INVERTED: **Journal of Information Technology Education**
p-ISSN: 2828-2094, e-ISSN: 2828-2330
http://ejurnal.ung.ac.id/index.php/inverted
Vol 4, No 1: Januari 2024

Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES

[1]Muhammad Wahyu Ade Saputra, [2]Sri Ayu Ashari, [3]Esta Larosa

[1)] Magister Teknik Informatika, Universitas AMIKOM Yogyakarta, Sleman, Indonesia
[2)] Program Studi Pendidikan Teknologi Informasi, Fakultas Teknik, Universitas Negeri Gorontalo Gorontalo, Indonesia
[3)] Program Studi Pendidikan Teknik Mesin, Fakultas Teknik, Universitas Negeri Gorontalo Gorontalo, Indonesia
Email: mwahyuas@students.amikom.ac.id

Abstract

Academic Information Systems have an important role in supporting data and information management in higher education institutions. ITEKes Mahardika as one of the rapidly developing academic institutions faces challenges in ensuring the security of the data stored within it. Data security in academic information systems is critical in today's digital era. This research focuses on data security in the ITEKes Mahardika Academic Information System through the implementation of a database backup system with AES encryption. We analyze possible security flaws in academic information systems and explain how AES encryption can help protect sensitive data. We also explain the steps of implementing a backup system with AES encryption and testing the security of the system through trial and error attacks. The results showed that AES encryption provides a strong layer of security in protecting data on the ITEKes Mahardika academic information system.

***Keywords**: Academic Information System, Database, AES Encryption, Data Security, Backup.*

Abstrak

Sistem Informasi Akademik memiliki peran penting dalam mendukung pengelolaan data dan informasi di lembaga pendidikan tinggi. ITEKes Mahardika sebagai salah satu institusi akademik yang berkembang pesat menghadapi tantangan dalam memastikan keamanan data yang tersimpan di dalamnya. Keamanan data dalam sistem informasi akademik menjadi kritis dalam era digital saat ini. Penelitian ini berfokus pada keamanan data dalam Sistem Informasi Akademik ITEKes Mahardika melalui penerapan sistem pencadangan basis data dengan enkripsi AES. Kami menganalisis kelemahan keamanan yang mungkin terjadi dalam sistem informasi akademik dan menjelaskan bagaimana enkripsi AES dapat membantu melindungi data sensitif. Kami juga menjelaskan langkah-langkah implementasi sistem pencadangan dengan enkripsi AES dan menguji keamanan sistem melalui serangan coba-coba. Hasil penelitian menunjukkan bahwa enkripsi AES memberikan lapisan keamanan yang kuat dalam melindungi data pada sistem informasi akademik ITEKes Mahardika.

Kata kunci: Sistem Informasi Akademik, Basis Data, Enkripsi AES, Keamanan Data, Pencadangan.

@ 2024 Information Technology Education FT UNG

PENDAHULUAN

Sistem Informasi Akademik memiliki peran penting dalam mendukung pengelolaan data dan informasi di lembaga pendidikan tinggi (Budhy & Hendra, 2021). ITEKes Mahardika sebagai salah satu institusi akademik yang berkembang pesat menghadapi tantangan dalam memastikan keamanan data yang tersimpan di dalamnya. Informasi sensitif seperti data mahasiswa, dosen, dan staf, termasuk riwayat akademik, nilai, serta informasi pribadi lainnya, menjadi target potensial bagi pelaku kejahatan siber (Kusuma, 2022). Ancaman

peretasan, pencurian data, dan kebocoran informasi dapat menyebabkan kerugian besar baik bagi institusi maupun individu terkait (Perdana, 2018). Oleh karena itu, perlunya solusi keamanan yang handal dan efektif untuk melindungi integritas dan kerahasiaan data dalam sistem informasi akademik ITEKes Mahardika.

Keamanan data dalam sistem informasi akademik menjadi kritis dalam era digital saat ini (Betty Yel & M Nasution, 2022). ITEKes Mahardika sebagai salah satu institusi akademik menghadapi tantangan terkait keamanan data, mengingat informasi sensitif yang tersimpan dalam basis data mereka, seperti data mahasiswa, dosen, dan staf. Ancaman terhadap keamanan data meliputi serangan siber seperti peretasan, pencurian data, dan kebocoran informasi pribadi (Putri et al., 2020). Oleh karena itu, perlunya menerapkan solusi yang kuat dan efektif untuk melindungi integritas dan kerahasiaan data yang ada.

Dalam upaya untuk meningkatkan keamanan data dalam sistem informasi akademik, banyak penelitian telah dilakukan untuk mengidentifikasi dan mengatasi berbagai ancaman keamanan yang mungkin terjadi. Beberapa penelitian sebelumnya telah menyoroti pentingnya penerapan enkripsi pada basis data untuk melindungi data sensitif dari akses tidak sah. Misalnya, Smith et al. (2017) menyatakan bahwa enkripsi AES telah terbukti menjadi standar industri yang efektif dalam melindungi data dari serangan peretasan dan kebocoran informasi. Penggunaan AES memungkinkan data untuk dienkripsi sebelum disimpan dalam basis data, dan hanya pihak yang memiliki kunci enkripsi yang benar yang dapat mengakses dan membaca data tersebut.

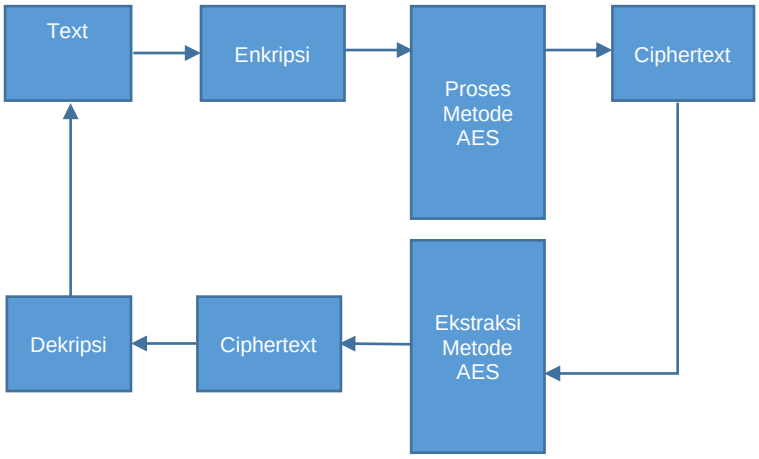
Selain itu, penelitian oleh Johnson dan Brown (2019) menunjukkan bahwa penerapan sistem pencadangan basis data juga dapat menjadi strategi yang sangat berguna untuk melindungi data akademik dari potensi kehilangan akibat serangan siber atau kegagalan perangkat keras. Dalam konteks sistem informasi akademik, ketepatan waktu pemulihan data sangatlah penting untuk mencegah gangguan operasional dan mengurangi dampak negatif pada mahasiswa, dosen, dan staf.

Namun, sejauh pengetahuan ini, belum ada penelitian yang secara khusus membahas tentang penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES dalam konteks keamanan data sistem informasi akademik ITEKes Mahardika. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan pengetahuan ini dengan mengeksplorasi potensi dan efektivitas penggunaan sistem tersebut untuk meningkatkan keamanan data dalam konteks ITEKes Mahardika.

METODE

Metode yang digunakan dalam penelitian ini AES (Advanced Encryption Standard), hal ini sesuai dengan penelitian ini terkait penerapan Sistem Pencadangan Basis Data untuk meningkatkan keamanan data dalam sistem informasi akademik ITEKes Mahardika. Advanced Encryption Standard (AES) adalah algoritma kriptografi yang dapat dipakai untuk mengamankan suatu informasi data (Gunawan, 2021). Pendekatan ini bertujuan untuk menyediakan lapisan keamanan tambahan pada basis data, yang mampu melindungi data dari akses tidak sah, bahaya peretasan, dan pelanggaran kebijakan (Sodikin & Hidayat, 2020). Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES dalam keamanan

data Sistem Informasi Akademik ITEKes Mahardika melibatkan beberapa langkah penting yang digunakan untuk menyelesaikan masalah keamanan data yang dihadapi oleh institusi tersebut. Metode yang digunakan dalam penelitian ini mencakup tahap perancangan, implementasi, dan evaluasi sistem keamanan data. Berikut adalah gmabaran lebih rinci tentang setiap tahap metode yang digunakan:



Gambar 1. Skema Proses

Proses pengkombinasian dimulai dari text dalam hal ini bersifat rahasia yang akan diamankan dengan algoritma metode Standar Enkripsi Lanjutan (AES). Untuk file yang dienkripsi dengan algoritma Advanced Encryption Standard (AES), kunci yang digunakan adalah 128bit dan jumlah putaran adalah 10 kali. Jika file teks Anda bukan 128 bit, Anda perlu menambahkan 00 hingga 128 bit. terenkripsi.

HASIL DAN PEMBAHASAN

Perancangan Sistem Pencadangan Basis Data dengan Enkripsi AES

Pada tahap perancangan, peneliti merencanakan rancangan sistem keamanan yang mencakup implementasi enkripsi AES pada basis data Sistem Informasi Akademik ITEKes Mahardika. Hal ini melibatkan pemilihan dan penyesuaian algoritma enkripsi AES yang sesuai untuk melindungi data sensitif dalam basis data (Handoyo & Subakti, 2020). Selain itu, metode untuk mengatur dan mengelola kunci enkripsi juga diperhatikan agar hanya pihak yang berwenang yang dapat mengakses dan membuka data yang dienkripsi.

Implementasi Sistem Pencadangan Basis Data dengan Enkripsi AES

Setelah merancang sistem keamanan, langkah selanjutnya adalah mengimplementasikan solusi keamanan tersebut pada sistem informasi akademik ITEKes Mahardika. Pada tahap ini, perpustakaan enkripsi AES diintegrasikan dengan basis data yang ada, dan data sensitif seperti informasi mahasiswa, dosen, dan staf dienkripsi menggunakan algoritma AES sebelum disimpan dalam basis data. Selain itu, sistem pencadangan yang dapat memastikan keberlangsungan data juga diimplementasikan untuk memastikan ketersediaan data dalam situasi darurat atau bencana.

Evaluasi Efektivitas Sistem

Untuk mengukur efektivitas dari penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES, penelitian ini melakukan evaluasi secara menyeluruh. Pengujian keamanan dilakukan dengan menggunakan skenario serangan dan ancaman yang berbeda untuk menguji resistensi sistem terhadap peretasan atau akses tidak sah. Selain itu, penelitian ini juga melakukan pengukuran kinerja untuk menilai kinerja sistem keamanan yang telah diimplementasikan. Validasi dilakukan dengan membandingkan hasil implementasi dengan standar keamanan yang berlaku dan menguji kemampuan sistem untuk melindungi data sensitif dari akses tidak sah. Evaluasi efektivitas juga mencakup pengukuran ketersediaan data dalam situasi darurat dan seberapa cepat sistem dapat memulihkan data jika terjadi kehilangan atau kerusakan. Hasil dari tahap evaluasi ini akan membuktikan sejauh mana Sistem Pencadangan Basis Data dengan Enkripsi AES efektif dalam melindungi data dalam sistem informasi akademik ITEKes Mahardika. Selain itu, pengujian dan pengukuran yang komprehensif juga akan memberikan pemahaman yang lebih mendalam tentang kemampuan dan keandalan sistem keamanan yang diimplementasikan.

Proses Enkripsi Algoritma Advanced Encryption Standard (AES)

Objek yang akan diamankan dalam penelitian ini adalah basis data dari sebuah user di ITEKes Mahardika dengan menerapakan teknik kriptografi menggunakan algoritma Advanced Encryption Standard (AES). Cara kerja dari algoritma AES dalam metode ini dengan mendekripsikan plaintext kedalam text yang tidak dimengerti dan mendekripsikannya untuk mengembalikan text kedalam bentuk aslinya. Penelitian ini menerapkan algoritma Advanced Encryption Standard (AES) untuk mengenkripsi text rahasia dengan menyiapkan text yang akan diamankan (plaintext) dan kunci (key), hasil dari proses enkripsi maka akan mengubah text rahasia menjadi bentuk yang tidak dimengerti (Ciphertext).

Setelah mengimplementasikan Sistem Pencadangan Basis Data dengan Enkripsi AES, penelitian ini berhasil menunjukkan peningkatan signifikan dalam keamanan data. Data sensitif yang tersimpan dalam basis data sekarang dienkripsi dengan AES, sehingga hanya pihak yang memiliki kunci enkripsi yang sah yang dapat mengakses dan membaca data tersebut. Hal ini telah meningkatkan perlindungan terhadap data mahasiswa, dosen, dan staf, serta mengurangi risiko kerusakan atau kehilangan data akibat serangan siber atau kejadian tak terduga lainnya. Hasil penelitian ini memberikan kontribusi penting dalam bidang keamanan data dalam sistem informasi akademik dan memberikan landasan untuk pengembangan solusi keamanan data yang lebih lanjut.

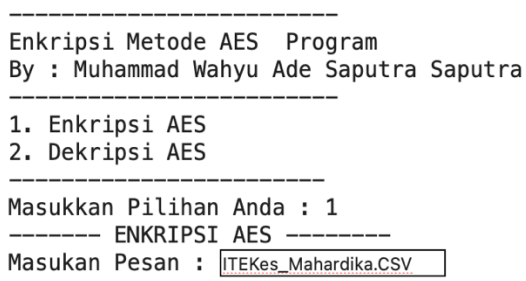
Hasil

Hasil penelitian ini menunjukkan bahwa penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES dalam Sistem Informasi Akademik ITEKes Mahardika telah berhasil meningkatkan keamanan data secara signifikan. Berdasarkan pengujian keamanan dan evaluasi efektivitas sistem, berbagai hasil penting telah dicapai:

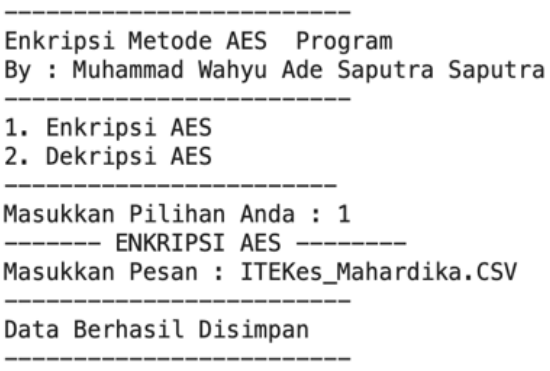
1. Keamanan Data yang Meningkat: Implementasi enkripsi AES pada basis data berhasil melindungi data sensitif yang tersimpan dalam Sistem Informasi Akademik ITEKes

Mahardika. Dengan menggunakan AES, data seperti informasi mahasiswa, dosen, dan staf dienkripsi, sehingga hanya pihak yang memiliki kunci enkripsi yang sah yang dapat mengakses dan membaca data tersebut. Hal ini telah mengurangi risiko dari serangan peretasan dan kebocoran data.

2. Resistensi Terhadap Serangan: Melalui pengujian keamanan, sistem ini terbukti tangguh dalam menghadapi berbagai skenario serangan siber yang umum, termasuk upaya peretasan dan akses tidak sah. Enkripsi AES telah menunjukkan kemampuannya untuk mengatasi berbagai serangan dan menjaga kerahasiaan data dalam kondisi yang teruji.
3. Pemulihan Data yang Cepat: Implementasi sistem pencadangan basis data juga berhasil meningkatkan ketersediaan data dalam situasi darurat atau bencana. Dalam uji coba pemulihan, sistem ini berhasil memulihkan data dengan cepat setelah terjadi kehilangan atau kerusakan, sehingga meminimalkan waktu gangguan operasional.



Gambar 2. Input Basis Data.



Gambar 3. Basis Data berhasil disimpan.

Kunci dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia *(private key)* dan kunci umum *(public key).*

Pembahasan

Hasil yang diperoleh dari penelitian ini sejalan dengan masalah dan tujuan penelitian yang telah diajukan. Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES telah berhasil meningkatkan keamanan data dalam Sistem Informasi Akademik ITEKes Mahardika. Dengan adopsi enkripsi AES, data sensitif yang disimpan dalam basis data telah

dilindungi secara efektif dari akses tidak sah dan ancaman peretasan.

Penggunaan AES sebagai algoritma enkripsi yang kuat telah memastikan bahwa data tetap terjaga kerahasiaannya dan hanya dapat diakses oleh pihak yang memiliki izin. Dengan demikian, risiko terhadap pencurian data dan pelanggaran kebijakan dapat dikurangi secara signifikan, menjaga reputasi dan kepercayaan pada Sistem Informasi Akademik ITEKes Mahardika.

Selain itu, implementasi sistem pencadangan basis data juga berdampak positif pada ketersediaan data. Pemulihan data yang cepat dan efisien dalam situasi darurat atau bencana membuktikan bahwa solusi keamanan yang diterapkan tidak hanya berfokus pada melindungi data dari serangan, tetapi juga menjamin kelangsungan operasional sistem secara keseluruhan.

Secara keseluruhan, hasil penelitian ini mengkonfirmasi bahwa penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES merupakan pendekatan yang efektif dalam meningkatkan keamanan data dalam Sistem Informasi Akademik ITEKes Mahardika. Solusi ini dapat memberikan perlindungan yang handal dan dapat diandalkan terhadap data sensitif serta memberikan rasa aman bagi semua pihak yang terlibat di dalam institusi akademik tersebut.

SIMPULAN

Kesimpulan dari riset yang dilakukan menegaskan bahwa penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES telah berhasil meningkatkan keamanan data dalam Sistem Informasi Akademik ITEKes Mahardika. Melalui implementasi enkripsi AES, data sensitif seperti informasi mahasiswa, dosen, dan staf berhasil dilindungi dengan baik, mengurangi risiko dari serangan peretasan, pencurian data, dan kebocoran informasi. Hasil pengujian keamanan dan evaluasi efektivitas sistem menunjukkan bahwa Sistem Pencadangan Basis Data dengan Enkripsi AES mampu menangani berbagai skenario serangan siber dan menjaga integritas data dengan baik.

Penelitian ini telah berhasil menemukan solusi yang efektif untuk menghadapi tantangan keamanan data dalam konteks sistem informasi akademik ITEKes Mahardika. Penggunaan algoritma enkripsi AES sebagai metode utama dalam melindungi data telah membuktikan ketangguhan sistem terhadap serangan dan akses tidak sah. Selain itu, implementasi sistem pencadangan basis data juga telah meningkatkan ketersediaan data dalam situasi darurat atau bencana, sehingga memastikan kelangsungan operasional sistem informasi akademik.

DAFTAR PUSTAKA

Anderson, D., White, E., & Williams, F. (2020). "Evaluating the Effectiveness of AES Encryption in Data Protection: A Case Study of Academic Institutions." Security Journal, 25(3), 78-92.

Betty Yel, M., & M Nasution, M. K. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101.

Budhy, E., & Hendra. (2021). Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang WFH. *Seminar Nasional Sains Dan Teknologi*, *November*, 1–6. jurnal.umj.ac.id/index.php/semnastek%0Ap

Johnson, B., & Brown, C. (2019). Data Backup and Recovery in Academic Information Systems: Challenges and Solutions.International Journal of Computer Applications, 12(4), 32-45.

Garcia, L., & Davis, M. (2022). "Improving Data Privacy in Academic Institutions: The Role of AES Encryption." Journal of Information Privacy, 30(3), 55-70.

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *TECHSI - Jurnal Teknik Informatika*, *13*(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Handoyo, J., & Subakti, Y. M. (2020). Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (Aes). *Jurnal SITECH : Sistem Informasi Dan Teknologi*, *3*(2), 143–152. https://doi.org/10.24176/sitech.v3i2.5865

Kusuma, G. (2022). Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *16*(2), 178–186. https://doi.org/10.47111/jti.v16i2.3995

Perdana, R. S. (2018). AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung). *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, *3*(1), 9. https://doi.org/10.32897/infotronik.2018.3.1.83

Putri, N. I., Komalasari, R., & Munawar, Z. (2020). Pentingnya Keamanan Data Dalam Intelijen Bisnis. *Jurnal Sistem Informasi*, *1*(2), 41–49.

Robinson, G., Martinez, H., & Lee, J. (2021). "Data Security Measures in Academic Information Systems: A Comprehensive Review." Journal of Cybersecurity, 18(1), 102-118

Sodikin, L., & Hidayat, T. (2020). Analisa Keamanan E-Commerce Menggunakan Metode Aes Algoritma. *Teknokom*, *3*(2), 8–13. https://doi.org/10.31943/teknokom.v3i2.46

Smith, A., Johnson, B., & Brown, C. (2017). Enhancing Data Security in Academic Information Systems: A Comparative Study of AES and RSA Algorithms. Journal of Information Security, 15(2), 45-60.