Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Implementasi Keamanan Formulir Data Siswa Pada Web Pendaftaran Dengan Metode AES

Noris Astahadi[1], Riska Nurtantyo Sarbini[2], Iin Kurniasari[3] , Halimahtus Mukminna[4]
[1,2,3,4]Fakultas Teknik Komputer, Universitas Islam Kadiri
E-mail: [1]nurisasta55@gmail.com,[2]riskanurtantyosarbini@gmail.com,
[3]iin.kurniasari@uniska-kadiri.ac.id, [4]halimahtusm@uniska-kadiri.ac.id

Submit : 31 Mei 2025 | **Diterima** : 07 Jun 2025 | **Terbit** : 08 Jun 2025

ABSTRAK

Perkembangan teknologi digital yang pesat membawa manfaat besar bagi kehidupan sehari-hari, namun juga menimbulkan tantangan baru terkait keamanan data. Keamanan data menjadi semakin krusial, terutama dalam lingkungan pendidikan, di mana perlindungan data siswa sangat penting untuk mencegah penyalahgunaan oleh pihak yang tidak bertanggung jawab. SPS Tapos, sebagai lembaga pendidikan, menghadapi tantangan ini dalam mengelola formulir pendaftaran siswa yang mengandung informasi pribadi sensitif. Saat ini, proses pendaftaran masih dilakukan secara manual, yang rentan terhadap risiko keamanan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pendaftaran berbasis web yang mengamankan formulir data siswa di SPS Tapos menggunakan metode AES. Hasil dari penelitian ini menunjukkan bahwa sistem yang diusulkan mampu memberikan tingkat keamanan yang memadai, sesuai dengan kebutuhan lembaga pendidikan, dan efektif dalam melindungi data siswa dari potensi penyalahgunaan. Dengan adanya sistem ini, diharapkan keamanan data siswa dapat lebih terjamin dan proses pendaftaran dapat dilakukan dengan lebih aman dan efisien.

Kata Kunci *-- Metode AES, Kriptografi, Keamanan Dokumen*

ABSTRACT

The rapid development of digital technology brings great benefits to everyday life, but also raises new challenges related to data security. Data security is becoming increasingly crucial, especially in educational environments, where student data protection is essential to prevent misuse by irresponsible parties. SPS Tapos, as an educational institution, faces this challenge in managing student registration forms containing sensitive personal information. Currently, the registration process is still done manually, which is vulnerable to security risks. This study aims to design and implement a web-based registration system that secures student data forms at SPS Tapos using the AES method. The results of this study indicate that the proposed system is able to provide an adequate level of security, according to the needs of educational institutions, and is effective in protecting student data from potential misuse. With this system, it is hoped that student data security can be more guaranteed and the registration process can be carried out more safely and efficiently.

Keywords*— AES Method, Cryptography, Document Security*

PENDAHULUAN

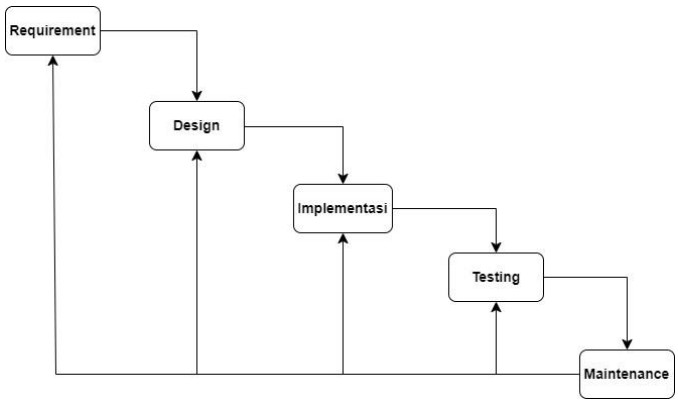
Era teknologi digital yang terus berkembang membawa berbagai peningkatan yang memberikan manfaat signifikan bagi kehidupan sehari-hari[1][2]. Namun, di balik kemajuan ini, isu keamanan data menjadi semakin penting. Perkembangan teknologi tidak hanya mempermudah dan meningkatkan efisiensi, tetapi juga membuka peluang bagi ancaman baru terhadap keamanan data. Celah-celah baru yang muncul dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk keuntungan pribadi, yang pada akhirnya dapat merugikan banyak orang. Oleh karena itu, keamanan data menjadi lebih krusial dari sebelumnya dalam lingkungan digital yang terus berkembang. Hal ini terutama relevan dalam konteks lembaga pendidikan, di mana data siswa harus dijaga kerahasiaannya dan tidak

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

boleh disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab[3].
SPS (Satuan PAUD Sejenis) adalah layanan PAUD non-formal yang menyediakan sarana pendidikan untuk membantu pertumbuhan dan perkembangan anak agar siap memasuki jenjang pendidikan lebih lanjut. SPS Tapos, sebagai salah satu lembaga pendidikan, memiliki tanggung jawab untuk melindungi data pribadi siswa yang telah mendaftar. Formulir pendaftaran yang digunakan oleh lembaga ini mengumpulkan berbagai informasi pribadi siswa, termasuk data-data sensitif seperti nama, alamat, tanggal lahir, nomor induk kependudukan, nomor akta kelahiran, dan nomor kartu keluarga. Saat ini, pendaftaran di SPS Tapos masih dilakukan secara manual, dengan pengisian kertas formulir, fotokopi kartu keluarga, dan fotokopi akta kelahiran. Oleh karena itu, sangat penting bagi SPS Tapos untuk memiliki sistem pendaftaran dan keamanan data yang efektif, yang dapat menjaga privasi data siswa dan mencegah penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab[4].
Salah satu cara untuk menjaga keamanan data adalah melalui penggunaan kriptografi. Algoritma kriptografi merupakan metode untuk melindungi data, dan salah satu algoritma yang banyak digunakan adalah Advanced Encryption Standard (AES). AES adalah algoritma kriptografi yang berfungsi untuk mengamankan data melalui enkripsi dan dekripsi. Enkripsi adalah proses mengubah data menjadi format yang tidak dapat dibaca (ciphertext), sementara dekripsi mengembalikan ciphertext ke bentuk aslinya (plaintext). AES dipilih karena kemampuannya mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, di mana perbedaan panjang kunci ini mempengaruhi jumlah putaran pada algoritma AES[5][6].

METODE PENELITIAN

Metode Dalam membuat tugas akhir penulis mengadopsi model waterfall, dimana model pengembangan ini melakukan pendekatan secara sistematis dan berurutan[12]. Disebut waterfall karena tahap demi tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan berurutan. Model pengembangan ini bersifat linear dari tahap awal pengembangan sistem yaitu tahap perencanaan sampai tahap akhir pengembangan sistem yaitu tahap pemeliharaan[13].



Gambar 1. Metode *waterfall*

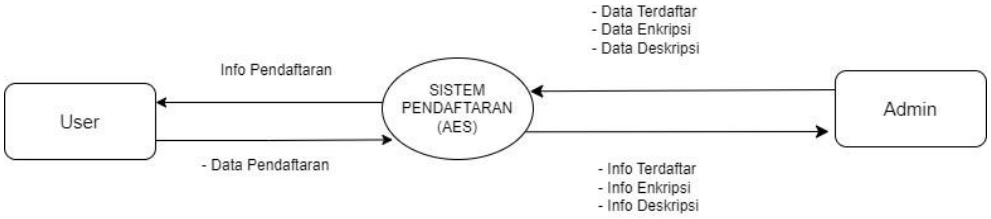
Alur Penelitian

Dalam penelitian ini, alur penelitian mengikuti metode waterfall yang terstruktur dan berurutan. Proses dimulai dengan penentuan judul, identifikasi masalah, penentuan metode pengembangan aplikasi, dan tujuan penelitian. Setelah itu, penulis melakukan pengumpulan data melalui wawancara untuk memperoleh informasi yang valid dan akurat. Data yang diperoleh kemudian dianalisis pada tahap analisis, di mana semua informasi diolah untuk memenuhi kebutuhan aplikasi yang akan dikembangkan. Selanjutnya, pada tahap implementasi, penulis memodelkan sistem informasi dan aplikasi yang akan dibuat, kemudian menulis kode program sesuai dengan desain yang telah dibuat. Setelah implementasi selesai, aplikasi diuji untuk mengevaluasi enkripsi dan dekripsi dokumen menggunakan aplikasi yang telah dibuat[7]. Tahap terakhir melibatkan penarikan kesimpulan dan pemberian saran bagi peneliti selanjutnya yang berminat mengembangkan aplikasi tersebut lebih lanjut.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

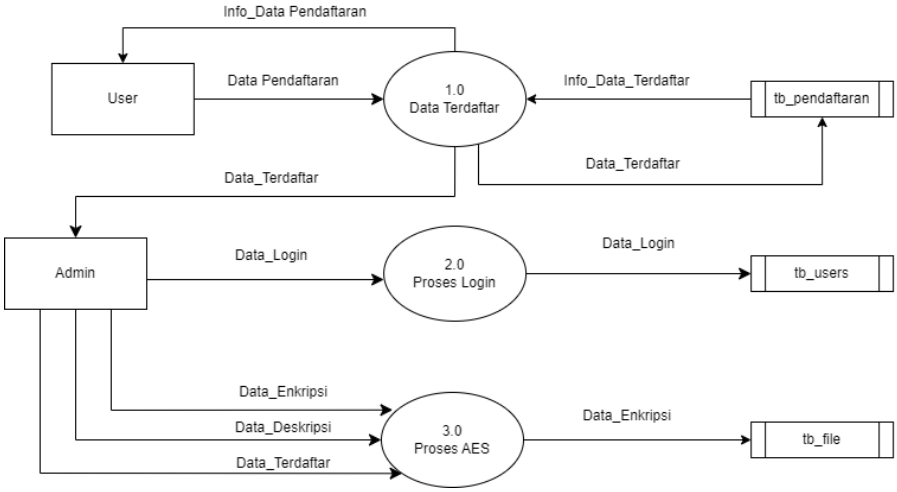
Rancangan Analisa Sistem

Perancangan sistem dibuat untuk memberikan visual atau gambaran bagaimana sistem akan bekerja bila telah tersusun dalam bentuk yang lengkap. Penulis menggunakan perancangan sistem berupa Data Flow Diagram (DFD)[8]. DFD dapat membantu dalam identifikasi dan mengatasi masalah yang ada dalam sistem serta membantu dalam perencanaan sistem yang akan dikembangkan.



Gambar 2 *Context Diagram*

Diagram di atas adalah DFD Level 0 sistem pendaftaran siswa menggunakan metode AES. Diagram ini menggambarkan interaksi antara pengguna (User), sistem pendaftaran (dengan enkripsi AES).



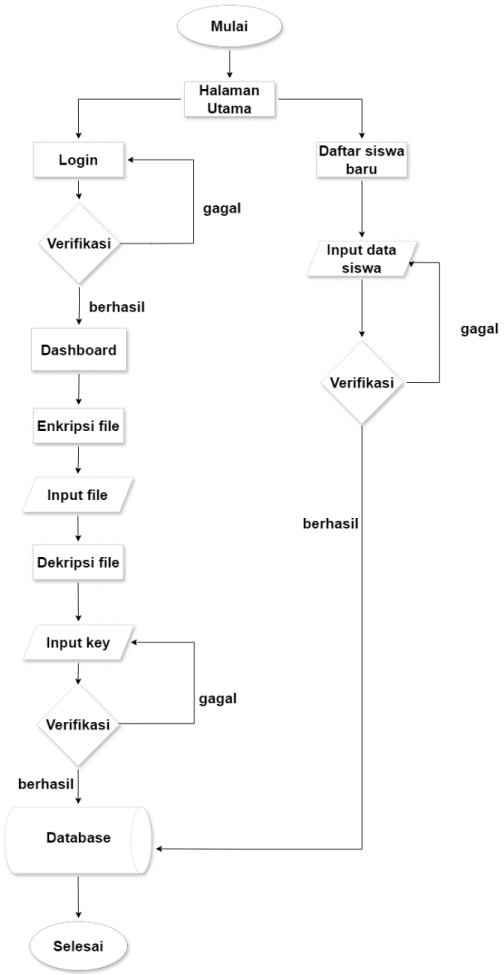
Gambar 3 DFD *Level* 1

Diagram DFD Level 1 menggambarkan rincian proses utama dalam sistem pendaftaran siswa dengan metode AES. Diagram ini terdiri dari tiga proses utama:

a. Data Terdaftar (1.0): Proses ini menerima data pendaftaran dari pengguna (User) dan menyimpan informasi tersebut ke dalam tabel pendaftaran (tb_pendaftaran). Data terdaftar ini kemudian digunakan untuk memberikan informasi pendaftaran kembali kepada pengguna dan admin.
b. Proses Login (2.0): Proses ini menangani login admin, dimana data login dari admin diverifikasi dalam tabel pengguna (tb_users).
c. Proses AES (3.0): Proses ini bertanggung jawab untuk enkripsi dan deskripsi data. Data terdaftar yang diterima dari proses 1.0 dienkripsi menggunakan metode AES dan hasil enkripsinya disimpan dalam tabel file (tb_file). Data yang telah dienkripsi dan didekripsi juga dikirimkan kepada admin sesuai kebutuhan.

Flowchart adalah rangkaian bagan yang menggambarkan urutan suatu proses kegiatan dalam mencapai tujuan yang diinginkan[9]. Berikut adalah *flowchart* dari rancangan sistem yang telah dibuat.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 4. Rancangan Alur Sistem Aplikasi.

HASIL DAN IMPLEMENTASI

Setelah melewati tahap rancangan dari konsep sistem yang telah dibuat, selanjutnya adalah tampilan dari aplikasi yang telah dibuat berdasarkan konsep sistem yang telah dirancang. Adapun detail tampilan aplikasi yang telah dibuat adalah sebagai berikut :

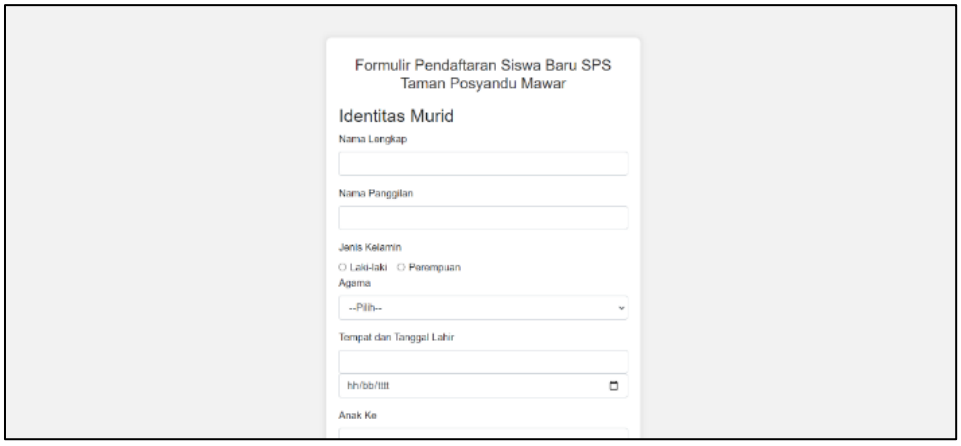
1 Tampilan Halaman Utama

Gambar 5 Tampilan Halaman Utama

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Pada desain halaman utama, terdapat informasi singkat tentang SPS Tapos dan bagaimana cara siswa melakukan pendaftaran di SPS Tapos Mawar Ngancar

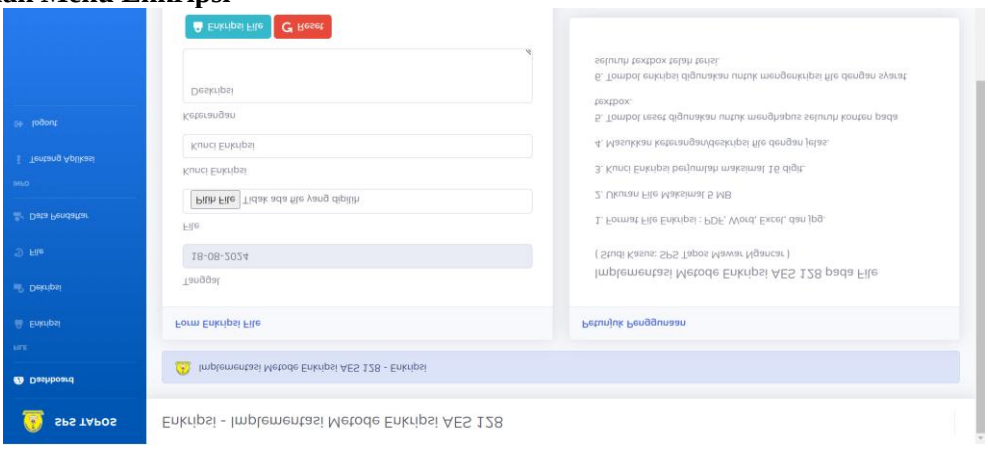
2 Tampilan Halaman Pendaftaran Siswa



Gambar 6 Tampilan Halaman Pendaftaran

Halaman ini digunakan melakukan pendaftaran, wali murid diharuskan mengisi formulir yang telah disediakan dengan benar dan teliti. Pastikan semua data yang dimasukkan sesuai dengan dokumen resmi. Selain itu, wali murid juga perlu menyiapkan foto Kartu Keluarga (KK) yang akan diunggah sebagai salah satu persyaratan pendaftaran. Foto KK ini harus jelas dan dapat terbaca dengan baik.

3 Tampilan Menu Enkripsi

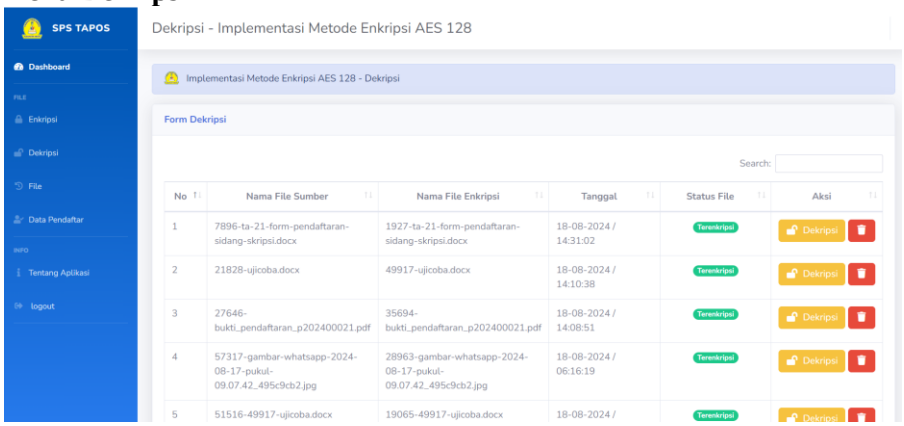


Gambar 7 Tampilan Menu Enkripsi

Pada menu enkripsi kolom "plilih file" digunakan untuk menginput file yang akan dienkripsi. Setelah memilih file, admin akan memasukkan *key* enkripsi yang berfungsi sebagai password untuk mengamankan file tersebut. Di bawah kolom *key*, terdapat menu untuk memberikan keterangan tambahan mengenai file yang diunggah. lalu, ada kolom petunjuk penggunaan yang membantu admin dalam menjalankan proses enkripsi. Untuk file yang dienkripsi tidak hanya formulir data siswa saja, tapi admin juga dapat mengenkripsi file yang memiliki format Word, PDF, Excel, dan JPG.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

4.Tampilan Menu Dekripsi



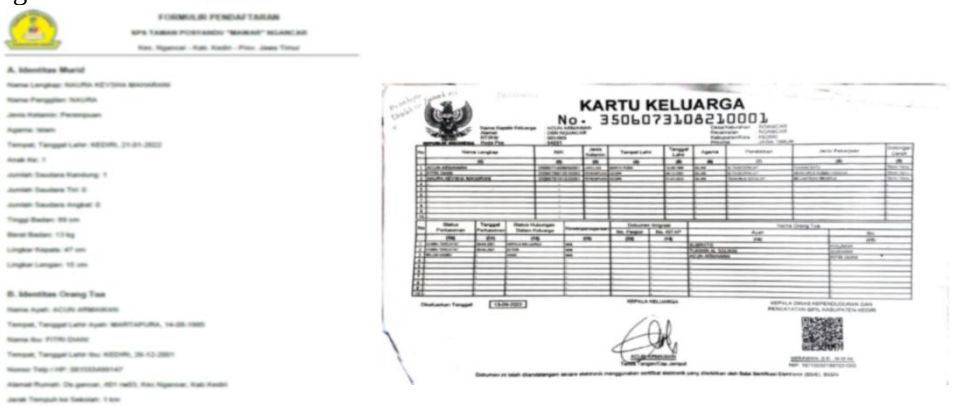
Gambar 8 Tampilan Menu Dekripsi

Pada menu dekripsi terdapat informasi nama file, tanggal, status file dan aksi. Pada kolom aksi ada tombol hapus untuk menghapus file dan tombol dekripsi ketika di klik maka akan masuk halaman proses dekripsi file.

Tampilan Berkas Enkripsi

1.Tampilan berkas sebelum dienkripsi

Gambar berikut adalah formulir pendaftaran dalam bentuk plaintext, yang masih dapat dibaca. Data ini nantinya akan diamankan menggunakan enkripsi AES-128 yang telah diterapkan dalam aplikasi yang dikembangkan.



Gambar 9 Tampilan berkas sebelum dienkripsi

2.Tampilan berkas setelah terenkripsi

Gambar berikut menunjukkan tampilan setelah proses enkripsi. Data formulir pendaftaran yang telah diinputkan akan melalui proses enkripsi untuk mengamankan informasi tersebut. Setelah dienkripsi, data akan berubah menjadi karakter atau simbol acak yang tidak dapat dibaca, atau yang dikenal sebagai ciphertext.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Gambar 10 Tampilan berkas setelah dienkripsi

Pengujian AES

Pada tahapan pengujian sistem bertujuan untuk menguji fungsionalitas sistem yang dibuat untuk melihat apakah sistem yang telah dibuat memenuhi persyaratan kebutuhan[10]. Pengujian terhadap kriptografi *Advanced Encryption Standard* (AES) merupakan langkah krusial untuk memastikan bahwa algoritma ini dapat diandalkan dalam menjaga keamanan data. Proses pengujian ini melibatkan berbagai metode, termasuk pengukuran *Avalanche Effect* untuk mengevaluasi seberapa sensitif perubahan kecil pada plaintext terhadap perubahan pada ciphertext, serta *Character Error Rate* (CER) untuk menilai tingkat kesalahan karakter yang terjadi selama proses enkripsi dan dekripsi. Kedua metode ini digunakan untuk menilai performa AES secara komprehensif, sehingga dapat dipastikan bahwa algoritma ini efektif dalam melindungi data dari ancaman keamanan.

1. Pengujian Avalanche Effect

Dalam pengujian enkripsi, peneliti menggunakan metode *Avalanche Effect* untuk mengevaluasi perubahan dalam ciphertext. Pengukuran dilakukan dengan menghitung "jumlah karakter yang berubah" dalam ciphertext sebagai dampak dari perubahan pada plaintext, serta membandingkannya dengan jumlah total karakter dalam ciphertext[11]. Penggunaan jumlah karakter sebagai satuan pengukur dipilih untuk memberikan gambaran yang lebih mendetail mengenai perubahan yang terjadi dalam ciphertext. Rumus yang digunakan untuk analisis ini adalah:

$$Avalanche\ Effect\ \frac{Jumlah\ Karakter\ Berubah}{Jumlah\ Total\ Karakter}\ x\ 100\%$$

Tabel 1 Pengujian Avalanche Effect

Data	Karakter	Jumlah Karakter Berubah	Jumlah Total Karakter	Avalanche Effect
Word				
Uji coba 1	252.404	252.408	504.812	50%
Uji coba 2	322.543	300.531	601.075	49%
Uji coba 3	322.543	300.531	601.075	49%
PDF				
Uji coba 1	155.048	222.504	377.552	58%
Uji coba 2	240.079	300.061	540.140	55%
Uji coba 3	273.225	263.423	536.648	49%
Excel				
Uji coba 1	4.368	4.368	8.736	50%
Uji coba 2	4.385	4.399	8.784	50%

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Data	Karakter	Jumlah Karakter Berubah	Jumlah Total Karakter	Avalanche Effect
Uji coba 3	4.385	4.399	8.784	50%
JPG				
Uji coba 1	200.351	220.051	420.366	52%
Uji coba 2	220.288	189.864	410.152	46%
Uji coba 3	179.702	210.162	389.864	53%
Rata-rata				50.92%

Hasil uji Avalanche Effect menunjukkan bahwa algoritma enkripsi bekerja efektif dengan rata-rata perubahan 50.92% pada output saat ada perubahan kecil pada input, mendekati ideal 50%. Untuk file Word, PDF, Excel, dan JPG, hasilnya konsisten menunjukkan bahwa enkripsi menghasilkan perubahan signifikan di berbagai format, dengan file PDF menunjukkan variasi tertinggi hingga 58%. Hasil ini mencerminkan keamanan yang kuat, di mana setiap perubahan kecil pada data input menghasilkan perbedaan besar pada output, menegaskan keandalan enkripsi yang diterapkan.

2. Pengujian Character Error Rate

Character Error Rate (CER) adalah metode pengujian yang digunakan untuk mengukur tingkat kesalahan pada karakter setelah proses enkripsi dan dekripsi dalam kriptografi[12]. Untuk menghitung CER, pertama-tama, teks asli dienkripsi menggunakan algoritma yang diuji, seperti AES, kemudian hasil enkripsi tersebut didekripsi kembali untuk mendapatkan teks hasil dekripsi. Setelah itu, perbandingan dilakukan antara teks asli dan teks hasil dekripsi, dengan menghitung jumlah karakter yang berbeda di antara keduanya.$Character\ Error\ Rate\ \frac{Jumlah\ Karakter\ Berbeda}{Jumlah\ Total\ Karakter}\ x\ 100\%$

Tabel 2 Pengujian Character Error Rate

Data	Jumlah Total Karakter	Jumlah Karakter Berbeda	Jumlah Karakter dikirim	CER
Word				
Uji coba 1	252.408	4	252.404	0,001%
Uji coba 2	322.544	1	322.543	0,0003%
Uji coba 3	322.544	1	322.543	0,0003%
PDF				
Uji coba 1	155.048	0	155.048	0%
Uji coba 2	240.087	8	240.079	0,003%
Uji coba 3	273.239	14	273.225	0,005%
Excel				
Uji coba 1	4.368	0	4.368	0%
Uji coba 2	4.392	7	4.385	0,1%
Uji coba 3	4.392	7	4.385	0,1%
JPG				
Uji coba	200.360	9	200.351	0,004%

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Data	Jumlah Total Karakter	Jumlah Karakter Berbeda	Jumlah Karakter dikirim	CER
1				
Uji coba 2	220.300	12	220.288	0,005%
Uji coba 3	179.716	14	179.702	0,007%
Rata-rata				0.0188%

Pengujian *Character Error Rate* (CER) menunjukkan tingkat kesalahan karakter yang sangat rendah, dengan rata-rata 0.0188%. Hasil ini mencerminkan bahwa proses enkripsi dan dekripsi pada berbagai format file, seperti Word, PDF, Excel, dan JPG, berjalan dengan akurasi tinggi. Uji coba pada format *Word* dan PDF menghasilkan CER mendekati 0%, menunjukkan hampir tidak ada perbedaan karakter setelah dekripsi. Meskipun Excel dan JPG menunjukkan CER yang sedikit lebih tinggi, tetap berada dalam kisaran yang sangat rendah, menegaskan keandalan dan efektivitas algoritma enkripsi yang digunakan.

3.Pengujian Black Box testing

Metode pengujian black box testing untuk memastikan bahwa semua fungsi pada sistem web bekerja sesuai dengan spesifikasi yang telah ditentukan. Black box testing menilai fungsionalitas sistem tanpa melihat ke dalam kode sumbernya. Hasil pengujian akan dicatat dan dibandingkan dengan hasil yang diharapkan untuk mengidentifikasi dan memperbaiki kesalahan yang ditemukan adalah sebagai berikut:

Tabel 3 Pengujian Black Box Testing

No	Deskripsi	Hasil Yang Diharapkan	Hasil Pengujian	Keterangan
1	User tidak melengkapi kolom pada formulir pendaftaran	Pendaftaran tidak berhasil	User akan tetap pada halaman pendaftaran	Berhasil
2	Admin tidak mengisi nama dan password	Tidak dapat masuk ke dashboard	Akan tetap pada halaman login	Berhasil
3	Admin salah memasukkan nama dan password	Tidak dapat masuk ke dashboard	Akan tetap pada halaman login	Berhasil
4	Melakukan enkripsi dan dekripsi file sesuai dengan format	Sistem dapat melakukan enkripsi dan dekripsi	Dapat melakakuan sesuai format Word, PDF, Excel, JPG	Berhasil
5	Mengenkripsi file dokumen yang tidak sesuai dengan format yang didukung.	Sistem menolak file dan tidak tersimpan	Sistem akan memberikan pemberitahuan bahwa format tersebut tidak didukung	Berhasil
6	Membuka file yang telah dienkripsi	Sistem dapat memverifikasi key/paassword benar atau salah	Sistem akan memverivikasi jika key/password benar maka file dapat terdekripsi	Berhasil
7	Sistem dapat menyimpan berkas pendaftaran dan berkas yang terenkripsi maupaun terdekripsi	Dapat menyimpan file berkas	Dapat menyimpan berkas pendafataran dan berkas yang terenkripsi maupaun terdekripsi	Berhasil

Jurnal Minfo Polgan
Volume 14, Nomor 1, Juni 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14860
e-ISSN : 2797-3298
p-ISSN : 2089-9424

No	Deskripsi	Hasil Yang Diharapkan	Hasil Pengujian	Keterangan
8	Dapat menghapus file yang tersimpan	Sistem dapat melakukan proses hapus file	Sistem dapat menghapus file yang tersimpan	Berhasil
9	Dapat memberikan informasi waktu kecepatan	Sistem dapat memberikan informasi kecepatan waktu	Sistem dapat memberikan informasi proses waktu kecepatan setelah melakukan enkripsi maupun dekripsi	Berhasil

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, kesimpulan mengenai aplikasi keamanan data siswa berbasis web dengan metode AES adalah Aplikasi berbasis web ini berhasil mengamankan data pendaftaran siswa yang bersifat sensitif. Aplikasi tersebut berfungsi dengan baik dan memenuhi tujuan penelitian. Metode enkripsi AES 128 terbukti efektif dalam melindungi seluruh data yang diproses, termasuk informasi pribadi dan file lainnya. Semua data yang dienkripsi sesuai dengan format yang telah ditentukan, memastikan keamanan dan integritas data. Penelitian yang telah dilakukan, beberapa saran untuk pengembangan sistem di masa mendatang penerapan 2FA dapat meningkatkan keamanan sistem dengan memerlukan kode verifikasi tambahan selain kata sandi, membuatnya lebih sulit diakses oleh pihak yang tidak berwenang. Meningkatkan batas ukuran file yang dapat diunggah serta mengoptimalkan proses pengolahan data akan membuat sistem lebih cepat dan efisien, terutama dalam menangani volume data yang besar. Menambahkan dukungan untuk format file lain selain Word, PDF, Excel, dan JPG akan membuat sistem lebih fleksibel dan memenuhi kebutuhan pengguna yang lebih luas.

DAFTAR PUSTAKA

M. Arief Hasan and D. setiawan, “Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data.”

I. Kurniasari, H. Al Fatta, and Kusrini, “Analisis Sentimen Opini Publik pada Instagram mengenai Covid-19 dengan SVM,” *JTECS J. Sist. Telekomun. Elektron. Sist. Kontrol Power Sist. Komput.*, vol. 1, no. 1, pp. 67–74, 2021.

D. Indra Gunawan Hutasuhut, F. Rozi Lubis, F. Aulia Pratama, H. Ikhsanul Hasan, and H. Aldi Farisi, “UNES Journal of Information System IMPLEMENTASI ALGORITMA KRIPTOGRAFI UNTUK KEAMANAN DATA SISWA PADA SMK TUNAS KARYA BATANG KUIS BERBASIS WEB IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS FOR STUDENT DATA SECURITY AT TUNAS KARYA VOCATIONAL SCHOOL BATANG KUIS,” vol. 8, no. 1, pp. 20–27, 2023, [Online]. Available: https://fe.ekasakti.org/index.php/UJIS

M. A. Sutejo and M. Hardjianto, “Pengamanan File Pendaftaran Siswa Baru Menggunakan Metode Algoritme Rc4 Di Tk Nurul Irfan Security of New Student Registration Files Using the Rc4 Algorithm Method in Tk Nurul Irfan,” *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, vol. 4, no. September, pp. 394–401, 2022.

M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, “Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES),” *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

T. M. Mudo, Ferdiansyah, and I. Susanti, “Penerapan Kriptografi Menggunakan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan Data Pengiriman Customer Agen JNE Andara,” *Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 2, no. 2, pp. 214–224, 2023, [Online].

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Available: https://senafti.budiluhur.ac.id/index.php/senafti/index%7C

R. N. Sarbini, D. N. Afiyah, and S. Supriyono, "Pelatihan Pemasaran Online Pakan Unggas Berbahan Dasar Jerami Bawang Merah di Desa Campur Kecamatan Gondang Kabupaten Nganjuk," *J. ABDINUS J. Pengabdi. Nusant.*, vol. 4, no. 1, pp. 75–82, 2020, doi: 10.29407/ja.v4i1.14617.

J. Informatika and S. Informasi, "INFORMASI (Jurnal Informatika dan Sistem Informasi) Volume 14 No.1 / Mei / 2022," vol. 14, no. 1, pp. 1–17, 2022.

W. Pramusinto, N. Wizaksono, and A. Saputro, "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman," *J. BIT (Budi Luhur Inf. Technol.*, vol. 16, no. 2, pp. 47–53, 2019.

H. Mukminna and D. A. W. Kusumastutie, "Geographic Information Systems for Road Damage Complaints Based on Mobile," *JTECS J. Sist. Telekomun. Elektron. Sist. Kontrol Power Sist. dan Komput.*, vol. 2, no. 1, p. 55, 2022, doi: 10.32503/jtecs.v2i1.2213.

Muslih Muslih and Lekso Budi Handoko, "Pengujian Avalanche Effect Pada Kriptografi Teks Menggunakan Autokey Cipher," *Semin. Nas. Teknol. dan Multidisiplin Ilmu*, vol. 2, no. 1, pp. 127–134, 2022, doi: 10.51903/semnastekmu.v2i1.162.

N. A. Karima, A. N. Aisyah, H. V. Silla, L. B. Handoko, and R. R. Sani, "Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit," *J. Masy. Inform.*, vol. 15, no. 1, pp. 1–13, 2024, doi: 10.14710/jmasif.15.1.60836.