

TUGAS AKHIR

**Perancangan dan Implementasi Keamanan Data
Kependudukan Desa Namo Buaya Menggunakan
Metode Enkripsi AES 128-bit berbasis Web**

Untuk Memenuhi Sebagian dari Syarat-Syarat
Yang Diperlukan untuk Memperoleh
Gelar Sarjana Teknik

Disusun Oleh:

EFENDI
NIM. 2005903040106



**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS TEUKU UMAR
MEULABOH
2023**



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS TEUKU UMAR
FAKULTAS TEKNIK
PROGRAM STUDI TEKNOLOGI INFORMASI
KAMPUS UTU, MEULABOH – ACEH BARAT 23615, PO BOX 59
Laman www.utu.ac.id; email teknik@utu.ac.id

LEMBAR PERSETUJUAN PEMBIMBING

PROPOSAL TUGAS AKHIR

**Perancangan dan Implementasi Keamanan Data Kependudukan
Desa Namo Buaya Menggunakan Metode Enkripsi
AES 128-bit berbasis Web**

Disusun Oleh:

NAMA : Efendi
NIM : 2005903040106
BIDANG : Teknologi Informasi

Meulaboh,, 2024

Disetujui Oleh:

Dosen Pembimbing Utama,

Dosen Pembimbing Pendamping,

Cut Mutia, SST., M.T.
NIP.....

Cukri Rahmi Niani, ST.,Msi.
NIP.....

Mengetahui:

Ketua Program Studi Teknologi Informasi,

Suryadi, S.T., M.Cs
NIP.



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS TEUKU UMAR
FAKULTAS TEKNIK
PROGRAM STUDI TEKNOLOGI INFORMASI
KAMPUS UTU, MEULABOH – ACEH BARAT 23615, PO BOX 59
Laman www.utu.ac.id; email teknik@utu.ac.id

LEMBAR PENGESAHAN PEMBIMBING

TUGAS AKHIR

**Perancangan dan Implementasi Keamanan Data Kependudukan
Desa Namo Buaya Menggunakan Metode Enkripsi
AES 128-bit berbasis Web**

Disusun Oleh:

NAMA : Efendi
NIM : 2005903040106
BIDANG : Teknologi Informasi

Meulaboh,, 2024

Disetujui Oleh:

Dosen Pembimbing Utama,

Dosen Pembimbing Pendamping,

Cut Mutia, SST., M.T.
NIP.....

Cukri Rahmi Niani, ST., Msi.
NIP.....

Mengetahui:

Ketua Program Studi xxx,

Dekan Fakultas Teknik,

Suryadi, S.T., M.Cs
NIP.

Nama Dekan
NIP.



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS TEUKU UMAR
FAKULTAS TEKNIK
PROGRAM STUDI TEKNOLOGI INFORMASI
KAMPUS UTU, MEULABOH – ACEH BARAT 23615, PO BOX 59
Laman www.utu.ac.id; email teknik@utu.ac.id

LEMBAR PENGESAHAN PENGUJI

TUGAS AKHIR

**Perancangan dan Implementasi Keamanan Data Kependudukan
Desa Namo Buaya Menggunakan Metode Enkripsi
AES 128-bit berbasis Web**
Disusun Oleh:

NAMA : Efendi
NIM : 2005903040106
BIDANG : Teknologi Informasi

Meulaboh,, 2024

Disetujui Oleh:

Dosen Penguji I,

Dosen Penguji II,

Cut Mutia, STT., MT
NIP.....

Cukri Rahmi Niani, S.T., Msi
NIP.....

Mengetahui,
Ketua Program Studi Teknologi Informasi,

Suryadi, S.T., M.Cs
NIP.

KATA PENGANTAR

Assalamu'alaikum wr. wb. Puji syukur kepada Allah SWT, yang telah melimpahkan rahmat serta hidayah-Nya sehingga penulis dapat menyelesaikan Laporan Tugas Akhir. Keberhasilan penulisan ini tidak terlepas dari partisipasi dan dukungan dari semua pihak yang turut membantu. Oleh sebab itu, penulis mengucapkan terima kasih banyak kepada:

1. Bapak Prof. Dr. Ishak Hasan, M.Si selaku Rektor Universitas Teuku Umar.
2. Bapak Dr. Ir. Irwansyah, ST., M.Eng, IPM selaku Dekan Fakultas Teknik Universitas Teuku Umar.
3. Bapak/ibu xxx selaku Ketua Prodi xxx Fakultas Teknik Universitas Teuku Umar.
4. Bapak/Ibu..... selaku Dosen Pembimbing Pertama.
5. Bapak/Ibuselaku Pembimbing Kedua.
6. Kedua orang tua yang sangat saya sayangi, terima kasih banyak untuk doa dan semua dukungannya.
7. Teman-teman kos milenial penulis yang juga ikut membantu.

Penulis menyadari masih banyak kekurangan dari penulisan Tugas Akhir ini, dan semoga bermanfaat bagi penulis khususnya, pihak Universitas Teuku Umar serta pembaca pada umumnya. Dengan kerendahan hati penulis mengharapkan kritik dan saran yang membangun demi perbaikan penyusunan Laporan Tugas Akhir ini selanjutnya.

Wassalamu'alaikum Wr. Wb.

Meulaboh,2024
Penulis

Efendi
2005903040106

**JUDUL TUGAS AKHIR DITULIS SINGKAT, JELAS DAN
MENGAMBARKAN TEMA POKOK**

Nama Mahasiswa : Efendi
NIM : 2005903040106
Pembimbing : Cut Mutia, STT., M.T
Email : efendi.tif20@gmail.com

ABSTRAK

Sistem suspensi kendaraan terdiri dari sistem massa, pegas, peredam. *Shock absorber* merupakan bagian utama yang berfungsi meredam getaran yang ditransmisikan dari sumber getaran, pegas berfungsi untuk memberikan kekakuan pada sistem dan mentransformasi energi kinetik menjadi energi potensial. Banyak peneliti mengembangkan tentang *hydraulic regenerative suspension*, tipe desain yang ada pada saat ini, yaitu *Linear Electromagnetic Shock Absorber*, *Rack Pinion Electromagnetic Suspension*, *Ball Screw Electromagnetic Suspension*, *Hydraulic Electromagnetic Suspension*. Pengembangan suspensi *regenerative* harus memperhatikan dua aspek, yaitu kemampuan sistem meregenerasi energi dan kenyamanan yang diberikan. Pada penelitian ini sistem kerja *Hidro-Magneto-electric-regenerative shock absorber* (HMERSA) dengan 4 *input* dan *single output*. Langkah pertama, mensimulasikan aliran fluida kesetiap selinder hidrolik agar alirannya searah. Kemudian memberikan inputan pada ke empat selinder hidrolik dengan 4 variasi *input* dan *single output*. Hasil yang diamati adalah Kecepatan putaran motor hidrolik variasi 1 dari 0 sampai 2.33 detik adalah 140 Rpm, variasi 2 dari 0 sampai 0,63 detik adalah 41,4 Rpm, variasi 3 dari 0 sampai 1,2 detik adalah 140 putaran dan variasi ke 4 dari 0 sampai 0,63 detik adalah 8 putaran. Semakin sering pergerakan selinder hidrolik semakin tinggi putaran motor hidrolik yang dihasilkan. Gaya redam yang diperoleh dari variasi 1 dengan *frekuensi* 2 Hz sebesar -1004,84 Nm, *voltase* 58,36 volt, arus 1,98 ampere, dan daya listrik 115,86 watt.

Kata kunci : (Maksimal 5 Kata)

**JUDUL TUGAS AKHIR DITULIS SINGKAT, JELAS DAN
MENGAMBARAKAN TEMA POKOK**

Nama Mahasiswa	: Nama Mahasiswa
NIM	: Nomor Induk Mahasiswa
Pembimbing	: Dr.contoh nama, ST, M.Eng
Email	: mahasiswa123@utu.ac.id

ABSTRAK

Vehicle suspension system consists of a system of masses, springs, dampers. Shock absorber is the main part that serves to reduce vibration transmitted from the vibration source, spring serves to provide rigidity to the system and transform kinetic energy into potential energy. Many researchers develop on hydraulic regenerative suspension, the type of design that exist at the moment, namely Linear Electromagnetic Shock Absorber, Rack Pinion Electromagnetic Suspension, Ball Screw Electromagnetic Suspension, Hydraulic Electromagnetic Suspension. The development of regenerative suspension should pay attention to two aspects, namely the system's ability to regenerate energy and comfort provided. In this research work systems Hydro-Magneto-electric- shock absorber regenerative (HMERSA) with 4 inputs and single output. The first step, simulate fluid flow to the rest of the hydraulic cylinder so that the flow is unidirectional. Then provide input to the hydraulic cylinder to four with 4 variations of input and single output. The results observed are hydraulic motor rotation speed variation 1 from 0 to 2:33 seconds is 140 rpm, variation 2 from 0 to 0.63 seconds is 41.4 rpm, variation 3 from 0 to 1.2 seconds is 140 rounds and variation 4 from 0 to 0.63 seconds is 8 rpm. The more often the movement of the hydraulic cylinder the higher the resulting hydraulic motor rotation. Style damping obtained from variation 1 with a frequency of 2 Hz for -1004.84 Nm, voltage of 58.36 volts, the current is 1.98 amperes, and 115.86 watts of electrical power

Kata kunci : (Maksimal 5 Kata)

DAFTAR ISI

LEMBAR PENGESAHAN PROGRAM STUDI.....	i
KATA PENGANTAR.....	ii
DAFTAR ISI.....	iii
DAFTAR TABEL.....	iv
DAFTAR GAMBAR.....	v
BAB I PENDAHULUAN	
1.1. Latar Belakang.....	x
1.2. Tujuan Penelitian.....	x
BAB II TINJAUAN PUSTAKA	
2.1 Definisi Konsep dan Operasional.....	x
BAB III METODE PENELITIAN	
3.1 Metode dan Pendekatan Penelitian.....	x
BAB IV HASIL DAN PEMBAHASAN	
4.1 Deskripsi Objek Penelitian.....	x
4.2 Hasil Penelitian.....	x
4.3 Pembahasan Penelitian.....	x
BAB V KESIMPULAN	
5.1. Kesimpulan.....	x
5.2 Saran.....	x
LAMPIRAN.....	x

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah memberikan dampak yang signifikan dalam berbagai bidang. Salah satu dampak negatif di dalam perkembangan teknologi adalah adanya pencurian data, termasuk data kependudukan. Data kependudukan merupakan aset penting bagi sebuah desa atau wilayah administratif lainnya, penting untuk melindungi informasi pribadi dan sensitif seperti data kependudukan dari akses yang tidak sah atau penyalahgunaan.

Kerahasiaan suatu informasi sangat erat dengan risiko kebocoran informasi, terutama informasi yang bersifat pribadi. Sesuai dengan Pasal 1 Ayat 1 dalam Undang-Undang Perlindungan data pribadi, data pribadi merujuk pada segala informasi mengenai individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik melalui sistem elektronik maupun bukan. Informasi kependudukan juga termasuk dalam kategori data pribadi yang memerlukan perlindungan kerahasiaan. Karena data ini memiliki peran krusial dalam berbagai proses administratif dan transaksi seperti pembukaan rekening bank, penggunaan kartu kredit, kepemilikan sertifikat, dan kegiatan serupa.

Desa Namo Buaya mengalami tantangan dalam menjaga keamanan data kependudukan karena kurangnya pengamanan yang memadai terhadap file-file yang tersimpan di kantor desa. Situasi ini semakin diperparah dengan penggunaan perangkat yang bisa diakses oleh beberapa pegawai kantor desa, meningkatkan risiko akses yang tidak sah terhadap data tersebut.

Selain itu data kependudukan yang disimpan oleh Desa Namo Buaya kota Subulussalam disimpan secara offline di dalam perangkat komputer dan tidak memiliki cadangan penyimpanan data yang terjamin. Oleh karena itu, perlu menjaga keamanan data tersebut agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Desa Namo Buaya sebagai salah satu desa yang terletak di Kecamatan Sultan Daulat yang berjarak sekitar 11 Km dari pusat Kota Subulussalam, yang sebagian kecil dari penduduk Desa terdiri dari pedagang,

petani, dan pegawai negeri sipil. Lokasi Desa yang sedikit jauh dari pusat kota membuat masyarakat yang berada di desa kurang dalam memiliki kemampuan di bidang TI (Teknologi informasi) sehingga minimnya pengetahuan mengenai Sistem Informasi terkini mengenai desa dan peningkatan akses internet di daerah tersebut telah membuka peluang baru, tetapi juga menimbulkan risiko keamanan yang signifikan, ancaman ini semakin meningkat dengan meningkatnya aktivitas online, baik oleh penduduk setempat maupun oleh pihak eksternal yang mencari keuntungan dari kelemahan sistem keamanan.

Oleh karena itu salah satu cara untuk meningkatkan keamanan data kependudukan adalah dengan menggunakan enkripsi. Enkripsi adalah proses mengonversi data menjadi bentuk terenkripsi atau tersandi sehingga hanya pihak yang memiliki kunci deskripsi yang dapat membacanya. Metode enkripsi yang populer dan banyak digunakan adalah *Advanced Encryption Standard* (AES) dengan panjang kunci 128-bit.

AES (*Advanced Encryption Standard*) merupakan sistem penyandian blok yang berkarakter non-Faistel, karena AES memakai komponen yang selalu mempunyai invers dengan panjang blok 128, 192 dan 256 bit. Penyandian AES menggunakan proses yang iteratif atau disebut juga ronde. Pada tahun 90-an, setelah beberapa tahun standart penyandian simetris DES (Data Encryption Standart) dianggap tidak aman lagi, lembaga standart Amerika Serikat National Institute of Standart and Technology (NIST) membuat sayembara untuk menggantikan DES dengan sebuah sistem penyandian Advanced Encryption Standart pada tanggal 12 September 1997. Kemudian NIST memberi beberapa spesifikasi untuk AES, yakni memiliki panjang blok 128 bit, serta mampu support panjang kunci 128, 192 dan 256 (Wibowo et al., no date)

Berdasarkan hal tersebut, diperlukan pembangunan sistem yang menggunakan metode enkripsi dan dekripsi file kependudukan yang handal dan dapat diakses secara online. Metode Enkripsi AES 128 Bit dianggap sebagai salah satu metode kriptografi simetris yang efektif jika digunakan untuk mengamankan file kependudukan. Metode ini telah dirancang untuk mengatasi kekurangan yang ada pada metode-metode sebelumnya seperti DES, Triple DES, dan lain-lain.

Dengan mengimplementasikan metode ini dalam bentuk aplikasi berbasis web yang dapat diakses secara online, akan mempermudah pengguna, terutama pada Desa Namo Buaya, dalam proses enkripsi dan dekripsi file kependudukan.

Implementasi keamanan data kependudukan dengan metode enkripsi AES 128-bit berbasis web memungkinkan akses dan pengelolaan data kependudukan menjadi lebih efisien dan terpusat.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, dapat dirumuskan masalah sebagai berikut:

- a) Bagaimana mengimplementasikan enkripsi AES 128-bit untuk meningkatkan keamanan data kependudukan di Desa Namo Buaya?
- b) Apakah sistem yang dikembangkan dapat mengenkripsi dan dekripsi File Kependudukan?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi hal-hal berikut:

- a) Sistem keamanan data kependudukan yang dikembangkan berbasis web dan hanya mencakup proses enkripsi/dekripsi, penyimpanan, dan akses data kependudukan yang terenkripsi.
- b) Data yang akan dienkripsi maupun didekripsi berbentuk file.
- c) Penggunaan metode enkripsi AES 128 Bit (Rijndael) diterapkan pada file-file dengan tipe txt, doc, pdf, dan xls.
- d) Implementasi metode enkripsi AES 128 Bit (Rijndael) menghasilkan berkas dengan format *.rda yang berisi ciphertext.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang diajukan, tujuan penelitian yang dapat ditetapkan adalah sebagai berikut:

- a) Penelitian ini bertujuan untuk meningkatkan tingkat keamanan data kependudukan Desa Namo Buaya dengan menerapkan sistem enkripsi dan dekripsi.
- b) Membangun suatu sistem yang mampu melakukan enkripsi dan dekripsi file data kependudukan dengan menggunakan metode AES 128 Bit

1.5 Manfaat Penelitian

1. Manfaat bagi Desa

- a) Meningkatkan keamanan data kependudukan Desa Namo Buaya dengan mengimplementasikan enkripsi AES 128-bit. Enkripsi data ini dapat membantu melindungi informasi sensitif seperti nama, alamat, tanggal lahir, dan nomor identitas dari akses tidak sah atau penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab.
- b) Meminimalisir risiko pencurian dan penyalahgunaan data kependudukan yang sensitif di Desa Namo Buaya. Dengan menerapkan enkripsi AES 128-bit, data kependudukan akan disandikan sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengakses informasi tersebut.
- c) Menjadi langkah awal dalam meningkatkan kemampuan teknologi informasi masyarakat Desa Namo Buaya. Penelitian ini dapat mendorong masyarakat untuk mempelajari dan mengadopsi teknologi keamanan data yang lebih maju di masa mendatang.

2. Manfaat bagi penulis

- a) Meningkatkan pemahaman dan penguasaan penulis/peneliti tentang metode enkripsi AES 128-bit dan implementasinya untuk melindungi keamanan data.
- b) Memberikan kesempatan bagi penulis/peneliti untuk mengaplikasikan pengetahuan dan keterampilan dalam bidang keamanan data, enkripsi, dan pengembangan aplikasi web dalam kasus nyata.
- c) Memperoleh pengalaman praktis dalam melakukan penelitian, mulai dari mengidentifikasi masalah, merumuskan tujuan, menerapkan metode penelitian, hingga menganalisis dan menyajikan hasil.
- d) Meningkatkan kepercayaan diri penulis/peneliti dalam menghadapi tantangan penelitian dan memecahkan masalah terkait keamanan data di lingkungan yang memiliki keterbatasan sumber daya atau pengetahuan teknologi informasi.

- e) Meningkatkan kemampuan penulis/peneliti dalam menganalisis dan mengevaluasi tingkat keamanan sistem enkripsi yang diimplementasikan serta mengidentifikasi area perbaikan.

BAB II TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Didalam sebuah penelitian maka harus memiliki referensi yang sesuai dengan penelitian yang akan dilakukan, yang mana tujuannya untuk memudahkan dan membantu penulis dalam melakukan penelitian. Adapun penelitian terdahulu dapat dilihat pada tabel 2.1

Tabel 2.1

No	Nama penelitian	Judul	Tahun	Isi
1	1. Muklas Adik Putra,	Perancangan Aplikasi	2022	Penelitian ini menyoroti pentingnya keamanan data yang sensitif menggunakan kriptografi, dengan fokus pada algoritma Triple-DES. Penelitian ini bertujuan merancang aplikasi kriptografi untuk dokumen berbasis web. Metode penelitian melibatkan pengumpulan data dari jurnal, dengan penjelasan proses enkripsi dan dekripsi menggunakan gambar. Implementasi aplikasi dilakukan dengan PHP. Hasilnya menunjukkan keberhasilan
	2. Dadang Iskandar Mulyana,	Enkripsi & Deskripsi pada Dokumen File		
	3. Runi Amanda Amalia,	Dengan Algoritma Triple DES		
	4. Mirsandi	Berbasis Web		

				dalam mengamankan file dokumen pengarsipan, menciptakan sistem keamanan web yang efisien dalam proses keamanan data, pencarian, dan pengunduhan.
2	1. Fandi Ahmad Sitorus, 2. Nurcahyo Budi Nugroho, 3. Usti Fatimah Sari Sitorus Pane	Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA.	2020	Penelitian tersebut, membahas perlunya pembangunan sistem untuk mengamankan data transaksi penjualan di PT. MITSUBISHI ELECTRIC INDONESIA dengan menggunakan kriptografi AES 128 bit. Sistem ini diharapkan dapat membantu perusahaan dalam menangani masalah keamanan data. Hasil penelitian ini adalah pengembangan aplikasi yang menggunakan AES 128 bit untuk mengamankan data transaksi penjualan, membantu admin dalam menjaga keamanan data perusahaan.
3	Dimas Ridho	Implementasi	2022	Penelitian ini fokus pada

Amali		Metode Enkripsi Aes 128 Bit (Rijndael) Pada Keamanan File Kependudukan (Studi Kasus: Kelurahan Gunung Lingai, Samarinda)		mengamankan data kependudukan, terutama Nomor Induk Kependudukan (NIK), Kartu Keluarga, dan data pribadi lainnya, menggunakan metode enkripsi AES 128 Bit. Mereka mengembangkan sistem untuk mengenkripsi dan maendekripsi data dalam format file PDF, DOC, XLS, dan TXT. Evaluasi kinerja menunjukkan tingkat akurasi dekripsi sebesar 90%,
4	1. Raudatul Firdaus, 2. Reva Ragam Santika	Penerapan Algoritma Aes- 128 Untuk Enkripsi Dokumen Di Pt Caveo Biometric Security	2022	Tujuan penelitian tersebut adalah untuk melakukan pengujian terhadap proses pengamanan data yang dilakukan oleh PT Caveo Biometric Security melalui penggunaan Algoritma Kriptografi AES-128. Dengan melakukan pengujian ini, Selain itu, penelitian ini juga bertujuan untuk menguji kehandalan metode

				enkripsi dan dekripsi AES-128 dalam melindungi dokumen-dokumen yang dimasukkan ke dalam aplikasi, serta untuk memverifikasi bahwa akses langsung terhadap data tersebut dapat dihindari oleh pihak yang tidak berwenang.
5	1. Imelda Asih Rohani Simbolon 2. Indra Gunawan 3. Ika Okta Kirana 4. Rafiq Dew 5. S. Solikhun	Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar	2020	penelitian ini berfokus pada implementasi Advanced Encryption Standard (AES) dalam mengamankan data penduduk oleh Dinas Kependudukan dan Pencatatan Sipil. Penelitian ini menyoroti pentingnya menjaga keamanan dan kerahasiaan data penduduk karena melibatkan identitas individu. Menggunakan metode AES untuk diimplementasikan dalam lingkungan tersebut, termasuk bagaimana kunci-kunci enkripsi dihasilkan dan dikelola,

				<p>bagaimana data penduduk dienkripsi dan didekripsi, serta bagaimana efektivitas sistem tersebut dievaluasi. Selain itu, deskripsi juga dapat mencakup contoh kasus atau skenario di mana sistem keamanan data ini diterapkan.</p>
6	1. Fikri Prasetyo 2. Titin Fatimah 3. Mardi Hardjjianto 4. Subandi	Implementasi Algoritma Aes- 128 Untuk Keamanan File Data Kependudukan Berbasis Web Pada Desa Bogares Kidul	2023	<p>Penelitian ini berfokuskan pada Desa Bogares Kidul yang memiliki file dokumen terkomputerisasi, termasuk data kependudukan, yang diamankan menggunakan metode kriptografi AES. Sistem keamanan data berbasis web dikembangkan dengan PHP dan MySQL, menerapkan enkripsi AES pada file data. Hasil menunjukkan bahwa waktu enkripsi dan dekripsi bervariasi berdasarkan ukuran file, dengan AES terbukti efektif dalam menjaga keamanan isi file dalam</p>

Penelitian ini memiliki beberapa perbedaan mendasar dibandingkan dengan penelitian yang terdapat pada Muklas Adik Putra, Dkk (2022) dengan judul “Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen File Dengan Algoritma Triple DES Berbasis Web”. Perbedaan tersebut terutama terletak pada poin-poin berikut:

- a) Penelitian Terdahulu menggunakan algoritma Triple-DES (Data Encryption Standard), yang merupakan salah satu algoritma kriptografi kunci simetri yang lebih tua dan lebih lambat dibandingkan dengan algoritma yang lebih baru. Sedangkan penelitian ini menggunakan algoritma AES (Advanced Encryption Standard) 128-bit, yang dikenal lebih aman, cepat, dan efisien dibandingkan Triple-DES.
- b) Penelitian terdahulu fokus pada pengamanan dokumen berbasis web secara umum. Sedangkan Penelitian ini Fokus spesifik pada keamanan data kependudukan Desa Namo Buaya.
- c) Penelitian terdahulu, hasil penelitian menunjukkan keberhasilan dalam mengamankan file dokumen pengarsipan berbasis web secara cepat dan efisien. Sedangkan penelitian ini mencakup implementasi nyata di Desa Namo Buaya.

Penelitian lainya juga terdapat pada Fandi Ahmad Sitorus, Dkk (2020). Penelitian ini bertujuan untuk mengamankan data transaksi penjualan di PT. MITSUBISHI ELECTRIC INDONESIA dengan menerapkan Algoritma Advanced Encryption Standard (AES) 128 bit. Dengan implementasi ini, diharapkan sistem dapat membantu pihak perusahaan dalam mengatasi masalah keamanan data yang mungkin timbul. Hasil penelitian berupa aplikasi pengamanan data transaksi penjualan yang menggunakan AES 128 bit, membantu admin dalam menjaga

kerahasiaan dan integritas data transaksi di perusahaan tersebut.

Sementara itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan keamanan data kependudukan Desa Namo Buaya dengan menggunakan metode enkripsi AES 128-bit berbasis web. Fokus penelitian ini adalah pada keamanan data kependudukan dalam konteks desa, yang berbeda dengan objek penelitian dari penelitian terdahulu. Meskipun menggunakan algoritma kriptografi yang sama, implementasi dan konteks aplikasi dari kedua penelitian ini menjadi pembeda utama.

Penelitian lainya juga terdapat pada Dimas Ridho Amali, (2022). Dengan judul” IMPLEMENTASI METODE ENKRIPSI AES 128 BIT (RIJNDAEL) PADA KEAMANAN FILE KEPENDUDUKAN (Studi Kasus: Kelurahan Gunung Lingai, Samarinda)”. Penelitian ini bertujuan untuk mengamankan data kependudukan dengan cara mengenkripsi dan mendekripsi file (PDF, DOC, XLS, dan TXT) menggunakan metode enkripsi & dekripsi AES 128 Bit (Rijndael). Penelitian ini menyoroti pentingnya menjaga kerahasiaan data pribadi dan menghindari penyalahgunaan data kependudukan. Hasilnya adalah implementasi sistem yang mampu menghasilkan file kependudukan yang terenkripsi, dengan tingkat akurasi kemiripan antara file asli dan file yang telah didekripsi mencapai 90%.

Sementara itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan keamanan data kependudukan Desa Namo Buaya menggunakan metode enkripsi AES 128-bit berbasis web. Fokus penelitian ini adalah pada pengamanan data kependudukan secara keseluruhan dalam konteks web. Berbeda dengan penelitian terdahulu yang lebih fokus pada pengamanan file data dalam berbagai format, fokus penelitian ini adalah pada keamanan data kependudukan dalam konteks desa, yang berbeda dengan objek penelitian dari penelitian terdahulu. Meskipun menggunakan algoritma kriptografi yang sama, implementasi dan konteks aplikasi dari kedua penelitian ini juga menjadi pembeda utama.

Penelitian lainya juga terdapat pada penelitian Raudatul Firdaus dengan Reva

Ragam Santika, (2022). Dengan judul penelitian “PENERAPAN ALGORITMA AES-128 UNTUK ENKRIPSI DOKUMEN DI PT CAVEO BIOMETRIC SECURITY”. Penelitian ini bertujuan untuk menguji dan mengamankan data dalam sebuah aplikasi yang dikembangkan oleh PT Caveo Biometric Security. Penelitian ini menggunakan metode enkripsi dan dekripsi dengan Algoritma Advanced Encryption Standard (AES-128) untuk menjaga kerahasiaan dan keamanan data yang dimasukkan ke dalam aplikasi tersebut. Metode pengujian yang digunakan adalah metode black box, yang memungkinkan untuk menguji fungsionalitas aplikasi tanpa harus memperhatikan strukturnya.

Sementara itu, penelitian ini lebih berfokus pada perancangan dan implementasi keamanan data kependudukan Desa Namo Buaya menggunakan metode enkripsi AES 128-bit dalam konteks web. Tujuan penelitian ini adalah untuk mengamankan data kependudukan secara keseluruhan dalam aplikasi web, dengan mengintegrasikan metode enkripsi ke dalam sistem untuk menjaga kerahasiaan dan integritas data.

Penelitian lainya juga terdapat pada penelitian Imelda Asih Rohani Simbolon, Dkk (2020), dengan judul penelitian” Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar”. Perbedaan antara penelitian ini dengan penelitian tersebut adalah fokusnya pada institusi dan lingkup penelitian yang berbeda. Penelitian terdahulu meneliti pengamanan data kependudukan di Dinas Dukcapil Kota Pematangsiantar, sedangkan penelitian Anda lebih terfokus pada implementasi keamanan data kependudukan di tingkat desa, yaitu Desa Namo Buaya. Meskipun keduanya menggunakan metode enkripsi AES 128-bit, penelitian ini lebih menitikberatkan pada konteks dan kebutuhan spesifik pada desa tersebut.

Penelitian lainya juga terdapat pada penelitian Fikri Prasetyo, Dkk (2023). dengan judul” IMPLEMENTASI ALGORITMA AES-128 UNTUK KEAMANAN FILE DATA KEPENDUDUKAN BERBASIS WEB PADA DESA BOGARES KIDUL” Perbedaan penelitian ini dengan penelitian tersebut terletak pada fokus dan konteks implementasi. Penelitian tersebut berfokus pada Desa Bogares Kidul

dengan penekanan pada implementasi kriptografi untuk pengamanan file data kependudukan menggunakan algoritma AES-128 dalam sebuah sistem keamanan data berbasis web. Sementara itu, penelitian ini lebih menekankan perancangan dan implementasi keamanan data kependudukan di Desa Namo Buaya dengan metode enkripsi AES 128-bit berbasis web.

2.2 Xampp

Xampp merupakan sebuah aplikasi yang mampu mengubah komputer menjadi server. Xampp memiliki fungsi utama sebagai penyedia jaringan lokal, memungkinkan pengguna untuk membuat website secara offline di komputer masing-masing. Fungsi utama dari Xampp adalah sebagai server website yang digunakan untuk menjalankan website tersebut. Komputer yang menggunakan Xampp harus memberikan layanan untuk mengakses web, sehingga komputer tersebut harus berperan sebagai server. Secara keseluruhan, Xampp adalah sebuah aplikasi yang menyediakan paket perangkat lunak yang mencakup konfigurasi Web Server, Apache, PHP, dan MySQL, membantu dalam proses pembuatan aplikasi web dengan menyatukan komponen-komponen tersebut sehingga mempermudah pengguna dalam mengembangkan program web (Hariyanto, 2012).

2.4 *My Structured Query Language (Mysql)*

MySQL adalah sebuah perangkat lunak yang menyediakan sistem manajemen database SQL (Database Management System) atau DBMS yang bersifat multithread dan multi-user. Penggunaan MySQL cukup luas dengan jumlah pengguna mencapai sekitar 6 juta di seluruh dunia. MySQL AB, yang beroperasi di bawah lisensi GNU General Public License (GPL), menjadikan MySQL tersedia sebagai perangkat lunak gratis. (Parulian, 2017).

MySQL memberikan keuntungan karena dapat digunakan secara bebas oleh siapa pun tanpa perlu membeli lisensi (open source). Ini merupakan sebuah server database yang dapat diakses melalui jaringan internet dari jarak jauh. MySQL memiliki kapasitas yang besar, bahkan mencapai gigabyte, serta memiliki sistem perangkat lunak yang ringan dan tidak membebani kinerja server dari komputer karena bekerja di latar belakang. Selain itu, MySQL dapat diakses oleh berbagai

aplikasi, seperti Visual Basic dan Delphi, dan juga aman karena membutuhkan kata sandi untuk akses, didukung oleh field yang dijadikan sebagai kunci primer dan kunci unik (Putra, 2019).

Dengan demikian, MySQL dapat disimpulkan sebagai sebuah bahasa pemrograman yang ditujukan untuk pengelolaan basis data. Penggunaan MySQL adalah untuk menyimpan data dalam kapasitas besar. Keunggulan MySQL termasuk keamanan database dan ketersediaan tanpa perlu pembelian lisensi.

2.3 Website

Website disebut juga site, situs, situs web, atau portal. Merupakan kumpulan halaman web yang berhubungan antara satu dengan lainnya, halaman pertama sebuah website adalah home page, sedangkan halaman demi halamannya secara mandiri disebut web page, dengan kata lain website adalah situs yang dapat diakses dan dilihat oleh para pengguna internet diseluruh dunia. Website adalah situs yang dapat diakses dan dilihat oleh para pengguna Internet. Pengguna Internet semakin hari semakin bertambah banyak, sehingga hal ini adalah potensi pasar yang berkembang terus (Abbas, 2013).

2.4 Bahasa Pemrograman

Bahasa pemrograman, atau sering diistilahkan juga dengan bahasa komputer atau bahasa pemrograman komputer, adalah instruksi standar untuk memerintah komputer. Bahasa pemrograman ini merupakan suatu himpunan dari aturan sintaks dan semantik yang dipakai untuk mendefinisikan program komputer. Bahasa ini memungkinkan seorang programmer dapat menentukan secara persis data mana yang akan diolah oleh komputer, bagaimana data ini akan disimpan/diteruskan, dan jenis langkah apa secara persis yang akan diambil dalam berbagai situasi.

Menurut tingkat kedekatannya dengan mesin komputer, bahasa pemrograman terdiri dari:

- a) Bahasa Mesin, yaitu memberikan perintah kepada komputer dengan memakai kode bahasa biner, contohnya 01100101100110,
- b) Bahasa Tingkat Rendah, atau dikenal dengan istilah bahasa rakitan

(bah.Ingggris Assembly), yaitu memberikan perintah kepada komputer dengan memakai kode-kode singkat (kode mnemonic), contohnya kode_mesin|MOV, SUB, CMP, JMP, JGE, JL, LOOP, dsb.

- c) Bahasa Tingkat Menengah, yaitu bahasa komputer yang memakai campuran instruksi dalam kata-kata bahasa manusia (lihat contoh Bahasa Tingkat Tinggi di bawah) dan instruksi yang bersifat simbolik, contohnya {, }, ?, <<, >>, &&, ||, dsb.
- d) Bahasa Tingkat Tinggi, yaitu bahasa komputer yang memakai instruksi berasal dari unsur kata-kata bahasa manusia, contohnya begin, end, if, for, while, and, or, dsb. Komputer dapat mengerti bahasa manusia itu diperlukan program compiler atau interpreter.


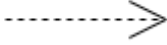
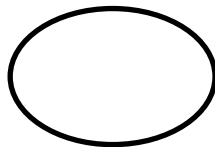
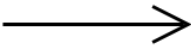
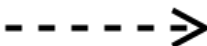
Sebagian besar bahasa pemrograman digolongkan sebagai Bahasa Tingkat Tinggi, hanya bahasa C yang digolongkan sebagai Bahasa Tingkat Menengah dan Assembly yang merupakan Bahasa Tingkat Rendah." (Saragih, 2016, hal. 13).

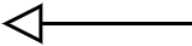
2.4 Use Case

Dalam pemrograman berbasis OOP, untuk mendeskripsikan sistem dapat menggunakan diagram UML. Diagram tersebut terdiri dari 13 jenis diagram yaitu activity, class, communication, component, composite structure, deployment, interaction overview, object, package, sequence, state machine, timing dan use case. Use case merupakan deskripsi fungsi dari sebuah sistem dari perspektif atau sudut pandang para pengguna sistem. Use case mendefinisikan apa yang akan diproses oleh sistem dan komponen-komponennya. Use case bekerja dengan menggunakan scenario yang merupakan deskripsi dari urutan atau langkah-langkah yang menjelaskan apa yang dilakukan oleh user terhadap sistem maupun sebaliknya. Use case mengidentifikasi fungsionalitas yang dimiliki sistem, interaksi user dengan sistem dan keterhubungan antara user dengan fungsionalitas sistem" (Arifin & Hs, 2017, hal. 42–49).

Untuk menggambarannya digunakan beberapa notasi dan simbol untuk itu simbol-simbol Use Case Diagram terdapat pada tabel 2.2

Tabel 2.2 Simbol-Simbol Use Case Diagram


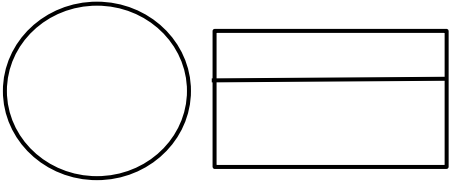
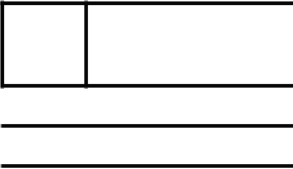
Gambar	Nama	Keterangan
	<i>Actor</i>	Aktor menjelaskan siapa yang berinteraksi dengan sistem. Aktor akan memberikan informasi kepada sistem, serta menerima informasi dari sistem. Keduanya bisa terjadi secara bersamaan.
	<i>Generalisasi</i>	Menunjukkan spesialisasi aktor untuk dapat berpartisipasi dengan use case
	<i>Use Case</i>	Abstraksi dan interaksi antara sistem dan <i>aktor</i> . Untuk menghasilkan suatu hasil yang terukur bagi suatu aktor
	<i>Assosiacion</i>	Abstraksi dari penghubung antara aktor dengan <i>use case</i> . Yang menghubungkan antara objek satu dengan objek yang lainnya.
	<i>Include</i>	Untuk mengidentifikasi hubungan antara 2 <i>use case</i> , dimana <i>use case</i> yang satu akan memanggil <i>use case</i> yang lainnya.

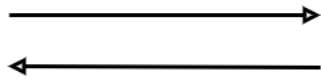
	<i>extend</i>	dimana use case yang dituju berdiri sendiri tanpa harus melewati sebuah proses yang lain
---	---------------	--

2.5 Data Flow Diagram (DFD)

Data Flow Diagram (DFD) adalah representasi grafis yang mengilustrasikan aliran informasi di dalam sebuah sistem, menggunakan simbol-simbol khusus untuk menggambarkan pergerakan data selama proses sistem. Fungsinya meliputi pemodelan sistem, pembuatan model, dan penyampaian desain sistem. Simbol-simbol yang digunakan dalam DFD dapat ditemukan dalam tabel 2.4.

Tabel 2.4 Simbol-Simbol Data flow diagram (DFD)

SIMBOL	KETERANGAN
	<i>External entity</i> , merupakan kesatuan dilingkungan luar sistem yang bisa berupa orang, organisasi atau sistem lain.
	<i>Process</i> , merupakan proses seperti perhitungan aritmatik penulisan suatu formula atau pembuatan laporan.
	<i>DataStore</i> (Simpan Data), dapat berupa suatu file atau database pada sistem komputer atau catatan manual.



Data Flow (Arus Data), arus data ini mengalir diantara proses, simpan data dan kesatuan luar.

Sumber : <https://lamanit.com/data-flow-diagram/>

2.6 *Entity Relationship Diagram (ERD)*

Entity Relationship Diagram (ERD) adalah representasi visual dari model data konseptual yang menghubungkan entitas satu dengan yang lain dalam proses pengembangan basis data relasional. ERD berperan penting sebagai panduan dalam pembuatan database dan memberikan gambaran tentang bagaimana data akan terorganisir dalam database yang akan dibuat (Afiifah, Azzahra & Anggoro, 2022). Untuk mengilustrasikannya, digunakan berbagai notasi dan simbol yang dapat ditemukan dalam tabel 2.3.

Tabel 2.3 Simbol-Simbol *Entity Relationship Diagram (ERD)*

Notasi	Keterangan
	Entitas yaitu kumpulan dari objek yang dapat diidentifikasi secara unik.
	Relasi, yaitu hubungan yang terjadi antara satu atau lebih entitas. Jenis hubungan antara lain: satu ke satu, satu ke banyak, dan banyak ke banyak
	Atribut, yaitu karakteristik dari entity atau relasi yang merupakan penjelasan detail tentang entitas.
	Garis hubungan antara entity dengan atributnya dan himpunan entitas dengan himpunan relasi.



Input/Output data, yaitu proses input/output data, parameter, informasi.

Sumber : <https://kapanpunbisa.blogspot.com/2013/05/pengertian-entity-relationship-diagram.html>

2.7 Data Pribadi

Menurut Kamus Besar Bahasa Indonesia, data adalah keterangan yang benar dan nyata yang dapat dijadikan dasar kajian. Sedangkan 'Pribadi' sendiri memiliki arti manusia sebagai perseorangan (diri manusia atau diri sendiri), sehingga dapat disimpulkan bahwa data pribadi merupakan keterangan yang benar dan nyata yang dimiliki oleh manusia sebagai perseorangan.

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik tidak secara tegas memberikan definisi hukum mengenai data pribadi. Namun, jika dilihat dari sudut pandang penafsiran resmi tentang hak privasi dalam Pasal 26 ayat (1), data pribadi mencakup urusan kehidupan pribadi termasuk riwayat komunikasi seseorang dan informasi tentang individu. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, pada Pasal 1 ayat 27, mendefinisikan data pribadi sebagai "data perseorangan tertentu yang disimpan, dirawat, dijaga kebenarannya, serta dilindungi kerahasiaannya.

Menurut penjelasan dalam Pasal 1 ayat 1 Data Protection Act Inggris tahun 1998, data diartikan sebagai setiap informasi yang diproses melalui peralatan otomatis yang merespons instruksi-instruksi yang diberikan untuk tujuan tertentu dan disimpan dengan maksud untuk diproses. Data juga mencakup informasi yang merupakan bagian dari catatan kesehatan, kerja sosial, pendidikan, atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan. Selain itu, Data Protection Act Inggris tahun 1998 juga menjelaskan bahwa data pribadi adalah informasi yang terkait dengan individu yang masih hidup dan dapat diidentifikasi dari data atau informasi yang dimiliki atau akan dimiliki oleh pengendali data. Data pribadi juga dapat berhubungan dengan karakteristik responden seperti jenis

kelamin, usia, nama, dan lain-lain (Satria, 2022).

2.8 Kriptografi

Kriptografi (Cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu krypto dan graphia. Krypto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi (Ariyus, 2006).

Kriptografi adalah bidang ilmu yang mengkaji metode untuk menyampaikan pesan secara rahasia kepada pihak tujuan. Dengan pesan yang tersampaikan secara tersembunyi, tidak sembarang orang dapat mengaksesnya tanpa memiliki kunci yang sesuai. Kunci dalam kriptografi memegang peranan penting dalam membongkar isi dari pesan yang dikirimkan. Kunci sering kali mengandung petunjuk atau instruksi langsung untuk mengungkap makna dari pesan yang disampaikan (Amara, 2023).

Terdapat beberapa pengertian kriptografi menurut ahli. Nah berikut ini adalah definisi menurut para ahli.

- **Menurut Talbot dan Welsh (2006)**, kriptografi adalah sebuah teknik rahasia dalam penulisan, dengan menggunakan karakter khusus, dan menggunakan huruf dan karakter di luar bentuk aslinya ataupun dengan metode-metode yang lain yang hanya bisa dipahami pihak-pihak yang memproses kunci. Jadi secara umum bisa diartikan sebagai seni menulis atam memecahkan cipher.
- **Menurut Oppliger (2005)** menyatakan bahwa kriptografi bisa diartikan sebagai sebuah proses untuk melindungi data dalam arti yang luas.
- **Menurut Menezes, Oorschot dan Vanstone (1996)**, kriptografi adalah sebuah studi teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, otentikasi entitas serta otentikasi keaslian data dan integritas data. Tidak hanya penyediaan keamanan informasi saja, tetapi juga sebuah himpunan teknik-teknik.

Kriptografi adalah ilmu yang mempelajari atau berfokus pada berbagai teknik matematika yang berhubungan dengan keamanan informasi (otentikasi dan kerahasiaan).

2.9 Plaintext dan Ciphertext

"*Ciphertext* merujuk pada bentuk pesan yang telah dienkripsi dalam kriptografi, yang awalnya dibuat sebagai *plaintext*. Algoritma yang diterapkan untuk melakukan enkripsi pesan dikenal sebagai cipher. Dalam *ciphertext* terdapat informasi dari *plaintext* asli. Proses enkripsi mengubah *plaintext* menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi yang sesuai. Algoritma cipher yang digunakan untuk menghasilkan *ciphertext* merupakan bagian penting dari proses enkripsi.

Ciphertext adalah hasil dari penerapan algoritma enkripsi. Sebelum perkembangan perangkat elektromekanis dan prototipe komputer, algoritma cipher biasanya diterapkan secara manual menggunakan pena dan kertas. Terdapat berbagai jenis cipher, seperti substitusi, substitusi polialfabet, dan transposisi (S, 2023).

Cipherteks (ciphertext): pesan yang telah disandikan sehingga tidak bermakna lagi.

- Tujuan: agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.
- Nama lain: kriptogram (*cryptogram*)
- Cipherteks harus dapat dikembalikan menjadi *plainteks* (Munir, 2006).

Contoh:

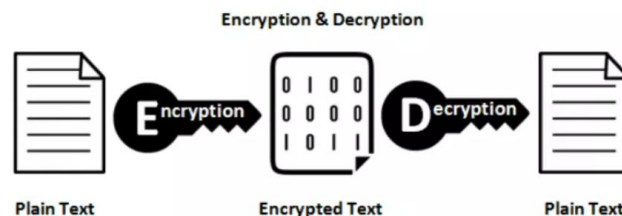
- **Plainteks** : culik anak itu jam 11 siang
- **Cipherteks** : t^\$gfUi89rewoFpfdWqL:p[uTcxz

2.10 Enkripsi dan Dekripsi

Enkripsi adalah proses mengubah bentuk data yang mudah dipahami menjadi kode yang sulit dipahami. Tujuan utama enkripsi adalah untuk meningkatkan keamanan data. Enkripsi digunakan untuk melindungi data dari berbagai jenis kejahatan *cyber* seperti peretasan email, *phishing*, pencurian data, carding, dan lain sebagainya. Caranya dilakukan dengan mengacak data sensitif sehingga menjadi tidak dikenali dalam bentuk aslinya. Dengan demikian, jika

hacker berhasil memperoleh data tersebut, mereka tidak akan dapat dengan mudah menggunakannya (Fuji N, 2022).

Sedangkan Dekripsi merupakan aktivitas mengembalikan data yang telah dienkripsi kembali ke bentuk aslinya yang dapat dibaca. Data yang sebelumnya diubah menjadi tidak terbaca melalui enkripsi akan dikembalikan ke bentuk semula, baik itu berupa teks atau gambar, sehingga dapat dibaca oleh pihak lain termasuk sistem komputer. Proses dekripsi dapat dilakukan secara otomatis atau manual (Arsip Digital, 2020).



Gambar 2.1 contoh proses enkripsi deksripsi

Sumber : <https://www.niagahoster.co.id/blog/apa-itu-enkripsi/>

2.11 Algoritma *Advanced Encryption Standard* (AES) 128 bit (Rijndael)

Advanced Encryption Standard (AES) merupakan sebuah algoritma kriptografi simetris yang digunakan untuk mengamankan data informasi. Algoritma ini merupakan standar enkripsi yang menggunakan kunci simetris. Berbagai mode operasi dapat diterapkan pada algoritma AES, termasuk *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), dan *Output Feedback* (OFB). Implementasi AES dengan mode ECB, CBC, CFB, dan OFB memiliki kelebihan dan kekurangan masing-masing dalam hal tingkat keamanan data. Algoritma kriptografi yang dikenal sebagai Rijndael, dirancang oleh Vincent Rijmen dan John Daemen dari Belgia, menjadi pemenang dalam kontes yang diadakan oleh NIST (*National Institutes of Standards and Technology*) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma *Rijndael* kemudian diadopsi menjadi standar algoritma kriptografi resmi yang dikenal sebagai *Advanced Encryption Standard* (AES) setelah melalui proses standarisasi

oleh NIST pada 2 Mei 2002. Pada tahun 2006, AES telah menjadi salah satu algoritma yang paling populer dalam kriptografi dengan kunci simetris (Prayudha, 2019).

BAB III

METODE PENELITIAN

3.1 Metode dan Pengembangan

Dalam penyusunan penelitian ini, tujuan utama adalah untuk mengidentifikasi, mengatasi, dan memperluas pemahaman mengenai keamanan data kependudukan Desa Namo Buaya. Dengan menggunakan metode enkripsi AES 128-bit berbasis web, penelitian ini bertujuan untuk menawarkan solusi yang kokoh dan efektif dalam melindungi data sensitif tersebut. Penelitian ini tidak hanya mencari jawaban atas masalah yang dihadapi, tetapi juga berupaya untuk membuka wawasan baru melalui pendekatan ilmiah yang sistematis.

Dengan demikian, proses penelitian ini tidak hanya menjadi sarana untuk mengatasi tantangan keamanan data yang ada, tetapi juga menjadi kesempatan untuk menghasilkan pengetahuan yang berharga dalam domain ini. Secara lebih spesifik, penelitian ini akan mengadopsi pendekatan yang komprehensif dalam merancang dan menerapkan sistem keamanan berbasis web. Melalui penerapan metode enkripsi AES 128-bit, penelitian ini bertujuan untuk memberikan solusi yang terukur dan efektif dalam melindungi integritas dan kerahasiaan data kependudukan Desa Namo Buaya.

3.2 Bahan/Data

Dalam proses penelitian, terdapat bahan atau data yang akan diolah untuk mendukung pembuatan sistem yang direncanakan, dalam pengembangan sistem enkripsi ini, data yang menjadi fokus adalah File Kependudukan yang di peroleh dari Desa Namo Buaya, berupa data penduduk setempat yang merupakan informasi yang sangat penting dan bersifat rahasia, seperti Nomor Induk Kependudukan (NIK), Nama Lengkap, Jenis Kelamin, Alamat, dan informasi pribadi lainnya. Seperti yang ditunjukkan dalam **Gambar 3.1**.

Gambar 3. 1 File Kependudukan Desa Namo Buaya

3.2.1 Metode Pengumpulan Data

Metode yang digunakan untuk mengumpulkan data dalam penelitian ini adalah melalui penggunaan data primer. Data primer merujuk pada data yang diperoleh langsung oleh peneliti dari instansi terkait dengan tujuan khusus untuk menyelesaikan permasalahan yang ada. Pengumpulan data dilakukan di Desa Namo Buaya dan data tersebut diperoleh dalam bentuk dokumen file. Data ini nantinya akan menjadi sampel yang digunakan dalam implementasi metode enkripsi AES 128 Bit pada file kependudukan.

3.2.2 Analisis Sistem Lama

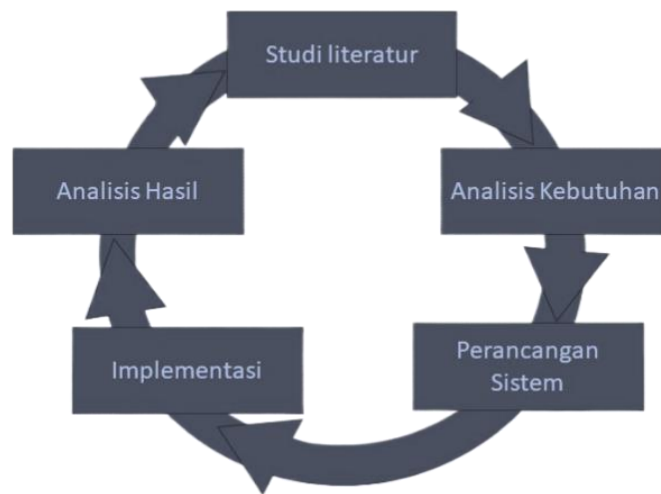
Saat ini, sistem yang digunakan adalah penyimpanan data kependudukan dalam format file Excel atau Teks di komputer Kantor Desa. Sistem ini tidak memiliki cadangan data yang tersimpan secara online dan aman. Kekurangan ini sangat signifikan karena ketika perangkat mengalami kerusakan atau data bocor, kemungkinan penyalahgunaan oleh pihak yang tidak bertanggung jawab sangat besar. Sistem yang berjalan pada saat ini hanya sebatas user menginput data yang menyimpan data secara offline dan akan di simpan di perangkat komputer tersebut. Kantor desa Namo buaya memiliki beberapa kekurangan dalam sistem yang digunakan saat ini, termasuk:

- a) Tidak adanya cadangan penyimpanan file kependudukan secara online.
- b) Tidak ada perlindungan keamanan data untuk menjaga kerahasiaan file kependudukan.

Tanpa sistem yang memadai untuk menyimpan dan melindungi file kependudukan, akan timbul ancaman terhadap kerahasiaan informasi yang dimiliki oleh Kantor Desa . Keterbatasan ini mendorong Kantor Desa Namo Buaya untuk memiliki sistem keamanan data yang lebih baik lagi .

3.3 Tahap Penelitian

Tahapan penelitian untuk judul "Perancangan dan Implementasi Keamanan Data Kependudukan Desa Namo Buaya Menggunakan Metode Enkripsi AES 128-bit berbasis Web" dapat di lihat sebagai gambar 3.4 berikut :



Gambar 3.4 Tahap Penelitian

Pada gambar 3.4 menjelaskan bahwa tahapan pertama adalah dengan melakukan :1. Tahapan Studi literatur, langkah ini untuk memahami konsep dasar tentang keamanan data, enkripsi, dan metode AES (Advanced Encryption Standard) 128-bit. Meneliti juga tentang implementasi keamanan data berbasis web. 2. Analisis Kebutuhan, Menganalisis kebutuhan keamanan data khususnya dalam konteks kependudukan Desa Namo Buaya. Ini termasuk jenis data yang akan dienkripsi, tingkat keamanan yang diinginkan, dan infrastruktur teknologi yang tersedia. 3. Perancangan Sistem, dengan Merancang sistem keamanan data berbasis web yang menggunakan metode enkripsi AES 128-bit. Ini mencakup desain arsitektur sistem, struktur basis data, antarmuka pengguna, dan algoritma enkripsi yang akan digunakan. 4. Implementasi, Mengimplementasikan sistem keamanan data yang telah dirancang ke dalam lingkungan nyata Desa Namo Buaya. Ini

melibatkan pengembangan perangkat lunak, konfigurasi server, dan integrasi dengan infrastruktur IT yang sudah ada. Dan tahapan terakhir ialah 5. Analisis Hasil, Menganalisis hasil pengujian dan evaluasi untuk mengevaluasi keefektifan sistem keamanan data yang telah diimplementasikan. Mengidentifikasi kekuatan dan kelemahan sistem serta mengevaluasi apakah sistem telah memenuhi kebutuhan keamanan data yang telah ditetapkan.

Dengan mengikuti tahapan-tahapan tersebut, penelitian ini diharapkan dapat menghasilkan implementasi yang efektif dan efisien dari sistem keamanan data berbasis web menggunakan metode enkripsi AES 128-bit untuk Desa Namo Buaya.

3.3 Lokasi dan Objek Penelitian

Lokasi dan objek dalam penelitian Perancangan dan Implementasi Keamanan Data Kependudukan Desa Namo Buaya Menggunakan Metode Enkripsi AES 128-bit berbasis Web dapat dilihat sebagai berikut:

3.3.1 Lokasi

Untuk memperoleh data yang diperlukan dalam penelitian ini, penelitian dilakukan di Kantor Kepala Desa Namo Buaya, Kecamatan Sultan Daulat, Kota Subulussalam

3.3.2 Objek Penelitian

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan data yang bertujuan untuk melindungi informasi kependudukan Desa Namo Buaya. Sistem ini menggunakan metode enkripsi AES (Advanced Encryption Standard) 128-bit sebagai mekanisme utama untuk mengamankan data. Implementasi sistem dilakukan dalam lingkungan web, memungkinkan akses data kependudukan secara online. Dengan demikian, warga Desa Namo Buaya dan pihak berwenang dapat mengakses data dengan aman melalui antarmuka web yang telah disediakan.

Langkah-langkah yang akan diambil dalam penelitian ini mencakup memahami konsep dasar tentang keamanan data, analisis kebutuhan keamanan data, perancangan sistem keamanan berbasis web, implementasi teknologi enkripsi AES 128-bit, serta menganalisis hasil pengujian dan evaluasi untuk mengevaluasi keefektifan sistem keamanan data yang telah diimplementasikan. Diharapkan

bahwa hasil penelitian ini akan memberikan kontribusi dalam meningkatkan keamanan dan kerahasiaan data kependudukan Desa Namo Buaya serta menjadi model bagi desa-desa lainnya yang ingin meningkatkan keamanan informasi mereka.

3.4 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem adalah langkah kunci dalam siklus pengembangan sistem yang memastikan bahwa sistem yang dibangun akan memenuhi tujuan bisnis dan kebutuhan pengguna dengan efektif, berikut adalah analisis sistem yang diperlukan untuk mencapai tujuan penelitian, dalam Perancangan dan Implementasi Keamanan Data Kependudukan Desa Namo Buaya Menggunakan Metode Enkripsi AES 128-bit berbasis Web.

3.4.1 Analisis Fungsional

Analisis Fungsional merupakan analisis yang berkaitan dengan fitur atau fasilitas yang diperlukan oleh sistem secara umum. Kebutuhan Fungsional pada sistem yang akan dibangun meliputi :

a) Analisis Kebutuhan Input:

1. Input Data Kependudukan: Informasi yang dimasukkan dalam sistem berupa file kependudukan yang mencakup NIK, Nama, Jenis Kelamin, Tempat Lahir, Agama, Status, Pekerjaan, dan Alamat.
2. Input Kunci Simetri untuk Enkripsi: Kunci yang digunakan dalam proses enkripsi dan dekripsi, harus terdiri dari 16 karakter dan digunakan sebagai parameter untuk mengamankan data.

b) Analisis Kebutuhan Proses:

1. Proses Pra-Pemrosesan: Proses awal untuk mempersiapkan file kependudukan sebelum dilakukan enkripsi.
2. Proses Enkripsi: Tahap dimana file kependudukan diubah dari bentuk teks biasa (plaintext) menjadi kode yang tidak mudah dimengerti (ciphertext) menggunakan kunci simetri.
3. Proses Dekripsi: Proses terbalik dari enkripsi, dimana file ciphertext

dikembalikan menjadi plaintext dengan menggunakan kunci yang sama.

c) Analisis Kebutuhan Output:

1. Output Enkripsi: Hasil dari proses enkripsi disimpan dalam format file *.rda yang berisi ciphertext, yaitu teks terenkripsi.
2. Output Dekripsi: Hasil dari proses dekripsi disimpan dalam format file yang sama dengan file input awal, sehingga data kembali dalam bentuk yang dapat dibaca dan dimengerti.

3.5.2 Analisis Non-Fungsional

Kebutuhan non-fungsional mencakup spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini. Rincian kebutuhan non-fungsional adalah sebagai berikut:

1) Perangkat Keras (Hardware):

- Laptop MSI Modern14 sebagai perangkat utama untuk membangun dan mengimplementasikan sistem.
- Prosesor Intel Core i3.
- Memori RAM sebesar 8 GB.
- Harddisk dengan kapasitas 1 TB , serta SSD sebesar 256 GB.

2) Perangkat Lunak (Software):

- Visual Studio Code digunakan sebagai editor teks untuk pengembangan aplikasi menggunakan bahasa pemrograman PHP.
- XAMPP digunakan sebagai server lokal untuk pengembangan website.

Dengan memenuhi kebutuhan non-fungsional ini, diharapkan penelitian dapat dilakukan dengan efisien dan sistem dapat berjalan dengan baik dalam lingkungan yang telah ditentukan.

3.5 Perancangan Sistem

Dalam perancangan sistem untuk implementasi keamanan data kependudukan Desa Namo Buaya menggunakan metode enkripsi AES 128-bit berbasis web, beberapa langkah perlu dilakukan diantaranya sebagai berikut.

3.5.1 Perancangan Use Case Diagram

Use Case Diagram akan memberikan gambaran yang jelas tentang bagaimana

aktor-aktor berinteraksi dengan sistem keamanan data dan fungsi-fungsi utama yang diperlukan untuk mencapai tujuan implementasi keamanan data kependudukan Desa Namo Buaya seperti berikut.



Gambar 3.5 Use Case Diagram

Pada gambar 3.5 terdapat 1 aktor yaitu Admin yang terlibat dalam sebuah sistem, dimana admin berperan dalam melakukan enkripsi dan dekripsi pada file kependudukan

3.6 Diagram Konteks

Diagram konteks digunakan untuk menggambarkan relasi-relasi antar sistem, berikut merupakan diagram konteks pada Perancangan dan Implementasi Keamanan Data Kependudukan Desa Namo Buaya Menggunakan Metode Enkripsi AES 128-bit berbasis Website.

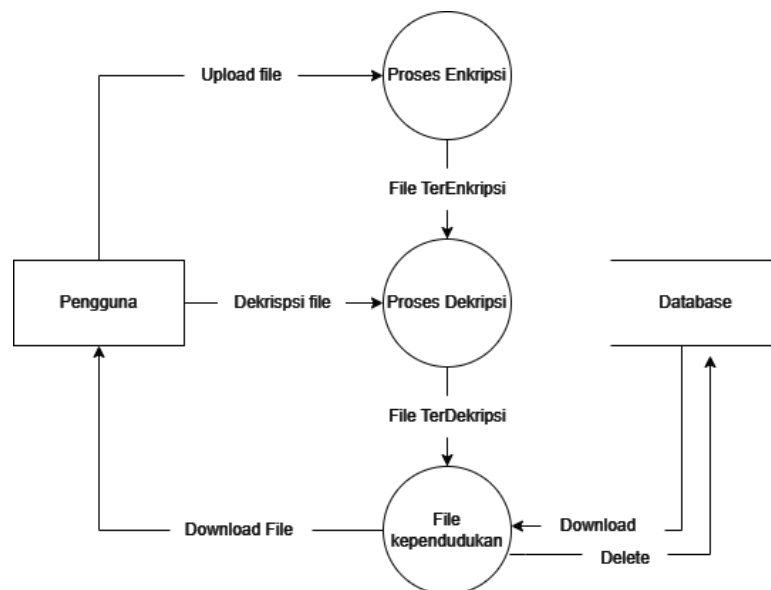


Gambar 3.6 Digram Konteks

Dalam Gambar 3.6 dapat di pahami bahwa Admin melakukan akses kepada sistem website keamanan data kependudukan pada Desa Namo Buaya dengan mengelola file kependudukan untuk melakukan enkripsi serta dekripsi pada file kependudukan Namo Buaya dan setelah melakukan Enkripsi Dekripsi maka akan tersimpan pada database nantinya.

3.7 Rancangan Data Flow Diagram (DFD) level 0 Proses Enkripsi dan Dekripsi

DFD level 1 Proses Enkripsi menyajikan gambaran yang jelas tentang alur data dalam sistem saat proses enkripsi dilakukan. Ini membantu dalam memahami interaksi antara entitas, proses, dan data dalam sistem yang terlibat dalam proses keamanan informasi, rancangan DFD level 0 pada sistem keamanan file kependudukan desa Namo Buaya dapat di lihat pada gamabar berikut:

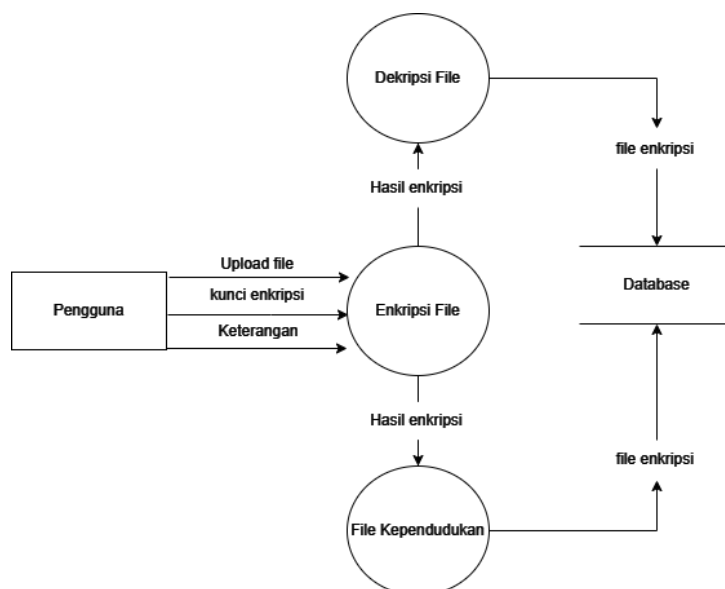


Gambar 3.7 DFD level 0 Proses Enkripsi dan Dekripsi

Dalam Gambar 3.7 dapat di pahami bahwa Rancangan *Data Flow Diagram* (DFD) Level 0 mendeskripsikan rincian proses dari diagram konteks yang menjelaskan kegiatan yang dilakukan oleh Pengguna terhadap sistem yang akan digunakan yang terdiri dari pengguna melakukan upload file terlebih dahulu dan melakukan proses enkripsi file pada file kependudukan yang akan di enkripsi, dan setelah melakukan enkripsi file otomatis akan masuk kedalam menu dekripsi untuk di dekripsikan nantinya sehingga bisa membuka file tersebut. Dan setelah melakukan enkripsi dekripsi maka semua file tersebut akan masuk ke dalam menu file kependudukan yang tersimpan pada database, di dalam menu file kependudukan tersebut juga dapat melakukan download file jika di inginkan.

3.8 Rancangan *Data Flow Diagram* (DFD) level 1 Proses Enkripsi

DFD level 1 Proses Enkripsi memberikan gambaran yang jelas tentang bagaimana data mengalir dalam sistem selama proses enkripsi dilakukan. Ini membantu dalam memahami interaksi antara entitas, proses, dan data yang terlibat dalam menjaga keamanan informasi melalui enkripsi, rancangan DFD level 1 pada sistem keamanan file kependudukan desa Namo Buaya dapat di lihat pada gamabar berikut:

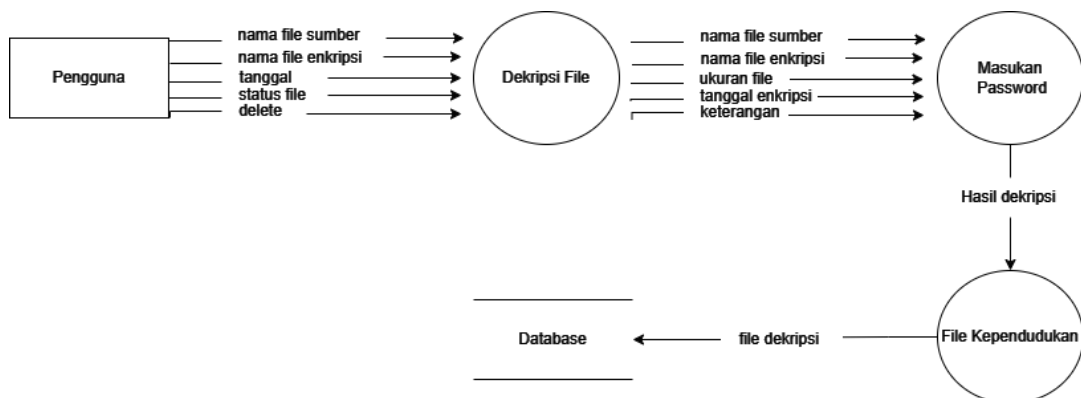


Gambar 3.8 Rancangan *Data Flow Diagram* (DFD) level 1 Proses Enkripsi

Dalam Gambar 3.8 dapat di pahami bahwa Rancangan *Data Flow Diagram* (DFD) Level 1 mendeskripsikan rincian proses dari *enkripsi* file kependudukan pada desa Namo Buaya yang berawal dari pengguna mengupload file kependudukan yang akan di enkripsi,dan menguncinya dengan kata sandi yang akan di berikan, lalu memberikan keterangan pada file tersebut, dan melakukan proses *Enkripsi* sehingga file yang telah di enkripsi akan berlanjut ke dalam penDekripsian file lalu file itu akan masuk kedalam database, begitu juga dengan hasil enkripsi yang berlanjut ke dalam file kependudukan yang di mana menampung semua file yang sudah di enkripsi dan di dekripsi sehingga tertampung kedalam database.

3.9 Rancangan *Data Flow Diagram* (DFD) level 2 Proses Dekripsi

DFD level 2 Proses Dekripsi memberikan gambaran yang lebih terperinci tentang bagaimana data mengalir dalam sistem saat proses dekripsi dilakukan. Ini membantu dalam memahami interaksi antara entitas, proses, dan data dalam sistem yang terlibat dalam menjaga keamanan informasi dengan mengembalikan data terenripsi ke bentuk aslinya, rancangan DFD level 1 pada sistem keamanan file kependudukan desa Namo Buaya dapat di lihat pada gamabar berikut:



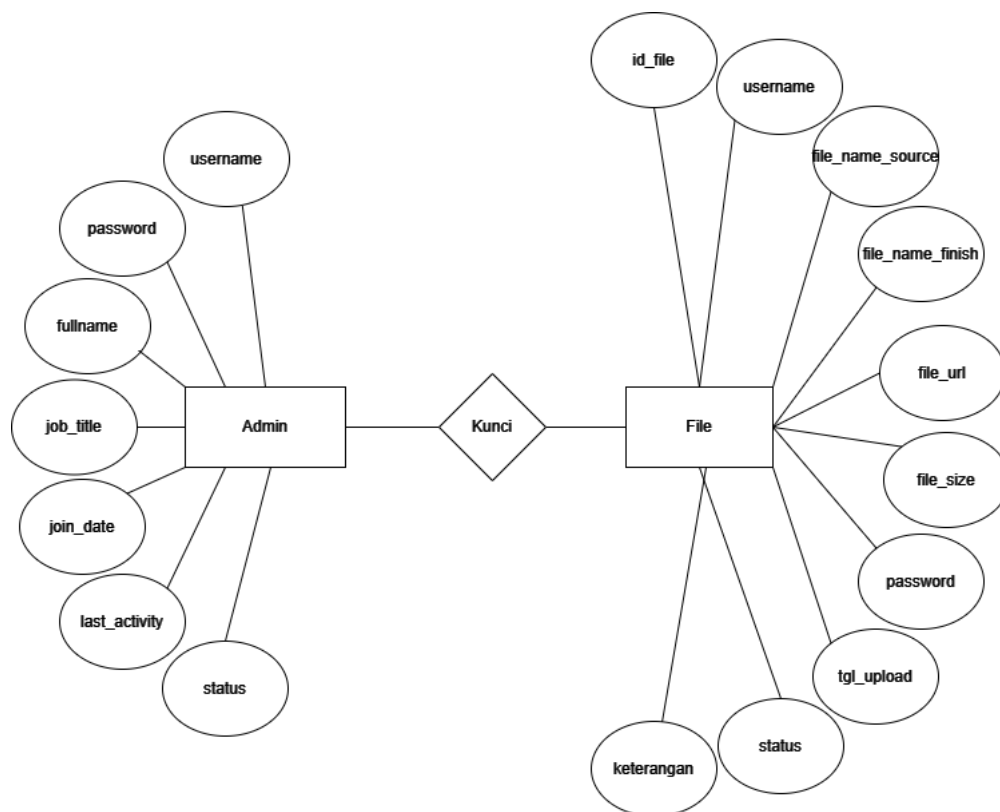
Gambar 3.9 Rancangan *Data Flow Diagram* (DFD) level 2 Proses Dekripsi

Dalam Gambar 3.9 dapat di pahami bahwa Rancangan *Data Flow Diagram* (DFD) Level 1 mendeskripsikan rincian proses dari *Dekripsi* file kependudukan pada desa Namo Buaya yang berawal dari pengguna dapat melihat nama file sumber (nama

awal file), nama file *enkripsi* (nama setelah di *enkripsi*), serta dapat melihat tanggal file, status file, serta menghapusnya, lalu masuk pada proses dekripsi file yang di mana akan menampilkan nama file, nama file enkripsi, ukuran file, tanggal enkripsi, dan keterangan, setelah itu memasukan kata kunci (password) setelah memasukan password maka hasil dekripsi akan masuk kedalam menu file kependudukan, di dalam file kependudukan akan masuk ke dalam database.

3.10 Rancangan *Entity Relationship Diagram* (ERD)

Entity Relationship Diagram (ERD) bertujuan untuk mempermudah perancangan database. Berikut merupakan *Entity Relationship Diagram* pada Perancangan dan Implementasi Keamanan Data Kependudukan Desa Namo Buaya Menggunakan Metode Enkripsi AES 128-bit berbasis Website.



Gambar 3.7 *Entity Relationship Diagram* (ERD)

Pada gambar 3.7 merupakan *Entity Relationship Diagram* (ERD) yang menjelaskan hubungan antar data dalam basis data berdasarkan objek data yang mempunyai hubungan dalam relasi, Terdapat dua komponen utama dalam gambar

ini, yaitu pengguna (Admin) dan berkas (file kependudukan). Setiap komponen memiliki atribut-atributnya sendiri, sebagaimana terlihat dalam gambar tersebut.

3.11 Rancangan User Interface

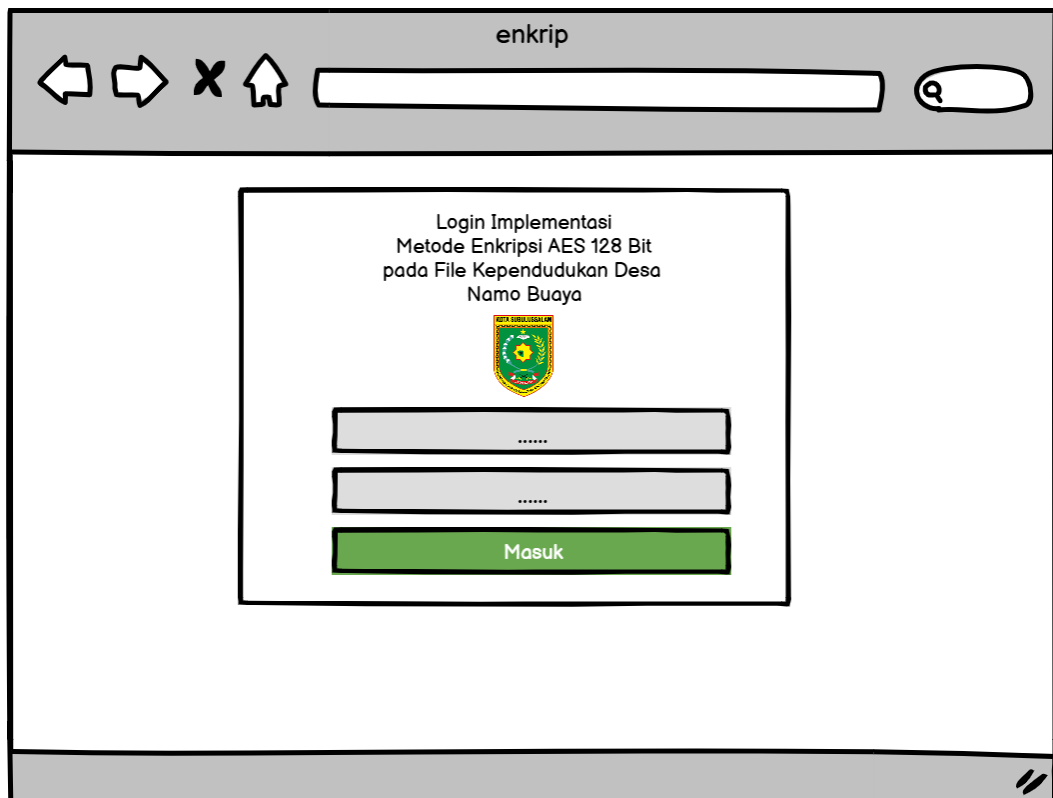
Rancangan User Interface (UI) untuk sistem keamanan data kependudukan Desa Namo Buaya akan mempertimbangkan kebutuhan pengguna dalam mengakses dan mengelola data dengan aman dan efisien.

a) Rancangan User Interface

Rancangan *User Interface* (UI) ini akan memperhatikan prinsip-prinsip desain UX (User Experience) untuk memberikan pengalaman pengguna yang intuitif, efisien, dan aman dalam mengakses dan mengelola data kependudukan dengan metode enkripsi AES 128-bit berbasis web.

1. Halaman Login

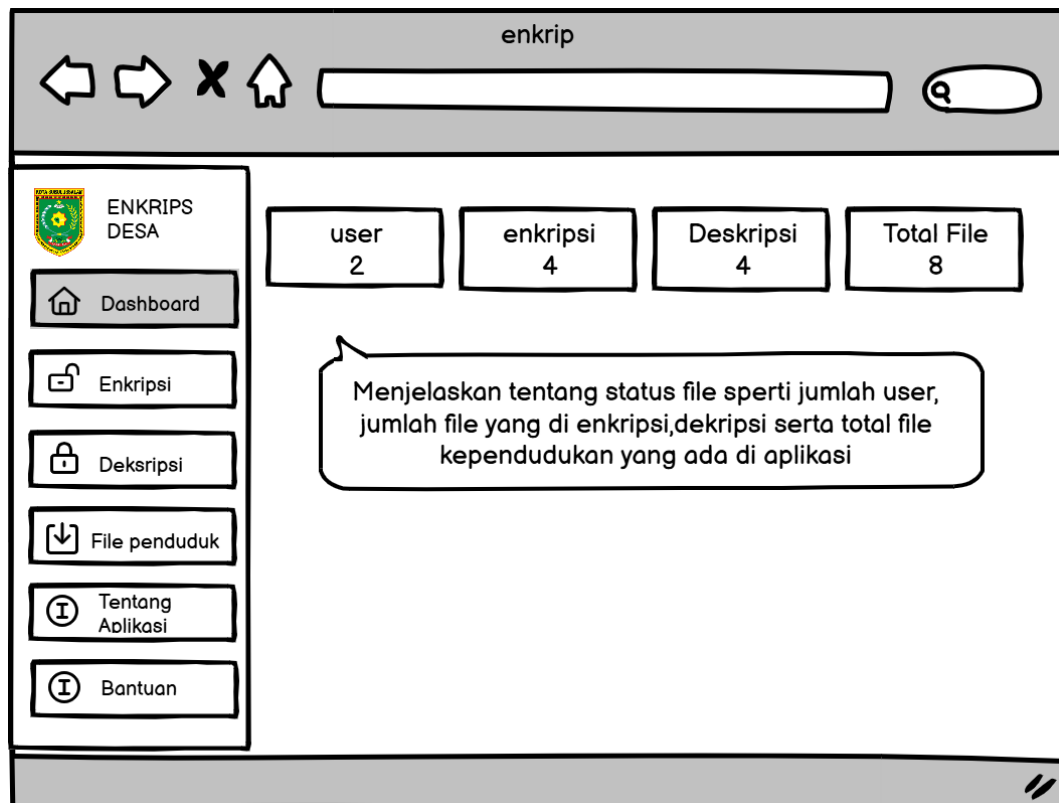
Pada Halaman login ini dirancang dengan fokus pada kemudahan penggunaan dan keamanan. Desainnya bersih dan minimalis, dengan form login yang mencakup kolom input untuk username dan password. Tombol masuk yang terletak di bawah form memudahkan pengguna untuk masuk ke dalam sistem. Terdapat juga lambang kota subulussalam dengan tulisan “Login Implementasi Metode Enkripsi AES 128 Bit Pada File Kependudukan Desa Namo Buaya. Desain responsif memastikan tampilan yang baik di berbagai perangkat, Dengan demikian, halaman login memberikan pengalaman yang intuitif dan aman bagi pengguna. Berikut adalah gambaran halaman login pada gambar 3.8.



Gambar 3.8 Rancangan halaman login Admin.

2. Halaman Dashboard

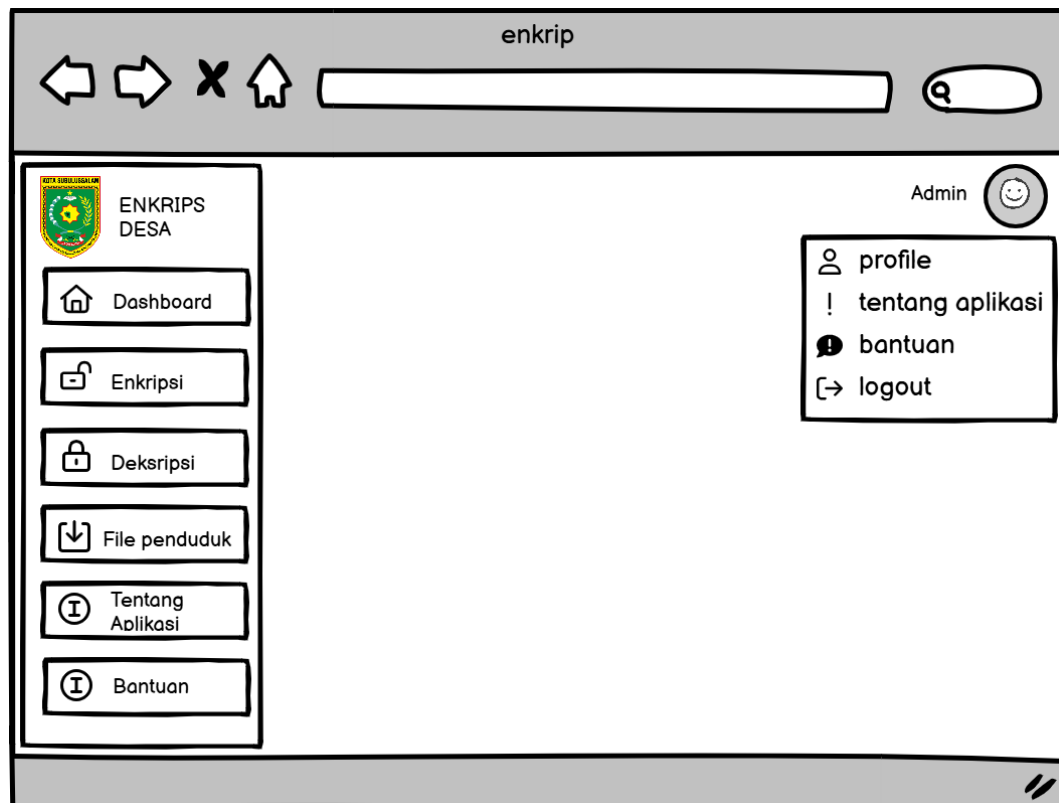
Halaman dashboard admin adalah pusat kontrol yang memberikan informasi terkini tentang sistem. Di sini, admin dapat melihat status penting, termasuk jumlah pengguna terdaftar, jumlah file yang telah dienkripsi dan didekripsi, serta total keseluruhan file kependudukan dalam aplikasi. Desainnya dirancang untuk memberikan informasi ini dengan jelas dan mudah dipahami. Selain itu, grafik atau diagram dapat digunakan untuk memberikan visualisasi yang lebih baik tentang aktivitas enkripsi dan dekripsi. Desain responsif memastikan tampilan yang baik di berbagai perangkat, memungkinkan admin untuk mengakses dashboard dengan mudah seperti pada gambar 3.9 berikut.



Gambar 3.9 Rancangan Halaman Dashbord

3. Pop Up Profile Admin

Halaman pop-up profil admin adalah antarmuka yang muncul ketika admin mengklik atau mengarahkan kursor mereka ke profil mereka sendiri. Desainnya bertujuan untuk memberikan akses cepat dan intuitif ke informasi profil penting tentang admin. Di sini, admin dapat melihat dan mengedit informasi profil mereka, seperti nama, alamat email, dan gambar profil. Selain itu, halaman pop-up admin mungkin juga memuat fitur tambahan, seperti tentang aplikasi, bantuan serta Logout untuk keluar dari akun. Desainnya harus sederhana dan mudah dipahami,. Desain responsif penting agar halaman pop-up profil dapat diakses dengan baik seperti pada gambar 3.10.



Gambar 3.10 Pop Up *Profile* Admin

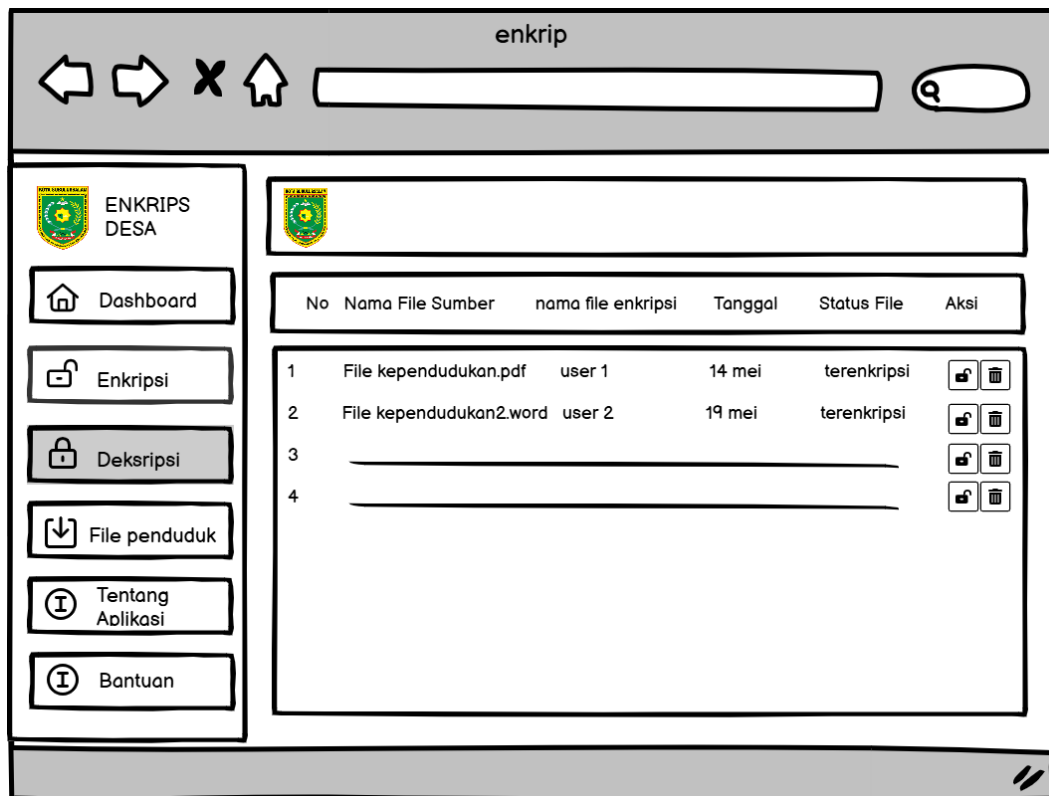
4. Halaman Enkripsi File

Pada Halaman enkripsi dirancang untuk memfasilitasi proses enkripsi file dengan cara yang sederhana dan efisien. Pengguna, dalam hal ini admin, dapat dengan mudah mengunggah file yang ingin dienkripsi melalui area yang disediakan. Mereka juga dapat memasukkan kunci enkripsi yang diperlukan dan memberikan keterangan tambahan tentang file tersebut. Setelah semua informasi dimasukkan, admin hanya perlu menekan tombol "Enkripsi File" untuk memulai proses enkripsi. Tombol "Reset" juga tersedia untuk memungkinkan admin membatalkan atau mengulang proses jika diperlukan. Halaman ini didesain untuk memberikan pengalaman pengguna yang intuitif dan efisien, memastikan bahwa admin dapat dengan mudah mengamankan file mereka dengan enkripsi seperti pada gambar 3.11 berikut.

Gambar 3.11 Halaman *User Interface Enkripsi*

5. Halaman Dekripsi File

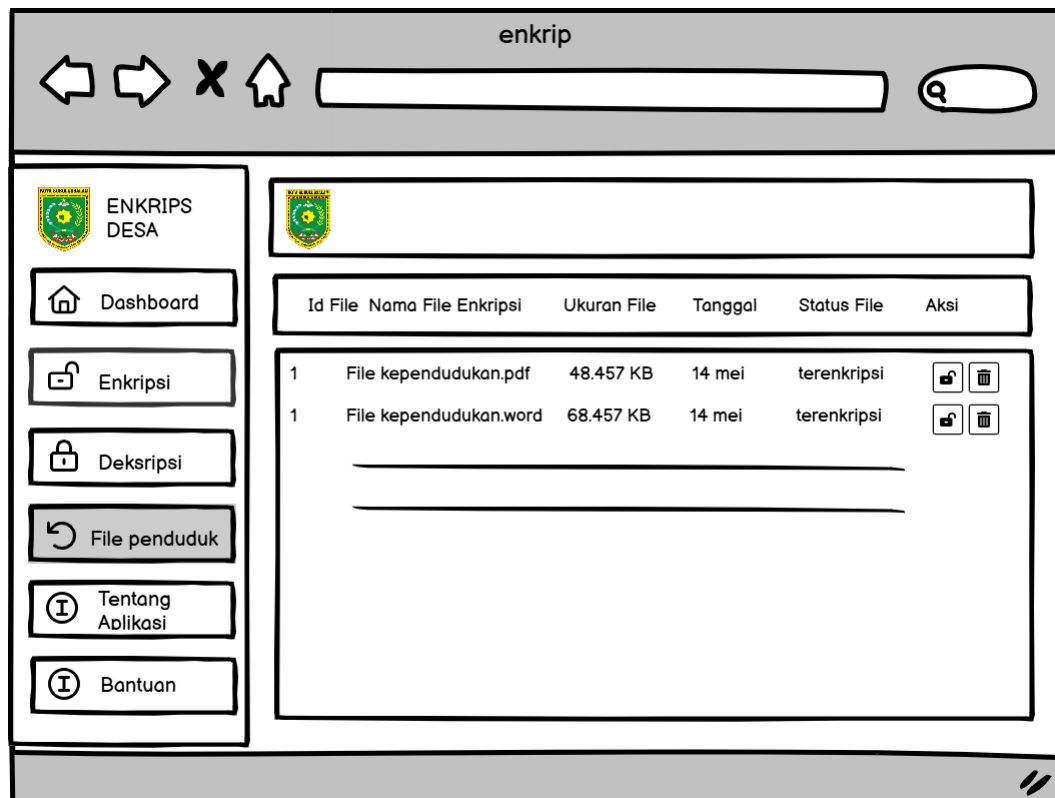
Pada halaman dekripsi file disiapkan untuk memudahkan proses dekripsi dengan efisiensi. Admin dapat dengan jelas melihat daftar file yang siap untuk didekripsi. Informasi yang ditampilkan meliputi nomor urut file, nama file sumber sebelum enkripsi, nama file yang dienkrpsi, tanggal enkripsi, dan status file. Setiap file dilengkapi dengan tombol aksi, seperti "Hapus" untuk menghapus file yang tidak diperlukan lagi dan "Dekripsi" untuk memulai proses dekripsi. Halaman ini didesain untuk memberikan pengalaman pengguna yang lancar dan efektif dalam mengelola file yang dienkrpsi seperti pada gambar 3.12 berikut.



Gambar 3.12 Rancangan User Interface Dekripsi

6. Halaman File Kependudukan

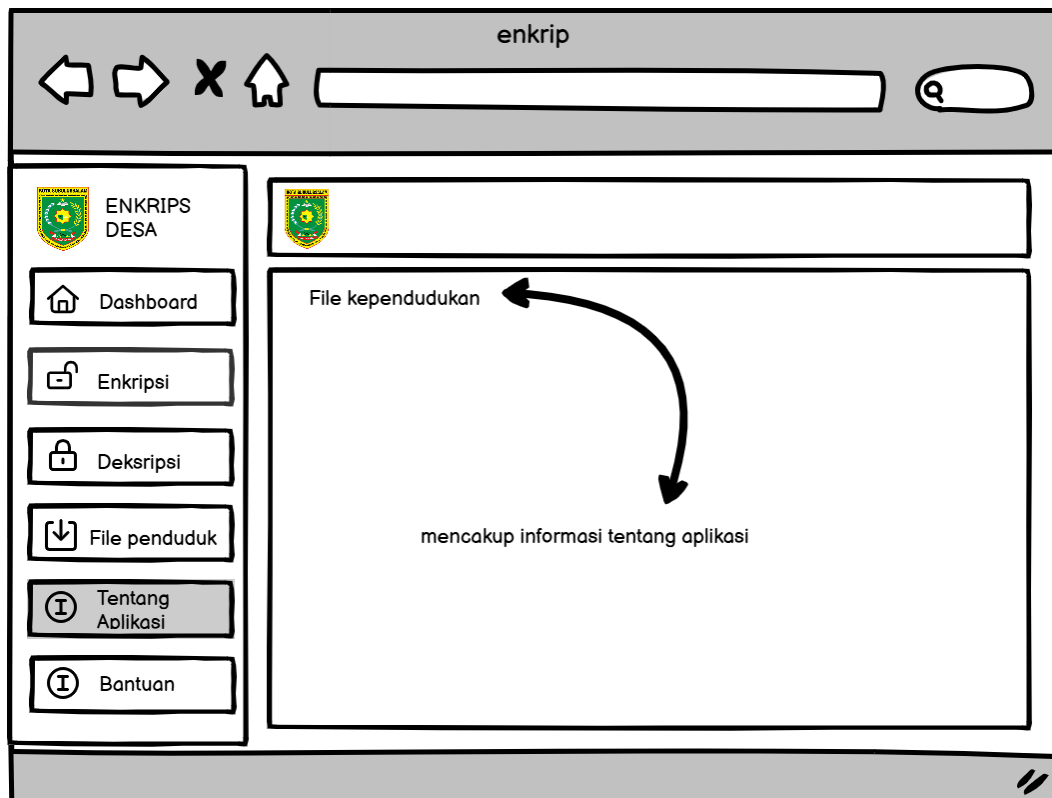
Pada halaman File Kependudukan dirancang untuk memberikan admin informasi terkait file kependudukan dalam sistem dengan jelas dan mudah diakses. Di sini, admin dapat melihat kolom-kolom seperti Id File yang menunjukkan nomor identifikasi unik untuk setiap file, Nama File Enkripsi untuk mengidentifikasi nama file yang telah dienkripsi, Ukuran File untuk mengetahui seberapa besar setiap file, Tanggal untuk melacak kapan file tersebut dibuat atau dimasukkan ke dalam sistem, Status File untuk mengetahui apakah file aktif atau tidak, dan tombol Aksi yang menyediakan opsi seperti melihat, mengedit, atau menghapus file. Dengan desain yang jelas dan informatif, halaman ini memungkinkan admin untuk mengelola file kependudukan dengan efisiensi dan akurasi seperti pada gambar 3.13 berikut.



Gambar 3.13 Rancangan User Interface Halaman File Kependudukan

7. Halaman Tentang Aplikasi

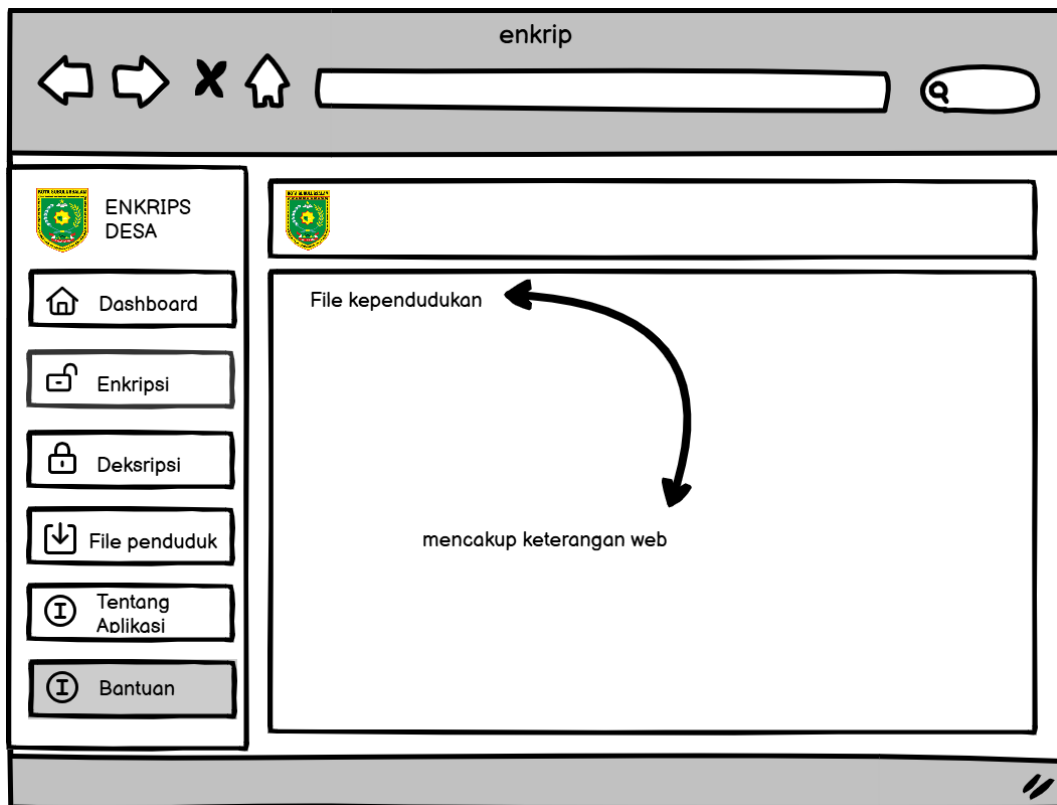
Pada halaman Tentang Aplikasi adalah bagian penting dari antarmuka pengguna yang memberikan informasi rinci tentang aplikasi tersebut. Di sini, pengguna dapat menemukan deskripsi singkat tentang tujuan dan tujuan aplikasi, serta informasi tentang tim pengembang atau perusahaan di balik aplikasi. Halaman ini juga dapat mencakup fitur-fitur utama dari aplikasi, panduan pengguna, dan FAQ yang berguna untuk membantu pengguna memahami cara menggunakan aplikasi dengan lebih baik. Desainnya biasanya sederhana dan informatif, dengan penekanan pada keterbacaan dan navigasi yang intuitif. Halaman Tentang Aplikasi bertujuan untuk membangun kepercayaan pengguna terhadap aplikasi, memberikan pemahaman yang jelas tentang apa yang bisa diharapkan dari aplikasi tersebut, dan menyediakan sumber informasi yang berguna bagi pengguna yang ingin mengetahui lebih lanjut tentang aplikasi seperti pada gambar 3.14 berikut.



Gambar 3.14 Halaman Tentang Aplikasi

8. Halaman Bantuan

Halaman Bantuan adalah sumber informasi yang penting bagi pengguna yang membutuhkan panduan atau bantuan terkait penggunaan aplikasi. Di sini, pengguna dapat menemukan berbagai artikel bantuan, tutorial, dan petunjuk langkah-demi-langkah tentang cara menggunakan fitur-fitur aplikasi dengan efektif. Halaman ini juga dapat mencakup daftar pertanyaan umum (FAQ) yang sering diajukan oleh pengguna beserta jawabannya. Desainnya dirancang untuk mudah dinavigasi, dengan kategori yang jelas dan penjelasan yang singkat tentang setiap topik bantuan. Selain itu, Dengan menyediakan sumber informasi yang komprehensif dan mudah diakses, halaman Bantuan bertujuan untuk meningkatkan pengalaman pengguna dengan memastikan bahwa pengguna memiliki akses ke bantuan yang mereka butuhkan saat menggunakan aplikasi seperti pada gambar 3.15 berikut.



Gambar 3.15 Rancangan User Interface Halaman Bantuan

- Wibowo, Y. A., Nugroho, N. B., & Andika, B. (2022). Penerapan Algoritma AES 128 Bit Untuk Keamanan Data Peminjaman Senjata Api Pada DENPOM I/5 Medan. *Jurnal Cyber Tech*, 2(12).
- Abdulloh, R. (2015). *Web Programing is Easy*. Jakarta: PT Elex Media Komputindo.
- Hariyanto, B. (2012). **Esensi-Esensi Bahasa Pemograman Java: revisi keempat**. Bandung: Informatika.
- Putra, A. B. (2019, October). Perancangan dan Pembangunan Sistem Informasi E-Learning Berbasis Web (Studi Kasus Pada Madrasah Aliyah Kare Madiun). In *Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi (SENATIK)* (Vol. 2, No. 1, pp. 81-85).
- Abbas, W. (2013). Analisa kepuasan mahasiswa terhadap website Universitas Negeri Yogyakarta (UNY). In *Prosiding Seminar Sains Nasional dan Teknologi* (Vol. 1, No. 1).
- Saragih, R. R. (2016). Pemrograman dan bahasa Pemrograman. *STMIK-STIE Mikroskil*, 1-91.
- Arifin, M., & Hs, R. H. H. (2017). Perancangan Sistem Informasi Pusat Karir Sebagai Upaya Meningkatkan Relevansi Antara Lulusan dengan Dunia Kerja Menggunakan UML. *IC-Tech*, XII(2), 42–49.
- Satria, M., & Handoyo, S. (2022). Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia. *Journal de Facto*, 8(2), 108-121.

- Amara, C. (2023). "Kriptografi Adalah: Pengertian, Sejarah, Tujuan, Algoritma & Contoh - Ilmu Elektro." *Ilmu Elektro*. Available at: <https://ilmuelektro.id/kriptografi-adalah/> [Accessed 13 May 2024].
- Ariyus, D. (2006). Kriptografi Keamanan Data dan Kriptografi. Yogyakarta: Penerbit Andi Offset.
- S, A. (2023). *Apa itu Ciphertext?* [online] BitDegree. Available at: <https://id.bitdegree.org/crypto/belajar/istilah-dalam-crypto/apa-itu-ciphertext> [Accessed 13 May 2024].
- Fuji, N. (2022). "Apa Itu Enkripsi? Pengertian, Manfaat, dan Contoh Penggunaan." *Niagahoster Blog*. Available at: <https://www.niagahoster.co.id/blog/apa-itu-enkripsi/> [Accessed 13 May 2024].
- Arsip Digital (2020). *Pengertian Enkripsi Dan Dekripsi*. [online] Arsip Digital. Available at: <https://www.arsipdigital.net/pengertian-enkripsi-dan-dekripsi/> [Accessed 13 May 2024].
- Prayudha, J. (2019). "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)." **Sains dan Komputasi**, 18(2).