Volume 7 Nomor 1 Edisi Agustus 2025
E-ISSN: **2714-8599**

PENGEMBANGAN APLIKASI KEAMANAN FILE DIGITAL INTERNAL BERBASIS ENKRIPSI AES

(Design and Development of an Internal Digital File Security Application Using AES Encryption)

I Putu Fredika Putra
Afiliasi
Email korespondensi: 2232061.putu@uib.ac.id

Abstrak

Kegiatan Pengabdian kepada Masyarakat (PkM) ini dilatarbelakangi oleh kebutuhan mitra dalam mengamankan dokumen digital internal secara efektif dan efisien. Permasalahan utama adalah sistem pengelolaan file yang belum terenkripsi, sehingga berisiko terhadap kebocoran data. Kegiatan ini bertujuan merancang dan mengimplementasikan aplikasi DanusCrypt, sebuah sistem enkripsi file berbasis AES, yang dapat diakses secara internal melalui jaringan lokal perusahaan. Metode yang digunakan adalah simulasi ipteks dan pelatihan teknis langsung kepada mitra. Hasil implementasi menunjukkan bahwa sistem dapat dioperasikan dengan baik, mendukung keamanan data internal, serta mudah digunakan oleh staf non-teknis. Evaluasi menunjukkan bahwa tujuan kegiatan tercapai dan sistem diterima dengan baik oleh mitra. Dokumentasi teknis juga disusun sebagai panduan penggunaan dan pengelolaan lanjutan.

Kata Kunci: *keamanan berkas, enkripsi AES, sistem internal, DanusCrypt, perlindungan dokumen digital*

Abstract

This community service (PkM) activity was motivated by the partner's need to secure internal digital documents effectively and efficiently. The main problem was the lack of encryption in the file management system, creating a data leakage risk. This program aimed to design and implement DanusCrypt, a file encryption system using AES, accessible through the company's local network. The method applied was a technology simulation and technical training for the partner. Implementation results showed that the system operates reliably, supports internal data protection, and is user-friendly for non-technical staff. Evaluation indicates that the objectives were met and the system was well received by the partner. A technical manual was also prepared to guide future use and system maintenance.

Keywords: *file security, AES encryption, internal system, DanusCrypt, digital document protection*

Pendahuluan

Perkembangan teknologi informasi mendorong institusi untuk menjaga integritas dan keamanan data secara lebih serius. Di tengah kebutuhan akan efisiensi dan kerahasiaan informasi, banyak perusahaan belum memiliki sistem perlindungan data yang memadai. Hal ini membuka potensi risiko seperti akses tidak sah, manipulasi data, hingga kebocoran informasi (Liu & Xiaoyan, 2022). Salah satu upaya yang dapat dilakukan adalah penerapan sistem enkripsi internal yang mendukung perlindungan file digital secara otomatis dan sistematis (Gao, 2025).

Berbagai pendekatan telah digunakan dalam melindungi data digital, seperti penggunaan antivirus, pengamanan jaringan, hingga kontrol akses berbasis pengguna. Namun, pendekatan ini belum cukup apabila tidak disertai dengan enkripsi file yang tersimpan di dalam sistem. Tujuan kegiatan ini adalah untuk mendesain, mengembangkan, dan mengimplementasikan aplikasi DanusCrypt sebagai solusi perlindungan file digital internal yang ringan dan mudah digunakan.

Masalah

Permasalahan yang dihadapi oleh PT BPR Dana Nusantara adalah belum tersedianya sistem khusus yang mampu mengamankan file internal perusahaan secara efektif. Pengelolaan file yang masih dilakukan secara manual atau melalui sistem tanpa enkripsi yang memadai menimbulkan risiko tinggi terhadap kebocoran dan penyalahgunaan data (Liu & Xiaoyan, 2022; Sola-Thomas & Imtiaz, 2025). Selain itu, absennya sistem pemantauan aktivitas file menyebabkan lemahnya kontrol terhadap siapa saja yang mengakses, mengubah, atau mengunduh dokumen penting. Tidak adanya audit trail atau log aktivitas file juga membuat proses pelacakan jika terjadi insiden keamanan menjadi sulit (Gao, 2025). Kebutuhan akan sistem yang user-friendly namun tetap aman menjadi semakin mendesak seiring meningkatnya volume dan sensitivitas dokumen digital (Kaur & Singh, 2023).

Metode

Metode yang digunakan dalam pengembangan DanusCrypt adalah pendekatan Waterfall, yang terdiri dari lima tahapan utama: analisis kebutuhan, perancangan, implementasi, pengujian, dan evaluasi. Tahap pertama adalah analisis kebutuhan yang dilakukan dengan observasi dan diskusi bersama staf TI perusahaan untuk mengidentifikasi permasalahan utama dan kebutuhan sistem pengamanan dokumen. Tahap perancangan melibatkan desain antarmuka pengguna, struktur database, serta logika enkripsi-dekripsi file menggunakan algoritma AES-256 yang terbukti andal dan cepat dalam berbagai penelitian (Alam et al., 2021; Fatima, Rehman, & Iqbal, 2022).

Tahap implementasi menggunakan Laravel untuk backend serta HTML, CSS, dan JavaScript untuk frontend. Fitur yang dikembangkan meliputi autentikasi pengguna, unggah dan unduh file, proses enkripsi-dekripsi, serta pencatatan aktivitas pengguna (Choudhury & Kumar, 2023). Sistem diuji secara internal dengan skenario penggunaan umum dan simulasi terhadap data sensitif guna menilai performa, keamanan, dan stabilitas. Evaluasi melibatkan pengguna internal dan menghasilkan sejumlah umpan balik positif yang menunjukkan penerimaan sistem secara luas.

Pembahasan

Implementasi aplikasi DanusCrypt dilaksanakan sesuai dengan rencana kerja proyek yang telah ditetapkan, yang berlangsung dari tanggal 3 Februari 2025 hingga 6 Juni 2025. Proses pengembangan dilakukan oleh satu orang pengembang utama dengan pendampingan teknis dari mentor perusahaan, serta diskusi berkala dengan staf divisi TI yang berjumlah satu orang. Pengujian dilakukan pada jaringan internal perusahaan untuk menjamin keamanan dan kestabilan aplikasi sebelum digunakan secara aktif. Tahapan implementasi disesuaikan dengan model Waterfall yang telah dirancang sebelumnya.

Luaran utama dari kegiatan ini adalah aplikasi DanusCrypt, sebuah sistem web internal berbasis Laravel yang memungkinkan pengguna untuk mengenkripsi dan mendekripsi file penting secara otomatis. Fitur utama mencakup login multiuser, upload/download file, enkripsi dengan AES-256, dekripsi file, dan log aktivitas pengguna. Tampilan antarmuka dibuat responsif dan mudah digunakan, bahkan untuk staf yang tidak memiliki latar belakang teknis. Dokumentasi penggunaan dan panduan teknis juga disusun dalam bentuk digital dan cetak.

Keunggulan utama dari aplikasi ini adalah tingkat keamanan file yang tinggi melalui penggunaan algoritma AES-256 serta kemudahan penggunaan yang mendukung efisiensi kerja. Aplikasi ini juga memperkuat kontrol internal karena hanya dapat diakses melalui jaringan lokal. Namun, kelemahan utamanya terletak pada keterbatasan fleksibilitas akses, karena tidak dapat diakses secara daring dari luar kantor, yang bisa menjadi tantangan jika perusahaan ingin menerapkan sistem kerja hybrid. Selain itu, dokumentasi teknis masih perlu disesuaikan lebih lanjut agar mudah dipahami oleh seluruh pengguna non-teknis.

Tingkat kesulitan pelaksanaan kegiatan tergolong sedang. Hambatan teknis utama terletak pada proses integrasi antara enkripsi-dekripsi file dan sistem manajemen file Laravel, serta kebutuhan untuk menyesuaikan format file agar tetap terbaca pasca-dekripsi. Tantangan lainnya adalah koordinasi komunikasi dengan tim yang memiliki waktu kerja berbeda-beda. Namun, hambatan tersebut berhasil diatasi dengan penggunaan pertemuan rutin serta penjadwalan ulang yang fleksibel.

Simpulan

Kegiatan pengembangan aplikasi DanusCrypt telah berhasil mencapai target yang ditetapkan, yaitu menghadirkan sebuah sistem keamanan file internal yang efektif dan sesuai kebutuhan mitra. Sistem telah diuji dan diterapkan dalam jaringan internal perusahaan serta mendapatkan respons positif dari pengguna internal yang menyatakan kemudahan penggunaan dan keamanan file yang lebih terjamin.

Dampak dan manfaat dari kegiatan ini terlihat dari meningkatnya kesadaran staf terhadap pentingnya perlindungan data digital, serta berkurangnya risiko kebocoran dokumen internal. Selain itu, sistem yang dikembangkan mendukung efisiensi kerja dengan proses enkripsi-dekripsi yang terotomatisasi.

Untuk pengembangan kegiatan berikutnya, disarankan agar sistem DanusCrypt ditingkatkan dengan penambahan fitur remote access yang aman, integrasi audit trail yang lebih detail, serta pelatihan intensif bagi staf pengguna non-teknis untuk memaksimalkan pemanfaatan sistem.

Ucapan terima kasih disampaikan kepada seluruh pihak yang telah memberikan dukungan, terutama PT BPR Dana Nusantara sebagai mitra kegiatan, mentor pembimbing di perusahaan, dan staf divisi TI yang telah mendukung proses pengembangan serta memberikan masukan berharga sepanjang kegiatan berlangsung.

Daftar Pustaka

Alam, T., Ahmad, R., & Fatima, S. (2021). Comparative analysis of AES and RSA encryption algorithms. *International Journal of Computer Applications*, 183(48), 1-4. https://doi.org/10.5120/ijca2021921614

Choudhury, A., & Kumar, R. (2023). Enhancing data security in cloud using AES-256 encryption. *International Journal of Engineering Trends and Technology (IJETT)*, 71(7), 116–121. https://doi.org/10.14445/22315381/IJETT-V71I7P214

Gao, L. (2025). Enterprise internal audit data encryption based on blockchain technology. *PLOS ONE, 20*(1), e0315759. https://doi.org/10.1371/journal.pone.0315759

Kaur, H., & Singh, S. (2023). Securing sensitive data using AES algorithm in modern digital applications. *Journal of Cybersecurity and Privacy, 3*(2), 67–81. https://doi.org/10.3390/jcp3020006

Liu, Y., & Xiaoyan, H. (2022). Research on information security transmission using optimized AES. *Applied Sciences, 14*(24), 11887. https://doi.org/10.3390/app142411887

Fatima, S., Rehman, T., & Iqbal, M. (2022). Comparative analysis of AES and RSA algorithms for data security in cloud computing. *Engineering Proceedings, 20*, 14. https://doi.org/10.3390/engproc202202001