

PENGEMBANGAN SISTEM KEAMANAN FILE BERBASIS HYBRID ENCRYPTION MENGGUNAKAN ADVANCED ENCRYPTION STANDARD DAN SHA-256

Nur Azizah, Riyan Achmad Zhamroni, Muhlis Tahir

Pendidikan Informatika, Universitas Trunojoyo Madura

Jl. Raya Telang PO BOX 2 Kamal Bangkalan, Indonesia

230631100118@student.trunojoyo.ac.id

ABSTRAK

Perkembangan teknologi informasi telah meningkatkan penggunaan file digital dalam berbagai aktivitas penyimpanan dan pertukaran data. Namun, penggunaan file digital yang semakin luas juga meningkatkan risiko pencurian data, manipulasi informasi, dan akses tidak sah yang dapat mengancam kerahasiaan serta integritas data. Penelitian ini bertujuan mengembangkan sistem keamanan file berbasis hybrid encryption menggunakan algoritma Advanced Encryption Standard (AES) dan Secure Hash Algorithm 256 (SHA-256). Metode yang digunakan meliputi implementasi AES untuk proses enkripsi dan dekripsi file, serta SHA-256 untuk pembentukan kunci dan verifikasi integritas data. Sistem dikembangkan menggunakan bahasa pemrograman Python dan framework Flask berbasis web, kemudian diuji menggunakan metode black-box testing pada fitur unggah file, enkripsi, dekripsi, verifikasi kata sandi, dan penghapusan file. Hasil penelitian menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan baik, menghasilkan file terenkripsi dalam bentuk ciphertext, mengembalikan file ke bentuk semula tanpa perubahan data, serta menolak proses dekripsi ketika kata sandi yang dimasukkan tidak sesuai. Dengan demikian, sistem yang dikembangkan mampu meningkatkan keamanan file digital dari aspek kerahasiaan dan integritas data.

Kata kunci: Keamanan Data, Hybrid Encryption, AES, SHA-256, Kriptografi, Flask

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong peningkatan penggunaan data digital dalam berbagai bidang, seperti pendidikan, pemerintahan, bisnis, dan layanan publik. File digital menjadi media utama dalam penyimpanan dan pertukaran informasi karena kemudahan akses serta efisiensi yang ditawarkan. Namun, meningkatnya penggunaan data digital juga diikuti dengan meningkatnya ancaman keamanan, seperti pencurian data, manipulasi informasi, serta akses tidak sah yang dapat mengakibatkan kerugian bagi individu maupun organisasi [1]. Oleh karena itu, keamanan data menjadi aspek yang sangat penting untuk menjamin kerahasiaan dan integritas informasi yang tersimpan dalam file digital.

Salah satu permasalahan yang sering terjadi dalam pengelolaan file digital adalah belum tersedianya mekanisme perlindungan yang mampu menjaga data dari ancaman pihak yang tidak berwenang. Data yang tersimpan tanpa perlindungan yang memadai berisiko mengalami kebocoran, perubahan isi, maupun penyalahgunaan informasi. Selain menjaga kerahasiaan data, diperlukan pula mekanisme yang dapat memastikan bahwa data tidak mengalami perubahan selama proses penyimpanan maupun pengiriman. Dengan demikian, diperlukan suatu sistem keamanan yang mampu memberikan perlindungan terhadap aspek kerahasiaan (confidentiality) dan integritas (integrity) data secara bersamaan [2].

Kriptografi merupakan salah satu metode yang banyak digunakan untuk mengamankan data digital. Melalui proses kriptografi, data asli (plaintext) diubah

menjadi data yang tidak dapat dibaca (ciphertext) menggunakan algoritma tertentu sehingga hanya pihak yang memiliki kunci yang sesuai yang dapat mengakses informasi tersebut [3]. Salah satu algoritma kriptografi simetris yang banyak digunakan adalah Advanced Encryption Standard (AES). Algoritma AES dikenal memiliki tingkat keamanan yang tinggi, efisiensi yang baik, serta telah digunakan secara luas dalam berbagai sistem keamanan informasi [4]. Selain itu, untuk memastikan integritas data dapat digunakan algoritma Secure Hash Algorithm 256 (SHA-256) yang menghasilkan nilai hash unik dari suatu data. Perubahan sekecil apa pun pada data akan menghasilkan nilai hash yang berbeda sehingga manipulasi data dapat dideteksi dengan mudah [5].

Beberapa penelitian sebelumnya telah menunjukkan efektivitas penggunaan algoritma kriptografi dalam pengamanan data. Maulana dkk. [6] mengembangkan sistem keamanan file menggunakan metode hybrid encryption dan menunjukkan bahwa kombinasi beberapa teknik kriptografi dapat meningkatkan perlindungan data digital. Penelitian yang dilakukan oleh Indrayani dkk. [2] menunjukkan bahwa AES-256 mampu memberikan tingkat keamanan yang tinggi pada berbagai format file dengan proses enkripsi dan dekripsi yang efisien. Sementara itu, Erwanto dkk. [5] membuktikan bahwa SHA-256 dapat digunakan untuk menjaga integritas data melalui mekanisme verifikasi hash yang akurat. Berdasarkan hasil penelitian tersebut, kombinasi AES dan SHA-256 dinilai memiliki potensi untuk menghasilkan sistem keamanan file yang lebih baik karena mampu menjaga kerahasiaan sekaligus integritas data.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan sistem keamanan file berbasis hybrid encryption menggunakan algoritma Advanced Encryption Standard (AES) dan Secure Hash Algorithm 256 (SHA-256). Sistem yang dikembangkan diharapkan mampu meningkatkan keamanan file digital dengan melindungi data dari akses tidak sah serta memastikan integritas data tetap terjaga selama proses penyimpanan dan pengelolaan file.

Untuk mencapai tujuan tersebut, penelitian dilakukan dengan merancang dan mengimplementasikan sistem keamanan file berbasis web menggunakan bahasa pemrograman Python dan framework Flask. Algoritma AES digunakan untuk proses enkripsi dan dekripsi file, sedangkan SHA-256 digunakan untuk pembentukan kunci enkripsi serta verifikasi integritas data. Selanjutnya, sistem diuji menggunakan beberapa jenis file untuk memastikan bahwa proses enkripsi, dekripsi, dan verifikasi data dapat berjalan dengan baik sesuai dengan fungsi yang diharapkan

2. TINJAUAN PUSTAKA

Penelitian mengenai keamanan file menggunakan metode kriptografi telah banyak dilakukan. Maulana dkk. [5] mengembangkan sistem keamanan file menggunakan metode enkripsi hybrid untuk melindungi data. Penelitian tersebut menunjukkan bahwa beberapa kombinasi algoritma kriptografi mampu meningkatkan keamanan data digital. Indrayani dkk. [2] melakukan penelitian mengenai penggunaan algoritma AES 256 Bit pada pengamanan file dengan berbagai format. Hasil penelitian menunjukkan bahwa AES mampu memberikan tingkat keamanan yang tinggi serta proses enkripsi dan dekripsi yang efisien. Erwanto dkk. [4] menerapkan algoritma SHA-256 pada aplikasi pengolahan data untuk menjaga integritas data. Penelitian tersebut membuktikan bahwa SHA-256 mampu mendeteksi perubahan data dengan baik melalui nilai hash yang dihasilkan.

2.1. Data Keamanan

Keamanan data merupakan upaya untuk melindungi informasi agar tidak diakses, digunakan, maupun dimodifikasi oleh pihak yang tidak berwenang. Ancaman keamanan data dapat berupa pencurian data, penyadapan, maupun manipulasi informasi yang dapat merugikan pengguna [6].

2.2. Kriptografi

Kriptografi merupakan teknik pengamanan data dengan cara mengubah plaintext menjadi ciphertext melalui proses enkripsi dan dekripsi [7]. Kriptografi dibagi menjadi dua jenis utama yaitu kriptografi simetris dan asimetris.

2.3. Standar Enkripsi Lanjutan (AES)

AES merupakan algoritma kriptografi simetris yang menggunakan metode block cipher dalam proses enkripsi data. AES memiliki beberapa varian panjang kunci yaitu 128 Bit, 192 bit, dan 256 bit [3]. Semakin panjang kunci yang digunakan maka tingkat keamanan yang dihasilkan semakin tinggi.

2.4. Algoritma Hash Aman 256 (SHA-256)

SHA-256 merupakan algoritma hashing yang digunakan untuk menjaga integritas data dengan menghasilkan nilai hash unik dari suatu data. Algoritma ini banyak digunakan pada sistem keamanan digital karena mampu mendeteksi perubahan data dengan baik [4].

2.5. Enkripsi Hibrida

Enkripsi hibrid merupakan metode keamanan yang menggabungkan beberapa teknik kriptografi untuk meningkatkan keamanan sistem [5]. Dalam penelitian ini metode *enkripsi hybrid* diterapkan dengan mengombinasikan AES untuk menjaga kerahasiaan data dan SHA-256 untuk menjaga integritas data.

3. METODE PENELITIAN

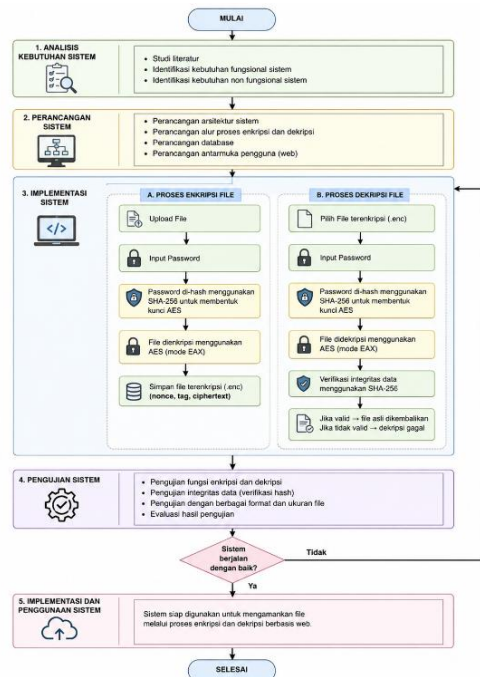
Pada penelitian ini digunakan metode implementasi sistem keamanan file berbasis hybrid encryption menggunakan algoritma Advanced Encryption Standard (AES) dan Secure Hash Algorithm 256 (SHA-256). Metode ini digunakan untuk menjaga kerahasiaan dan integritas data pada file digital melalui proses enkripsi, dekripsi, serta verifikasi data.

Tahapan penelitian dimulai dari analisis kebutuhan sistem yang meliputi identifikasi kebutuhan perangkat lunak dan kebutuhan fungsional sistem. Selanjutnya dilakukan perancangan sistem keamanan file berbasis web menggunakan bahasa pemrograman Python dan framework Flask. Sistem dirancang agar mampu melakukan proses upload file, enkripsi file, dekripsi file, serta verifikasi integritas data.

Pada tahap implementasi, algoritma AES digunakan untuk proses enkripsi dan dekripsi file dengan mode EAX sehingga data dapat diamankan dalam bentuk ciphertext. Password pengguna terlebih dahulu diubah menjadi kunci AES menggunakan algoritma SHA-256 agar keamanan kunci menjadi lebih baik. Selain digunakan untuk pembentukan kunci, SHA-256 juga dimanfaatkan untuk menjaga integritas data melalui proses hashing.

Tahap selanjutnya yaitu pengujian sistem untuk mengetahui keberhasilan proses enkripsi dan dekripsi file. Pengujian dilakukan dengan mencoba beberapa file dalam berbagai format untuk memastikan bahwa file yang dienkripsi dapat dikembalikan ke bentuk semula tanpa mengalami perubahan data. Selain itu, pengujian juga dilakukan untuk memastikan bahwa sistem mampu mendeteksi perubahan data melalui verifikasi hash yang dihasilkan.

Alur pengembangan sistem keamanan file berbasis *hybrid encryption* menggunakan algoritma AES dan SHA-256 dapat dilihat pada Gambar 1



Gambar 1. Alur pengembangan sistem keamanan

Berdasarkan Gambar 1 di atas, alur sistem dimulai dari tahap analisis kebutuhan sistem yang meliputi studi literatur serta identifikasi kebutuhan fungsional dan nonfungsional sistem. Selanjutnya dilakukan tahap perancangan sistem, seperti perancangan arsitektur sistem, alur proses enkripsi dan dekripsi, serta perancangan antarmuka berbasis web. Setelah proses perancangan selesai, sistem diimplementasikan menggunakan bahasa pemrograman Python dan framework Flask. Pada proses enkripsi, pengguna mengunggah file dan memasukkan password yang kemudian di-hash menggunakan SHA-256 untuk membentuk kunci AES sebelum file dienkripsi menggunakan AES mode EAX. Sedangkan pada proses dekripsi, sistem akan memverifikasi integritas data menggunakan SHA-256 sebelum file dikembalikan ke bentuk aslinya. Tahap selanjutnya yaitu pengujian sistem untuk memastikan proses enkripsi, dekripsi, dan verifikasi data berjalan dengan baik. Jika sistem berhasil berjalan sesuai fungsi yang diharapkan, maka sistem siap digunakan untuk mengamankan file berbasis web.

4. HASIL DAN PEMBAHASAN

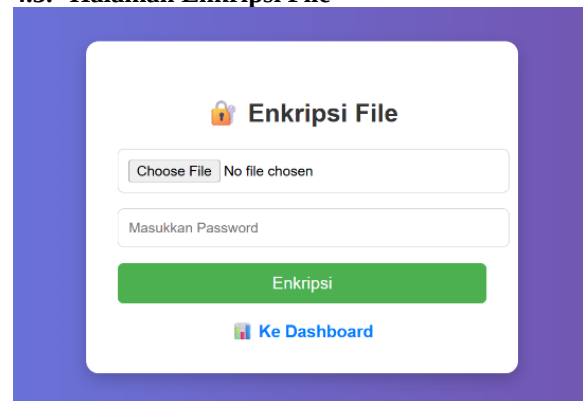
4.1. Hasil Implementasi Sistem antarmuka

Penelitian ini menghasilkan sistem keamanan file berbasis *enkripsi hybrid* menggunakan algoritma AES dan SHA-256 berbasis web. Sistem dikembangkan menggunakan bahasa pemrograman Python dengan framework Flask. antarmuka sistem dirancang sederhana agar pengguna dapat melakukan proses enkripsi dan dekripsi file dengan mudah.

4.2. Hasil Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa proses enkripsi dan dekripsi file dapat berjalan dengan baik. Pengujian dilakukan menggunakan beberapa file dengan format berbeda seperti PDF dan dokumen teks. Hasil pengujian menunjukkan bahwa sistem mampu melakukan proses enkripsi file dengan baik sehingga file asli berubah menjadi file berekstensi “.enc” dan tidak dapat dibaca secara langsung. Selain itu, proses dekripsi juga berhasil mengembalikan file ke bentuk semula tanpa mengalami perubahan isi data ketika password yang dimasukkan sesuai.

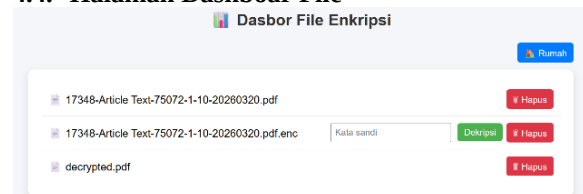
4.3. Halaman Enkripsi File



Gambar 2. Halaman Enkripsi File

Gambar 2 menunjukkan halaman utama proses enkripsi file. Pada halaman ini pengguna dapat memilih file yang akan diamankan melalui tombol *Choose File* kemudian memasukkan password sebagai kunci enkripsi. Kata sandi tersebut akan diproses menggunakan algoritma SHA-256 untuk membentuk kunci AES sebelum proses enkripsi dilakukan. Setelah tombol *Enkripsi* ditekan, sistem akan mengubah file asli menjadi file terenkripsi dalam bentuk *ciphertext* dengan ekstensi “.enc”.

4.4. Halaman Dashboar File



Gambar 3. Halaman Dashboar File

Gambar 3 menunjukkan halaman dashboard sistem yang berisi daftar file hasil proses enkripsi dan dekripsi. File yang berhasil dienkripsi akan memiliki ekstensi “.enc” sebagai tanda bahwa file telah diamankan menggunakan algoritma AES. Pada halaman ini pengguna dapat melakukan proses dekripsi dengan memasukkan password yang sesuai pada kolom kata sandi. Jika password yang dimasukkan benar, maka sistem akan mengembalikan file ke bentuk aslinya. Selain itu, sistem juga

menyediakan fitur hapus file untuk mengelola file yang tersimpan di server.

4.5. Hasil Pengujian Black-Box

Tabel 1 menunjukkan hasil pengujian sistem menggunakan metode *pengujian black-box*. Pengujian dilakukan pada fitur utama sistem untuk memastikan seluruh fungsi berjalan sesuai dengan rencana.

Tabel 1. Pengujian Black Box

No	Pengujian	Masukkan	Ouput	Hasil
1	Unggah file	Berkas PDF	File berhasil diunggah	Berhasil
2	Berkas Enkripsi	File + kata sandi	File berubah menjadi .enc	Berhasil
3	File Dekripsi	File .enc + kata sandi	File kembali normal	Berhasil
4	Verifikasi kata sandi	Kata sandi salah	Dekripsi gagal	Berhasil
5	Hapus file	Klik tombol hapus	File dihapus dari dashboard	Berhasil

Berdasarkan hasil pengujian *black-box*, seluruh fitur utama sistem yang berhasil berjalan sesuai dengan fungsi yang diharapkan. Sistem mampu melakukan proses enkripsi, dekripsi, serta pengelolaan file dengan baik sehingga dapat digunakan untuk membantu meningkatkan keamanan data digital.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, sistem keamanan file berbasis hybrid encryption menggunakan algoritma AES dan SHA-256 berhasil dikembangkan dan diimplementasikan dengan baik. Sistem mampu menjaga kerahasiaan data melalui proses enkripsi AES serta menjaga integritas data menggunakan SHA-256. Hasil pengujian menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi file dengan baik tanpa mengubah isi file asli. Untuk pengembangan selanjutnya, sistem dapat ditambahkan fitur manajemen kunci yang lebih aman serta dilakukan pengujian terhadap berbagai ukuran dan jenis file untuk mengetahui performa sistem secara lebih detail.

DAFTAR PUSTAKA

- [1] W. Berutu, I. S. Nasution, U. Setiani, M. A. Mubaraq, T. A. Siregar, dan J. O. Ritonga, "Analisis Penerapan Kriptografi Advanced

Encryption Standard (AES) Untuk Meningkatkan Keamanan Data Pengguna Pada Sistem Informasi," *Jurnal Inspirasi Pembelajaran*, vol. 7, no. 1, 2026.

- [2] R. Indrayani, P. Ferdiansyah, dan M. Koprari, "Analisis Penggunaan Kriptografi Metode AES 256 Bit Pada Pengamanan File Dengan Berbagai Format," *Digital Transformation Technology*, vol. 4, no. 2, pp. 1245–1251, 2024.
- [3] R. S. Saputra, M. A. F. Syakir, S. Aminah, D. Febrianti, dan N. A. Athalia, "Analisis Komparasi Performansi Algoritma Kriptografi RSA dan AES Pada Keamanan Data Teks," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 10, no. 2, pp. 1866–1870, 2026.
- [4] M. Erwanto, F. Sholihah, dan S. Wahyudi, "Penerapan Algoritma Kriptografi Elgamal dan SHA-256 Pada Aplikasi Pengolahan Data ATP-WTP Untuk Pengamanan Data Responden," *Journal of Computation Science and Artificial Intelligence (JCSAI)*, vol. 3, no. 1, 2026.
- [5] H. Maulana, M. Tahir, N. Farrohah, F. Maulana, dan R. R. Apriliyani, "Perancangan Sistem Keamanan File Menggunakan Hybrid Encryption Untuk Perlindungan Data," *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer*, vol. 7, no. 1, pp. 87–96, 2025.
- [6] M. F. A. Romadhan, M. Tahir, L. F. Puja, A. N. Affan, dan Y. A. N. Hadi, "Penggunaan Log Analytics Dengan Python Untuk Analisis Jejak Digital Dalam Keamanan Jaringan Nirkabel," *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer*, vol. 7, no. 1, pp. 51–60, 2025.
- [7] A. Singh, S. Meshram, T. Gujar, dan P. R. Wankhede, "Baggage Tracing and Handling System Using RFID and IoT for Airports," in *International Conference on Computing, Analytics and Security Trends (CAST)*, 2016, pp. 466–470.
- [8] T. Sharma dan S. L. Aarthy, "An Automatic Attendance Monitoring System Using RFID and IOT Using Cloud," in *International Conference on Green Engineering and Technologies (IC-GET)*, 2016, pp. 1–4.
- [9] O. T. Arulogun, A. Olatunbosun, O. A. Fakolujo, dan O. M. Olaniyi, "RFID-Based Student's Attendance Management System," *International Journal of Scientific & Engineering Research*, vol. 4, no. 2, pp. 1–9, 2013.
- [10] K. Ding dan P. Jiang, "RFID-Based Production Data Analysis in an IoT-Enabled Smart Job-Shop," *IEEE/CAA Journal of Automatica Sinica*, 2017.