INFOMATEK: Jurnal Informatika, Manajemen dan Teknologi
Volume 27 Nomor 1, Juni 2025

IMPLEMENTASI ENKRIPSI AES DALAM SISTEM ARSIP SURAT DI KONI PROVINSI SUMATERA UTARA

Enriko Vincentius Manurung*, Putri Harliana

Program Studi Ilmu Komputer, Universitas Negeri Medan, Indonesia

Abstrak: Perkembangan teknologi informasi mempengaruhi berbagai sektor, termasuk dalam pengelolaan arsip digital. Salah satu tantangan utama dalam sistem arsip digital adalah menjaga keamanan data dari akses yang tidak sah. Penelitian ini bertujuan untuk mengimplementasikan enkripsi AES (Advanced Encryption Standard) dalam sistem arsip surat di KONI Provinsi Sumatera Utara. Metode yang digunakan adalah penelitian deskriptif dengan pendekatan studi kasus, di mana data dikumpulkan melalui wawancara, observasi, dan dokumentasi. Hasil penelitian menunjukkan bahwa enkripsi AES berhasil diterapkan untuk melindungi surat-surat yang diunggah dalam sistem, memastikan kerahasiaan dokumen dan mengamankan akses melalui sistem login yang terproteksi. Meskipun implementasi ini efektif, tantangan terkait dengan pengelolaan kunci enkripsi perlu diatasi untuk meningkatkan keamanan lebih lanjut. Penelitian ini memberikan kontribusi penting dalam meningkatkan sistem pengelolaan arsip yang aman di KONI Provinsi Sumatera Utara.

Kata kunci: Enkripsi AES, Sistem Arsip Surat, Keamanan Data, KONI Provinsi Sumatera Utara, Pengelolaan Arsip

I. PENDAHULUAN

Perkembangan teknologi informasi telah membawa dampak signifikan dalam berbagai sektor, termasuk dalam pengelolaan arsip (Hapsari & Ariyani, 2018). Pengelolaan arsip yang efisien dan aman menjadi kebutuhan utama dalam lembaga-lembaga pemerintahan maupun organisasi, seperti KONI (Komite Olahraga Nasional Indonesia) Provinsi Sumatera Utara. Arsip surat yang menjadi bagian penting dalam administrasi organisasi harus dapat dikelola dengan baik agar dapat mendukung kelancaran operasional dan menjaga kerahasiaannya. Namun, meskipun banyak organisasi yang telah menggunakan sistem arsip digital, masalah terkait keamanan data masih menjadi isu yang cukup besar (Saefulrahman et al., 2025), (Ariani et al., 2016), (Muhidin et al., 2016).

Salah satu tantangan utama dalam sistem arsip digital adalah bagaimana melindungi data agar tidak mudah diakses oleh pihak yang tidak berwenang (Detharie et al., 2024). Penggunaan metode enkripsi menjadi solusi yang relevan untuk menjamin keamanan data arsip. Salah satu algoritma enkripsi yang banyak digunakan dan memiliki tingkat keamanan yang tinggi adalah Advanced Encryption Standard (AES). AES telah diadopsi secara luas dalam berbagai sistem keamanan karena kemampuannya untuk mengenkripsi data dengan tingkat keamanan

*) enricomnrg08@mhs.unimed.ac.id

Diterima: 19 April 2025
Direvisi: 28 Mei 2025
Disetujui:24 Juni 2025
DOI: 10.23969/infomatek.v27i1.24158

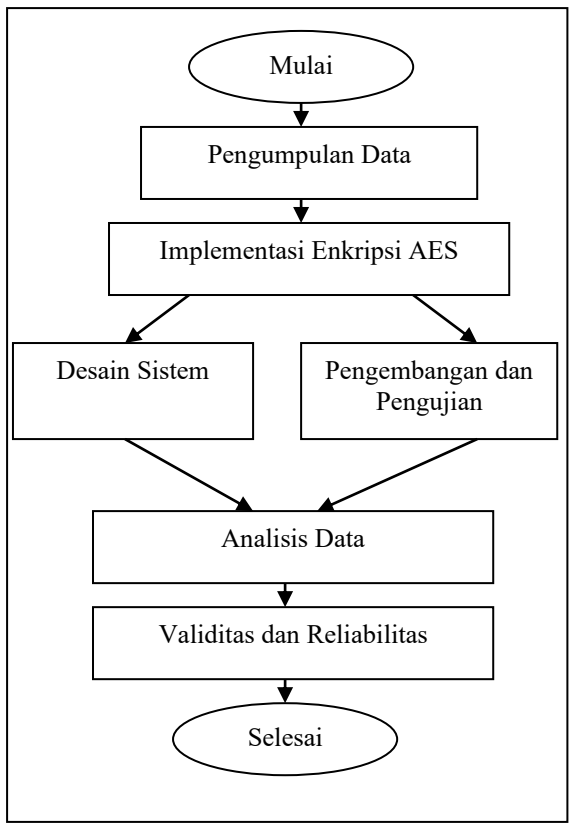
yang sangat baik dan efisiensi yang tinggi (Indraka & Romli, 2025), (Hendarwati, 2014). Namun, meskipun AES sudah banyak diterapkan dalam berbagai sektor, implementasinya dalam sistem arsip surat di KONI Provinsi Sumatera Utara masih terbatas, sehingga diperlukan kajian lebih lanjut untuk mengetahui sejauh mana penerapan AES dalam mengamankan arsip digital di lingkungan organisasi tersebut.

Gap yang ada antara penggunaan teknologi enkripsi dalam sistem arsip di lembaga pemerintahan dan organisasi olahraga seperti KONI Provinsi Sumatera Utara menjadi alasan pentingnya kajian ini dilakukan. Penelitian ini bertujuan untuk mengidentifikasi tantangan, manfaat, dan implementasi dari enkripsi AES dalam sistem arsip surat di KONI Provinsi Sumatera Utara. Dengan begitu, hasil penelitian ini diharapkan dapat memberikan kontribusi yang signifikan bagi perbaikan dan peningkatan keamanan arsip surat dalam organisasi tersebut.

II. METODOLOGI

2.1. Desain Penelitian

Penelitian ini menggunakan metode deskriptif dengan pendekatan studi kasus, di mana peneliti akan mengidentifikasi dan menganalisis implementasi enkripsi AES pada sistem arsip surat di KONI Provinsi Sumatera Utara. Studi kasus ini dilakukan untuk menggali berbagai aspek terkait dengan penggunaan AES, mulai dari tahap perencanaan, penerapan, hingga evaluasi sistem. Pendekatan ini memungkinkan peneliti untuk mengumpulkan data yang mendalam dan kontekstual yang relevan dengan situasi yang ada di KONI Provinsi Sumatera Utara.



Gambar 1. Alur Penelitian

2.2. Pengumpulan Data

Pengumpulan data melalui studi dokumentasi sistem arsip yang ada, termasuk perangkat lunak yang digunakan, serta prosedur yang telah diterapkan dalam pengelolaan arsip surat. Data ini akan dianalisis untuk menentukan sejauh mana enkripsi AES dapat diterapkan dalam sistem yang ada.

2.3. Implementasi Enkripsi AES

Setelah pengumpulan data, langkah selanjutnya adalah melakukan implementasi enkripsi AES pada sistem arsip surat di KONI Provinsi Sumatera Utara. Peneliti akan menggunakan perangkat lunak yang mendukung algoritma AES, seperti OpenSSL atau library AES dalam bahasa pemrograman yang relevan. Langkah-langkah implementasi

meliputi Desain Sistem serta Pengembangan dan Pengujian.

2.4. Analisis Data

Data yang terkumpul melalui wawancara, observasi, dan dokumentasi akan dianalisis secara kualitatif dengan menggunakan analisis tematik. Peneliti akan mengidentifikasi tema-tema utama yang muncul terkait implementasi enkripsi AES, termasuk kelebihan, kekurangan, dan hambatan-hambatan yang dihadapi selama proses implementasi. Hasil dari analisis ini diharapkan dapat memberikan wawasan yang lebih jelas mengenai bagaimana enkripsi AES dapat meningkatkan keamanan sistem arsip surat di KONI Provinsi Sumatera Utara.

2.5. Validitas dan Reliabilitas

Untuk memastikan validitas dan reliabilitas hasil penelitian, uji coba sistem yang diterapkan juga akan dilakukan untuk memastikan bahwa implementasi enkripsi AES berjalan sesuai harapan dan dapat memberikan perlindungan terhadap data arsip surat.

III. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi AES (AES-128)

Berikut ini adalah proses enkripsi AES (AES-128)

1. **Ukuran Blok dan Ukuran Kunci:**
   - **AES-128** menggunakan kunci sepanjang 128-bit (16 byte) dan memproses data dalam blok berukuran 128 bit (16 byte).
2. **Padding:**
   - Jika data yang ingin dienkripsi tidak pas dengan ukuran blok 128-bit (misalnya panjang data 15 karakter), maka padding akan ditambahkan. Padding yang umum digunakan adalah **PKCS7**, yang menambahkan byte sehingga total ukuran data menjadi kelipatan dari ukuran blok.

Contoh Perhitungan Enkripsi AES

1. **Data Input:**
   Misalnya kita ingin mengenkripsi teks: "ARSIPDOKUMEN123"
   - Panjang data input: 15 karakter (120 bit).
2. **Padding:**
   Karena AES bekerja dengan blok 128-bit, kita perlu menambahkan padding agar data menjadi 128-bit (16 byte). Data setelah ditambahkan padding bisa menjadi seperti ini: "ARSIPDOKUMEN123\x01", di mana \x01 adalah satu byte padding.
3. **Konversi ke Format Hexadecimal:**
   Setiap karakter dalam string diubah menjadi nilai ASCII dalam format hexadecimal (nilai desimal ke hexadecimal):

Karakter	ASCII	Hexadecimal
A	65	41
R	82	52
S	83	53
I	73	49
P	80	50
D	68	44
O	79	4F
K	75	4B
U	85	55
M	77	4D
E	69	45
N	78	4E
1	49	31
2	50	32
3	51	33
\x01	1	01

4. Jadi, plaintext (dalam hex) adalah:
5. mathematica
6. SalinEdit
7. 41 52 53 49 50 44 4F 4B 55 4D 45 4E 31 32 33 01

8. **Kunci Enkripsi (128-bit):**

Misalnya, kunci yang digunakan adalah: "KUNCIRAHASIA1234"

- Dalam format hexadecimal, kunci menjadi:

mathematica
SalinEdit
4B 55 4E 43 49 52 41 48 41 53 49 41 31 32 33 34

9. **Proses AddRoundKey (Ronde 0):**

Pada ronde pertama, plaintext akan di-XOR dengan kunci untuk menghasilkan nilai ciphertext sementara.

- **Plaintext (hex)**:

mathematica
SalinEdit
41 52 53 49 50 44 4F 4B 55 4D 45 4E 31 32 33 01

- **Kunci (hex)**:

mathematica
SalinEdit
4B 55 4E 43 49 52 41 48 41 53 49 41 31 32 33 34

- Hasil XOR antara plaintext dan kunci adalah:

mathematica
SalinEdit
0A 07 1D 0A 19 16 0E 03 14 1E 0C 0F 00 00 00 35

Contoh Perhitungan XOR untuk 1 Byte:

- Plaintext byte: 0x41 (A) → 01000001 (biner)
- Key byte: 0x4B (K) → 01001011 (biner)

Hasil XOR:
scss
SalinEdit
0x0A → 00001010 (biner)

10. **Proses AES Selanjutnya (SubBytes, ShiftRows, MixColumns, dll.)**

Setelah langkah AddRoundKey, langkah-langkah lainnya seperti **SubBytes**, **ShiftRows**, dan **MixColumns** dilakukan sesuai dengan standar AES. Operasi ini menggunakan **S-Box** untuk substitusi byte dan **Transformasi Matriks** untuk MixColumns.

11. **Hasil Akhir Ciphertext**

Setelah semua ronde selesai, hasil akhirnya akan berupa ciphertext yang disimpan dalam format hexadecimal atau base64, seperti contoh berikut (setelah 10 ronde):
mathematica
SalinEdit
A9 6B D8 52 33 7A 19 FA E3 4D D2 10 B2 A5 73 6C

12. **Proses Dekripsi:** Dekripsi dilakukan dengan membalik urutan proses enkripsi, yaitu:

- **Invers ShiftRows**
- **Invers SubBytes**
- **AddRoundKey**
- **Invers MixColumns**

Hasil dekripsi akan kembali ke bentuk plaintext awal setelah semua langkah dekripsi selesai.
Plaintext akhir (hex):
mathematica
SalinEdit
41 52 53 49 50 44 4F 4B 55 4D 45 4E 31 32 33 01
Plaintext (ASCII):
nginx
SalinEdit
ARSIPDOKUMEN123
(Padding 01 dihilangkan pada saat pembacaan.)

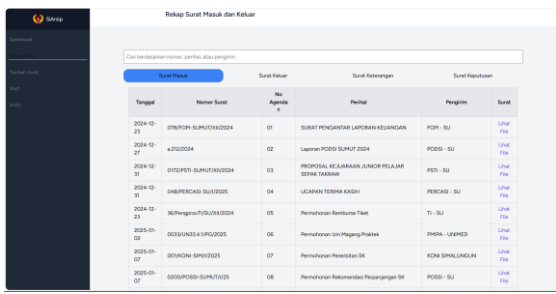
3.2 Tampilan

Sebagai interface pada user, beberapa tampilan dirumuskan agar mudah digunakan dan informatif.

Gambar 2. Tampilan Login

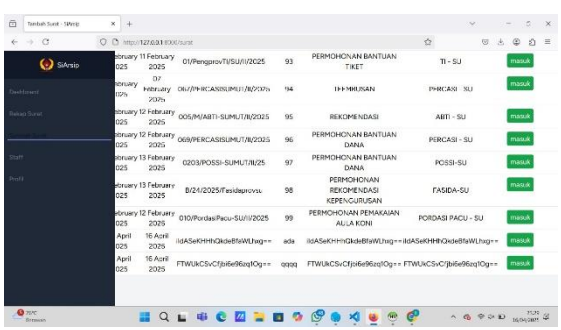
Gambar 2 menunjukkan tampilan awal dari sistem login **Sistem Arsip Surat** KONI Provinsi Sumatera Utara. Sistem ini memiliki antarmuka pengguna yang sederhana dan

mudah digunakan, dengan dua kolom utama untuk memasukkan username dan password. Pengguna diminta untuk memasukkan data login yang valid untuk mengakses sistem, yang memberikan akses ke arsip surat yang dilindungi dengan enkripsi. Hal ini menunjukkan upaya untuk menjaga keamanan data arsip dengan membatasi akses hanya untuk pengguna yang berwenang.



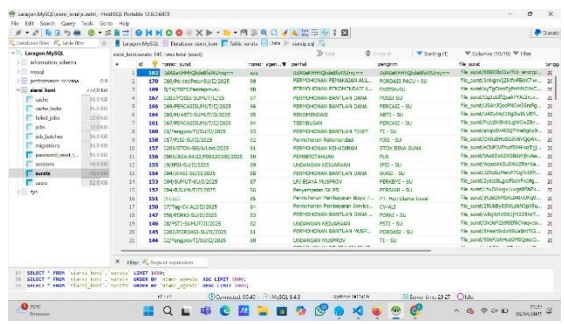
Gambar 3. Rekap Surat

Setelah berhasil login, **Gambar 3** menunjukkan tampilan utama dari sistem yang menampilkan rekap surat masuk dan keluar. Dalam hal ini, sistem menyajikan daftar surat beserta informasi terkait seperti tanggal, nomor surat, nomor agenda, perihal, pengirim, dan status dokumen yang dapat diunduh (lihat file). Enkripsi AES diterapkan pada file surat untuk menjaga kerahasiaan dokumen yang ada. Setiap file yang diunggah dalam sistem ini telah di-enkripsi, sehingga hanya pihak yang berwenang yang dapat mengakses dan membuka file tersebut.



Gambar 4. Tambah Surat

Pada **Gambar 4**, terdapat tampilan untuk menambah surat, yang memungkinkan pengguna untuk mengunggah surat baru ke dalam sistem. Halaman ini juga menyediakan fitur untuk memilih file yang akan diunggah dan di-enkripsi menggunakan AES. Setiap surat yang diunggah akan melalui proses enkripsi, yang memastikan bahwa data tersebut terlindungi dengan baik dari potensi akses yang tidak sah.



Gambar 5. Database Arsip Surat

Gambar 5 menampilkan hasil dari pengelolaan data surat dalam database menggunakan MySQL. Di sini, tampak bahwa informasi mengenai surat-surat yang di-upload sudah tercatat dengan jelas dalam database, termasuk nomor surat, agenda, perihal, dan pengirim. Kolom "file_surat" menunjukkan bahwa setiap surat telah di-enkripsi sebelum disimpan dalam database, yang mengindikasikan bahwa enkripsi AES diterapkan dengan benar pada setiap data yang diunggah ke dalam sistem.

Berdasarkan hasil implementasi, sistem ini berhasil mengimplementasikan enkripsi AES secara efektif untuk menjaga keamanan arsip surat. Penggunaan enkripsi AES tidak hanya melindungi kerahasiaan surat yang diunggah tetapi juga mengamankan akses ke file melalui proses login yang aman. Meskipun demikian, terdapat beberapa tantangan terkait dengan pengelolaan kunci enkripsi dan pengujian sistem yang harus dilakukan untuk

memastikan bahwa data dapat dengan mudah didekripsi hanya oleh pengguna yang berwenang.

IV. KESIMPULAN

Implementasi enkripsi AES dalam sistem arsip surat di KONI Provinsi Sumatera Utara berhasil meningkatkan keamanan arsip digital dengan efektif, melindungi data dari akses yang tidak sah. Meskipun penerapan enkripsi AES berjalan baik, tantangan utama terletak pada pengelolaan kunci enkripsi dan pengujian sistem untuk memastikan bahwa hanya pihak berwenang yang dapat mengakses dokumen. Dengan demikian, penelitian ini menunjukkan bahwa enkripsi AES adalah solusi yang tepat untuk mengamankan arsip surat di organisasi tersebut, meskipun ada kebutuhan untuk memperbaiki sistem manajemen kunci di masa depan.

DAFTAR PUSTAKA

Ariani, N. A., & Alamsyah, A. (2016). Analisis Preservasi Arsip Statis di Kantor Perpustakaan dan Arsip Kota Semarang. *Jurnal Ilmu Perpustakaan*, 5(3), Article 3.

Detharie, L. T., Herdiansah, A. G., & Zainuddin, Z. I. (2024). Optimalisasi Penggunaan Data Center Berbasis Server Lokal dalam Preservasi Arsip Digital di Arsip Nasional Republik Indonesia. *Responsive: Jurnal Pemikiran Dan Penelitian Bidang Administrasi, Sosial, Humaira Dan Kebijakan Publik*, *7*(3), 141–154.

Hapsari, N. F. A., & Ariyani, C. L. T. (2018). Urgency Preservation of Digital Archives. *Record and Library Journal, 4*(2), Article 2.

Hendarwati, W. P. (2014). Isu-isu preservasi arsip digital dan strategi preservasi sumber-sumber informasi digital. *Visi Pustaka, 16*(2), 129–134.

Indraka, A. P., & Romli, M. A. (2025). Security of Bumijo Village Archives Using Advanced Encryption Standard (AES-128) Method Based on Web Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES-128) Berbasis Web. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *5*(1), 232–241. https://doi.org/https://doi.org/10.57152/malcom.v5i1.1728

Muhidin, S. A., Winata, H., & Santoso, B. (2016). Pengelolaan arsip digital. Jurnal *Pendidikan Bisnis dan Manajemen, 2*(3), 178-83.

Saefulrahman, I., Muhammadi, R., Sakti, M. F. D., & Alpasha, J. N. (2025). Implementasi Sistem Manajemen Kearsipan Digital di Dinas Perpustakaan Dan Kearsipan Kota Bandung Mini. *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora*, *5*(1), 1–12. https://doi.org/https://doi.org/10.53697/iso.v5i1.2171