ENKRIPSI REPOSITORI IIB DARMAJAYA DENGAN ADVANCED ENCRYPTION STANDARD (AES)

Nadia Permatasari, Rionaldi Ali
Teknik Informatika, Institut Informatika Dan Bisnis Darmajaya
Jl. ZA. Pagar Alam No.93, Rajabasa, Indonesia
nadiaapermatasari21@gmail.com

ABSTRAK

Perkembangan teknologi digital telah mendorong penerapan sistem repositori di institusi pendidikan tinggi untuk mengelola dokumen akademik. Namun, repositori publikasi digital IIB Darmajaya saat ini masih menyimpan dokumen dalam format teks biasa tanpa perlindungan enkripsi. Kondisi ini memunculkan permasalahan kerentanan terhadap risiko akses tidak sah, pencurian data, dan serangan *cyber* jika terjadi pembobolan sistem. Oleh karena itu, penelitian ini bertujuan untuk meningkatkan keamanan dan kerahasiaan data pada sistem repositori Darmajaya. Metode pengembangan sistem yang digunakan dalam penelitian ini adalah model *Waterfall*. Pengamanan data diimplementasikan menggunakan metode kriptografi algoritma *Advanced Encryption Standard* (AES). Proses enkripsi dilakukan secara otomatis saat dokumen diunggah, sedangkan dekripsi dilakukan saat dokumen diunduh melalui antarmuka web terpusat. Hasil pengujian menunjukkan bahwa sistem berhasil mengamankan dokumen dengan baik. Berkas tersimpan diubah menjadi teks sandi (*ciphertext*) dengan ekstensi .bin sehingga dokumen asli tidak dapat dibaca tanpa kunci dekripsi yang tepat. Pengujian *Wireshark* juga membuktikan transmisi data aman. Kesimpulannya, penerapan algoritma AES efektif melindungi dokumen repositori dari ancaman pencurian data.

Kata kunci : *Repositori Digital Publikasi Darmajaya, Enkripsi AES.*

1. PENDAHULUAN

Perkembangan teknologi digital telah berdampak besar pada banyak hal, termasuk manajemen informasi di institusi pendidikan tinggi. Perkembangan ini mencakup penerapan sistem repositori digital yang memungkinkan penyimpanan, pengelolaan, dan penyebaran dokumen akademik seperti skripsi, tesis, dan laporan ilmiah. Meskipun repositori digital memudahkan pengguna untuk mengakses data, hal ini juga menghadirkan tantangan baru, terutama dalam hal keamanan data.

Penyimpanan berkas dalam bentuk aslinya tanpa perlindungan keamanan tambahan adalah masalah umum dalam sistem repositori. Kondisi ini memungkinkan orang yang tidak berwenang untuk mengakses berkas secara langsung jika terjadi pelanggaran sistem. Serangan *cyber* seperti peretasan dan pencurian data dapat mengancam keamanan informasi dan merusak reputasi institusi. Dalam beberapa situasi, situs web institusi yang tidak memiliki keamanan yang cukup sering menjadi sasaran serangan *cyber*. Jika sistem diretas, penyerang dapat mengakses semua data, termasuk dokumen penting dan informasi pengguna. Penyalahgunaan sistem seperti mengubah konten web tanpa izin juga dapat terjadi, yang menegaskan bahwa keamanan sistem repositori adalah hal yang sangat vital.

Untuk mengatasi masalah ini, diperlukan sistem perlindungan data yang dapat mengamankan informasi dalam file, bahkan dalam kasus di mana pihak yang tidak berwenang berhasil mendapatkan akses ke media penyimpanan. Salah satu solusi yang dapat digunakan adalah metode kriptografi, khususnya algoritma *Advanced Encryption Standard* (AES). AES adalah algoritma kriptografi simetris berbasis *cipher blok* yang digunakan untuk mengamankan data dengan mengubah teks biasa (*plaintext*) menjadi teks tersandi (*ciphertext*).

Penerapan AES dalam sistem repositori akan dilakukan selama proses penyimpanan dan pengambilan data. Metode ini mengenkripsi berkas sehingga tidak dapat diakses tanpa otoritas (kunci) yang sesuai. Selain itu, sistem repositori memiliki akses terpusat melalui situs web resmi yang memastikan bahwa setiap aktivitas pengunduhan file harus melewati proses otentikasi dan kontrol akses yang telah ditetapkan sebelumnya.

Melalui penggabungan perlindungan enkripsi data dan kontrol akses terpusat ini, sistem dapat memberikan tingkat keamanan yang jauh lebih tinggi bagi dokumen akademik. Oleh karena itu, penelitian ini bertujuan untuk meningkatkan keamanan dan kerahasiaan data dengan menerapkan algoritma AES pada sistem repositori Darmajaya.

2. TINJAUAN PUSTAKA

Pada studi sebelumnya yang mendukung penelitian tentang penggunaan algoritma Advanced Encryption Standard (AES) untuk mengamankan sistem repositori digital dibahas dalam bagian ini.

2.1. Kriptografi

Kriptografi adalah bidang yang menyelidiki cara-cara untuk melindungi kerahasiaan data dengan mengubah data menjadi cara yang tidak dapat dipahami oleh orang yang tidak berwenang. Istilah kriptografi berasal dari kata yunani "*cryptos*" yang berarti "rahasia", dan "*graphein*" yang berarti

"menulis". Dengan berkembangnya kriptografi tidak hanya digunakan untuk menjaga kerahasiaan data tetapi juga untuk memperkuat elemen keamanan lainnya seperti integritas, otoritas, dan non-repudasi.

Jenis kriptografi modern yang paling umum adalah simetris dan asimetris. Dalam kriptografi simetris, enkripsi dan dekripsi dilakukan dengan kunci yang sama, sedangkan dalam kriptografi asimetris digunakan sepasang kunci yang berbeda. [1]

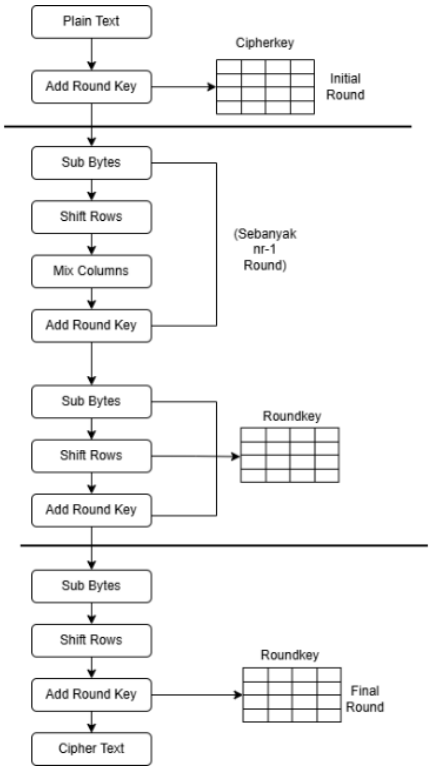
2.2. Advanced Encryption Standard

Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris yang dikembangkan oleh National Institut of Standard (NIST) sebagai pengganti Data Encryption Standard (DES). AES mendukung panjang kunci 128 bit, 192 bit, dan 256 bit. Menggunakan metode cipher blok dengan ukuran tetap sebesar 128 bit.[2]

Tabel 1. Putaran Kunci AES

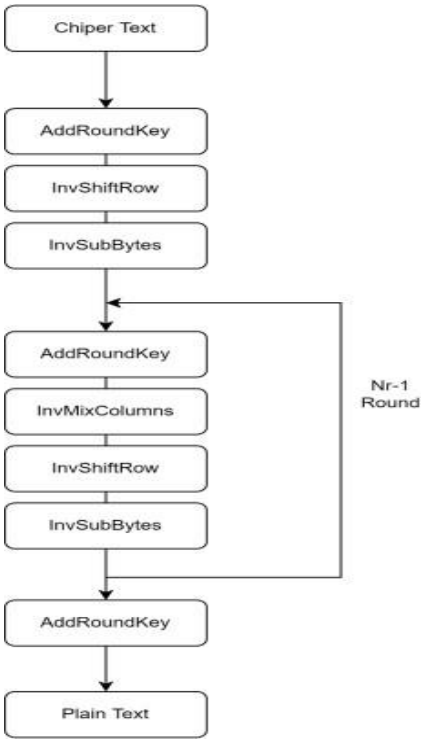
AES (Bits)	Panjang Kunci (Nk Words)	Ukuran Blok (Nb Words)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES256	8	4	14

AES menggunakan beberapa tahapan transformasi dalam proses enkripsi, seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey[3]. Tahap transformasi ini diulang sesuai dengan panjang kunci, dengan jumlah putaran 14 untuk AES-256.



Gambar 1. Proses Enkripsi AES

Proses dekripsi dilakukan dengan membalikkan tahap transformasi ini menggunakan operasi invers.



Gambar 2. Proses Dekripsi AES

AES banyak digunakan dalam berbagai sistem keamanan data, termasuk aplikasi berbasis web dan penyimpanan digital, karena sangat aman dan efisien.

2.3. Sistem Repositori Digital

Sistem yang menyimpan, mengawasi, dan memberikan akses terpusat ke dokumen digital dikenal sebagai repositori digital. Repositori umumnya digunakan di institusi pendidikan tinggi untuk menyimpan karya akademik seperti skripsi, tesis dan laporan penelitian.[4]

Namun, sistem repositori menghadapi ancaman keamanan, terutama jika file tidak dienkripsi. File yang disimpan dalam bentuk asli dapat dengan mudah diakses juka terjadi pelanggaran sistem. Untuk melindungi data yang disimpan di dalam repositori, mekanisme keamanan tambahan diperlukan.

2.4. Pengamanan Data

Data biasanya termasuk dalam dua kategori utama yaitu data rahasia dan data non-rahasia. Data non-rahasia biasanya memiliki resiko yang rendah jika diakses oleh orang lain, sementara data rahasia memiliki nilai yang tinggi karena mengandung informasi penting yang harus dilindungi dari akses yang tidak sah.

Data non rahasia lebih rentan terhadap penyalahgunaan karena sifat data digital yang dapat disalin dan didistribukan dengan mudah. Oleh karena itu, orang yang tidak bertanggung jawab sering melakukan berbagai upaya untuk mendapatkan data

tersebut, termasuk metode ilegal seperti peretasan sistem dan interpretasi data. Hal ini menunjukkan bahwa melindungi data pribadi sangat penting untuk menjaga keamanan data, terutama pada sistem yang mengelola banyak data seperti repositori digital.[5]

2.5. Web Mobile

Aplikasi web adalah sistem yang dibuat menggunakan bahasa pemrograman seperti PHP, HTML, dan JavaScript, yang berjalan di sisi klien dan didukung oleh basis dara seperti MySQL. Aplikasi web dapat menampilkan informasi dalam berbagai format multimedia, seperti teks, gambar, audio, dan animasi, disimpan di server dan dapat diakses melalui protokol hypertext.[6]

2.6. Laragon

Laragon adalah program sumber terbuka yang mendukung berbagai sistem operasi dan menawarkan lingkungan pengembangan untuk pemrograman PHP, MySQL, sebagai sistem penyimpanan basis data dan Apache sebagai server web.[7]

2.7. Laravel

Laravel adalah kerangka kerja PHP yang dirilis dibawah lisensi MIT dan dibangun berdasarkan konsep Model-View-Controller (MVC). Tujuan laravel adalah untuk meningkatkan kualitas perangkat lunak dengan mengurangi biaya pengembangan dan pemeliharaan awal serta meningkatkan pengalaman pengembangan melalui sintaks yang ekspresif, jelas, dan efisien waktu.[8]

2.8. Wireshark

Wireshark adalah perangkat lunak analisis jaringan yang digunakan untuk menangkap dan memantau paket data yang dikirimkan secara *real-time* melalui jaringan. Dengan keamanan website untuk mengetahui apakah data pengiriman masih menunjukkan isi dokumen asli atau telah dienkripsi.[9]

2.9. Penelitian Terdahulu

Penelitian sebelumnya tentang masalah ini menunjukkan bahwa algoritma AES secara efektif meningkatkan keamanan data. Penelitian ini dilakukan oleh Muhammad Edwin Fijratulloh dan Rahmalia Syahputri, menunjukkan bahwa algoritma AES dapat mengubah file menjadi teks sandi dalam sistem repositori digital, sehingga file tidak dapat dibaca tanpa kunci yang tepat dan meningkatkan perlindungan terhadap akses yang tidak sah. [10]

Menurut Risma Arifa, Husaini Husaini, dan Fachri Yannuar Rudi, menunjukkan bahwa menggunakan AES dalam sistem berbasis web secara efektif menjadi kerahasiaan dokumen [11]. penelitian oleh Mohammad Fajar, Audri Billy Kambidji, dan Izmy Alwiah Musdar, Juga menunjukkan bahwa algoritma AES bekerja dengan baik dan memiliki tingkat keamanan yang tinggi untuk melindungi data pengguna [12].

Berdasarkan studi tersebut, dapat disimpulkan bahwa algoritma AES adalah cara terbaik untuk meningkatkan keamanan data dalam sistem repositori digital.

3. METODE PENELITIAN

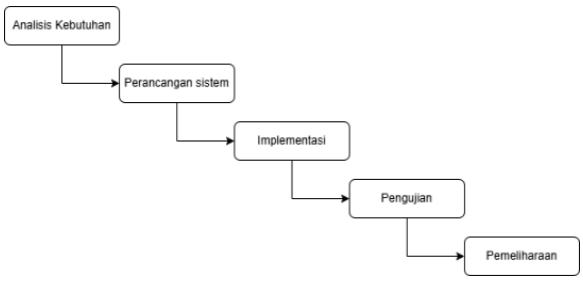
3.1. Metode Pengumpulan Data

Data dikumpulkan untuk mengetahui kebutuhan sistem dan masalah keamanan repositori. Teknik yang digunakan termasuk :

a. Observasi
   Dilakukan dengan melihat secara langsung proses pengunggahan dan pengunduhan file di repositori IIB Darmajaya. Ini dilakukan untuk menemukan kemungkinan resiko keamanan yang mungkin terjadi terutama ketika file dalam bentuk teks biasa disimpan.
b. Studi Pustaka
   Dilakukan dengan meninjau buku atau jurnal akademik tentang kriptografi, algoritma AES dan sistem keamanan data untuk mendukung perancangan sistem.

3.2. Metode Pengembangan Sistem

Pengembangan sistem menggunakan metode waterfall yang dilakukan secara bertahap dan sistematis sebagai berikut :[13]



Gambar 3. Metode Waterfall

3.3. Analisis Kebutuhan

Tahapan analisis kebutuhan dilakukan untuk menemukan masalah dan kebutuhan sistem. Pengamatan di repositori IIB Darmajaya menunjukkan bahwa sistem masih menyimpan dokumen format text biasa tanpa enkripsi, yang meningkatkan kemungkinan data bocor.

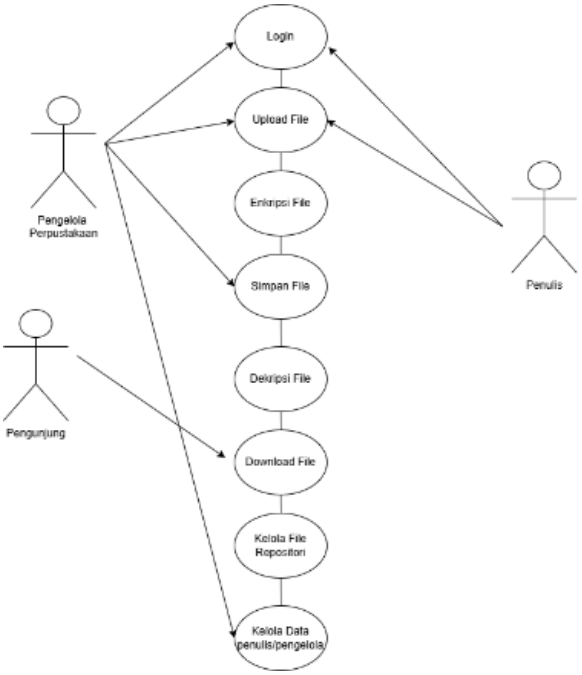
Terdapat dua jenis kebutuhan yaitu fungsional dan non fungsional. Fungsional mencangkup dalam hal keamanan, kemudahan dan kompatibilitas sistem dengan berbagai perangkat. Sementara itu, non-fungsional mencangkup kemampuan sistem untuk melakukan enkripsi file selama proses unggah dan dekripsi selama proses unduh.

3.4. Pernacangan Program

Pada tahap implementasi, tahap perancangan program dilakukan untuk menggambarkan alur kerja sistem. Pada tahap imi, arsitektur sistem, struktur basis data, dan antarmuka pengguna dirancang.[14]

3.5. Use Case Diagram

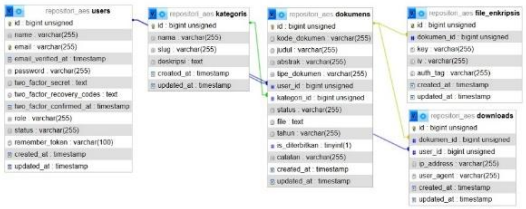
Interaksi antara sistem repositori dan pengguna digambarkan dalam digram[15]. Admin, penulis dan pengunjung adalah tiga aktor utama dalam sistem ini.



Gambar 4. Use Case Diagram

3.6. Class Diagram

Sistem repositori ini memiliki beberapa class utama, termasuk pengguna, dokumen, kategori, dan riwayat unduhan. Diagram class menunjukkan struktur sistem hubungan antar entitas dalam basis data [16].



Gambar 5. Class Diagram

3.7. Implementasi Algoritma AES

Advanced Encryption Standard (AES) digunakan dalam mode CTR, enkripsi *plaintext* menjadi *ciphertext* dengan menggunakan operasi XOR antara data dan *keystream* yang dibuat oleh fungsi AES.

$$C_i = P_i \oplus AES_{K(CTR_i)}$$

Sedangkan proses dekripsi menggunakan operasi sama, karena AES merupakan algoritma kriptografi simetris :

$$P_i = C_i \oplus AES_{K(CTR_i)}$$

Proses berikut digunakan untuk menerapkan ini :

a. Upload file : file dienkripsi sebelum disimpan di server.
b. Unduh file : file didekripsi sebelum dikirimkan kepada pengguna.

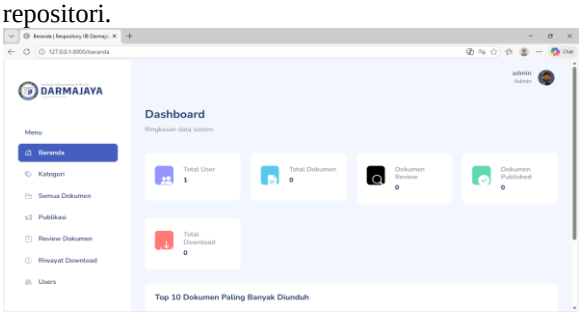
Metode ini memastikan bahwa file yang disimpan dalam bentuk sistem tetap dalam bentuk terenkripsi sehingga tidak dapat diakses tanpa kunci yang sesuai.

4. HASIL DAN PEMBAHASAN

Pada penelitian ini, penulis berhasil mengembangkan website repositori IIB Darmajaya.

4.1. Hasil Dashboard Admin

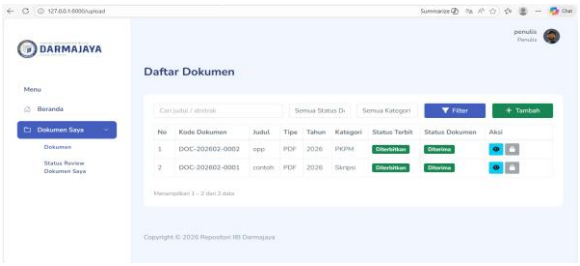
Halaman dashboard admin website repositori IIB Darmajaya. Halaman ini berfungsi sebagai halaman utama yang menampilkan ringkasan aktivitas sistem repositori.



Gambar 6. Dashboard Admin

4.2. Hasil Dashboard Penulis

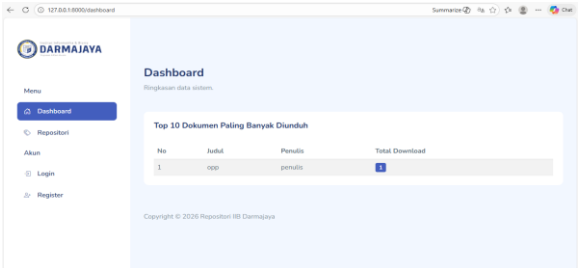
Dashboard penulis menampilkan informasi tentang proses pengunggahan dokumen penulis, seperti jumlah dokumen yang diunggah, status dokumen, dan jumlah yang sudah diterbitkan.



Gambar 7. Dashboard Penulis

4.3. Hasil Dashboard Pengunjung

Dashboard pengunjung menampilkan informasi umum tentang dokumen yang tersedia di sistem repositori. Ini termasuk daftar dokumen yang diterbitkan, dokumen yang paling sering diunduh, dan fitur pencarian yang memungkinkan pengguna dengan mudah menemukan dokumen.

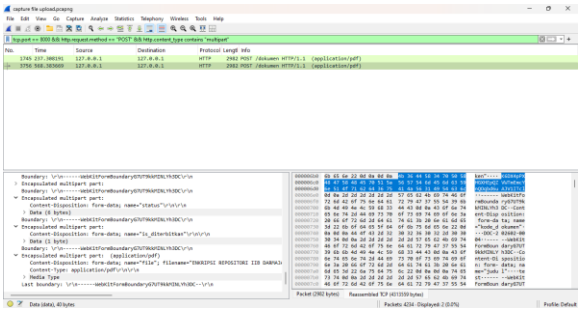


Gambar 8. Dashboard Pengunjung

4.4. Hasil Pengujian Wireshark

Selama proses pengunggahan file, pengujian keamanan dengan wireshark dilakukan untuk memeriksa file yang dikirimkan. Hasil pengujian menunjukkan bahwa data/file yang ditangkap tidak mengandung isi dokumen asli, tetapi dalam bentuk terenkripsi.

Hal ini menunjujjan bahwa enkripsi tidak hanya melindungi data yang disimpan tetapi juga melindungi selama proses transmisi data.



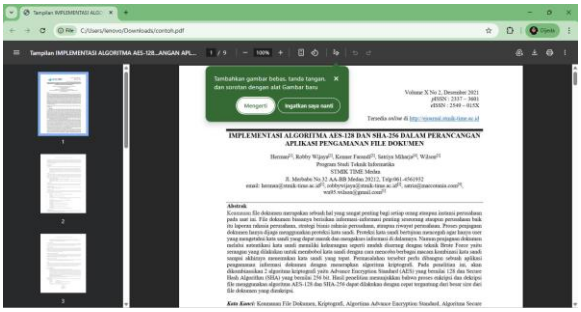
Gambar 9. Wireshark

4.5. Hasil Proses Enkripsi dan Dekripsi

Hasil uji coba menunjukkan nahwa enkripsi AES berhasil mengubah file menjadi bentuk yang tidak dapat dikenali. Jika file disimpan, mereka memiliki nama acak dan ekstensi *.bin*, sehingga tidak dapat membuka tanpa proses dekripsi.

Gambar 10. Hasil Proses Enkripsi

Sementara itu, proses dekripsi berhasil mengembalikan file ke bentuk aslinya tanpa merubah konten atau menyebabkan kerusakan data, menunjukkan bahwa algoritma AES yang digunakan sangat akurat dalam menjaga integritas data.



Gambar 11. Hasil Proses Dekripsi

4.6. Hasil Pengujian Website

Untuk memastikan bahwa semua fitur website berfungsi sesuai dengan persyaratan, pengujian fungsional dilakukan. Hasil pengujian menunjukkan hal berikut:

Tabel 2. Hasil Pengujian Website

No	Item Uji	Berhasil	Gagal
1	Halaman Login	✓	-
2	Halaman Register	✓	-
3	Halaman Dashboard (admin)	✓	-
4	Halaman Kategori (admin)	✓	-
5	Halaman Semua Dokumen (admin)	✓	-
6	Halaman Publikasi (admin)	✓	-
7	Halaman Review (admin)	✓	-
8	Halaman Download (admin)	✓	-
9	Halaman Dashboard (penulis)	✓	-
10	Halaman Dokumen (penulis)	✓	-
11	Halaman Status Review Dokumen (penulis)	✓	-
12	Halaman Dashboard (pengunjung)	✓	-
13	Halaman Repositori (pengunjung)	✓	-
14	Halaman User	✓	-
15	Halaman Profil	✓	-

5. KESIMPULAN DAN SARAN

Berdasarkan dari hasil dan pembahasan, maka dapat menyimpiulkan bahwa untuk meningkatkan keamanan data, penelitian ini berhasil menggunakan algoritma Advanced Encryption Standard (AES) dalam website Repositori IIB Darmajaya. Hasil pengujian menunjukkan bahwa berkas yang disimpan berada dalam bentuk teks terenkripsi dan tidak dapat diakses secara langsung, sementara data yang dikirim tidak mengungkap dokumen asli, menunjukkan keefektifan sistem data. Selain itu, penggabungan enkripsi data dengan kontrol akses pusat meningkatkan keamanan dengan membatasi akses ke file hanya melalui situs web resmi. Peningkatan keamanan yang diperoleh jauh lebih besar daripada penurunan kinerja untuk file berukuran besar. Oleh karena itu, penelitian lebih lanjut disarankan untuk mengembangkan teknik manajemen kunci dan enkripsi *hybrid* yang lebih baik untuk meningkatkan efisiensi sistem dan keamanan secara keseluruhan.

DAFTAR PUSTAKA

[1] A. S. Aswandi, M. Nurtanzis Sutoyo, and A. Pradipta, "ANALISIS PERFORMA DAN KEAMANAN IMPLEMENTASI KRIPTOGRAFI AES UNTUK PENYANDIAN DOKUMEN BERBASIS WEB," 2025.

[2] W. Putra *et al.*, "Implementasi Algoritma Advanced Encryption Standard Untuk Kemanan Dokumen," *Teknologi Dan Informasi V*, vol. 1, no. 2, pp. 76–83, 2023, [Online]. Available: https://journal.grahamitra.id/index.php/jurikti

[3] N. E. Muhammad Irvai, "OPTIMALISASIENKRIPSI FILE MENGGUNAKAN ALGORITMA AES-256BERBASIS WEBDENGAN INTEGRASI

KOMPRESI ADAPTIF," *jurnal ilmiah betrik*, vol. 15, no. 13, 2024.

[4] H. R. Wasilah, "Pengembangan Aplikasi Unggah Mandiri Repositori Karya Ilmiah Perpustakaan," *JUPITER*, vol. 13, no. 02, pp. 7–14, 2021.

[5] D. Nurnaningsih and A. A. Permana, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," *JURNAL TEKNIK INFORMATIKA*, vol. 11, no. 2, pp. 177–186, Nov. 2018, doi: 10.15408/jti.v11i2.7811.

[6] A. Jati, M. Fauzan Azima, and S. N. Laila, "Impelmentasi Restful Api Untuk Seleksi Asisten Laboratorium Berbasis Web Mobile(Studi Kasus : Laboratorium Insti tut Informatika Dan Bisnis Darmajaya)," 2024. [Online]. Available: https://journal.darmajaya.ac.id/index.php/AI2M Tech

[7] A. Tahari, T. Umi Kalsum, and J. Fredricka, "Create An E-Raport Application Using The Laravel Framework And Mysql," *Jurnal Media Computer Science*, vol. 4, no. 2, pp. 373–384, 2025, doi: 10.37676/jmcs.v4i2.

[8] A. Aziz, "RANCANG BANGUN APLIKASI SISTEM INFORMASI PEMINJAMAN RUANGAN BERBASIS WEB MENGGUNAKAN LARAVEL FRAMEWORK: STUDI KASUS DI PESANTREN DARUL QURAN MULIA," 2023.

[9] I. Made, R. B. Suputra, I. Kadek, A. Asmarajaya, K. Noppi, and A. Jaya, "Analisis Perbandingan Keamanan Data pada Website Repository UNHI dan Website SRUTI UNHI Terhadap Sniffing Process Menggunakan Aplikasi Wireshark," Jan. 2025.

[10] M. E. Firjatulloh and R. Syahputri, "PTES-Based Security System for Personal Data Protection of Rural Area Websites," *International Journal of Technology, Law, and Economic Management Systems*, vol. 1, no. 1, pp. 1–14, 2025, doi: 10.22437/ijstphas.vxix.xxx.

[11] R. Arifa, F. F. Yannuar Rudi, and J. B. Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe Jln, "JAISE : Journal of Artificial Intelligence and Software Engineering Implementasi Aplikasi Enkripsi Dekripsi File Dokumen Menggunakan Algoritma Aes Pada Cloud Computing (Studi Kasus Prodi Teknologi Rekayasa Komputer Jaringan)."

[12] M. Fajar, A. Billy Kambodji, I. Alwiah Musdar, and J. Algoritma STMIK Kharisma Makassar Jl Baji, "Implementasi Algoritma Advanced Encryption Standard untuk Pengamanan Data Pengguna Aplikasi Media Sosial VirCle." [Online]. Available: https://jurnal.itg.ac.id/

[13] Z. J. T. P. B. M. G. R. F. A. Ratnasari, "Penerapan Model Waterfall Pada Pengembangan Aplikasi Pengajuan Bantuan Sosial Berbasis Web," *Jurnal Informatika*, vol. Vol. 11, pp. 34–45, 2022.

[14] A. Sapaatullah and M. Darip, "Pengamanan Dokumen Digital Berbasis Web dengan Algoritma AES-128 di Lembaga Pendidikan TK."

[15] S. Adrianto, B. Agus Herlambang, and R. Renaldy, "Optimizing Customer Data Security in Water Meter Data Management Based on RESTful API and Data Encryption Using AES-256 Algorithm," 2025. [Online]. Available: http://jurnal.polibatam.ac.id/index.php/JAIC

[16] Siska Narulita, Ahmad Nugroho, and M. Zakki Abdillah, "Diagram Unified Modelling Language (UML) untuk Perancangan Sistem Informasi Manajemen Penelitian dan Pengabdian Masyarakat (SIMLITABMAS)," *Bridge : Jurnal publikasi Sistem Informasi dan Telekomunikasi*, vol. 2, no. 3, pp. 244–256, Aug. 2024, doi: 10.62951/bridge.v2i3.174.