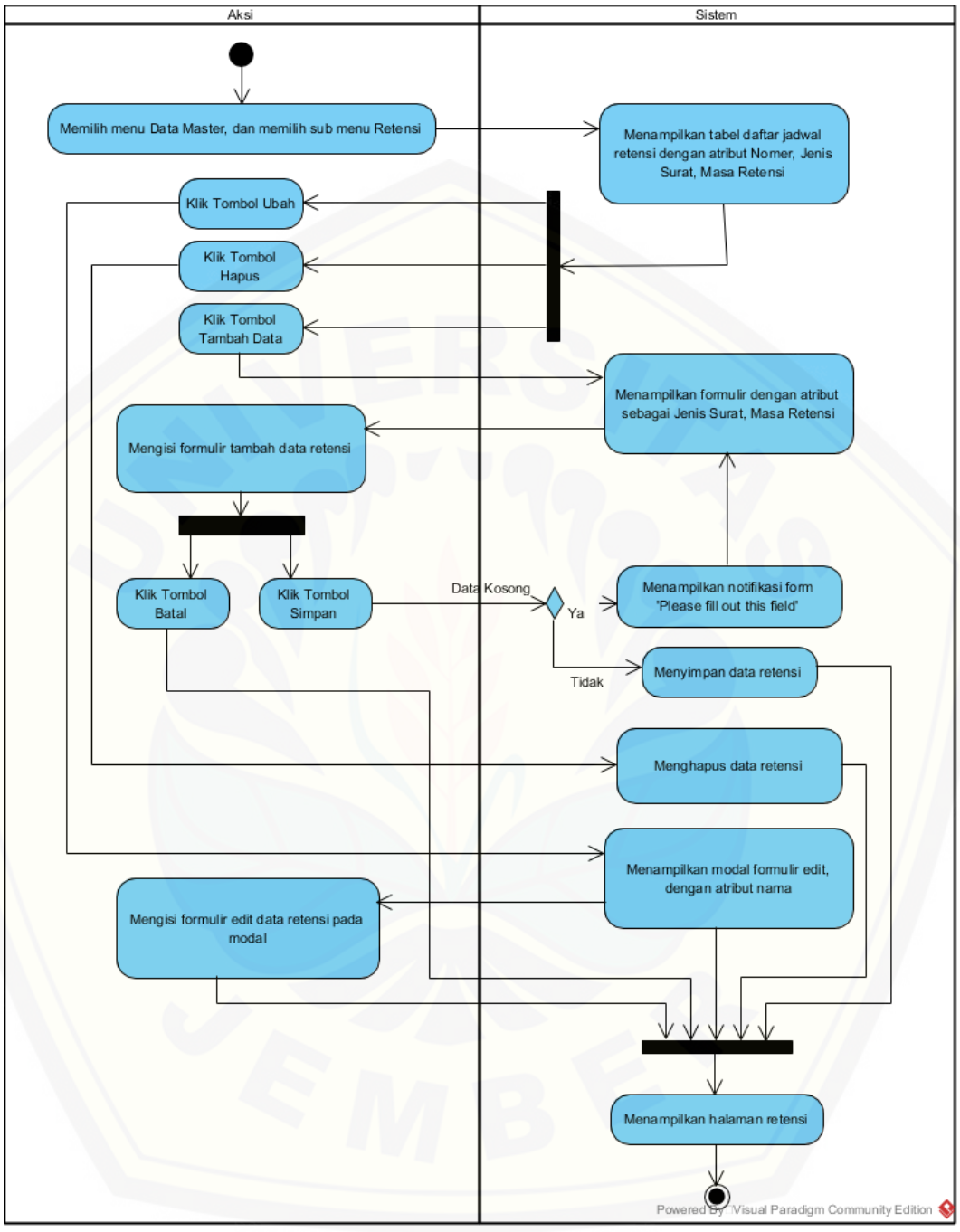
C5. *Activity Diagram* Mengelola Data Jabatan



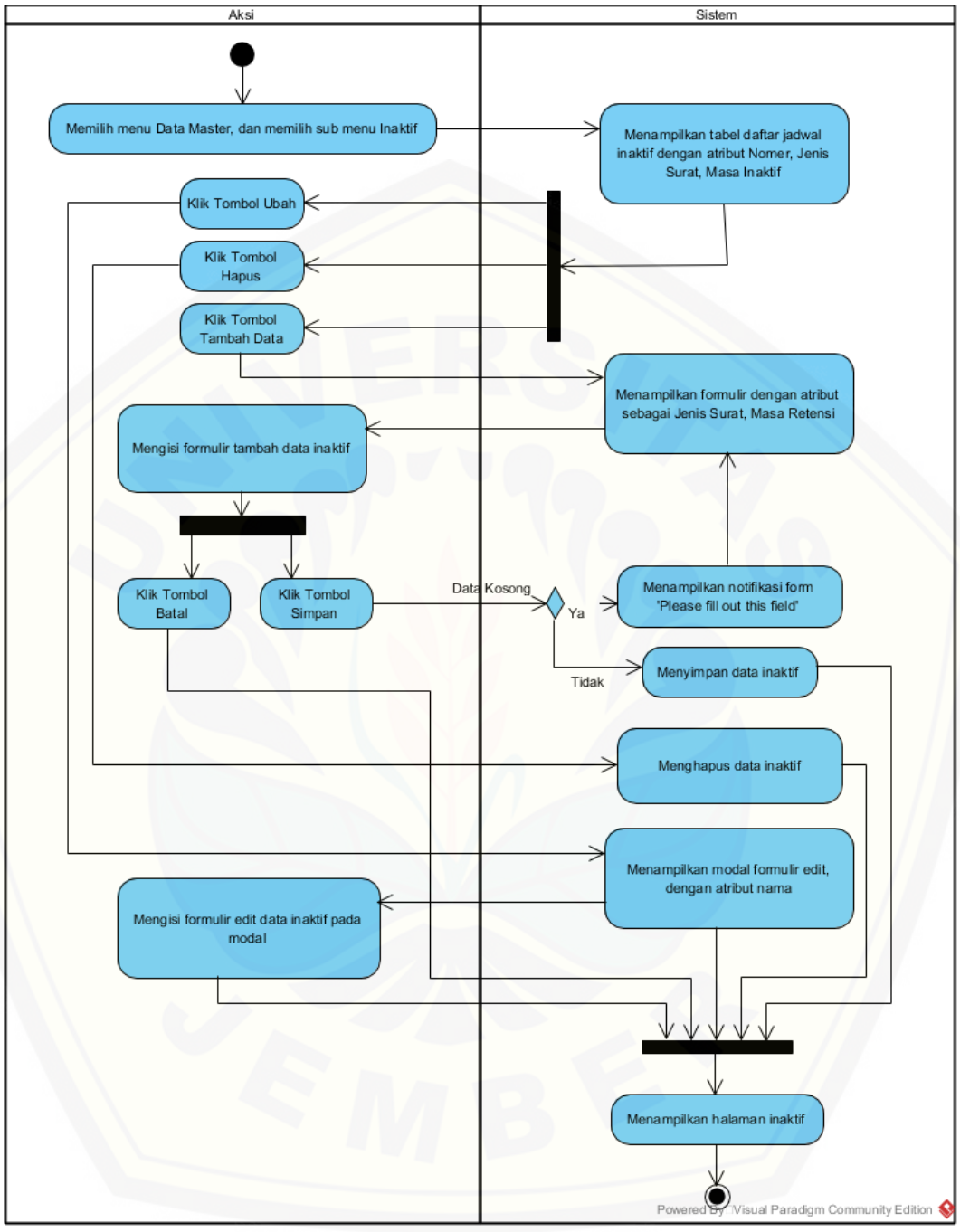
C6. *Activity Diagram* Mengelola Data Pegawai



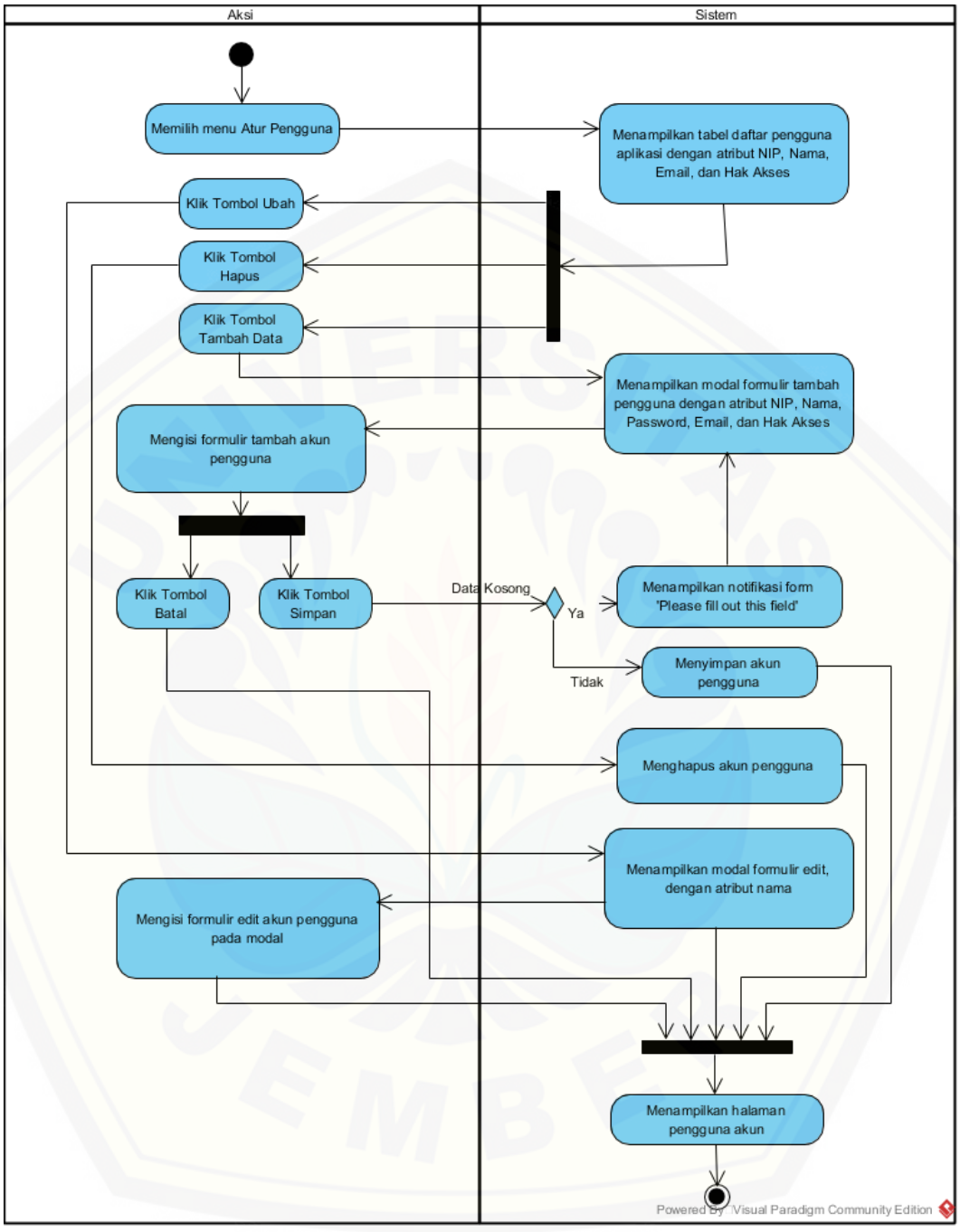
C7. *Activity Diagram* Mengelola Data Retensi



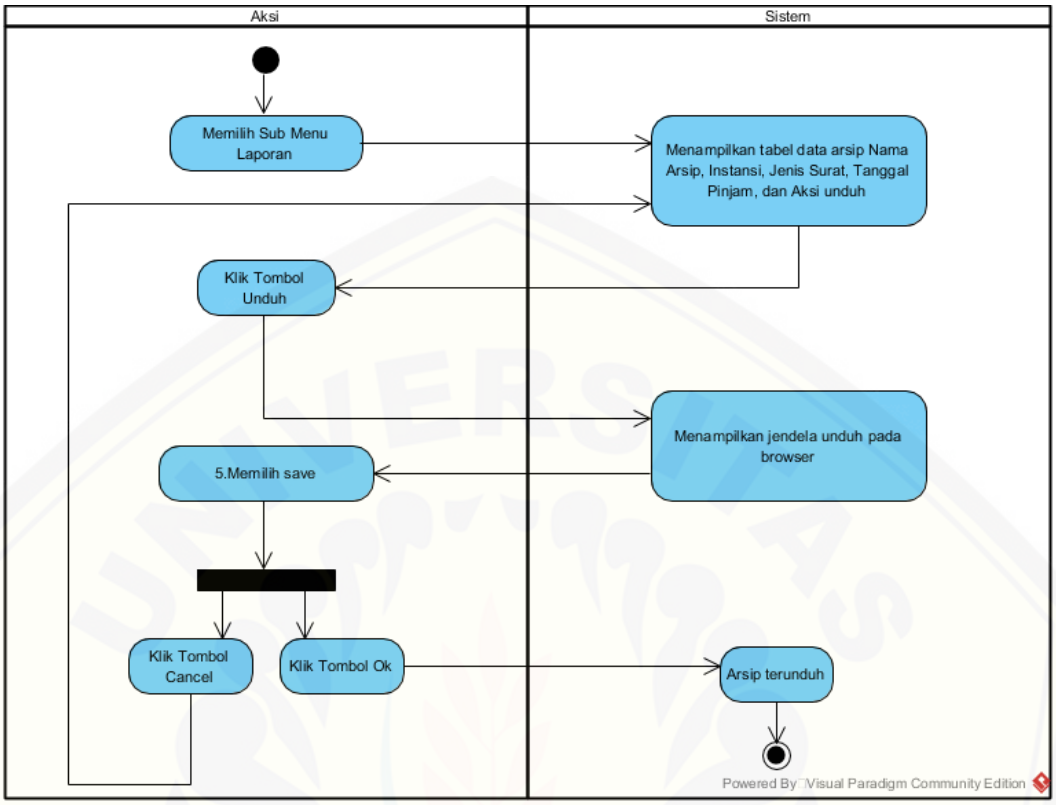
C8. *Activity Diagram* Mengelola Data Inaktif



C9. *Activity Diagram* Mengelola Akun Pegawai



C10. *Activity Diagram* Mengunduh Laporan




C11. *Activity Diagram* Dekripsi Arsip