Jurnal Komputer Antartika
Volume 4 Nomor 2 2026 Halaman 80-86
ISSN (Online) 2988-5272
DOI: https://doi.org/10.70052/jka.v4i2.1354

Implementasi Algoritma AES dan SHA-256 untuk Acces Control dalam Pengamanan Data Siswa Berbasis Web

Zulfatul Mufida[1*], Muhlis Tahir[2], Adinda Mulya Rahayu[3]

[1,2,3] Universitas Trunojoyo Madura
Jl. Raya Telang, PO BOX 2, Kecamatan Kamal, Kabupaten Bangkalan, Madura, Jawa Timur, Indonesia

e-mail korespondensi : zulfatulmufida@gmail.com

Submit: 03-05-2026 | Revisi: 22-05-2026 | Terima: 16-06-2026 | Terbit online: 26-06-2026

Abstrak - Pengembangan sistem berbasis web dalam dunia pendidikan meningkatkan efisiensi pengelolaan data siswa, namun juga memperbesar risiko kebocoran data dan akses tidak sah. Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan data siswa melalui integrasi algoritma kriptografi dan pembatasan hak akses. Metode yang digunakan adalah *experimental research* yang mencakup tahap perancangan, implementasi, dan pengujian sistem. Sistem keamanan ini dibangun dengan menerapkan fungsi *hashing Secure Hash Algorithm 256* (SHA-256) untuk mengamankan proses autentikasi *login* pengguna. Sementara itu, kerahasiaan data siswa dijaga menggunakan enkripsi *Advanced Encryption Standard* (AES-GCM) sebelum disimpan ke database, serta didukung oleh mekanisme *access control* untuk membatasi hak pengaksesan data. Hasil pengujian menunjukkan bahwa sistem berhasil meningkatkan proteksi data siswa melalui pendekatan *multi-layer security*. Integrasi ketiga metode ini terbukti efektif dalam menjaga aspek kerahasiaan, integritas data, serta mencegah akses dari pihak yang tidak berwenang.

Kata Kunci: Keamanan data, AES-GCM, SHA-256, Access control, Sistem web

Abstract - The development of web-based systems in education enhances the efficiency of student data management, yet it increases the risks of data breaches and unauthorized access. This study aims to implement a secure student data management system by integrating cryptographic algorithms and access restrictions. The method employed is experimental research, spanning system design, implementation, and testing phases. The security system is built by applying the Secure Hash Algorithm 256 (SHA-256) hashing function to secure the user authentication login process. Meanwhile, the confidentiality of student data is maintained using Advanced Encryption Standard (AES-GCM) encryption prior to database storage, supported by an access control mechanism to restrict data exposure. The testing results demonstrate that the system successfully enhances student data protection through a multi-layer security approach. The integration of these three methods proves effective in ensuring confidentiality, data integrity, and preventing unauthorized access.

Keywords: Data security, AES-GCM, SHA-256, Access control, Web system

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong pemanfaatan sistem berbasis web dalam berbagai bidang, termasuk pendidikan. Sistem berbasis web memungkinkan pengelolaan data siswa secara lebih efektif, cepat, dan terintegrasi. Namun, kemudahan tersebut juga diiringi dengan meningkatnya risiko keamanan data, seperti kebocoran informasi, manipulasi data, dan akses tidak sah oleh pihak yang tidak berwenang. Permasalahan ini menjadi penting karena data siswa termasuk data sensitif yang harus dijaga kerahasiaan dan integritasnya dalam sistem digital [1], [11].

Untuk mengatasi permasalahan tersebut, diperlukan mekanisme keamanan yang kuat, salah satunya melalui penerapan teknik kriptografi. Algoritma *Advanced Encryption Standard* (AES) merupakan salah satu metode enkripsi yang digunakan karena memiliki tingkat keamanan tinggi serta efisiensi dalam proses enkripsi dan dekripsi data. Penelitian sebelumnya menunjukkan bahwa AES efektif dalam mengamankan data pada sistem berbasis web, termasuk pada autentikasi login dan perlindungan data pengguna [3], [4]s. Selain itu, implementasi AES-256 juga terbukti mampu meningkatkan keamanan data akademik berbasis web dalam menjaga kerahasiaan informasi [6], [12].

Selain kerahasiaan data, aspek integritas data juga menjadi hal yang penting dalam sistem keamanan. Untuk itu digunakan fungsi hash seperti *Secure Hash Algorithm* 256 (SHA-256), yang mampu menghasilkan nilai hash unik sehingga setiap perubahan data dapat terdeteksi. Penggunaan SHA-256 dalam sistem keamanan telah banyak diterapkan, terutama dalam validasi data dan sistem ujian berbasis komputer [15]. Kombinasi antara AES

dan SHA-256 terbukti mampu meningkatkan keamanan sistem karena menggabungkan proses enkripsi dan hashing dalam satu mekanisme yang saling melengkapi [1], [8].

Berbagai penelitian telah mengimplementasikan kombinasi AES dan SHA-256 dalam pengamanan data digital, seperti dokumen, transaksi, dan sistem berbasis web. Hasil penelitian menunjukkan bahwa kombinasi tersebut efektif dalam mencegah berbagai serangan siber, termasuk manipulasi data dan *SQL Injection* [5], [13]. Selain itu, pendekatan *hybrid encryption* juga menunjukkan bahwa integrasi beberapa teknik kriptografi dapat meningkatkan keamanan data secara lebih optimal dibandingkan penggunaan metode tunggal [10], [14].

Meskipun demikian, sebagian besar penelitian sebelumnya masih berfokus pada aspek enkripsi dan hashing tanpa mengintegrasikannya dengan mekanisme *access control*. Padahal, *access control* memiliki peran penting dalam mengatur hak akses pengguna terhadap sistem sehingga hanya pihak yang berwenang yang dapat mengakses data tertentu. Penelitian menunjukkan bahwa penerapan *role-based access control* yang dikombinasikan dengan enkripsi mampu meningkatkan keamanan sistem secara menyeluruh, khususnya dalam pengelolaan data berbasis web [11], [9].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan implementasi algoritma AES dan SHA-256 yang terintegrasi dengan mekanisme *access control* dalam sistem berbasis web untuk pengamanan data siswa. Kebaruan (*novelty*) dari penelitian ini terletak pada integrasi tiga aspek utama keamanan, yaitu enkripsi, hashing, dan pengendalian akses dalam satu sistem yang terpadu. Dengan pendekatan ini, diharapkan sistem mampu memberikan perlindungan data secara menyeluruh, baik dari segi kerahasiaan, integritas, maupun kontrol akses pengguna.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan *experimental research* yang berfokus pada implementasi dan pengujian sistem keamanan data siswa berbasis web dengan mengintegrasikan algoritma *Advanced Encryption Standard* (AES), *Secure Hash Algorithm* 256 (SHA-256), serta mekanisme *access control*. Pendekatan ini dilakukan untuk memastikan bahwa sistem yang dibangun mampu memberikan perlindungan data secara menyeluruh, baik dari aspek kerahasiaan, integritas, maupun pembatasan akses pengguna.

2.1. Desain Penelitian

Desain penelitian dilakukan dengan membangun sistem keamanan berbasis web yang mengintegrasikan proses autentikasi, enkripsi data, serta pengendalian akses pengguna dalam satu sistem terpadu. Sistem dirancang untuk mengamankan data siswa melalui proses hashing pada autentikasi dan enkripsi pada penyimpanan data. Selain itu, sistem juga menerapkan pembatasan akses berdasarkan peran pengguna untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data tertentu. Pendekatan ini sejalan dengan penelitian yang menunjukkan bahwa integrasi enkripsi dengan *role-based access control* mampu meningkatkan keamanan data pada sistem digital [11].

2.2. Prosedur Penelitian

Prosedur penelitian dilakukan secara kronologis dimulai dari tahap analisis kebutuhan hingga pengujian sistem. Pada tahap awal dilakukan identifikasi terhadap kebutuhan sistem, meliputi jenis data yang akan diamankan serta peran pengguna dalam sistem. Selanjutnya dilakukan perancangan sistem berbasis web yang mencakup modul autentikasi, pengamanan data, dan pengendalian akses.

Tahap implementasi dilakukan dengan menerapkan algoritma SHA-256 pada proses autentikasi untuk mengamankan password pengguna agar tidak disimpan dalam bentuk *plaintext*. Setelah itu, data siswa yang dimasukkan ke dalam sistem akan dienkripsi menggunakan algoritma AES sebelum disimpan dalam database. Proses ini bertujuan untuk menjaga kerahasiaan data sehingga tidak dapat dibaca tanpa proses dekripsi. Selanjutnya, sistem menerapkan mekanisme *access control* untuk membatasi hak akses pengguna terhadap data.

Pendekatan ini didukung oleh penelitian yang menyatakan bahwa implementasi AES-256 efektif dalam mengamankan data sensitif pada sistem berbasis web [2], serta kombinasi teknik enkripsi dan hashing mampu meningkatkan keamanan data digital secara signifikan [1], [13].

2.3. Algoritma Sistem

Algoritma yang digunakan dalam penelitian ini terdiri dari tiga bagian utama, yaitu autentikasi menggunakan SHA-256, enkripsi data menggunakan AES, serta pengendalian akses menggunakan *access control*. Proses autentikasi dilakukan dengan cara pengguna memasukkan *username* dan *password*, kemudian sistem melakukan hashing terhadap password menggunakan SHA-256 dan membandingkannya dengan data yang tersimpan dalam database. Jika hasilnya sesuai, maka pengguna dinyatakan valid dan dapat mengakses sistem.

Selanjutnya, data siswa yang diinput ke dalam sistem akan diproses menggunakan algoritma AES untuk menghasilkan data dalam bentuk *ciphertext*. Data yang telah dienkripsi kemudian disimpan dalam database sehingga tidak dapat dibaca secara langsung tanpa proses dekripsi. Selain itu, sistem juga menerapkan mekanisme *access control* yang berfungsi untuk menentukan hak akses pengguna terhadap data. Pengguna yang memiliki hak

akses dapat melihat data dalam bentuk asli melalui proses dekripsi, sedangkan pengguna yang tidak memiliki hak akses hanya dapat melihat data dalam bentuk terenkripsi. Penggunaan kombinasi algoritma AES dan SHA-256 dalam sistem keamanan telah terbukti mampu meningkatkan perlindungan data terhadap berbagai ancaman, termasuk manipulasi dan akses tidak sah [8], [7].

2.4. Flowchart Sistem

Alur sistem dimulai dari proses login pengguna dengan memasukkan *username* dan *password*. Sistem kemudian melakukan hashing menggunakan SHA-256 untuk proses autentikasi. Jika proses autentikasi berhasil, maka data siswa akan dienkripsi menggunakan algoritma AES sebelum disimpan ke dalam database. Selanjutnya, sistem akan menerapkan mekanisme *access control* untuk menentukan hak akses pengguna terhadap data. Pengguna yang memiliki hak akses dapat melihat data dalam bentuk asli, sedangkan pengguna yang tidak memiliki hak akses hanya dapat melihat data dalam bentuk terenkripsi. Alur ini menunjukkan integrasi antara autentikasi, enkripsi, dan pengendalian akses dalam sistem keamanan.

2.5. Akuisisi Data dan Pengujian Sistem

Data yang digunakan dalam penelitian ini berupa data siswa serta data autentikasi pengguna, yaitu *username* dan *password*. Data tersebut digunakan sebagai data uji untuk mengevaluasi kinerja sistem dalam mengamankan informasi. Proses pengujian dilakukan dengan menguji setiap komponen sistem, meliputi autentikasi, enkripsi, dan *access control*. Pengujian autentikasi dilakukan untuk memastikan bahwa password telah diamankan menggunakan SHA-256. Pengujian enkripsi dilakukan untuk memastikan bahwa data telah dienkripsi menggunakan AES dan tidak dapat dibaca tanpa proses dekripsi. Selain itu, pengujian *access control* dilakukan untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat mengakses data dalam bentuk asli.

Pendekatan pengujian ini sejalan dengan penelitian yang menunjukkan bahwa penggunaan kombinasi enkripsi dan mekanisme keamanan tambahan mampu meningkatkan keandalan sistem dalam menjaga keamanan data digital [15], [9].

3. Hasil dan Pembahasan

Bagian ini menyajikan hasil implementasi sistem keamanan data siswa berbasis web yang mengintegrasikan algoritma *Advanced Encryption Standard* (AES-GCM), *Secure Hash Algorithm* 256 (SHA-256), serta mekanisme *access control*. Hasil penelitian ditampilkan dalam bentuk visual sistem untuk menunjukkan proses autentikasi, enkripsi, dan pengendalian akses secara langsung. Selain itu, pembahasan dilakukan untuk menilai efektivitas sistem serta kontribusi yang dihasilkan.

3.1 Implementasi Halaman Login

Sistem dimulai dari halaman login yang berfungsi sebagai proses autentikasi pengguna. Pengguna diminta memasukkan *username* dan *password*, kemudian sistem akan memproses password menggunakan algoritma SHA-256 sebelum dilakukan verifikasi dengan data yang tersimpan.

Gambar 1. Halaman Login Sistem

Gambar 1 menunjukkan tampilan antarmuka login yang digunakan sebagai pintu masuk sistem. Proses autentikasi dilakukan dengan mengamankan password menggunakan SHA-256 sehingga password tidak disimpan dalam bentuk *plaintext*. Pendekatan ini lebih aman dibandingkan metode konvensional karena mampu mengurangi risiko pencurian data akibat kebocoran database.

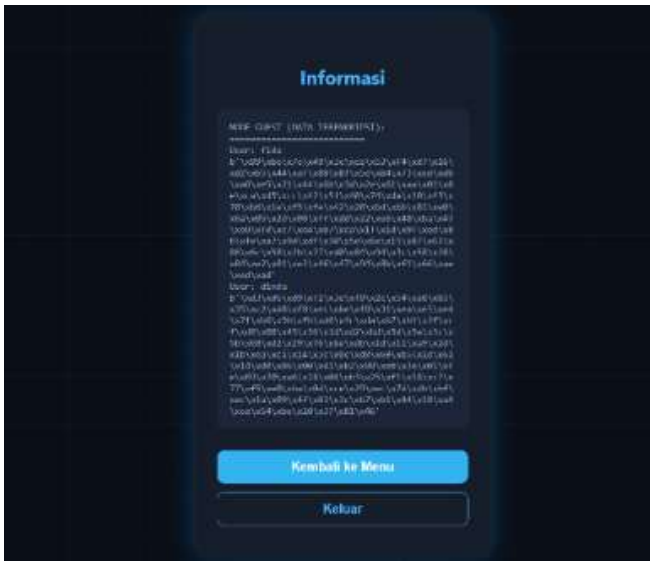
3.2 Proses Autentikasi Menggunakan SHA-256

Pada proses autentikasi, password yang dimasukkan oleh pengguna diubah menjadi nilai hash menggunakan algoritma SHA-256 sebelum dibandingkan dengan data dalam database. Hasil hashing tidak ditampilkan pada antarmuka pengguna, melainkan digunakan sebagai mekanisme pengamanan internal sistem.

Penggunaan SHA-256 meningkatkan keamanan autentikasi karena password tidak dapat dikembalikan ke bentuk semula (*one-way function*). Dengan demikian, meskipun terjadi kebocoran data, informasi password tetap sulit untuk disalahgunakan. Hal ini menunjukkan bahwa sistem telah memenuhi aspek keamanan dasar dalam perlindungan data pengguna.

3.3 Hasil Enkripsi Data Menggunakan AES-GCM

Data siswa yang tersimpan dalam sistem telah dienkripsi menggunakan algoritma AES-GCM sebelum disimpan ke dalam database. Proses ini memastikan bahwa data tidak dapat dibaca secara langsung tanpa proses dekripsi.

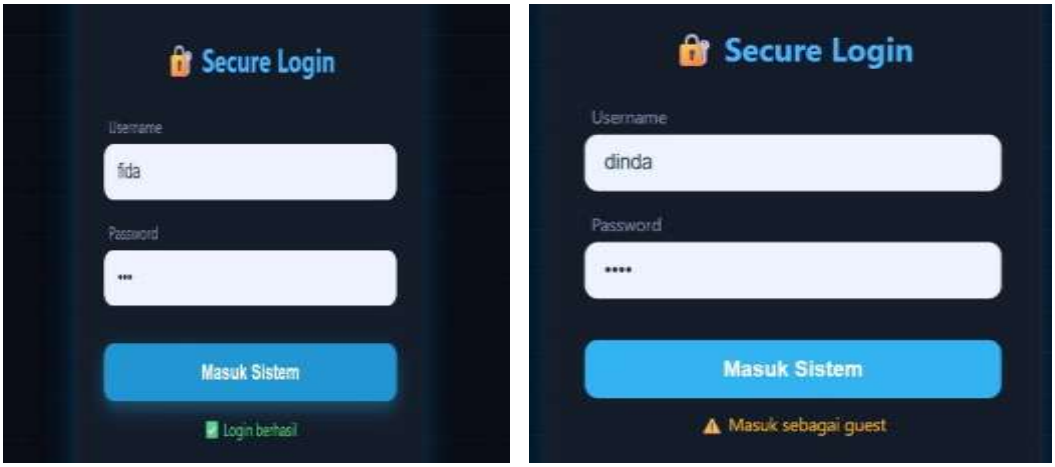


Gambar2.DataTerenkripsi(ModeGuest)

Gambar 2 menunjukkan data dalam bentuk *ciphertext* yang ditampilkan saat pengguna tidak memiliki hak akses. Data yang ditampilkan berupa karakter acak sehingga tidak dapat dipahami secara langsung. Hal ini membuktikan bahwa algoritma AES-GCM efektif dalam menjaga kerahasiaan data, karena informasi hanya dapat diakses melalui proses dekripsi oleh pengguna yang berwenang.

3.4 Implementasi Access Control

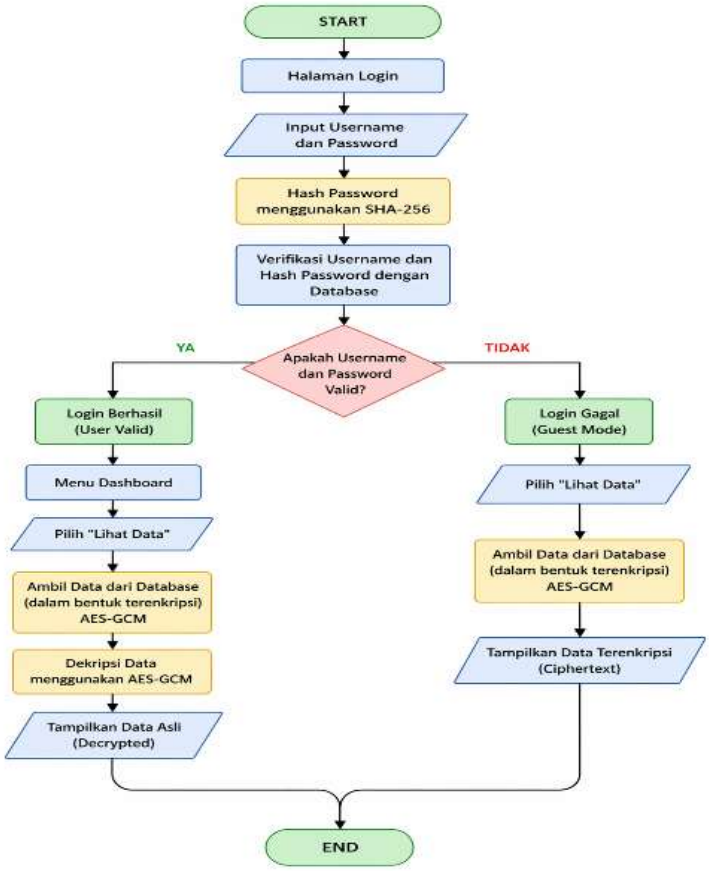
Sistem menerapkan mekanisme *access control* untuk membedakan hak akses antara pengguna yang valid dan pengguna tidak valid (*guest*). Pengguna yang berhasil login dapat melihat data dalam bentuk asli, sedangkan pengguna *guest* hanya dapat melihat data dalam bentuk terenkripsi.



Gambar 3. Perbedaan Hak Akses Pengguna

Berdasarkan Gambar 3, pengguna yang memiliki hak akses dapat melihat data dalam bentuk asli setelah proses dekripsi dilakukan, sedangkan pengguna yang tidak memiliki hak akses hanya dapat melihat data dalam bentuk terenkripsi. Mekanisme ini menunjukkan bahwa sistem mampu menerapkan pembatasan akses secara efektif, sehingga mencegah akses tidak sah terhadap data sensitif.

3.5 Flowchart Sistem Alur sistem menggambarkan proses mulai dari login, hashing password, enkripsi data, hingga pembatasan akses pengguna.



Gambar 4. Flowchart Sistem Keamanan

Berdasarkan Gambar 4, proses utama diawali pada halaman *login*, di mana pengguna diwajibkan untuk menginput kredensial berupa *username* dan *password*. Demi menjaga kerahasiaan data sejak awal, kata sandi yang dimasukkan oleh pengguna dalam bentuk teks biasa (*plaintext*) tidak langsung dikirim ke database, melainkan dikonversi terlebih dahulu oleh sistem menjadi nilai unik menggunakan fungsi *hash* satu arah algoritma SHA-256. Nilai hash hasil enkripsi inilah yang kemudian ditransmisikan untuk dicocokkan dengan data kredensial yang telah tersimpan di dalam database sistem.

Setelah proses pencocokan nilai hash selesai, sistem akan melakukan pemeriksaan validitas melalui sebuah parameter keputusan (*decision*) untuk menentukan apakah kombinasi *username* dan *password* tersebut valid atau tidak. Jika kredensial terbukti valid, pengguna dinyatakan berhasil masuk dan langsung diarahkan menuju halaman utama atau *dashboard* sistem. Ketika pengguna valid tersebut memilih menu untuk melihat data siswa, sistem akan memanggil data siswa dari database yang kondisi fisiknya masih terenkripsi oleh algoritma AES-GCM. Namun, karena status pengguna adalah valid dan memiliki otoritas penuh, sistem secara otomatis akan melakukan proses dekripsi menggunakan algoritma AES-GCM tersebut, sehingga data siswa dapat dikembalikan ke bentuk asli (*plaintext*) dan ditampilkan secara utuh pada layar pengguna.

Sebaliknya, apabila kredensial yang dimasukkan di awal terdeteksi tidak valid atau salah, sistem tidak memblokir akses secara total melainkan mengalihkan pengguna ke dalam mode tamu (*Guest Mode*). Pada mode ini, apabila pengguna *guest* mencoba mengakses atau memilih menu untuk melihat data siswa, sistem tetap akan menarik data dari database. Akan tetapi, karena pengguna tidak memiliki hak akses atau otoritas dekripsi, sistem akan menolak perintah dekripsi dan langsung menampilkan data tersebut apa adanya dalam bentuk karakter acak (*ciphertext*). Integrasi berlapis (*multi-layer security*) ini membuktikan bahwa meskipun terjadi kegagalan autentikasi atau upaya akses tidak sah, kerahasiaan data siswa di dalam database tetap terjaga dengan aman.

3.6 Pembahasan dan Kontribusi Penelitian

Hasil implementasi menunjukkan bahwa sistem yang dibangun mampu mengamankan data siswa melalui tiga lapisan keamanan utama, yaitu hashing password menggunakan SHA-256, enkripsi data menggunakan AES-GCM, serta pembatasan akses melalui mekanisme *access control*. Kombinasi ketiga metode ini menghasilkan sistem keamanan berlapis (*multi-layer security*) yang lebih efektif dibandingkan penggunaan satu metode saja. Dibandingkan dengan sistem yang menyimpan data dalam bentuk *plaintext*, pendekatan ini memberikan tingkat keamanan yang lebih tinggi karena data tidak dapat diakses secara langsung tanpa proses autentikasi dan dekripsi. Selain itu, penerapan *access control* memberikan kontrol tambahan dalam membatasi hak akses pengguna terhadap data.

Kontribusi utama dari penelitian ini terletak pada integrasi algoritma AES-GCM, SHA-256, dan *access control* dalam satu sistem berbasis web yang sederhana namun efektif. Pendekatan ini memberikan solusi praktis dalam meningkatkan keamanan data siswa, khususnya pada sistem informasi berbasis web. Implikasi dari penelitian ini menunjukkan bahwa metode yang digunakan dapat diterapkan pada berbagai sistem informasi yang membutuhkan tingkat keamanan tinggi, seperti sistem akademik, aplikasi berbasis web, maupun sistem penyimpanan data digital lainnya.

4. Kesimpulan

Penelitian ini bertujuan untuk mengimplementasikan algoritma *Advanced Encryption Standard* (AES-GCM) dan *Secure Hash Algorithm* 256 (SHA-256) dalam pengamanan data berbasis web dengan dukungan mekanisme *access control*. Berdasarkan hasil dan pembahasan, tujuan tersebut telah tercapai, di mana sistem yang dikembangkan mampu meningkatkan keamanan data melalui penerapan *multi-layer security* yang mencakup proses hashing pada autentikasi, enkripsi data, serta pembatasan hak akses pengguna. Hal ini menunjukkan adanya kesesuaian antara permasalahan yang diuraikan pada bagian pendahuluan dengan hasil yang diperoleh.

Penelitian ini memiliki prospek untuk dikembangkan lebih lanjut, khususnya dalam penguatan aspek manajemen kunci (*key management*), peningkatan kompleksitas sistem keamanan, serta integrasi dengan metode keamanan tambahan. Oleh karena itu, penelitian selanjutnya direkomendasikan untuk mengembangkan pendekatan keamanan yang lebih komprehensif guna meningkatkan ketahanan sistem terhadap berbagai potensi ancaman.

Referensi

[1] A. Halimi, A. Tholib, and M. A. Yaqin, "Optimasi Keamanan Data Penerimaan Mahasiswa Menggunakan AES-256, SHA-256, dan Base64," *JUSTIFY*, vol. 3, no. 1, pp. 38–45, 2024. doi: 10.35316/justify.v3i1.5107

[2] M. R. Fachrezi et al., "Perancangan dan Implementasi Sistem Enkripsi Data Sensitif Menggunakan AES-256-CBC pada Aplikasi Berbasis Web Sederhana," vol. 2, no. 1, pp. 55–62, 2026.

[3] F. Fadlullah et al., "Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi," *Jurnal Bintang Pendidikan Indonesia*, vol. 1, no. 2, pp. 251–263, 2023. **doi:** https://doi.org/10.64803/juikti.v2i1.100

[4] M. Fajar, A. B. Kambodji, and I. A. Musdar, "Implementasi Algoritma AES untuk Pengamanan Data Pengguna," *Jurnal Algoritma*, vol. 20, no. 2, pp. 398–409, 2023. Doi: https://doi.org/10.33364/algoritma/v.20-2.1466

[5] G. A. Fauzi and A. Rahmatulloh, "Kombinasi AES dan HMAC SHA-256 untuk Pengamanan Parameter URL," *Jurnal Informatika dan Multimedia*, vol. 17, no. 1, pp. 46–59, 2025. https://doi.org/10.33795/jtim.v17i1.6596

[6] H. A. Putri et al., "Pengamanan Data Akademik Berbasis Web dengan AES-256," *Jnatia*, vol. 3, no. 3, 2025. doi: https://doi.org/10.24843/JNATIA.2025.v03.i03.p26

[7] B. O. P. I. Irawan et al., "Implementasi Kriptografi AES pada Keamanan Data," *Jurnal Simantec*, vol. 11, no. 2, pp. 167–174, 2023. doi: https://doi.org/10.21107/simantec.v11i2.20034

[8] I. Setiadi et al., "Implementasi Kriptografi Pengamanan Data Soal Ujian Menggunakan AES-256 dan SHA-256," *Jurnal Penelitian Rumpun Ilmu Teknik*, vol. 4, no. 3, pp. 65–90, 2025. doi: https://doi.org/10.55606/juprit.v3i4.4569

[9] F. M. Kaaffah et al., "Sistem Enkripsi Dokumen Digital dengan AES dan SHA-256," *Jurnal Ilmiah FIFO*, vol. 17, no. 1, p. 78, 2025. doi: 10.22441/fifo.2025.v17i1.009

[10] H. Maulana et al., "Perancangan Sistem Keamanan File Menggunakan Hybrid Encryption," *Jurnal RESTIKOM*, vol. 7, no. 1, pp. 87–96, 2025. doi:https://doi.org/10.52005/restikom.v7i1.420

[11] M. Naufal et al., "Digital Archiving Using AES-256 and Role-Based Access Control," vol. 14, no. 3, pp. 381–391, 2026.

[12] N. A. Kafa and D. V. S. Y. Sakti, "Implementasi AES-256 dan Kompresi Huffman untuk Pengamanan File," *Jurnal Ticom*, vol. 12, no. 2, pp. 50–55, 2024. doi:https://doi.org/10.70309/ticom.v12i2.109

[13] M. Rabtsani et al., "Combination of AES and SHA-256 for Data Security," *SAGA Journal*, vol. 2, no. 1, pp. 175–189, 2024. doi: https://doi.org/10.58905/saga.v2i1.250
[14] A. E. Standard et al., "Dokumen dan Testing Kriptografi," pp. 1044–1052, 2024.
[15] F. P. Utama et al., "Implementasi AES 256 CBC dan SHA-256 dalam Pengamanan Data Ujian Online," *JTIIK*, vol. 10, no. 5, pp. 945–954, 2023. doi: 10.25126/jtiik.2023106558