

Kriptografi

## Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data pada Aplikasi E-Pariwisata

*Teguh Wijaya Lingga<sup>\*</sup>, Oris Krianto Sulaiman, Khairuddin Nasution*

*Fakultas Teknik, Program Studi Informatika, Universitas Islam Sumatera Utara, Medan, Indonesia*

### INFORMASI ARTIKEL

Diterima Redaksi: 03 Juni 2025  
Revisi Akhir: 11 Juni 2025  
Diterbitkan Online: 11 Juni 2025

### KATA KUNCI

*Cloud Computing*  
*E-Pariwisata*  
*Advanced Encryption Standard (AES)*

### KORESPONDENSI (\*)

Phone: +62 821-7438-0023  
E-mail: [teguhlingga13@gmail.com](mailto:teguhlingga13@gmail.com)

### A B S T R A K

Perkembangan teknologi informasi telah mendorong pemanfaatan cloud computing sebagai solusi penyimpanan data yang efisien dan dapat diakses kapan saja dan di mana saja melalui jaringan internet. Dinas Pariwisata Kota Medan, yang bertanggung jawab menyebarkan informasi potensi wisata kepada masyarakat, masih menghadapi kendala karena sistem penyebaran informasi yang bersifat manual dan kurang efisien. Penelitian ini bertujuan untuk merancang dan membangun sistem informasi e-pariwisata berbasis cloud computing guna mempermudah akses publik terhadap informasi wisata di Kota Medan. Sistem ini akan menyediakan informasi tata letak lokasi objek wisata, gambar, video pendek, serta informasi fasilitas dan biaya tiket masuk secara cepat dan efisien.

Untuk menjaga keamanan data yang tersimpan dan diproses pada cloud server, penelitian ini menerapkan algoritma Advanced Encryption Standard (AES). Dalam otorisasi dan otentikasi data yang akan diproses pada server cloud yang diterapkan algoritma AES (Advanced Encryption Standard) didalam sistem e- pariwisata untuk menjaga keamanan cloud server. Algoritma AES dipilih karena memiliki tingkat keamanan yang tinggi dengan enkripsi simetris dan panjang kunci 128, 192, atau 256bit, yang sulit ditembus menggunakan serangan brute force. Hasil penelitian menunjukkan bahwa sistem e-pariwisata berbasis cloud computing mampu menyebarkan informasi secara efektif dan efisien serta memberikan tingkat keamanan data yang optimal dengan implementasi algoritma AES.

### PENDAHULUAN

Cloud Computing merupakan gabungan dari pemanfaatan teknologi pembangunan berbasis komputer dan internet. Secara umum public cloud merupakan layanan cloud yang disediakan untuk publik atau masyarakat umum. Masyarakat baik individual atau organisasi seperti perusahaan dapat mendaftar dan mendapatkan layanan public cloud. Perkembangan teknologi telah menghasilkan beberapa metode komputasi, salah satunya cloud computing yang akhir-akhir ini semakin berkembang. Teknologi ini sangat dibutuhkan sebagai media penyimpanan murah yang dapat diakses dimana saja dan kapan saja dengan menggunakan jaringan internet. Untuk membangun sistem informasi publik yang saat ini kurang efisien dan efektif [1]. Dinas Pariwisata Kota Medan bertanggung jawab untuk memberikan informasi publik mengenai potensi pariwisata kepada masyarakat, namun saat ini informasi tersebut belum tersedia secara online dan hanya dapat diakses melalui kunjungan langsung ke kantor.

Kota Medan merupakan salah satu daerah di Provinsi Sumatera Utara yang memiliki berbagai destinasi wisata kota seperti istana maimun, masjid raya, dan bangunan london. Akan tetapi dalam penyebaran informasi seputar wisata di daerah Kota Medan masih bersifat manual, antara lain dalam hal pemberian informasi tata letak lokasi bersifat brosur, pamflet, poster, dan spanduk-spanduk kepada wisatawan yang ingin berkunjung ke suatu objek wisata di Kota Medan. mengingat tingginya potensi wisata kota Medan dan dukungan teknologi sebagai media membaca, maka teknologi dapat membuat

penyebaran informasi di Sumut menjadi lebih mudah dan efisien [2].

Pada Dinas Pariwisata Kota Medan masih kurang adanya sistem informasi untuk penyebaran informasi dan pengumpulan data yang terkait pada sektor potensi pariwisata sehingga peneliti akan merancang dan membangun sistem informasi ini, sehingga mempunyai banyak informasi untuk publik mengenai kegiatan kecamatan ini, atau hanya sekedar memberikan informasi kepada masyarakat sekitar. Makin banyak juga penyedia layanan jenis ini yang tersedia dan dengan mudah ditemukan di internet. Media penyimpanan Cloud Storage cukup banyak memberikan kemudahan bagi pengguna internet.

Dengan membangun sistem e-pariwisata berbasis cloud computing, informasi mengenai potensi wisata akan lebih mudah diakses oleh masyarakat. Sistem ini akan menyediakan informasi tentang mengenai tata letak lokasi objek wisata yang disertai dengan menampilkan beberapa gambar dan video pendek pada titik lokasi wisata tersebut, serta memberi informasi tentang fasilitas dan biaya tiket masuk dengan lebih cepat dan efisien.

Dalam otorisasi dan otentikasi data yang akan diproses pada server cloud akan diterapkan AES (*Advanced Encryption Standard*) pada sistem e-pariwisata untuk menjaga keamanan cloud server. Algoritma AES digunakan sebab AES dianggap sangat aman karena menggunakan enkripsi simetris dengan panjang kunci yang dapat diatur (128, 192, atau 256 bit), membuatnya sulit untuk ditembus dengan serangan *brute force*.

Dalam penelitian [3][4] dengan judul “Mengenal Advance Encryption Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data” berkesimpulan bahwa algoritma AES berhasil diterapkan untuk melakukan pengamanan data. Kemudian dalam penelitian Muhammad Riyan Andriyanto pada tahun 2022 dengan judul “Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace” berkesimpulan bahwa algoritma AES dapat berjalan dengan baik dalam melakukan enkripsi data transaksi pembayaran dari pengguna dan waktu yang relatif cepat.

## TINJAUAN PUSTAKA

### *Cloud Computing*

*Cloud Computing* merupakan model yang memungkinkan untuk mengakses jaringandari manapun secara nyaman, cepat, dan sesuai dengan permintaan/kebutuhan kepada suatu kumpulan sumber daya komputasi yang dirilis dengan upaya manajemen interaksi penyedia layanan [5]. Menurut Peter Mell dan Timothy Grance definisi Cloud Computing adalah sebuah model yang memungkinkan untuk ubiquitous (dimanapun dan kapanpun), Nyaman, On-demand akses jaringan ke sumber daya komputasi (contoh: jaringan, server, storage, aplikasi, dan layanan) yang dapat dengan cepat dirilis atau ditambahkan. Cloud Computing sebagai suatu layanan teknologi informasi yang dapat dimanfaatkan oleh pengguna dengan berbasis jaringan/internet. Dimana suatu sumber daya, perangkat lunak, informasi dan aplikasi disediakan untuk digunakan oleh komputer lain yang membutuhkan. Cloud computing mempunyai dua kata “Cloud” dan “Computing”. Cloud yang berarti internet itu sendiri dan Computing adalah proses komputasi [6].

Konsep Cloud computing biasanya dianggap sebagai internet. Karena internet sendiri digambarkan sebagai awan (Cloud) besar (biasanya dalam skema jaringan, internet dilambangkan sebagai awan) yang berisi sekumpulan komputer yang saling terhubung. Cloud computing datang sebagai sebuah evolusi yang mengacu pada konvergensi teknologi dan aplikasi lebih dinamis. Dimana terdapat perubahan besar memiliki implikasi yang menyentuh hampir setiap aspek komputasi. Untuk end user, komputasi awan menyediakan sarana untuk meningkatkan layanan baru atau mengalokasikan sumber daya komputasi lebih cepat, Berdasarkan kebutuhan bisnis Cloud dibagi menjadi beberapa model, saat ini ada empat model cloud diantaranya:

1. Publik Cloud di mana infrastruktur fisik dimiliki dan dikelola oleh penyedia layanan.
2. Community Cloud di mana infrastruktur fisik dimiliki dan dikelola oleh konsorsium organisasi.
3. Private Cloud di mana infrastruktur dimiliki dan dikelola oleh organisasi tertentu.
4. Cloud hybrid yang mencakup kombinasi tiga model sebelumnya. Dimana meskipun secara entitas mereka tetap berdiri sendiri-sendiri, tapi dihubungkan oleh satu teknologi/mekanisme yang memungkinkan portabilitas data dan aplikasi antar cloud itu.

Berikut adalah perbedaan utama antara sistem tradisional dan berbasis cloud yaitu:

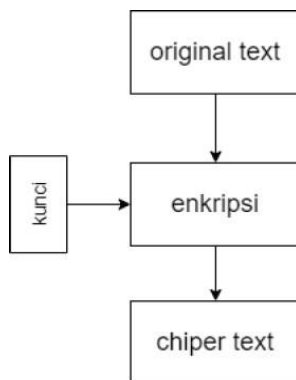
1. **Infrastruktur:**  
Sistem Tradisional: Sistem tradisional mengandalkan infrastruktur fisik yang ada di lokasi perusahaan, seperti server, pusat data, dan perangkat keras yang harus diinvestasikan dan dikelola secara lokal.  
Sistem Berbasis Cloud: Sistem berbasis cloud menggunakan infrastruktur yang dihosting oleh penyedia layanan cloud di data center mereka. Perusahaan tidak perlu mengelola perangkat keras fisik ini secara langsung.
2. **Akses:**  
Sistem Tradisional: Akses ke sistem tradisional sering kali terbatas pada lokasi fisik perusahaan atau melalui jaringan VPN yang kompleks.  
Sistem Berbasis Cloud: Sistem berbasis cloud memungkinkan akses dari mana saja dengan koneksi internet, memfasilitasi mobilitas dan kerja jarak jauh.
3. **Skalabilitas:**  
Sistem Tradisional: Skalabilitas pada sistem tradisional sering kali memerlukan investasi tambahan dalam perangkat keras fisik dan konfigurasi yang rumit.  
Sistem Berbasis Cloud: Sistem berbasis cloud memungkinkan organisasi untuk dengan mudah menambah atau mengurangi kapasitas sesuai dengan kebutuhan tanpa investasi besar.
4. **Biaya:**  
Sistem Tradisional: Sistem tradisional memerlukan investasi modal yang signifikan untuk membeli perangkat keras, lisensi perangkat lunak, dan pemeliharaan.  
Sistem Berbasis Cloud: Sistem berbasis cloud mengurangi biaya modal awal, karena organisasi membayar berdasarkan penggunaan, yang dapat mengurangi biaya operasional dalam jangka panjang.
5. **Keamanan:**  
Sistem Tradisional: Keamanan pada sistem tradisional sepenuhnya tergantung pada perusahaan untuk melindungi data dan infrastruktur mereka. Sistem Berbasis Cloud: Penyedia layanan cloud sering kali menyediakan lapisan keamanan yang kuat, tetapi perusahaan juga memiliki tanggung jawab untuk melindungi data mereka.
6. **Manajemen:**  
Sistem Tradisional: Manajemen infrastruktur, pemeliharaan, dan pembaruan perangkat keras dan perangkat lunak adalah tanggung jawab internal perusahaan.  
Sistem Berbasis Cloud: Penyedia layanan cloud mengelola sebagian besar infrastruktur dan pemeliharaan, sementara perusahaan fokus pada penggunaan dan manajemen aplikasi.

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

Algoritma Advanced Encryption Standard (AES) adalah metode enkripsi yang kuat dan simetris yang digunakan untuk melindungi data dalam dunia digital. AES dianggap sebagai penerus dari algoritma Data Encryption Standard (DES) yang lebih lama [7].

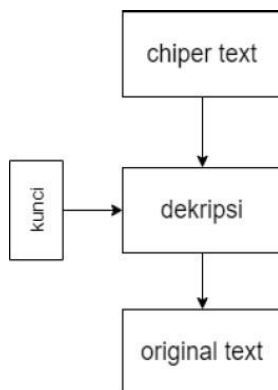
Dikembangkan pada tahun 1997 oleh dua kriptografer, Joan Daemen dari Belgia dan Vincent Rijmen dari Belgia, AES diadopsi oleh Pemerintah Amerika Serikat sebagai standar enkripsi yang disetujui oleh Badan Keamanan Nasional (NSA) pada tahun 2001. Penerapan keamanan server cloud juga penting dilakukan pada proses otorisasi pengguna dengan memanfaatkan AES (Advanced Encryption Standard). AES merupakan metode enkripsi yang kuat dan simetris yang digunakan untuk melindungi data dalam dunia digital sehingga dapat meminimalisir akses ilegal pada server cloud. AES merupakan blok kode simetris untuk menggantikan DES (Data Encryption Standard) [8]. Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran [9][10].

Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block cipher dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Algoritma AES merupakan algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi [11].



Gambar 1. Proses Enkripsi

Dalam proses enkripsi, peneliti akan menentukan key yang akan digunakan dalam melakukan enkripsi serta dekripsi. Setelah menentukan key maka key tersebut diubah dalam bentuk hex yang kemudian akan dimasukkan ke dalam box key [12]. Selanjutnya peneliti akan memasukkan pesan singkat yang dikirimkan ke dalam box message to encryp setelah itu klik next. Kemudian akan muncul hasil dari proses enkripsi tersebut berupa kode hex pada box yang bertuliskan AES Output.



Gambar 2. Proses Dekripsi

Proses dekripsi terhadap cipher teks merupakan oponent dari proses enkripsi. Setelah mendapatkan hex text pada proses enkripsi, hex text tersebut kita masukkan dalam kolom Message to Decrypt. Selain itu key yang digunakan juga masih sama seperti pada proses enkripsi sebelumnya. Selanjutnya peneliti akan memasukkan kode hex yang tadi didapatkan pada proses enkripsi yang dikirimkan ke dalam box message to decrypt setelah itu klik next. Kemudian akan muncul hasil dari proses dekripsi tersebut berupa pesan yang tadinya dimasukkan pada proses enkripsi pada box yang bertuliskan AES Output.

Algoritma AES merupakan algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah round (perputaran) yang dapat digambarkan dalam bentuk tabel dibawah ini.

Tabel 1. Algoritma AES

AES (Bits)	Panjang Kunci (NK Words)	Ukuran Blok (Nb Words)	Jumlah Putaran (Nr)
AES – 128	4	4	10
AES – 192	6	4	12
AES- 256	8	4	14

## METODOLOGI

### *Analisis Permasalahan*

Mengenali permasalahan merupakan langkah pertama yang dilakukan dalam tahap analisis sistem. Permasalahan dapat didefinisikan sebagai suatu pertanyaan yang dapat dipercahkan. Masalah inilah yang menyebabkan sasaran dari sistem tidak dapat dicapai. Oleh karena itu pada tahap analisis sistem langkah pertama yang harus dilakukan oleh analisis adalah mengidentifikasi masalah dimulai dengan mengkaji objek permasalahan yang ada berkaitan dengan pengembangan aplikasi e-pariwisata berbasis *cloud computing* pada instansi Dinas Pariwisata Kota Medan.

Dalam proses perancangan sistem e-pariwisata berbasis *cloud computing* dengan metode (*Advanced Encryption Standard*) AES diperlukan data-data pendukung dan alur perancangan yang tepat dimulai dari interface sampai perancangan laporan.

### *Metode AES*

Metode AES akan diterapkan pada sistem e-pariwisata berbasis *cloud* di bagian halaman login, untuk menjamin keamanan sistem dan pengguna. Berikut ini contoh sederhana penerapan metode AES pada halaman login misalnya sebagai berikut:

Kata sandi: Password123

Kunci Enkripsi (128-bit): mysecretkey12345 Algoritma: AES-128

Mode Operasi: ECB (Electronic Codebook)

Langkah 1: Konversi Data menjadi Format Biner (ASCII)

Setiap karakter dalam teks diubah menjadi representasi hexadecimal atau biner berdasarkan kode ASCII. Misal:

Password123 → dalam kode ASCII:

P = 50, a = 97, s = 115, s = 115, w = 119, o = 111, r = 114, d = 100,

l = 49, 2 = 50, 3 = 51

Dalam hexadecimal:

50 61 73 73 77 6F 72 64 31 32 33

Jika data kurang dari 128-bit (16 byte), ditambahkan *padding*. *Padding* yang umum adalah PKCS#7, yaitu menambahkan *byte* yang berisi jumlah *byte padding*. Misalnya:

Password123 (11 bytes) + 05 05 05 05 05 (5 bytes padding) Maka hasilnya:

50 61 73 73 77 6F 72 64 31 32 33 05 05 05 05

Langkah 2: Kunci Enkripsi (128-bit) Kunci yang digunakan adalah:

mysecretkey12345 Dalam hexadecimal:

6D 79 73 65 63 72 65 74 6B 65 79 31 32 33 34 35

Langkah 3: Proses Enkripsi dengan AES-128 (ECB Mode)

1. Pertama, kita pisahkan data input (kata sandi) menjadi blok-blok 128-bit (16 byte per blok).
2. Setiap blok akan dienkripsi secara independen menggunakan algoritma AES dengan kunci yang diberikan.

Misalnya, hasil enkripsi (dalam hexadecimal):

E3 F2 1C 3B 4A 5F D6 8E C8 23 9A 01 0A A5 3C D1

Langkah 4: Simpan Hasil Enkripsi dalam Database Hasil enkripsi kata sandi yang diperoleh adalah:

E3F21C3B4A5FD68EC8239A010AA53CD1

Kata sandi ini disimpan dalam database sebagai ciphertext. Ketika pengguna mencoba login, proses serupa dilakukan untuk kata sandi yang dimasukkan, lalu hasil enkripsinya dibandingkan dengan yang tersimpan di database.

Langkah 5: Proses Login (Dekripsi dan Verifikasi)

Saat pengguna mengetikkan kata sandi, sistem akan mengenkripsi input tersebut menggunakan AES-128 dan kunci yang sama. Hasil enkripsi dibandingkan dengan ciphertext di database. Jika cocok, login berhasil.

Berikut ini adalah contoh implementasi AES-128 dalam PHP untuk enkripsi dan dekripsi kata sandi dalam sistem login. Fungsi yang digunakan adalah bawaan PHP seperti `openssl_encrypt()` dan `openssl_decrypt()`.

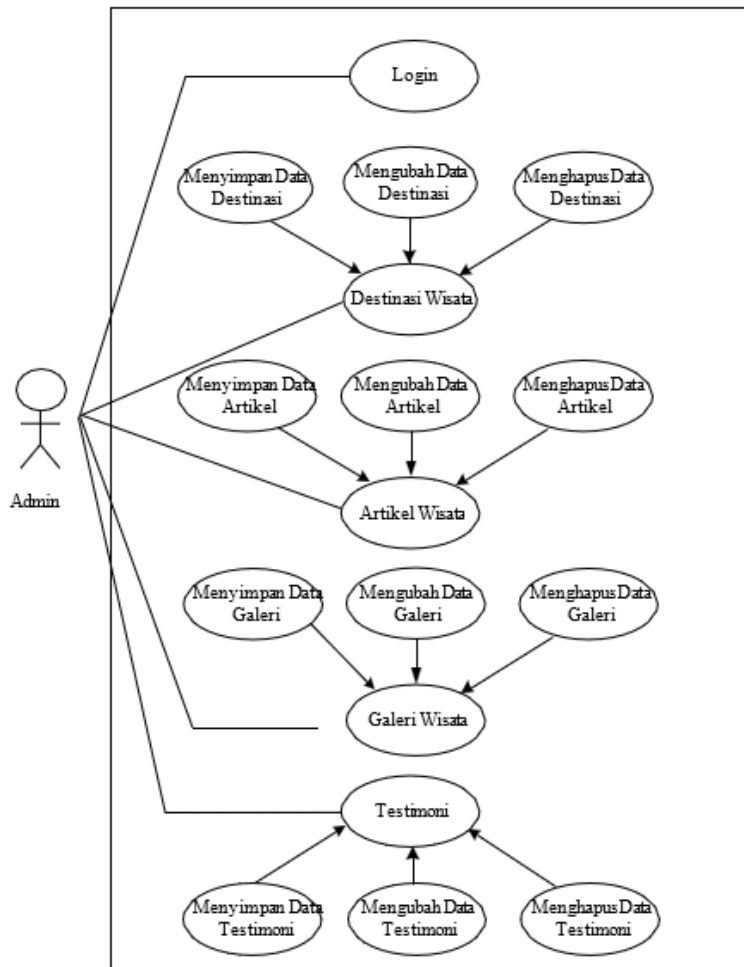
```
<?php
// Kunci Enkripsi dan Inisialisasi Data
$key = "mysecretkey12345"; // 16 karakter = 128-bit (AES-128)
$password = "Password123"; // Kata sandi yang akan dienkripsi
// Fungsi Enkripsi AES-128
function encryptAES($data, $key) {
    $cipher = "AES-128-ECB"; // Mode ECB
    $options = 0;
    // Enkripsi dan hasilnya dikonversi ke bentuk hexadecimal
    $encrypted = openssl_encrypt($data, $cipher, $key, $options);
    return $encrypted;
}
// Fungsi Dekripsi AES-128
function decryptAES($encryptedData, $key) {
    $cipher = "AES-128-ECB";
    $options = 0;
    // Dekripsi ciphertext menjadi teks asli
    $decrypted = openssl_decrypt($encryptedData, $cipher, $key, $options);
    return $decrypted;
}
// Proses Enkripsi Kata Sandi
$encryptedPassword = encryptAES($password, $key);
echo "Ciphertext: " . $encryptedPassword . PHP_EOL;
// Proses Dekripsi Kata Sandi
$decryptedPassword = decryptAES($encryptedPassword, $key);
echo "Decrypted Password: " . $decryptedPassword . PHP_EOL;
?>
```

### ***Perancangan Sistem***

Perancangan sistem adalah merancang atau mendesain suatu sistem yang baik, yang isinya adalah langkah-langkah operasi dalam proses pengolahan data dan prosedur untuk mendukung operasi sistem.

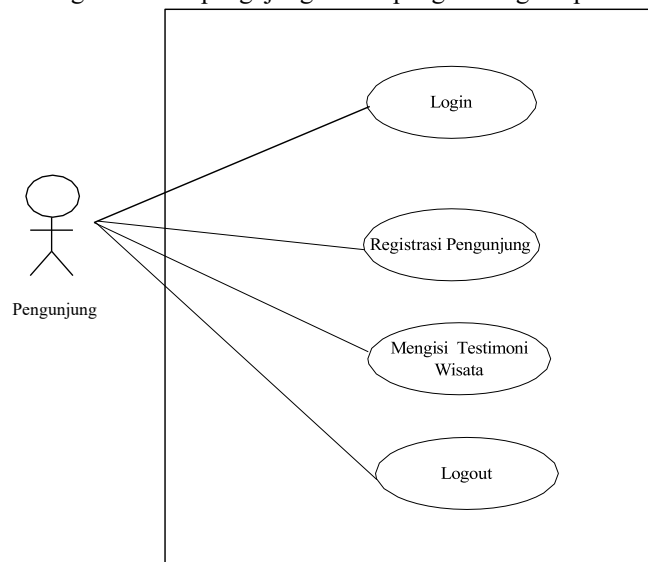
### ***Use Case Diagram***

*Use case* menunjukkan hubungan interaksi antar aktor dengan *use case* di dalam suatu yang bertujuan bagaimana aktor berinteraksi dengan sebuah sistem.



Gambar 3. Rancangan Use Case Diagram Admin

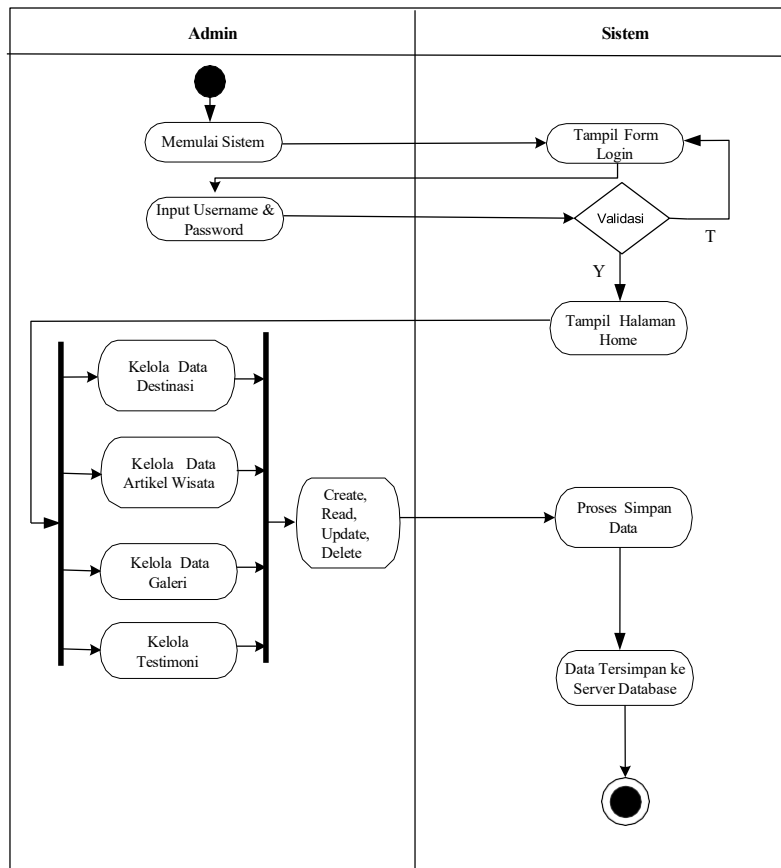
Adapun penggambaran use case diagram untuk pengunjung dalam pengembangan aplikasi e-pariwisata sebagai berikut.



Gambar 4. Rancangan Use Case Diagram Pengunjung

**Activity Diagram**

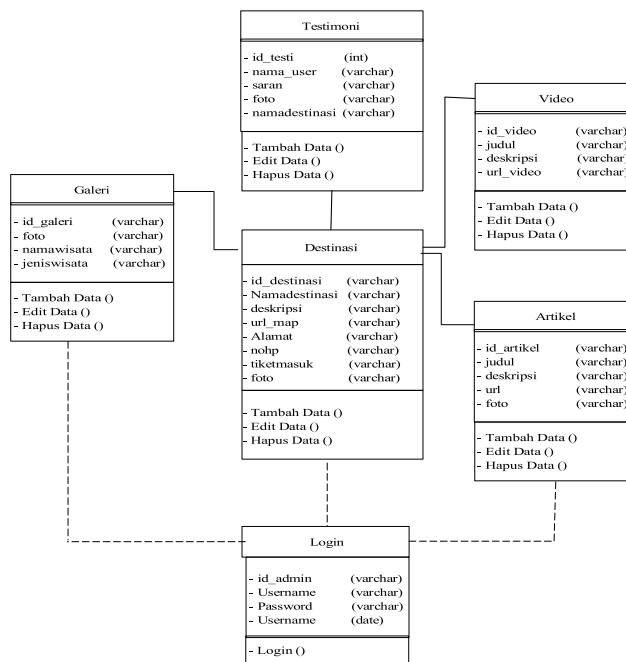
Bentuk *activity diagram* dari sistem untuk sistem e-pariwisata berbasis cloud computing dengan metode AES sebagai berikut :



Gambar 5. Activity Diagram Admin

**Class Diagram**

*Class diagram* menggambarkan struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem. Bentuk *Class Diagram* dari sistem e-pariwisata berbasis cloud computing dapat dilihat pada gambar dibawah ini.



Gambar 6. Class Diagram Sistem

## HASIL DAN PEMBAHASAN

### Hasil dan Pembahasan

Implementasi sistem merupakan tahapan dimana suatu sistem akan dijalankan dan diuji, apakah telah sesuai dengan rancangan atau tidak. Tahapan implementasi sistem dimulai dari *form* login kemudian lanjut ke *form* utama dan *form-form* data lainnya.

### Interface Sistem

#### Halaman Utama

Halaman utama pengunjung berfungsi untuk menampilkan tampilan awal website wisata dan informasi di Kota Medan. Berikut ini tampilan halaman utama pengunjung.



Gambar 7. Halaman Utama

#### Halaman Destinasi Wisata

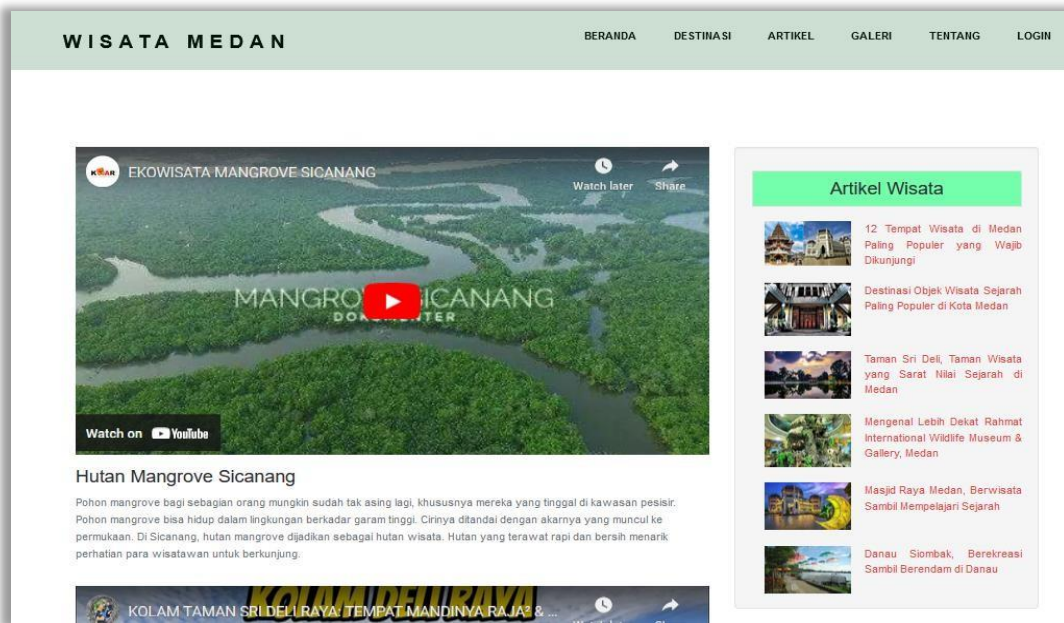
Halaman tampilan *form* destinasi wisata mengenai info terkini terkait destinasi pariwisata Kota Medan yaitu sebagai berikut. Admin harus mengupload 3 gambar untuk setiap destinasi dengan maksimal size 5 MB per gambar.



Gambar 8. Halaman Destinasi Wisata

*Halaman Video Wisata*

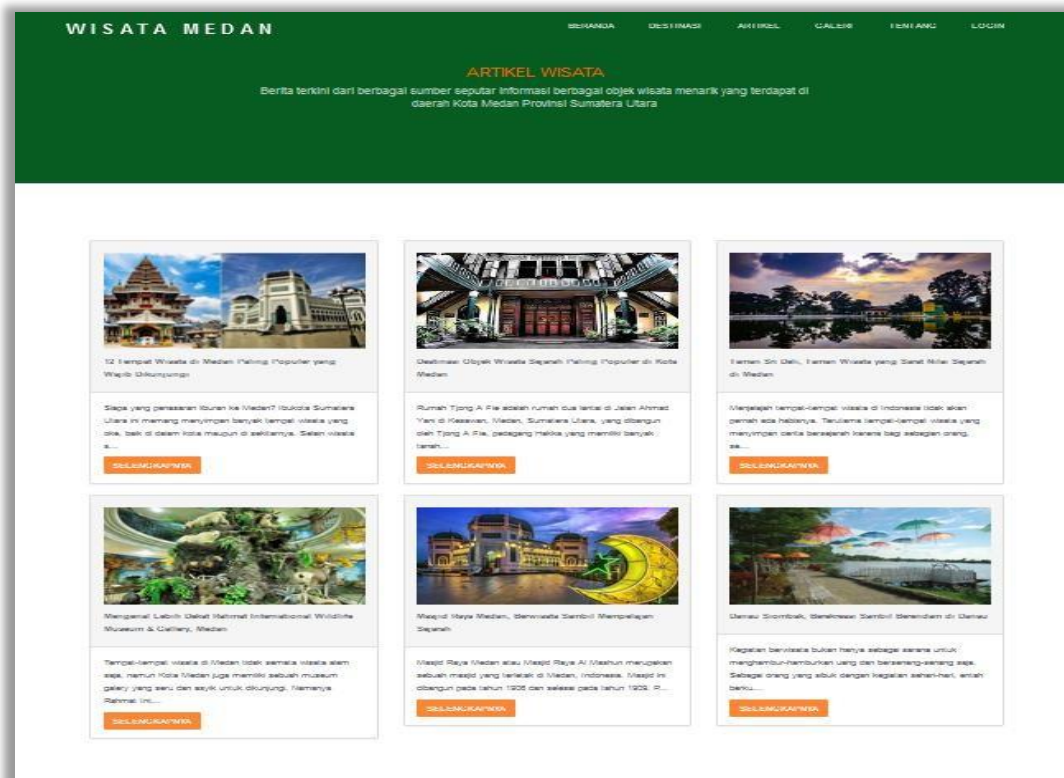
Halaman tampilan video mengenai informasi video wisata Kota Medan yang diambil dari Youtube. Admin harus mencopy link video dari Youtube yang ingin ditampilkan pada website.



Gambar 9. Halaman Video Wisata

*Halaman Artikel Berita*

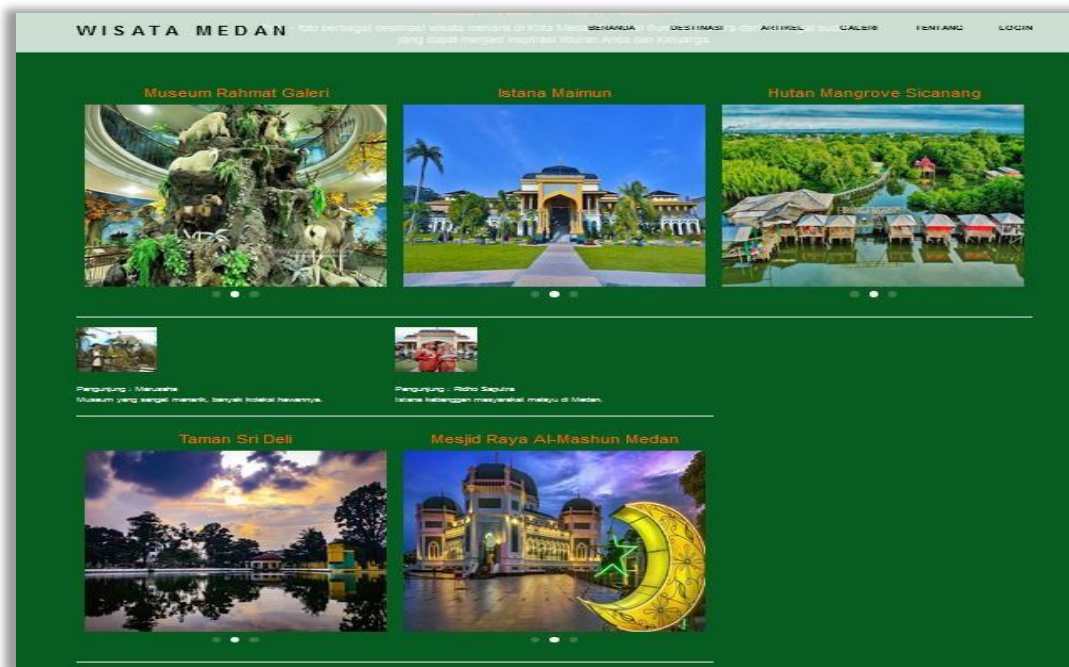
Halaman artikel berita mengenai informasi berita wisata Kota Medan yang diliput oleh berbagai sumber berita populer. Ketika link berita di klik maka akan terhubung ke website penyedia berita wisata tersebut. Berikut tampilan halaman artikel berita wisata.



Gambar 10. Form Artikel Berita

*Halaman Galeri Wisata*

Halaman galeri menampilkan beberapa foto terbaik mengenai destinasi wisata yang ada di Kota Medan. Berikut ini merupakan halaman tampilan galeri wisata.



Gambar 11. Halaman Galeri Wisata

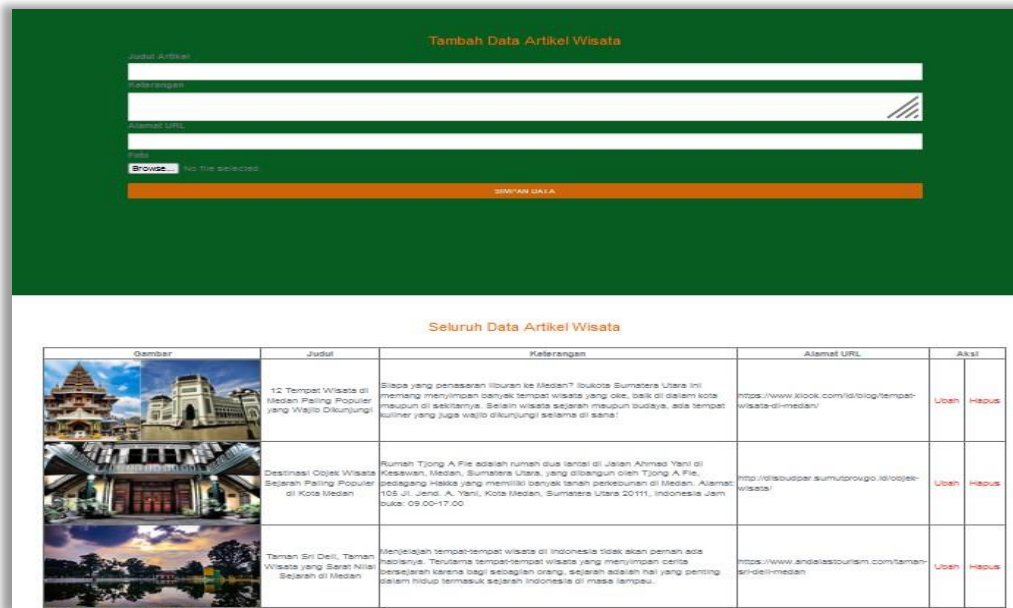
*Form Login Admin*

*Form login* merupakan tampilan form dimana admin diwajibkan untuk mengisi *username* dan *password* yang sudah sesuai yang telah teregistrasi dan tersimpan pada database. Jika *username* dan *password* yang diinput salah sistem akan menampilkan pesan atau peringatan. Berikut adalah tampilan *form login* untuk admin:

Gambar 12. *Form Login*

*Form Kelola Artikel Berita*

Tampilan *form* artikel merupakan halaman yang digunakan admin untuk mengelola data artikel wisata yang ditampilkan pada website. Berikut halaman form artikel berita.



Gambar 13. Form Artikel Berita

*Form Kelola Testimoni*

Tampilan *form* kelola testimoni merupakan halaman yang digunakan admin untuk mengelola data testimoni dari pengunjung wisata yang ditampilkan pada website. Berikut halaman form testimoni.



Gambar 14. Form Kelola Testimoni

*Form Kelola Video*

Tampilan *form* kelola video merupakan halaman yang digunakan admin untuk mengelola (menambah ataupun menghapus) data video wisata yang ditampilkan pada website. Admin harus mencopy link atau URL video dari Youtube yang ingin ditampilkan pada website. Berikut halaman form kelola video wisata yang ada pada sistem.

Judul Video	Deskripsi	URL VIDEO	Aksi	
Hutan Mangrove Sicanang	Pohon mangrove bagi sebagian orang mungkin sudah tak asing lagi, khususnya mereka yang tinggal di kawasan pesisir. Pohon mangrove bisa hidup dalam lingkungan berkadar garam tinggi. Cirinya ditandai dengan akarnya yang muncul ke permukaan. Di Sicanang, hutan mangrove dijadikan sebagai hutan wisata. Hutan yang terawat rapi dan bersih menarik perhatian para wisatawan untuk berkunjung.	https://www.youtube.com/embed/gCKcIT5yoPk	Ubah	Hapus
Taman Sri Deli	Menjelajah tempat-tempat wisata di Indonesia tidak akan pernah ada habisnya. Terutama tempat-tempat wisata yang menyimpan cerita bersejarah karena bagi sebagian orang, sejarah adalah hal yang penting dalam hidup termasuk sejarah Indonesia di masa lampau. Di Medan terdapat Taman Sri Deli yang bukan hanya sekedar taman, namun juga bersejarah.	https://www.youtube.com/embed/_6LS9lweRE?start=2	Ubah	Hapus
Istana Maimun Kota Medan, Sumatera Utara	Istana Maimun didirikan oleh Sultan Maimun Al Rasyid Perkasa Alamsyah, yang merupakan keturunan raja kesembilan Kesultanan Deli. Istana ini memadukan ornamen budaya banyak negara. Ada nuansa melayu, Islam, Spanyol, China, India, dan Italia. Nuansa melayu ditandai dengan warna kuning keemasan.	https://www.youtube.com/embed/BmqPla7UlyU	Ubah	Hapus

Gambar 15. Form Kelola Video

*Form Kelola Destinasi*

Tampilan *form* kelola destinasi merupakan halaman yang digunakan admin untuk mengelola data destinasi wisata pada website. Admin harus mengupload 3 gambar untuk setiap destinasi dengan maksimal size 5 MB per gambar.

Nama Destinasi	Deskripsi	Alamat	Nomor Kontak	Aksi	
Mesjid Raya Al-Mashun Medan	Mesjid Raya Al-Mashun adalah salah satu masjid ikonik di Medan, Sumatera Utara, yang dikenal dengan arsitektur megah dan kaya akan nilai sejarah. Dibangun pada tahun 1906 hingga 1909 pada masa Kesultanan Deli, masjid ini menampilkan perpaduan arsitektur Timur Tengah, India, dan Eropa yang unik. Pla...	Jl. Mahkamah No.74c, RT.02, Mesjid, Kec. Medan Kota, Kota Medan, Sumatera Utara 20212	Tidak Ada	Ubah	Hapus
Taman Sri Deli	Menjelajah tempat-tempat wisata di Indonesia tidak akan pernah ada habisnya. Terutama tempat-tempat wisata yang menyimpan cerita bersejarah karena bagi sebagian orang, sejarah adalah hal yang penting dalam hidup termasuk sejarah Indonesia di masa lampau. Di Medan terdapat Taman Sri Deli yang bukan h...	Jl. Sisingamangaraja, Mesjid, Kec. Medan Kota, Kota Medan, Sumatera Utara 20213	082339180403	Ubah	Hapus
Hutan Mangrove Sicanang	Pohon mangrove bagi sebagian orang mungkin sudah tak asing lagi, khususnya mereka yang tinggal di kawasan pesisir. Pohon mangrove bisa hidup dalam lingkungan berkadar garam tinggi. Cirinya ditandai dengan akarnya yang muncul ke permukaan. Di Sicanang, hutan mangrove dijadikan sebagai hutan wisata. H...	Jl. Pulau Sicanang, Belawan Pulau Sicanang, Medan Kota Belawan, Kota Medan, Sumatera Utara 20414	-	Ubah	Hapus
Istana Maimun	Istana Maimun didirikan oleh Sultan Maimun Al Rasyid Perkasa Alamsyah, yang merupakan keturunan raja kesembilan Kesultanan Deli. Istana ini memadukan ornamen budaya banyak negara. Ada nuansa melayu, Islam, Spanyol, China, India, dan Italia. Nuansa melayu ditandai dengan warna kuning keemasan...	Kel. Aur, Medan Maimun, Medan City, North Sumatra 20212	-	Ubah	Hapus
Museum Rahmat Galeri	Rahmat International Wildlife Museum & Gallery adalah museum unik yang menampilkan koleksi satwa liar yang berasal dari berbagai belahan dunia. Terletak di Medan, Sumatera Utara, museum ini didirikan oleh Rahmat Shah, seorang kolektor dan pecinta alam yang ingin mengedukasi masyarakat tentang keanek...	Jl. S. Parman No.309, Petisah Hulu, Kec. Medan Baru, Kota Medan, Sumatera Utara 20152	0614569964	Ubah	Hapus

Gambar 16. Form Kelola Destinasi

Berikut ini tampilan halaman untuk menambahkan foto destinasi wisata yang dapat digunakan oleh admin dengan maksimal size 5 MB setiap gambar.

Gambar 17. Halaman Tambah Destinasi

### Form Decrip Password Pengguna

Tampilan *form* decrip password pengguna merupakan halaman yang digunakan admin untuk mendekripsi password pengguna pada website.

Gambar 18. Form Decrip Password Pengguna

### Hasil Penerapan Algoritma AES

Proses enkripsi dengan algoritma AES dilakukan pada saat pengunjung melakukan registrasi seperti gambar di bawah ini.

Gambar 19. Halaman Registrasi Akun

```
function encryptAES($data, $key) {
    $method = "AES-256-CBC";
    $iv = openssl_random_pseudo_bytes(openssl_cipher_iv_length($method));
    $encrypted = openssl_encrypt($data, $method, $key, 0, $iv);
    return base64_encode($encrypted . '::' . $iv);
}
```

Sehingga akan dieksekusi kedalam database dengan menyimpan huruf hasil enkripsi tersebut. Berikut tampilan code programnya.

```
$nama_awal = $_POST['nama_awal'];
$username = $_POST['username'];
$password = $_POST['password'];
$key = "mysecretkey12345";
// Enkripsi password
$encrypted_password = encryptAES($password, $key);
// Simpan data ke database
$query = $pdo->prepare("INSERT INTO user (nama_awal, nama_akhir, username, password) VALUES (:nama_awal, :nama_akhir, :username, :password)");
$query->bindParam(':nama_awal', $nama_awal);
$query->bindParam(':nama_akhir', $nama_akhir);
$query->bindParam(':username', $username);
$query->bindParam(':password', $encrypted_password);
```

Kemudian berikut ini tampilan screenshot dari tabel user yang telah di enkripsi dengan algoritma AES.

id	nama_awal	nama_akhir	username	password	dibuat	diubah	status
14	Admin	Website	teguh	21232f297a57a5a743894a0e4a801fc3	2024-07-15 00:00:00	2024-07-15 00:00:00	1
15	Pratiwi	Sihombing	pratiwi	ef0a99abb0cf88003665bf30a14afc27	2024-09-09 01:24:55	2024-09-09 01:24:55	1
17	Indra	Permana	indra	e24f6e3ce19ee0728ff1c443e4ff488d	2024-09-22 02:56:07	2024-09-22 02:56:07	1
19	Diana Ratna	-	diana	L1J4b29oU1Vyd081ckxhajfFZXRZz090jo7KaFmBNknk,J4fzX...	2024-11-04 06:49:08	2024-11-04 06:49:08	1
20	Laras Dewi	-	laras	c0ZneWE5VE8vMjNyTmZJa3IMU5vZz09Ojq7BCdXhulaoXJz3...	2024-11-04 07:56:28	2024-11-04 07:56:28	1
21	Ridho Saputra	-	ridho	Q0xNTVJxMmZzVzVtMlxOTJxY1RlZz09Ojp9LkqNrqlsGCcYbU...	2024-11-04 08:00:17	2024-11-04 08:00:17	1
22	Marusaha	-	saha	aDRLa0x2ZS80TzBobGMxOHVQWwWBdz09OjrnMng01JRLOyoTk1a...	2024-11-04 08:17:18	2024-11-04 08:17:18	1

Gambar 20. Hasil Enkripsi Password

Selanjutnya proses dekripsi dengan algoritma AES akan dilakukan pada saat pengunjung login.

### LOGIN

Silahkan Login Pengunjung

Masuk

Belum Punya Akun? Registrasi Disini.

Gambar 21. Halaman Login Pengunjung

Berikut tampilan susunan kode program dalam proses dekripsi dengan algoritma AES.

```
function decryptAES($data, $key) {
    $method = "AES-256-CBC";
    list($encrypted_data, $iv) = explode(':', base64_decode($data), 2);
    return openssl_decrypt($encrypted_data, $method, $key, 0, $iv);
}
```

```
$username = $_POST['username'];
$password = $_POST['password'];
$key = "mysecretkey12345";
// Ambil password terenkripsi dari database
$query = $pdo->prepare("SELECT password FROM user WHERE username = :username");
$query->bindParam(':username', $username);
$query->execute();
$result = $query->fetch();
if ($result) {
    $encrypted_password = $result['password'];
    $decrypted_password = decryptAES($encrypted_password, $key);
    // Cek apakah password cocok
    if ($password == $decrypted_password) {
        include 'user.php';
        $user = new User();
        $kondisi['where'] = array(
            'username' => $_POST['username'],
            'status' => '1'
        );
        $kondisi['return_type'] = 'single';
        $userData = $user->getRows($kondisi);
    }
}
```

### Kelemahan dan Kelebihan Sistem

Kelebihan dari sistem e-pariwisata berbasis *cloud* dengan metode AES yaitu:

1. Program ini dapat digunakan dengan mudah oleh admin maupun masyarakat yang ingin mencari informasi pariwisata di Kota Medan.
2. Dengan program berbasis *cloud* ini dapat memotivasi kepada pihak lain untuk melakukan kegiatan yang *update*, mengikuti perkembangan zaman dan teknologi informasi.

Kelemahan dari sistem ini adalah keterbatasan sumber data, terbatas hanya dalam ruang lingkup sistem e-pariwisata di Kota Medan saja, dan fasilitas-fasilitas lain yang harusnya terdapat dalam suatu sistem e-pariwisata ini tidak ada dalam sistem ini, diantaranya:

1. Program ini belum mampu melakukan *backup database* secara otomatis.
2. Program ini tidak dapat melakukan *update* otomatis. Harus di *install* secara manual pada komputer *server* apabila ada yang mau diperbaharui.

## KESIMPULAN DAN SARAN

### Kesimpulan

Setelah melalui berbagai tahapan, diperoleh kesimpulan bahwa sistem berbasis cloud computing ini memudahkan wisatawan mencari informasi lengkap tentang destinasi wisata di Kota Medan. Sistem yang dibangun terbukti efektif dalam mengelola data destinasi wisata serta data pendukung lainnya, sekaligus menghasilkan laporan dengan cepat dan efisien. Sistem e-pariwisata ini juga membantu Dinas Pariwisata Kota Medan menyebarkan informasi wisata secara lengkap, dilengkapi dengan peta lokasi, informasi media sosial, serta foto dan video pendukung secara cepat kepada wisatawan. Program yang dirancang merupakan penyempurnaan dari sistem sebelumnya dan dapat membantu instansi terkait dalam mengatur pengelolaan data wisata di Kota Medan.

### Saran

Adapun saran yang dapat disampaikan kepada pembaca, kepada pihak pengguna dan kepada seluruh pihak yang berkaitan dengan perancangan sistem ini, maka diharapkan agar aplikasi ini dapat diperbaharui lagi, terutama dalam segi *interface*-nya. Supaya lebih menarik tampilannya dan lebih mudah digunakan. Dan dapat ditambahkan fitur untuk membackup data secara otomatis untuk mengurangi resiko kehilangan data penting. Diharapkan agar aplikasi ini dapat dikembangkan lebih lanjut sehingga data yang diolah dapat lebih optimal dan menyeluruh.

## DAFTAR PUSTAKA

- [1] J. Mulyadi, M. R. Katili, and B. Ahaliki, 'Pengembangan Sistem Informasi Pariwisata Menggunakan Metode Prototype Berbasis Web GIS Di Dinas Pariwisata Kabupaten Bone Bolango', *Diffus. J. Syst. Inf. Technol.*, vol. 4, no. 1, pp. 74–91, 2024, [Online]. Available: <https://ejurnal.ung.ac.id/index.php/diffusion/article/view/23651>
- [2] M. Alda, A. A. Haryada, M. Jannah, and H. Amri, 'Rancang Bangun Aplikasi Mobile "Wonderful Medan City" Sebagai Salah Satu Informasi Pariwisata Kota Medan', *J. Pendidik. Tambusai*, vol. 8, pp. 4763–4772, 2024, [Online]. Available: <https://www.jptam.org/index.php/jptam/article/view/13122>
- [3] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. Faizal Prianggara, and M. Yasin, 'Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data', *Digit. Transform. Technol.*, vol. Vol.03, no. No.1, pp. 1–10, 2023, [Online]. Available: <https://jurnal.itscience.org/index.php/digitech/article/view/2293>
- [4] Y. Agita, P. Tarigan, R. Aulia, and A. Marwan, 'Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web', vol. 17, no. 2, pp. 2580–2582, 2024.
- [5] A. S. Manalu, I. M. Siregar, N. J. Panjaitan, and H. Sugara, 'Rancang Bangun Infrastruktur Cloud Computing Dengan Openstack Pada Jaringan Lokal Menggunakan Virtualbox', *J. Tek. Inf. dan Komput.*, vol. 4, no. 2, p. 303, 2021, doi: 10.37600/tekinkom.v4i2.335.
- [6] K. Marlin, K. Mere, S. A. Fitri, D. S. Nugroho, and D. Koerniawati, 'Peran Teknologi Cloud Computing Dalam Meningkatkan Efisiensi Dan Keamanan Proses Akuntansi: Tinjauan Terhadap Perubahan Paradigma Dalam Manajemen Data Keuangan', *J. Darma Agung*, vol. 32, no. 2, pp. 1044–1055, 2024, [Online]. Available: <https://dx.doi.org.10.46930/ojsuda.v32i2.4152>
- [7] M. R. Andriyanto and P. Sukmasetya, 'Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace', *J. Comput. Syst. Informatics*, vol. 4, no. 1, pp. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.
- [8] O. G. Khoirunnisa and D. Djuniadi, 'Implementasi Algoritma AES untuk Keamanan Data Rekam Medis', *Petir*, vol. 15, no. 1, pp. 21–27, 2021, doi: 10.33322/petir.v15i1.1333.
- [9] H. A. Sagala, 'Perancangan Aplikasi Audit Internal Dengan Menerapkan Algoritma AES 128 Bit Untuk Pengamanan Data', *J. Glob. Technol. Comput.*, vol. 2, no. 2, pp. 75–86, 2023, doi: 10.47065/jogtc.v2i2.3348.
- [10] H. S. Ruhaedi, 'Skema pengamanan data dengan Kombinasi algoritma advanced encryption standard (AES) dan rivest shamir aldeman (RSA)', vol. 18, no. 2, pp. 177–190, 2024.
- [11] S. Saripa, 'Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi: Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi', *Progress. Information, Secur. Comput. Embed. Syst.*, vol. 1, no. 2, pp. 138–148, 2023.
- [12] M. L. Assidiq, F. Mahardika, and D. Santika, 'Implementasi Algoritma Kriptografi AES dan SHA-3 Dalam Mengamankan Data Sensitif Pengguna Pada Website Transaksi', *Simpatik J. Sist. Inf. dan Inform.*, vol. 4, no. 1, pp. 44–52, 2024, doi: 10.31294/simpatik.v4i1.3386.