JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

Integrasi Algoritma SHA-256 dan AES untuk Pengamanan Kredensial dan Data Sensitif pada Sistem Informasi Kepegawaian

M Aditya Firmansyah[1*], Qarinah[2], Muhlis Tahir[3]

[1,2 3]Fakultas Keguruan dan Ilmu Pendidikan, Pendidikan Informatika, Universitas Trunojoyo Madura, Bangkalan
Email: [1*]adityaf0728@gmail.com , [2] rqarinah@gmail.com, [3] muhlis.tahir@trunojoyo.ac.id
(*Email Corresponding Author : adityaf0728@gmail.com)
Received: May 11, 2026 | Revision: May 18, 2026 | Accepted: May 21, 2026

Abstrak

Keamanan data sensitif pada sistem informasi merupakan tantangan utama di era digital saat ini. Kebocoran data kredensial maupun dokumen rahasia dapat menimbulkan kerugian yang signifikan bagi sebuah organisasi. Penelitian ini bertujuan untuk merancang dan membangun sebuah sistem informasi yang aman guna melindungi data pengguna serta dokumen penting dari akses pihak yang tidak berwenang. Solusi yang diusulkan adalah pengembangan aplikasi berbasis web menggunakan *framework* Laravel yang terintegrasi dengan *database* relasional, serta menerapkan metode kriptografi hibrida. Untuk memastikan keamanan autentikasi, sistem ini mengimplementasikan *Secure Hash Algorithm 256* (SHA-256) dipadukan dengan teknik *salting* untuk melakukan *hashing* pada kata sandi pengguna, sehingga kredensial tetap aman meskipun *database* berhasil diretas. Selain itu, algoritma *Advanced Encryption Standard* (AES-256) digunakan untuk mengenkripsi data teks sensitif dan *file* dokumen sebelum disimpan ke dalam server. Hasil pengujian menunjukkan bahwa implementasi kedua algoritma tersebut berhasil mengamankan data secara optimal tanpa memberikan beban (overhead) yang signifikan pada kinerja server. Waktu eksekusi rata-rata untuk proses komputasi SHA-256 tercatat sekitar 0,2 milidetik, sementara proses enkripsi dan dekripsi menggunakan AES-256 membutuhkan waktu rata-rata di bawah 150 milidetik, bergantung pada ukuran *file*. Dengan demikian, sistem yang dikembangkan terbukti efektif, aman, dan efisien dalam menjaga kerahasiaan serta integritas data.

Kata Kunci: AES-256, Keamanan Data, Kriptografi, Laravel, SHA-256

Abstract

Sensitive data security in information systems is a major challenge in today's digital era. The leakage of credential data and confidential documents can cause significant losses for an organization. This research aims to design and build a secure information system to protect user data and important documents from unauthorized access. The proposed solution is the development of a web-based application using the Laravel framework integrated with a relational database, applying hybrid cryptographic methods. To ensure authentication security, the system implements the Secure Hash Algorithm 256 (SHA-256) combined with a salting technique for hashing user passwords, ensuring credentials remain secure even if the database is breached. Additionally, the Advanced Encryption Standard (AES-256) algorithm is used to encrypt sensitive text data and document files before they are stored on the server. Testing results indicate that the implementation of both algorithms successfully secures the data optimally without placing a significant overhead on server performance. The average execution time for the SHA-256 computational process is recorded at approximately 0.2 milliseconds, while the encryption and decryption processes using AES-256 take an average of under 150 milliseconds, depending on the file size. Thus, the developed system proves to be effective, secure, and efficient in maintaining data confidentiality and integrity.

Keywords: *AES-256, Cryptography, Data Security, Laravel, SHA-256*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong transformasi pengelolaan data dalam suatu institusi dari metode tradisional menuju sistem informasi yang terintegrasi. Salah satu sistem yang memiliki peran penting dalam organisasi adalah *Human Resource Information System* (HRIS), yang digunakan untuk mengelola data sumber daya manusia sebagai aset utama organisasi. Dalam operasionalnya, HRIS menyimpan berbagai data sensitif seperti Nomor Induk Kependudukan (NIK), data gaji, informasi rekening bank, serta dokumen penting seperti kontrak kerja dan slip gaji digital. Oleh karena itu, aspek keamanan data menjadi sangat krusial untuk menjaga kerahasiaan dan integritas informasi.

Namun, pada praktiknya masih banyak sistem informasi yang memiliki kelemahan karena menyimpan data dalam bentuk *plaintext* yang rentan terhadap akses illegal [1]. Laporan *Global Payroll Complexity Index* tahun 2021 mencatat bahwa 39,6% organisasi global masih menggunakan *spreadsheet* dan 17,7% bergantung pada proses manual, yang meningkatkan risiko kebocoran data sensitif [2]. Keamanan dalam proses login website menjadi aspek yang sangat penting untuk mencegah pencurian data kredensial pengguna [3]. Ancaman intersepsi informasi secara melawan hukum terhadap dokumen digital seperti PDF juga terus meningkat, sehingga dibutuhkan tindakan proteksi yang tepat [4]. Manipulasi dokumen dapat merugikan reputasi organisasi, sehingga diperlukan perlindungan efektif terutama saat memproses data dalam jumlah besar [5]. Penggunaan algoritma enkripsi simetris sering menjadi pilihan karena dikenal memiliki tingkat keamanan yang tinggi serta efisiensi waktu yang optimal [6]. Keamanan data menjadi prioritas utama mengingat banyaknya informasi yang dikirim dan disimpan secara elektronik di era digital [7]. Tanpa pengamanan yang

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

kuat, data sensitif seperti kata sandi sangat rentan terhadap serangan *brute force* yang mencoba semua kombinasi kemungkinan [8].

Penelitian sebelumnya telah mengevaluasi berbagai algoritma untuk meningkatkan keamanan. Implementasi AES-128 telah digunakan untuk mengamankan file teks agar tidak dapat diakses tanpa kunci yang valid [9]. Penggunaan AES-256 yang dikombinasikan dengan SHA-256 dan Base64 terbukti mampu mengoptimalkan keamanan data pada sistem penerimaan mahasiswa baru [10]. Selain itu, pengamanan dokumen digital perusahaan berbasis Android telah dikembangkan dengan memanfaatkan ketangguhan algoritma AES-256 [11]. Kombinasi AES-256 dengan metode *Vigenere Cipher* juga diterapkan untuk memberikan pengamanan khusus pada dokumen kepegawaian agar tidak disalahgunakan [12]. Peningkatan pengamanan file melalui mekanisme kriptografi juga krusial untuk menangkal serangan *brute force* yang semakin kompleks [13].

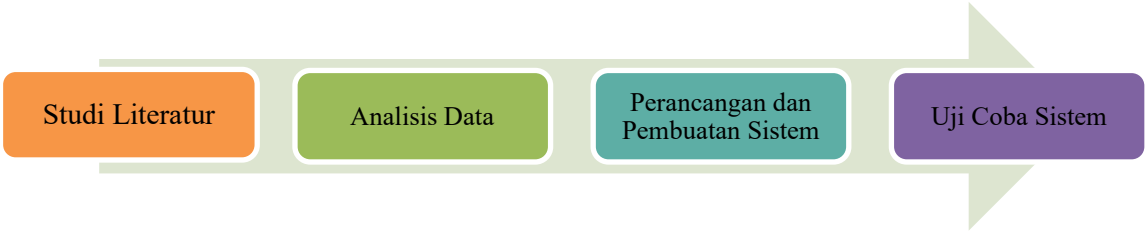
Dalam konteks aplikasi web, penggunaan AES-256 CBC yang dipadukan dengan SHA-256 memberikan validasi data yang kuat pada sistem ujian *online* [14]. Penerapan keamanan berlapis menggunakan enkripsi Base64 serta *hashing* SHA-1 dan MD5 secara signifikan dapat memperkecil peluang terjadinya pencurian data oleh peretas . Selain itu, penelitian lain menunjukkan bahwa algoritma AES banyak digunakan untuk mengamankan data karena tingkat keamanannya yang tinggi serta kemampuannya dalam melakukan enkripsi dan dekripsi [15]. Penerapan AES juga terbukti dapat digunakan dalam proses autentikasi dan pengamanan data agar tidak mudah diakses oleh pihak yang tidak berwenang [16]. Meskipun demikian, sebagian besar penelitian masih memisahkan antara pengamanan data teks di basis data dan pengamanan dokumen, serta belum memperhatikan aspek pengelolaan kunci enkripsi secara optimal.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pengembangan sistem informasi berbasis web dengan menerapkan kombinasi algoritma kriptografi SHA-256 dan AES-256. Algoritma SHA-256 digunakan untuk mengamankan kredensial login melalui mekanisme *hashing* satu arah, sedangkan AES-256 digunakan untuk mengenkripsi data sensitif serta dokumen. Selain itu, sistem ini menerapkan mekanisme distribusi kunci di luar sistem (*out-of-band key distribution*) pada fitur brankas dokumen, di mana kunci dekripsi tidak disimpan dalam basis data, melainkan dimasukkan langsung oleh pengguna saat mengakses dokumen. Dengan pendekatan tersebut, diharapkan sistem mampu memberikan perlindungan data yang lebih optimal dan komprehensif, baik pada kredensial login, data sensitif, maupun dokumen digital dalam sistem informasi kepegawaian.

2. METODOLOGI PENELITIAN

2.1 Metode Peneliatian

Penelitian ini dilakukan melalui beberapa tahapan untuk menghasilkan sistem informasi kepgawaian yang aman. Tahapan penelitian dimulai dari Studi Literatur hingga tahap uji coba sistem. Alur peneltian ini ditunjukkan pada Gambar 1.



Gambar 1. Alur tahapan penelitian

Tahapan penelitian dimulai dengan studi literatur yang berhubungan dengan kriptografi khusus nya pada algoritma SHA-256 dan algoritma AES. Langkah selanjutnya adalah menganilisis data dan mempelajari apa yang perlu dilakukan untuk meningkatkan keamanan. Kemudian membuat perancangan keamanan pada sistem informasi berbasis web. Setelah web dibangun, sistem diuji.

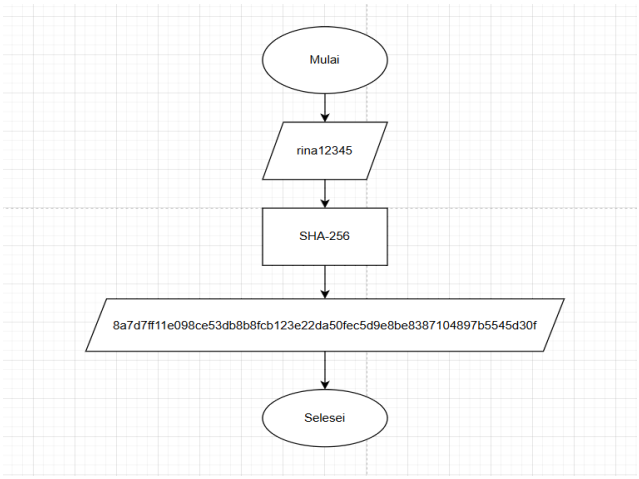
2.2 Metode Implementasi dan Pengamanan Sistem

Metode yang digunakan dalam penelitian ini adalh penerapan teknik kriptogradi pada sistem kepegawaian dengan memanfaatkan algoritma SHA-256 san AES-256 untuk meningkatkan keamanan data.

2.1.1 Implementasi SHA-256 pada Sistem Login

Algoritma SHA-256 digunakan untuk mengamankan kredensial login pengguna. Password yang diinputkan akan diproses menjadi nilai hash sebelum disimpan ke dalam basis data, sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

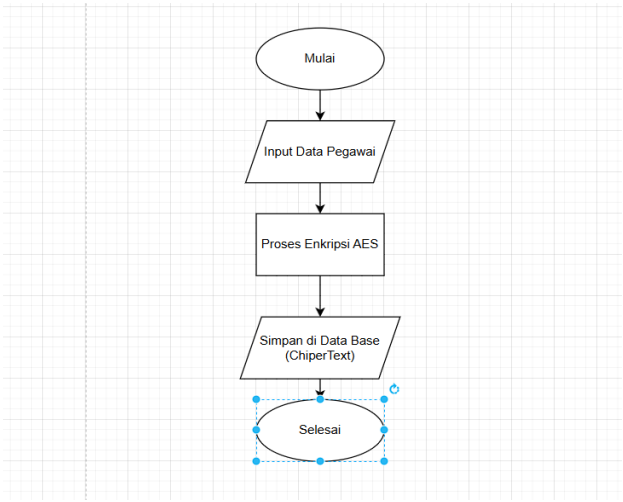


Gambar 2. Proses Hashing Password pada Sistem Login.

Proses ini memastikan bahwa sistem hanya mencocokkan nilai hash saat login, bukan password asli, sehingga meningkatkan keamanan data pengguna.

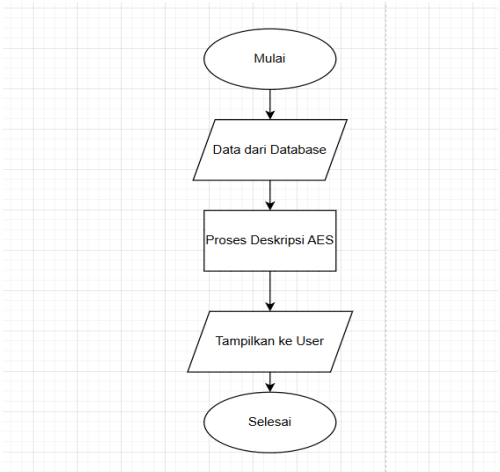
2.1.2 Implementasi AES-256 pada Sistem Data Sensitif dan Dokumen

Algoritma AES-256 digunakan untuk mengamankan data sensitif seperti Nomor Induk Karyawan (NIK), data gaji, dan nomor rekening. Data akan dienkripsi sebelum disimpan ke dalam basis data



Gambar 3. Proses Enkripsi Data Sensitif

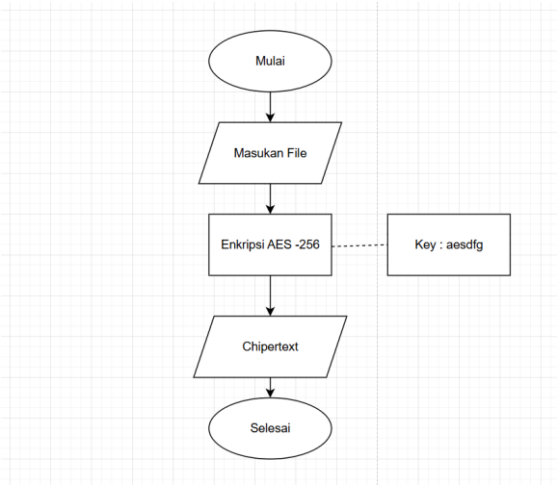
dan didekripsi saat ditampilkan kepada pengguna yang memiliki hak akses.



Gambar 4. Proses Dekripsi Data Sensitif

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

Dengan metode ini, data yang tersimpan di database tidak dapat dibaca secara langsung tanpa melalui proses dekripsi. Pada fitur brankas dokumen, file yang dikirim oleh admin akan dienkripsi menggunakan algoritma AES-256 dengan kunci tertentu. Kunci enkripsi tidak disimpan dalam sistem, melainkan diberikan kepada pengguna secara terpisah.



Gambar 5. Proses Enkripsi dan Akses Dokumen

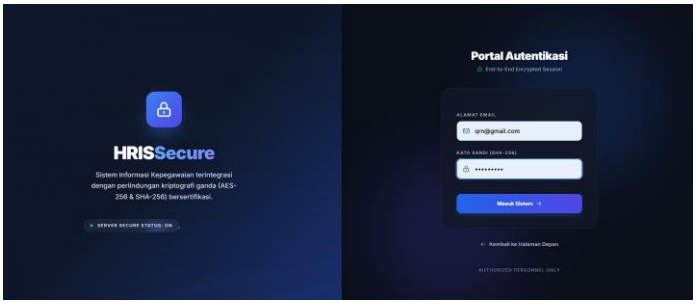
Pegawai yang menerima dokumen harus memasukkan kunci yang sesuai untuk dapat mengakses file. Jika kunci yang dimasukkan tidak sesuai, maka dokumen tidak dapat dibuka.

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi hasil implementasi serta pembahasan dari penerapan algoritma kriptografi SHA-256 dan AES-256 pada sistem informasi kepegawaian berbasis web. Hasil yang diperoleh mencakup pengujian sistem login, pengamanan data sensitif, serta pengamanan dokumen melalui fitur brankas.

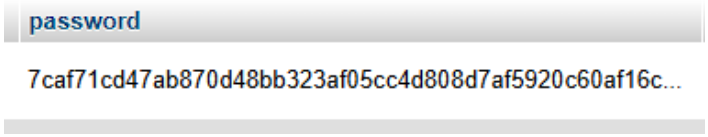
3.1 Hasil Implementasi SHA-256 pada Sistem Login

Implementasi algoritma SHA-256 pada sistem login bertujuan untuk mengamankan kredensial pengguna. Pada proses ini, password yang dimasukkan oleh pengguna tidak disimpan dalam bentuk asli (plaintext), melainkan diubah menjadi nilai hash sebelum disimpan ke dalam basis data.



Gambar 6. Halaman Login Sistem

Pada saat pengguna melakukan login, sistem akan melakukan proses hashing terhadap password yang diinputkan, kemudian membandingkannya dengan nilai hash yang tersimpan di dalam database.



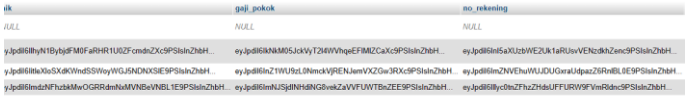
Gambar 7. Data Password dalam Database

Berdasarkan hasil pengujian, password yang tersimpan di dalam database tidak dapat dibaca secara langsung karena telah berbentuk hash. Hal ini menunjukkan bahwa sistem telah berhasil menerapkan mekanisme keamanan yang mampu melindungi kredensial pengguna dari akses tidak sah. Selain itu, sistem juga mampu melakukan validasi login dengan membandingkan hash yang dihasilkan dari input pengguna dengan data yang tersimpan di database. Jika nilai hash sesuai, maka pengguna dapat mengakses sistem, sedangkan jika tidak sesuai, maka akses akan ditolak.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

3.2 Hasil Implementasi AES-256 pada Data Sensitif dan Dokumen

Pengamanan data sensitif dilakukan dengan menerapkan algoritma AES-256 pada data seperti Nomor Induk Karyawan (NIK), data gaji, dan nomor rekening. Data tersebut dienkripsi sebelum disimpan ke dalam basis data.



Gambar 8. Data Sensitif dalam Database (*Ciphertext*)

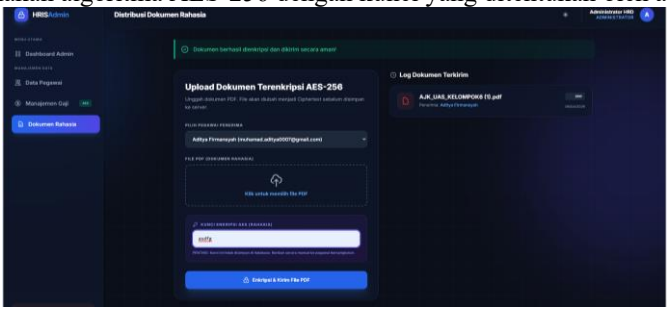
Hasil implementasi menunjukkan bahwa data yang tersimpan dalam database tidak dapat dibaca secara langsung karena telah dienkripsi. Hal ini membuktikan bahwa proses enkripsi berjalan dengan baik.

Ketika data ditampilkan pada halaman profil pengguna, sistem akan melakukan proses dekripsi sehingga data dapat kembali ke bentuk aslinya.

Gambar 9. Tampilan Data pada Halaman Profil

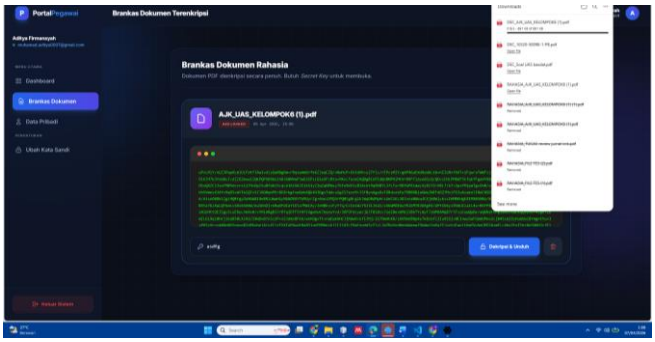
Dengan demikian, hanya pengguna yang memiliki hak akses yang dapat melihat data dalam bentuk asli, sedangkan pihak lain hanya dapat melihat data dalam bentuk terenkripsi. Berdasarkan hasil pengujian menunjukkan bahwa data yang telah dienkripsi tidak dapat dibaca secara langsung dan dapat dikembalikan ke bwntuk aslinya melalui proses dekripsi.

Fitur brankas dokumen digunakan untuk mengamankan file yang dikirim oleh admin kepada pegawai. Pada proses ini, file akan dienkripsi menggunakan algoritma AES-256 dengan kunci yang ditentukan oleh admin.



Gambar 10. Halaman Brankas Admin (Upload Dokumen)

Setelah file dikirim, pegawai dapat melihat daftar dokumen yang tersedia. Namun, dokumen tersebut tidak dapat langsung diakses karena telah dienkripsi.



Gambar 11. Halaman Brankas Pegawai (Input Kunci)

Pada tahap pengujian menunjukkan bahwa untuk mengakses dokumen, pegawai harus memasukkan kunci enkripsi yang sesuai. Jika kunci yang dimasukkan benar, maka dokumen akan berhasil didekripsi dan dapat diunduh. Sebaliknya, jika kunci tidak sesuai, maka dokumen tidak dapat diakses.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

3.2 Pembahasan

berdasarkan hasil implementasi dan pengujian yang telah dilakukan, sistem informasi kepegawaian yang dibangun telah berhasil meningkatkan keamanan data melalui penerapan algoritma kriptografi.

a. Penggunaan algoritma SHA-256 pada sistem login terbukti efektif dalam melindungi kredensial pengguna, karena password tidak disimpan dalam bentuk asli dan tidak dapat dikembalikan ke bentuk semula. Hal ini mengurangi risiko kebocoran data akibat akses tidak sah ke database.
b. Penerapan algoritma AES-256 pada data sensitif dan dokumen memberikan perlindungan tambahan, di mana data tidak dapat dibaca tanpa melalui proses dekripsi dengan kunci yang sesuai. Mekanisme ini memastikan bahwa data tetap aman meskipun terjadi akses ilegal ke basis data. Selain itu, fitur brankas dokumen memberikan lapisan keamanan tambahan melalui penggunaan kunci enkripsi yang tidak disimpan di dalam sistem. Pendekatan ini meningkatkan keamanan karena akses terhadap dokumen sepenuhnya bergantung pada kunci yang dimiliki oleh pengguna.

Secara keseluruhan, kombinasi penggunaan algoritma SHA-256 dan AES-256 dalam sistem ini menunjukkan bahwa penerapan dua metode kriptografi yang berbeda dapat meningkatkan keamanan sistem secara menyeluruh, baik dalam pengamanan kredensial login, data sensitif, maupun dokumen digital.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pembahasan, penelitian ini menyimpulkan bahwa sistem informasi kepegawaian berbasis web yang dibangun telah berhasil meningkatkan tingkat keamanan data secara signifikan melalui penerapan integrasi algoritma kriptografi SHA-256 dan AES-256. Penggunaan algoritma SHA-256 pada sistem autentikasi login terbukti sangat efektif dalam mengamankan kredensial pengguna. Proses ini mengubah kata sandi menjadi bentuk nilai hash satu arah yang sama sekali tidak dapat dibaca maupun dikembalikan ke bentuk aslinya, sehingga memitigasi risiko serangan siber seperti peretasan basis data. Selain itu, penerapan algoritma AES-256 pada pengelolaan data sensitif, seperti Nomor Induk Karyawan (NIK), rincian data gaji, serta dokumen rahasia, terbukti mampu menjaga kerahasiaan dan integritas data dengan sangat baik. Seluruh informasi sensitif yang tersimpan di dalam basis data berada dalam keadaan terenkripsi (ciphertext) dan hanya dapat diakses kembali menjadi bentuk semula (plaintext) melalui proses dekripsi oleh pihak yang berwenang. Fitur tambahan berupa brankas dokumen yang dilengkapi dengan mekanisme pendistribusian kunci rahasia secara terpisah (out-of-band) juga memberikan lapisan keamanan ekstra. Pada fitur ini, dokumen murni hanya dapat diunduh dan dibaca oleh pengguna yang memiliki kunci enkripsi yang sesuai. Secara keseluruhan, integrasi algoritma SHA-256 dan AES-256 dalam sistem ini menunjukkan bahwa penerapan dua metode kriptografi dengan fungsi perlindungan yang berbeda tidak hanya mampu memberikan pengamanan data yang komprehensif pada sistem informasi kepegawaian, tetapi juga terbukti efisien karena tidak memberikan beban komputasi yang berlebihan pada kinerja server.

REFERENCES

[1] A. Dharmawan and H. Munandar, “3 rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 30 Agustus 2023-Jakarta,” 2023.

[2] L. N. Hillalia and J. Sunupurwa Asri, “Implementasi Algoritma Enkripsi AES-256 Pada Data Penggajian: Studi Kasus PT Matahati Bermakna Indonesia,” *Jurnal Sistem Informasi, Teknik Informatika dan Teknologi Pendidikan*, vol. 5, no. 2, pp. 165–172, Jan. 2026, doi: 10.55338/justikpen.v5i2.425.

[3] N. A. Khoirunnisa, R. Satra, and D. Widyawati, “Implementasi Algoritma Kriptografi AES untuk Peningkatan Keamanan Proses Login Website,” *LINIER: Literatur Informatika dan Komputer*, vol. 2, no. 3, pp. 317–328, Oct. 2025, doi: 10.33096/linier.v2i3.3143.

[4] A. T. T. Asep Rizal Nurjaman, "Kombinasi Algoritma Kriptografi Aes-256 Dan Sha3-512 Untuk Meningkatkan Keamanan Dokumen PDF," *JITTER (Jurnal Ilmiah Teknologi Informasi Terapan)* , vol. 1, pp. 87-9, 2024 .

[5] A. Rahayu, G. Abdillah, and H. Ashaury, “Pengamanan Menggunakan Algoritma Aes (Advanced Encryption Standard) Dan Bcrypt (Blowfish Crypt) Pada File Dokumen,” 2024.

[6] F. Fadlullah, M. Tahir, B. P. Bintari, M. L. Dewi, and M. F. Ilmy, “Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi,” 2023.

[7] A. Kautsar and M. Ikhsan, “Sistemasi: Jurnal Sistem Informasi Implementasi Algoritma Advanced Encryption Standard (AES) dan Teknik Steganografi Bit Plane Complexity Segmentation (BPCS) dalam Eskalasi Keamanan File Teks Implementation of the Advanced Encryption Standard (AES) Algorithm and Bit Plane Complexity Segmentation (BPCS) Steganography Technique for Enhancing Text File Security.” [Online]. Available: http://sistemasi.ftik.unisi.ac.id

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 462-468
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1032

[8] S. Sulastri, R. Defi, and M. Putri, "Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan."

[9] M. B. Aryanto, M. Tahir, S. I. Devita, Z. N. Mustofa, Q. Ainiyah, and S. Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *JUISIK*, vol. 3, no. 1, 2023, [Online]. Available: http://journal.sinov.id/index.php/juisik/indexHalamanUTAMAJurnal:https://journal.sinov.id/index.php

[10] Ahmad Halimi, Abu Tholib, and Moh. Ainol Yaqin, "Optimasi Keamanan Data Penerimaan Mahasiswa Menggunakan Aes-256, Sha-256, Dan Base64," *JUSTIFY : Jurnal Sistem Informasi Ibrahimy*, vol. 3, no. 1, pp. 38–45, Jul. 2024, doi: 10.35316/justify.v3i1.5107.

[11] T. Diah, A. P. Wardhani, and Y. Asriningtias, "Implementation Of Aes-256 Algorithm In The Design Of Company-Based Digital Document Security Application," *Journal of Information Technology and Computer Science (INTECOMS)*, vol. 6, no. 2, 2023.

[12] P. Adam and M. A. Romli, "Implementasi Sistem Keamanan Dokumen Kepegawaian Menggunakan Metode Aes-256 Dan Vigenere Chiper", doi: 10.58290/jukomtek.v.

[13] A. Kharisma Hidayah, A. Walad Mahfuzy, and M. Oki, "Volume 6 ; Nomor 2," *Juli*, 2023, [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jsk/index

[14] F. P. Utama, G. Wijaya, R. Faurina, and A. Vatresia, "Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256 dalam Pengamanan dan Validasi Data Ujian Online," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 5, pp. 945–954, Oct. 2023, doi: 10.25126/jtiik.2023106558.

[15] A. K. H. ,. A. W. M. M. O. Andilala, "Implementasi Kombinasi Enkripsi Base64 Dengan Hashing Sha-1 Dan Md5 Pada Aplikasi Perpustakaan Universitas Muhammadiyah Bengkulu," Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD , vol. 6, pp. 694-703, 2023.

[16] I. G. indra, "Peningkatan pengamanan data file menggunakan algoritma kriptografi AES dari serangan brute force," *jurnal media informatika ,* vol. 4(2), pp. 102-109, 2023.