Jurnal Rekayasa Sistem Informasi dan Teknologi
Volume 2, No 1 – Agustus 2024
e-ISSN : 3025-888X

RANCANG BANGUN SISTEM E-ARSIP BERBASIS WEBSITE MENGGUNAKAN METODE ENKRIPSI AES (Advanced Encryption Standard) STUDI KASUS KPU SIDOARJO

Ravi Octian Nafis [1*], Mochamad Sidqon.[2]
[1], Universitas 17 Agustus 1945 Surabaya
ravioctiannafis@gmail.com[1*], sidqon@untag-sby.ac.id[2]

Received: 10-07- 2024	Revised: 25-07-2024	Approved: 30-07-2024

ABSTRAK

Studi ini bertujuan untuk merancang dan mengimplementasikan Sistem Informasi E-Arsip berbasis website di lingkungan Komisi Pemilihan Umum (KPU) Sidoarjo, dengan menerapkan metode pengembangan perangkat lunak Waterfall. Pusat perhatian utama penelitian adalah penerapan algoritma enkripsi AES dalam konteks manajemen arsip elektronik. Proses pengembangan melibatkan tahap analisis kebutuhan sistem, perancangan arsitektur, pembangunan website, dan penerapan algoritma secara berurutan, sesuai dengan prinsip-prinsip model Waterfall. Pada pengujian avalanche effect menunjukkan hasil yang memuaskan, dengan setiap perputaran bit mencapai rata-rata 50,15%, yang dianggap cukup baik. Evaluasi keberhasilan sistem akan dilakukan melalui pengukuran kehandalan, keamanan, dan efisiensi pencarian data, dengan metode validasi melalui evaluasi menyeluruh dan umpan balik pengguna untuk memastikan kecocokan sistem dengan kebutuhan khusus KPU Sidoarjo. Sebagai tambahan, penelitian ini juga akan memfokuskan perhatian pada pelatihan pengguna, dengan tujuan memastikan pemangku kepentingan, termasuk staf administratif dan petugas KPU, memahami secara mendalam penggunaan sistem, sehingga dapat meningkatkan penerapan optimal dan efektivitas sesuai dengan kebutuhan operasional KPU Sidoarjo.

***Kata Kunci** : Sistem Informasi E-Arsip, Metode Waterfall, Algoritma Enkripsi AES, avalanche effect.*

PENDAHULUAN

National Archives and Record Administration (NARA) mendefinisikan arsip elektronik sebagai dokumen yang disimpan dan diolah dalam suatu format dengan menggunakan komputer. Standar China untuk Penyimpanan dan Manajemen Arsip Elektronik menyatakan bahwa arsip elektronik adalah dokumen yang dibuat oleh perangkat digital. Dengan mempertimbangkan berbagai definisi tersebut, dapat disimpulkan bahwa arsip elektronik terdiri dari semua(Nyfantoro et al., 2020). Manajemen arsip merupakan komponen krusial dalam operasional kantor. Hampir setiap aktivitas dan proses di lingkungan kantor membutuhkan data dan informasi yang menjadi landasan kerja. Arsip, sebagai sumber data utama, berperan penting karena berfungsi sebagai bukti dan rekaman kegiatan. Pengolahan arsip dapat dilakukan secara konvensional melalui pendekatan manual, atau dengan metode elektronik yang melibatkan penggunaan perangkat computer (Amalia et al., 2019).

Karena itu, penerapan teknologi informasi dan komunikasi, terutama melalui perangkat komputer, menjadi sebuah alasan kuat mengapa pengelolaan arsip harus dilakukan secara elektronik. Dengan ketersediaan media elektronik, seperti komputer, serta beragam aplikasi desktop dan web, proses manajemen arsip dapat dilakukan dengan lebih efisien, mengurangi waktu yang dibutuhkan (Imron & Listyorini, 2022). Penggunaan komputer memungkinkan konversi arsip konvensional menjadi format digital atau bahkan menciptakan arsip dalam bentuk elektronik (Ninia Lina, 2020), Menurut (Azmi et al., 2023) Dengan memanfaatkan

teknologi berbasis web, pengelolaan arsip surat dapat dilakukan secara praktis dan presisi, sehingga risiko kehilangan surat dapat diminimalkan.

Komisi Pemilihan Umum (KPU) Sidoarjo, sebuah lembaga yang bertanggung jawab dalam mengelola data terkait pemilihan umum dan kepala daerah, mengalami kesulitan dalam mengorganisir arsip secara manual. Pendekatan manual dalam penyimpanan data telah menyebabkan gangguan dalam operasional. Untuk mengatasi tantangan ini, diperlukan pengembangan sistem e-arsip yang mengadopsi algoritma Sequential Search. Namun, demi meningkatkan tingkat keamanan data, peningkatan metode kriptografi Advanced Encryption Standard (AES) menjadi kebutuhan utama dalam pengembangan sistem tersebut (Tulloh et al., 2016). Dengan demikian, diharapkan implementasi sistem ini akan mampu meningkatkan keamanan serta efisiensi dalam pengelolaan data yang memiliki sensitivitas tinggi, sejalan dengan prinsip-prinsip keberlanjutan dalam pengelolaan informasi. AES, atau Standar Enkripsi Lanjutan, adalah sebuah algoritma enkripsi kunci simetris yang diterbitkan oleh National Institute of Standards and Technology pada tahun 2001(Alifudin & Rosyida, 2021). Algoritma ini dirancang untuk menggantikan DES karena DES memiliki kunci sandi yang relatif kecil dan algoritmenya cenderung lambat. Rijndael, yang dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen, diajukan oleh mereka sebagai kandidat untuk menjadi standar AES. AES memiliki tiga varian utama: AES-128, AES-192, dan AES-256, yang masing-masing memiliki ukuran blok 128 bit atau setara dengan 16 byte (Rachmayanti & Wirawan, 2022).

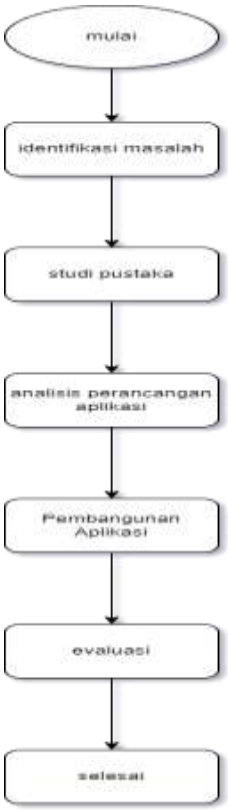
Dengan alasan tersebut, penelitian ini hadir sebagai usaha untuk mengatasi masalah sebenarnya yang dihadapi oleh KPU Sidoarjo dalam mengelola data arsip yang awalnya dilakukan secara manual. Kami ingin memanfaatkan algoritma Sequential Search dalam pembuatan Sistem Informasi E-Arsip untuk memberikan solusi yang praktis, efisien, dan sesuai kebutuhan yang akan membantu KPU Sidoarjo dalam meningkatkan cara mereka dalam mengelola data internal maupun data eksternal.

METODE PENELITIAN

Penelitian ini meliputi lima tahap utama:

1. Identifikasi masalah: Menganalisis kelemahan sistem arsip tradisional di KPU Sidoarjo melalui wawancara dengan pemangku kepentingan.
2. Studi pustaka: Memperdalam pemahaman tentang pengembangan sistem informasi arsip.
3. Analisis perancangan aplikasi: Merancang arsitektur, antarmuka pengguna, dan struktur basis data berdasarkan kebutuhan yang diidentifikasi.
4. Pembangunan aplikasi: Menerapkan metode enkripsi AES dan model pengembangan Waterfall.
5. Evaluasi: Menguji aplikasi di KPU Sidoarjo, mengukur performa, keandalan algoritma pencarian, keamanan, dan respons pengguna. Hasil evaluasi digunakan untuk penyempurnaan sistem.

Tujuan akhirnya adalah mengembangkan Sistem Informasi E-arsip yang efisien dan efektif untuk manajemen arsip di KPU Sidoarjo.

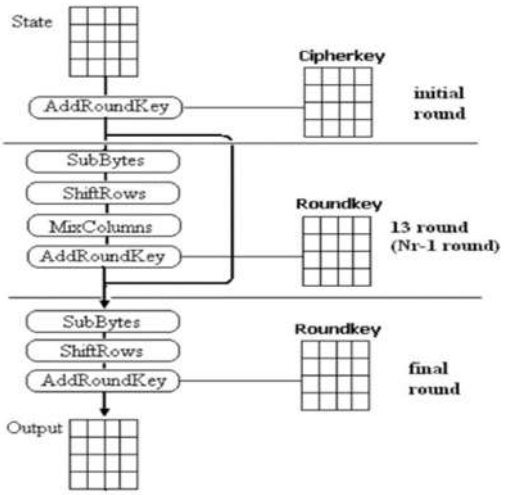


Gambar 1 Tahapan Penelitian

AES, atau Standar Enkripsi Lanjutan, adalah sebuah algoritma enkripsi kunci simetris yang diterbitkan oleh National Institute of Standards and Technology pada tahun 2001. Algoritma ini dirancang untuk menggantikan DES karena DES memiliki kunci sandi yang relatif kecil dan algoritmenya cenderung lambat. Rijndael, yang dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen, diajukan oleh mereka sebagai kandidat untuk menjadi standar AES. AES memiliki tiga varian utama: AES-128, AES-192, dan AES-256, yang masing-masing memiliki ukuran blok 128 bit atau setara dengan 16 byte (Rachmayanti & Wirawan, 2022) Ukuran kunci yang lebih besar cenderung memberikan tingkat keamanan yang lebih tinggi, karena ruang pencarian kunci yang lebih besar membuat serangan brute-force menjadi lebih sulit dilakukan.

Proses enkripsi AES (Advanced Encryption Standard) terdiri dari beberapa tahapan penting yang berfungsi untuk meningkatkan keamanan dan kompleksitas data yang dienkripsi. Tahapan-tahapan tersebut meliputi substitusi byte (SubBytes), pergeseran baris (ShiftRows), campuran kolom (MixColumns), dan penambahan kunci putaran (AddRoundKey). Setiap langkah ini memiliki peran spesifik dalam memastikan data terlindungi dengan baik dan sulit untuk dipecahkan oleh pihak yang tidak berwenang. Tahap pertama dalam proses enkripsi AES adalah SubBytes, di mana setiap byte dalam blok data dienkripsi dengan menggantinya menggunakan tabel substitusi yang disebut S-box. S-box ini dirancang untuk memberikan pengacakan yang tinggi, membuat hubungan antara input dan output tidak linear. Langkah berikutnya adalah ShiftRows, yang melibatkan pergeseran baris dalam matriks data. Pada tahap ini, baris kedua dari matriks digeser satu posisi ke kiri, baris ketiga digeser dua posisi ke kiri, dan baris keempat digeser tiga posisi ke kiri.

Selanjutnya adalah tahap MixColumns, di mana setiap kolom dalam matriks data diproses menggunakan transformasi linier. Tahap ini mencampur byte dalam setiap kolom, meningkatkan difusi lebih lanjut dan memastikan bahwa perubahan pada satu byte input mempengaruhi banyak byte output. Tahap terakhir dalam setiap putaran enkripsi adalah AddRoundKey, di mana blok data hasil dari tahapan sebelumnya ditambahkan dengan kunci putaran menggunakan operasi XOR. Kunci putaran ini berasal dari kunci enkripsi utama yang telah diperluas menjadi serangkaian kunci putaran untuk setiap tahap enkripsi.



Gambar 2 Proses Metode AES

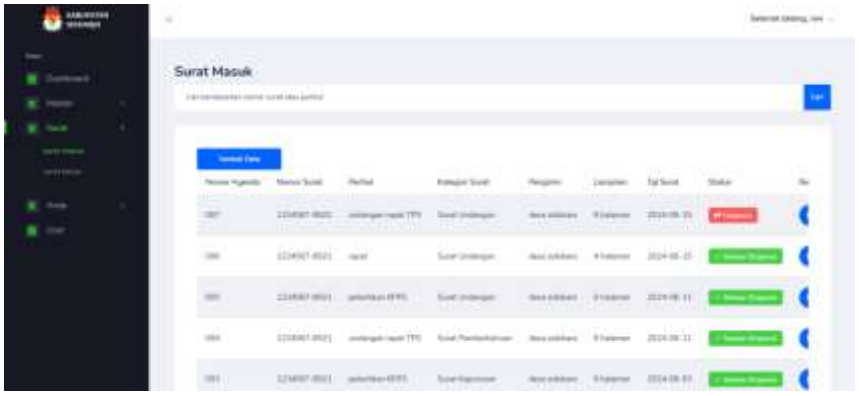
Menurut (Wahid Abdul, 2020) Metode air terjun (waterfall), yang sering disebut sebagai metode siklus hidup klasik atau "Linear Sequential Model," merujuk pada pendekatan sistematis dan berurutan dalam pengembangan perangkat lunak. Proses ini dimulai dengan merinci spesifikasi kebutuhan pengguna dan melanjutkan dengan langkah-langkah perencanaan, pemodelan, konstruksi, hingga penyerahan sistem kepada pengguna. Akhirnya, proses ini ditutup dengan memberikan dukungan penuh terhadap perangkat lunak yang telah dikembangkan. Pendekatan ini mencerminkan tahapan-tahapan yang terorganisir untuk mencapai pengembangan perangkat lunak yang lengkap.

Laravel adalah kerangka kerja PHP yang terdiri dari banyak plugins yang sudah terintegrasi dan menggunakan konsep Model, View, dan Controller (MVC). Laravel dimaksudkan untuk meningkatkan kualitas perangkat lunak dengan mengurangi biaya pengembangan awal dan pemeliharaan serta meningkatkan pengalaman bekerja dengan aplikasi dengan sintaks yang ekspresif, jelas, dan menghemat waktu (Prayudha & Rochmawati, 2018). Menurut studi kerangka kerja PHP, Laravel memungkinkan pengembangan kode PHP yang elegan dan sederhana (Laaziri et al., 2019), selain itu menurut (Lutfi, 2017) penelitian menunjukkan bahwa Laravel membantu berinteraksi dengan database. Sebuah kutipan yang relevan menyatakan bahwa Laravel membuat berinteraksi dengan database mudah.

Menurut (Aziz, 2021), Black Box Testing adalah suatu metode yang digunakan dalam pengujian perangkat lunak tanpa memerlukan perhatian terhadap detail-detail internal perangkat lunak tersebut. Dalam pengujian ini, fokus utama diberikan pada evaluasi nilai output yang dihasilkan berdasarkan input yang diberikan, tanpa memeriksa detail-detail implementasi perangkat lunak. Black Box Testing dilakukan untuk menunjukkan bagaimana perangkat

lunak berfungsi. Pengujian sistem menggunakan metode pengujian *Black Box* dapat menemukan kesalahan dalam beberapa kategori diantaranya adalah menemukan beberapa fungsi – fungsi yang tidak benar atau hilang, kesalahan *interface,* kesalahan struktur data, fitur yang tidak dapat diakses dan kesalahan kinerja (Achmad & Yulfitri, 2020).

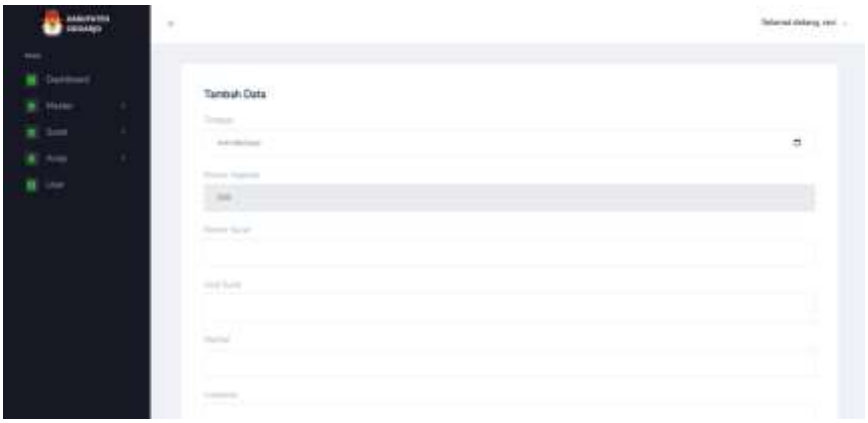
HASIL DAN PEMBAHASAN



Gambar 3 Dashboard Halaman Surat Masuk

Gambar 3 menggambarkan halaman surat masuk pada sistem e-arsip. Pada gambar tersebut, terlihat bahwa terdapat data surat yang telah didisposisi oleh ketua KPU, serta data surat yang sudah diterima oleh pihak yang ditunjuk untuk disposisi. Halaman ini dirancang untuk menampilkan status terkini dari setiap surat masuk, memudahkan pemantauan dan pengelolaan surat-surat yang masuk ke sistem.

Selain menampilkan status disposisi, halaman surat masuk ini juga menyediakan fitur bagi admin untuk menambah data surat baru. Admin memiliki akses untuk menginput data surat masuk yang baru, memastikan bahwa semua surat yang diterima dapat didokumentasikan dengan baik dan tepat waktu. Proses ini mencakup pengisian berbagai informasi penting terkait surat, seperti tanggal penerimaan, pengirim, subjek surat, dan detail lainnya yang relevan.

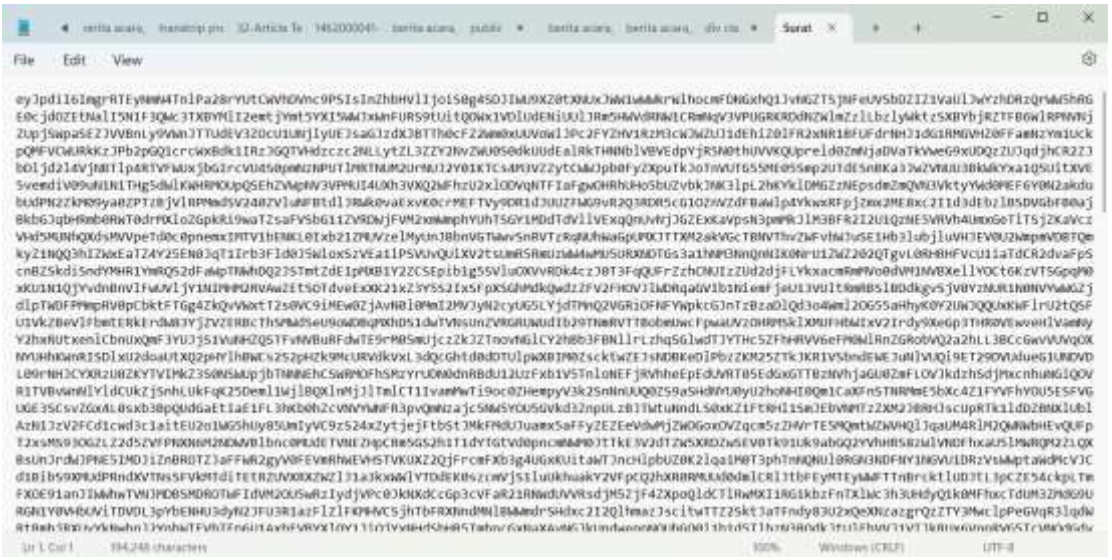


Gambar 4 Halaman Input Surat Masuk

Gambar 4 menunjukkan halaman tambah surat masuk, yang merupakan bagian dari sistem manajemen surat elektronik. Pada halaman ini, pengguna (user) diharuskan untuk menginputkan semua field atau kolom yang tersedia, seperti

nomor surat, tanggal surat, pengirim, penerima, perihal, dan isi surat. Setelah semua field diisi dengan lengkap dan benar, pengguna kemudian harus menekan tombol "Submit" untuk mengirimkan data tersebut ke sistem.

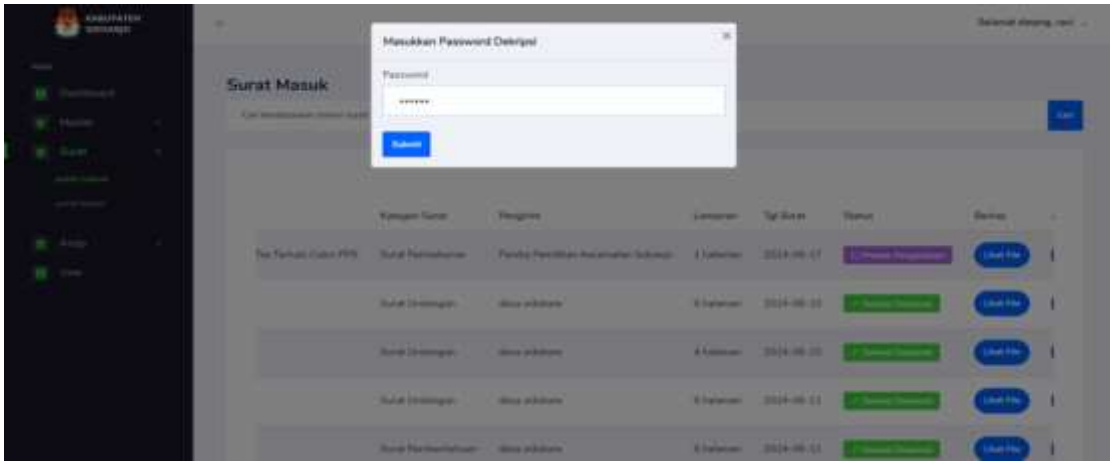
Penting untuk diperhatikan bahwa setiap data yang diinputkan pada halaman surat masuk ini harus dienkripsi sebelum dikirim dan disimpan dalam basis data. Enkripsi adalah proses mengubah informasi menjadi kode yang tidak bisa dibaca tanpa kunci dekripsi yang tepat. Tujuan dari enkripsi adalah untuk melindungi informasi sensitif dari akses yang tidak sah dan menjaga kerahasiaan data.



Gambar 5 Hasil file yang terenkripsi

Data yang diinputkan harus dienkripsi sehingga tidak dapat dibaca oleh pihak yang tidak berwenang. Enkripsi adalah proses mengubah informasi menjadi kode yang hanya dapat dibaca oleh mereka yang memiliki kunci dekripsi yang tepat. Hal ini memastikan bahwa data yang disimpan atau dikirim tetap aman dan terlindungi dari akses yang tidak sah.

Proses enkripsi harus dilakukan sedemikian rupa sehingga data yang telah dienkripsi tidak dapat dimengerti atau digunakan tanpa terlebih dahulu didekripsi. Dengan kata lain, bahkan jika seseorang berhasil mengakses file terenkripsi, mereka tidak akan dapat memahami isi file tersebut tanpa kunci dekripsi yang sesuai. Ini penting untuk melindungi informasi sensitif dan memastikan privasi data tetap terjaga.



Gambar 6 Modal input password dekripsi

Proses dekripsi data dilakukan melalui halaman antarmuka yang telah disediakan khusus untuk tujuan ini. Pada halaman antarmuka tersebut, pengguna diharuskan untuk menginputkan key atau kunci dekripsi yang benar. Kunci dekripsi ini adalah elemen penting yang diperlukan untuk mengubah data yang telah dienkripsi kembali ke bentuk aslinya yang dapat dibaca dan digunakan.

Ketika pengguna mengakses halaman dekripsi, mereka akan melihat sebuah field atau kotak input di mana mereka harus memasukkan kunci dekripsi. Proses ini memastikan bahwa hanya pengguna yang memiliki otorisasi dan akses ke kunci dekripsi yang dapat membuka data yang terenkripsi. Langkah ini sangat penting untuk menjaga keamanan dan integritas data yang sensitif.

Gambar 7 Hasil file yang telah terdekripsi

Pengguna dapat melihat hasil dari file yang telah didekripsi setelah mereka memasukkan kunci pada halaman antarmuka yang telah disediakan. Halaman antarmuka ini dirancang secara khusus untuk memudahkan pengguna dalam memasukkan kunci dekripsi yang diperlukan dan mengakses informasi yang sebelumnya dienkripsi dengan aman. Proses dekripsi ini memastikan bahwa hanya pengguna yang memiliki kunci yang benar yang dapat melihat isi file tersebut, sehingga menjaga kerahasiaan dan keamanan data.

Setelah pengguna membuka halaman antarmuka dekripsi, mereka akan melihat sebuah form atau kotak input di mana mereka harus memasukkan kunci dekripsi yang sesuai. Kunci ini berfungsi sebagai alat untuk membuka atau menguraikan data yang telah terenkripsi sebelumnya. Hal ini sangat penting karena tanpa kunci yang benar, data yang dienkripsi tidak dapat diakses atau dibaca, menjaga data tetap aman dari akses yang tidak sah.

Setelah memasukkan kunci dekripsi, pengguna akan menekan tombol "Submit" atau "Decrypt" yang ada di halaman tersebut. Sistem kemudian akan memverifikasi kunci dekripsi yang dimasukkan. Jika kunci yang dimasukkan benar, proses dekripsi akan dimulai. Proses ini menggunakan algoritma dekripsi yang sesuai untuk mengubah data yang telah terenkripsi kembali ke bentuk aslinya yang dapat dibaca dan digunakan.

Pada pengujian avalanche effect ini saya menggunakan rumus seperti berikut :

$$\frac{Jumlah\ Bit\ Berubah}{Total\ Bit} \times 100\%$$

Oleh karena itu, saya memutuskan untuk mengambil sampel berupa lima file yang telah tersedia dalam sistem saya. Setelah melalui proses analisis, saya memperoleh hasil Avalanche yang telah tercantum pada tabel. Perlu dicatat bahwa sebuah algoritma dianggap baik jika memiliki nilai persentase minimal sebesar 50% atau lebih.

Rata-rata hasil dari pengujian efek Avalanche yang saya lakukan menunjukkan angka sebesar 50,15%. Pengujian ini melibatkan analisis terhadap lima file yang ada dalam sistem saya, dan rata-rata tersebut dihitung berdasarkan hasil yang diperoleh dari setiap file yang diuji. Angka ini memberikan gambaran umum tentang kinerja algoritma yang diuji, menunjukkan bahwa algoritma tersebut memenuhi kriteria minimum yang diharapkan, yaitu efek Avalanche dengan persentase minimal sebesar 50%.

Efek Avalanche adalah fenomena di mana perubahan kecil pada input (seperti mengubah satu bit) menghasilkan perubahan besar pada output (dengan banyak bit yang berubah). Dalam konteks kriptografi dan keamanan data, efek ini sangat penting karena menunjukkan bahwa algoritma dapat dengan efektif menyebarkan perubahan kecil pada input ke seluruh output, sehingga meningkatkan keamanan dan mengurangi kemungkinan pola yang dapat dieksploitasi oleh pihak yang tidak berwenang.

Hasil pengujian ini menunjukkan bahwa algoritma yang diuji telah berhasil memenuhi kriteria dasar yang diharapkan, dengan mencapai rata-rata efek Avalanche di atas 50%. Hal ini penting karena memastikan bahwa algoritma tersebut memiliki performa yang dapat diandalkan dalam menjaga keamanan data. Efek Avalanche yang konsisten di atas 50% menunjukkan bahwa algoritma mampu menghasilkan output yang cukup acak dan tidak mudah diprediksi, yang merupakan salah satu indikator penting dalam evaluasi efektivitas algoritma enkripsi.

Tabel 3 Pengujian Avalanche

Nama File	key	Rata-Rata Avalanche Effect
undangan peluncuran kirab (PPK).pdf	27 karakter	50.3 %
Surat Permohonan Perlengkapan Tes Tulis.pdf	20 karakter	50.1%
undangan rakor PPK_Keu_0001[1].pdf	20 karakter	50%
yusrian,+1313-6418-4-PB.pdf	27 karakter	50%
Pendaftaran KPPS.pdf	20 karakter	50,4%
Undg Bimtek Keuangan PPK.pdf	20 karakter	50,1%
Pengumuman Kpu Sidoarjo 645 Tahun 2024 Hasil Seleksi Tertulis Calon Pps Pilkada Tahun 2024 (R).Pdf	27 karakter	50%
Ppk-1.Pdf	27 karakter	50.2%
Surat Tugas Nomor 501 Tahun 2023 tentang melaksanakan tugas Supervisi dan Monitoring Badan Adhoc.pdf	27 karakter	50.35%
145 Surat Ketua KPU Penyesuaian Jadwal Pembentukan Pantarlih.pdf	20 karakter	50.1%

KESIMPULAN

Penelitian ini berhasil mengembangkan dan menerapkan sistem e-arsip berbasis website dengan menggunakan metode enkripsi AES (Advanced Encryption Standard), yang dirancang khusus untuk memenuhi kebutuhan KPU Sidoarjo. Proses pengembangan sistem ini menggunakan model pengembangan perangkat lunak Waterfall, yang meliputi tahapan analisis kebutuhan, desain, implementasi, pengujian, dan pemeliharaan. Pendekatan yang terstruktur ini memastikan bahwa sistem dibangun sesuai dengan spesifikasi yang diinginkan dan memenuhi standar kualitas yang tinggi.

Hasil pengujian efek Avalanche, yang dilakukan untuk mengukur keandalan enkripsi, menunjukkan rata-rata sebesar 50,15%. Nilai ini diperoleh dari pengujian pada sepuluh file yang ada dalam sistem, dan hasil ini menunjukkan bahwa algoritma enkripsi AES yang digunakan memenuhi kriteria minimal yang diharapkan. Efek Avalanche mengukur seberapa besar perubahan yang terjadi pada output ketika terjadi perubahan kecil pada input, dan hasil yang mendekati atau melebihi 50% dianggap menunjukkan performa yang baik dalam keamanan data.

Pengujian ini menjadi indikator penting dalam mengevaluasi efektivitas algoritma enkripsi yang digunakan dalam sistem e-arsip. Hasil rata-rata sebesar 50,15% menunjukkan bahwa sistem ini mampu menyediakan tingkat keamanan data yang memadai melalui penggunaan algoritma AES. Selain itu, hasil pengujian juga menunjukkan bahwa setiap perubahan bit pada input menghasilkan perubahan yang signifikan pada output, yang penting untuk menjaga kerahasiaan dan integritas data.

DAFTAR PUSTAKA

[1] Achmad, Y. F., & Yulfitri, A. (2020). Pengujian Sistem Pendukung Keputusan Menggunakan Black Box Testing Studi Kasus E-Wisudawan Di Institut Sains Dan Teknologi Al-Kamal. *Jurnal Ilmu Komputer*, *5*, 42.

[2] Alifudin, M. I., & Rosyida, S. (2021). Sistem Informasi Manajemen Arsip Elektronik (E-Arsip) Berbasis Web Pada Marcom Bsi Group. *Jurnal Khatulistiwa Informatika*, *9*(2), 99–106. https://doi.org/10.31294/jki.v9i2.11346

[3] Amalia, A. N. N., Afifuddin, & Hayat. (2019). IMPLEMENTASI E-DOCUMENT DALAM PENGELOLAAN SURAT MASUK DAN KELUAR (Studi Kebijakan UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik di Bagian Umum Balai Kota Malang, Jawa Timur). *Jurnal Respon Publik*, *13*(3), 10–20.

[4] Aziz, A. (2021). Pengujian Black Box pada Aplikasi Keamanan Data Multimedia Message Service (MMS) Berbasis Android Menggunakan Teknik Equivalence Partitions. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *4*(1), 58. https://doi.org/10.32493/jtsi.v4i1.9074

[5] Azmi, M. C., Siddiq, T. A., & Nasution, Y. R. (2023). Perancangan Sistem Arsip Surat Masuk Dan Keluar Biro Administrasi Dan Pembangunan Provinsi Sumatera Utara Berbasis Web. *Simtek : Jurnal Sistem Informasi Dan Teknik Komputer*, *8*(1), 58–60. https://doi.org/10.51876/simtek.v8i1.174

[6] Imron, M. S., & Listyorini, T. (2022). Sistem Manajemen Arsip Surat Berbasis Web di Dinas Pendidikan dan Kebudayaan Pati. *Seminar Nasional Inovasi Vokasi*, *1*(1), 136–145.

http://prosiding.pnj.ac.id/index.php/sniv/article/view/4545%0Ahttp://prosiding.pnj.ac.id/index.php/sniv/article/viewFile/4545/2479

[7] Laaziri, M., Benmoussa, K., Khoulji, S., Mohamed Larbi, K., & Yamami, A. El. (2019). A comparative study of laravel and symfony PHP frameworks. *International Journal of Electrical and Computer Engineering (IJECE)*, *9*(1), 704. https://doi.org/10.11591/ijece.v9i1.pp704-712

[8] Lutfi, A. (2017). Sistem Informasi Akademik Madrasah Aliyah Salafiyah Syafi'iyah Menggunakan Php dan MySQL. *Jurnal AiTech*, *3*(2), 104–112.

[9] Ninia Lina, T. (2020). Sistem Informasi E-Arsip Berbasis Web (Studi Kasus: Pt Haleyora Powerindo Cabang Sorong). *Jurnal Jendela Ilmu*, *1*(1), 1–5. https://doi.org/10.34124/ji.v1i1.48

[10] Nyfantoro, F., Salim, T. A., & Mirmani, A. (2020). Perkembangan Pengelolaan Arsip Elektronik Di Indonesia: Tinjauan Pustaka Sistematis. *Diplomatika: Jurnal Kearsipan Terapan*, *3*(1), 1. https://doi.org/10.22146/diplomatika.48495

[11] Prayudha, R. A. E., & Rochmawati, D. R. (2018). *Perancangan Sistem Informasi Pelayanan Publik Menggunakan Framework Laravel & Mysql Di Kecamatan Coblong Kota Bandung*. 36–49.

[12] Rachmayanti, A., & Wirawan, W. (2022). Implementasi Algoritma Advanced Encryption Standard (AES) pada Jaringan Internet of Things (IoT) untuk Mendukung Smart Healthcare. *Jurnal Teknik ITS*, *11*(3). https://doi.org/10.12962/j23373539.v11i3.97042

[13] Tulloh, A. R., Permanasari, Y., Harahap, E., Matematika, P., Matematika, F., Ilmu, D., & Alam, P. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption. *Jurnal Matematika UNISBA*, *Vol 2*(1), 1–8.

[14] Wahid Abdul, A. (2020). Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi. *Jurnal Ilmu-Ilmu Informatika Dan Manajemen STMIK*, *November*, 1–5.