PERLINDUNGAN DATA AKADEMIK MAHASISWA MELALUI PENERAPAN ALGORITMA ENKRIPSI AES DAN RSA

Faustina Dalu[1], Maria Odilia Ade Siki[2], Jessica Mendonca[3]
istindallu@gmail.com[1], adeesiky@gmail.com[2], natajessica2512@gmail.com[3]
Universitas Timor

ABSTRAK

Data akademik mahasiswa seperti KRS, KHS, dan biodata merupakan informasi sensitif yang harus dilindungi dari akses tidak sah. Penelitian ini membahas penerapan algoritma Advanced Encryption Standard (AES) dan Rivest–Shamir–Adleman (RSA) untuk mengamankan data akademik dalam Sistem Informasi Akademik (SIAKAD). Pendekatan dilakukan melalui simulasi sistem dengan penerapan kedua algoritma untuk mengenkripsi data KRS dan KHS mahasiswa. Evaluasi dilakukan terhadap kecepatan dan keamanan enkripsi. Hasil menunjukkan bahwa kombinasi AES dan RSA dapat meningkatkan perlindungan data akademik dan mencegah kebocoran informasi di lingkungan perguruan tinggi.
Kata Kunci: AES, Data Akademik, Enkripsi, RSA, Sistem Informasi Akademik.

ABSTRACT

Academic data such as Study Plan Cards (KRS), Study Result Cards (KHS), and student personal records are sensitive information that must be protected from unauthorized access. This study discusses the implementation of the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms to secure academic data within Academic Information Systems (SIAKAD). The approach involves simulating a system that applies both algorithms to encrypt student data. Evaluation was carried out based on encryption speed and data security. The results show that the combination of AES and RSA can enhance academic data protection and prevent information leakage in universities.
Keywords: *Academic Data, AES, Encryption, Information System, RSA.*

PENDAHULUAN

Data akademik mahasiswa merupakan aset penting dalam dunia pendidikan tinggi. Dalam Sistem Informasi Akademik (SIAKAD), data seperti KRS, KHS, transkrip nilai, dan biodata pribadi mahasiswa dikelola secara digital. Namun, peningkatan digitalisasi ini membuka celah bagi pihak tidak bertanggung jawab untuk mengakses dan menyalahgunakan informasi tersebut. Beberapa kasus kebocoran data akademik di Indonesia menunjukkan pentingnya penerapan sistem keamanan data yang kuat.

Enkripsi adalah metode kriptografi yang digunakan untuk menjaga kerahasiaan data. AES merupakan algoritma simetris yang unggul dalam hal kecepatan, sedangkan RSA adalah algoritma asimetris yang cocok untuk manajemen kunci. Kombinasi keduanya dalam sistem informasi akademik dapat meningkatkan integritas dan keamanan data mahasiswa. Penelitian ini bertujuan mengimplementasikan algoritma AES dan RSA pada data akademik mahasiswa untuk menganalisis efektivitasnya dalam melindungi informasi dari potensi ancaman keamanan siber.

METODE PENELITIAN

Kegiatan ini dilaksanakan melalui pendekatan rekayasa sistem informasi untuk mengimplementasikan algoritma enkripsi AES dan RSA dalam pengamanan data akademik mahasiswa, seperti KRS dan KHS. Seluruh proses terdiri dari lima tahapan sebagai berikut:

1. Identifikasi Data dan Kebutuhan Sistem:

Tahap awal ini bertujuan mengumpulkan kebutuhan serta jenis data yang akan dilindungi, termasuk data pribadi mahasiswa (seperti nama dan NIM) serta data akademik seperti daftar mata kuliah dan nilai. Data yang digunakan bersifat fiktif namun dirancang menyerupai struktur data asli.

2. Perancangan Sistem Enkripsi:

Dirancang sebuah sistem berbasis hybrid encryption. Metode AES dipakai untuk mengenkripsi konten data, sementara RSA digunakan untuk mengenkripsi kunci AES agar lebih aman saat disimpan atau ditransmisikan. Arsitektur sistem mencakup komponen input data, enkripsi AES, enkripsi RSA, penyimpanan hasil, serta dekripsi.

3. Implementasi Simulasi:

Simulasi dikembangkan menggunakan bahasa Python, dengan pustaka 'pycryptodome' dan 'rsa'. Proses pengembangan mencakup pembuatan fungsi enkripsi/dekripsi menggunakan AES 128-bit dan RSA 2048-bit, serta penggabungan keduanya dalam sistem hybrid untuk keamanan optimal.

4. Pengujian Kinerja:

Uji coba dilakukan dengan berbagai skenario data untuk mengukur efisiensi waktu proses enkripsi/dekripsi, perubahan ukuran data hasil enkripsi, serta ketahanan terhadap serangan. Evaluasi dilakukan berulang dan dirata-rata untuk mendapatkan hasil yang representatif.

5. Validasi dan Analisis:

Hasil dekripsi dibandingkan dengan data asli untuk menilai keakuratan sistem. Selain itu, dilakukan analisis terhadap risiko kebocoran informasi apabila sistem tidak menggunakan metode enkripsi kombinasi.

HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sistem simulasi enkripsi data akademik yang mengimplementasikan algoritma AES dan RSA secara terintegrasi dalam pendekatan hybrid encryption. Proses pengujian dilakukan terhadap beberapa data akademik fiktif berupa informasi biodata mahasiswa, Kartu Rencana Studi (KRS), dan Kartu Hasil Studi (KHS) yang diolah melalui sistem berbasis Python.

1. Implementasi Sistem dan Proses Enkripsi

Sistem dirancang untuk memungkinkan pengguna memasukkan data akademik yang kemudian dienkripsi menggunakan algoritma AES dengan panjang kunci 128-bit. Selanjutnya, kunci enkripsi AES tersebut dienkripsi kembali menggunakan algoritma RSA 2048-bit. Tahapan ini memastikan bahwa meskipun data dapat diakses secara fisik oleh pihak ketiga, isi data tetap tidak dapat dibaca tanpa proses dekripsi RSA terhadap kunci simetrisnya.

Hasil uji coba menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan akurat, tanpa adanya perubahan isi data. Fungsi dekripsi mampu mengembalikan seluruh data ke bentuk semula, menandakan bahwa algoritma yang diterapkan berfungsi dengan baik.

2. Evaluasi Kinerja Algoritma

Pengujian kinerja dilakukan terhadap sepuluh sampel data akademik dengan ukuran bervariasi. Pengukuran dilakukan terhadap waktu enkripsi dan dekripsi, serta perubahan ukuran data pasca enkripsi. Hasilnya ditunjukkan pada Tabel 1.

Tabel 1. Hasil Evaluasi Kinerja Algoritma Enkripsi

Algoritma	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)	Ukuran File Terenkripsi	Efisiensi
AES	11.2	9.8	≈ 1x data asli	Tinggi
RSA	96.5	90.7	4–5x data asli	Rendah
Hybrid	14.3 (AES) + 98.1 (RSA key)	10.1 + 91.3	Efisien dan aman	Optimal

Dari hasil pengujian, AES terbukti sangat cepat dan efisien dalam mengenkripsi data akademik seperti KHS dan KRS. RSA, meskipun sangat kuat dalam aspek keamanan, tidak cocok jika digunakan untuk mengenkripsi seluruh isi data karena membutuhkan waktu lebih lama dan menghasilkan file yang lebih besar. Oleh karena itu, penggunaan RSA dibatasi hanya untuk mengenkripsi kunci AES sebagai bentuk pengamanan tambahan.

Hybrid encryption menggabungkan kelebihan dari kedua algoritma: kecepatan dari AES dan keamanan distribusi kunci dari RSA. Ini menjadikan pendekatan tersebut sebagai metode yang sangat cocok untuk sistem informasi akademik yang menuntut performa tinggi sekaligus keamanan maksimal.

3. Analisis Keamanan Sistem

Keamanan merupakan aspek utama dalam perlindungan data akademik, terutama dalam konteks sistem informasi berbasis web yang rentan terhadap berbagai bentuk serangan siber. Dengan implementasi hybrid encryption, potensi akses tidak sah terhadap data dapat diminimalkan. Meskipun pihak ketiga berhasil memperoleh akses ke file terenkripsi, data tidak dapat dibaca tanpa kunci RSA untuk mendekripsi kunci AES.

Pendekatan ini juga memitigasi risiko kebocoran data akibat praktik manajemen kunci yang buruk, karena RSA menjamin distribusi kunci dilakukan dengan cara yang aman. Dalam simulasi ini, tidak ditemukan kegagalan dekripsi selama proses berlangsung, yang berarti algoritma telah berjalan sesuai ekspektasi.

4. Pembahasan Temuan dan Relevansi

Temuan ini sejalan dengan studi terdahulu oleh Hasan dan Gunawan (2022), yang menekankan efektivitas hybrid encryption dalam sistem informasi akademik. Selain itu, penerapan kombinasi algoritma kriptografi menjadi kebutuhan mendesak di era digitalisasi pendidikan tinggi, di mana integritas dan kerahasiaan data mahasiswa harus dijaga.

Hasil penelitian ini memberikan kontribusi praktis dalam perancangan arsitektur sistem informasi akademik yang aman. Penerapan metode ini tidak hanya menjamin kerahasiaan, tetapi juga dapat meningkatkan kepercayaan mahasiswa dan pemangku kepentingan terhadap sistem digital yang digunakan oleh institusi.

KESIMPULAN

Penerapan kombinasi algoritma AES dan RSA pada sistem informasi akademik terbukti meningkatkan perlindungan data mahasiswa, terutama pada komponen penting seperti KRS dan KHS. AES sangat efisien untuk mengenkripsi konten data, sedangkan RSA berperan penting dalam menjaga keamanan distribusi kunci. Kombinasi keduanya memberikan keseimbangan antara efisiensi dan keamanan data. Penelitian lanjutan dapat dilakukan dengan menguji sistem ini pada data akademik nyata dan mengintegrasikannya langsung ke dalam SIAKAD universitas.

DAFTAR PUSTAKA

Rahardjo, B. (2023). Kriptografi dan Keamanan Informaski. Jakarta: Elex Media Komputindo.

Setyawan, T., & Purnama, D. (2022). Perlindungan Data Mahasiswa dalam Sistem Akademik Berbasis Web. Jurnal Teknologi Informasi dan Komputer, 6(1), 21–30.

Hasan, M., & Gunawan, R. (2022). Evaluasi Algoritma RSA dan AES dalam Sistem Informasi Akademik. Journal of Information Security and Cybercrime, 4(2), 54–63.

Widodo, A. (2021). Implementasi RSA dalam Sistem Informasi Perguruan Tinggi. Jurnal Sistem Informasi, 5(2), 100–110.

Zhang, Y., Liu, H., & Wang, J. (2022). Hybrid Encryption Model for Public Service Systems. Journal of Cybersecurity Research, 12(1), 56–67.

Kumar, R., & Sinha, S. (2022). A Comparative Analysis of Cryptographic Algorithms: AES and RSA. International Journal of Computer Science and Security, 16(3), 123–130.

Boundless. (2016). Politics. Boundless Sociology. Retrieved June 2016, from https://www.boundless.com/sociology/...

Samovar, L. A., Richard, J., Bond, J., & Carolyn, S. R. (2013). Communication between cultures: Eighth edition. Wadsworth: Cengage Learning.

Miles, M. B., & Huberman, A. M. (1992). Qualitative data analysis. Jakarta: UI Press.

Würtz, E. (2005). Intercultural communication on websites. Journal of Computer-Mediated Communication, 11(2), 274–299. DOI: http://dx.doi.org/10.30659/ijocs.1.2.153-165.