RANCANG BANGUN PROTOTIPE APLIKASI SIAKAD POLTEKAD BERBASIS ANDROID DENGAN IMPLEMENTASI KEAMANAN DATA MENGGUNAKAN ENKRIPSI AES

Muhammad Ishar Shafawi[1)], Yohanes Dwi Cahyono[2))], Vincensius Arga Y[3)]
[1)]Politeknik Angkatan Darat, [2)] Asrama Politeknik Angkatan Darat, [2)] Asrama Politeknik Angkatan Darat
nasutionishar18@gmail.com[1)] Yohanes@poltekad.ac.id[2)]
vincensius.arga@gmail.com[3)]

Abstract: *The need for a secure and effective academic information system (SIAKAD) is increasing in the current computer and internet era, especially for higher education institutions such as the Army Polytechnic (POLTEKAD). The purpose of this research is to create a prototype of an Android-based siakad application that uses the Advanced Encryption Standard (AES) encryption algorithm to protect data. Analysis, design, implementation, testing, and maintenance are the steps in the Waterfall Model used for development. The results show that adding aes encryption to the siakad application can improve the data security of students, lecturers, and administration. This is especially true for protecting personal and academic data from people who are not entitled to access it. The Black Box testing process is used to ensure that the system operates according to the expected specifications. This application makes the academic process at poltekad more organized, effective, and secure. The need for a secure and effective academic information system (SIAKAD) is increasing in the current computer and internet era, especially for higher education institutions such as the Army Polytechnic (POLTEKAD). The purpose of this research is to create a prototype of an Android-based siakad application that uses the Advanced Encryption Standard (AES) encryption algorithm to protect data. Analysis, design, implementation, testing, and maintenance are the steps in the Waterfall Model used for development. The results show that adding aes encryption to the siakad application can improve the data security of students, lecturers, and administration. This is especially true for protecting personal and academic data from people who are not entitled to access it. The Black Box testing process is used to ensure that the system operates according to the expected specifications. This application makes the academic process at poltekad more organized, effective, and secure.*
Keywords: Siakad, Android, Data Security, AES Encryption, Poltekad.
Abstrak: Kebutuhan akan sistem informasi akademik (SIAKAD) yang aman dan efektif semakin meningkat di era komputer dan internet saat ini, terutama untuk lembaga pendidikan tinggi seperti Politeknik Angkatan Darat (POLTEKAD). Tujuan penelitian ini adalah untuk membuat prototipe aplikasi siakad berbasis Android yang menggunakan algoritma enkripsi *Advanced Encryption Standard* (AES) untuk melindungi data. Analisis, perancangan, implementasi, pengujian, dan pemeliharaan adalah langkah-langkah dalam Model *Waterfall* yang digunakan untuk pengembangan. Hasil penelitian menunjukkan bahwa menambahkan enkripsi aes ke aplikasi siakad dapat meningkatkan keamanan data mahasiswa, dosen, dan administrasi. Ini terutama berlaku untuk melindungi data pribadi dan akademik dari orang yang tidak berhak mengaksesnya. Proses pengujian Black Box digunakan untuk memastikan bahwa sistem beroperasi sesuai dengan spesifikasi yang diharapkan. Aplikasi ini membuat proses akademik di poltekad lebih terorganisir, efektif, dan aman.
Kata kunci*:* Siakad, Android, Keamanan Data, Enkripsi AES, Poltekad.

PENDAHULUAN

Dalam era digital saat ini, perkembangan teknologi informasi telah memungkinkan institusi pendidikan untuk mengelola data akademik secara lebih efisien. Salah satu sistem yang berperan penting dalam manajemen data akademik adalah Sistem Informasi Akademik (SIAKAD). SIAKAD digunakan untuk mengelola berbagai informasi akademik, termasuk data mahasiswa, nilai, jadwal perkuliahan, dan informasi administrasi lainnya. Di Politeknik Angkatan Darat (Poltekad), SIAKAD menjadi bagian esensial dalam mendukung proses akademik dengan menyediakan akses cepat dan transparan bagi mahasiswa, dosen, serta staf akademik. Sistem ini memungkinkan pengambilan keputusan berbasis data, seperti perencanaan jadwal pengajaran dan evaluasi program studi, yang pada akhirnya berkontribusi pada peningkatan kualitas pendidikan (Safrizal dan Afkar, 2023).

Seiring dengan manfaat yang ditawarkan, penggunaan SIAKAD juga menghadapi tantangan besar dalam aspek keamanan data. Data akademik yang tersimpan dalam SIAKAD bersifat sensitif, mencakup identitas mahasiswa (NIM, nama, alamat, nomor telepon), riwayat akademik (nilai, kehadiran, skripsi), serta informasi dosen dan staf (jadwal pengajaran, data penilaian, publikasi ilmiah). Kerentanan dalam sistem keamanan dapat menyebabkan kebocoran data, baik akibat kesalahan konfigurasi, serangan siber, maupun eksploitasi celah keamanan oleh pihak yang tidak berwenang.

Salah satu bentuk serangan yang sering terjadi pada sistem informasi akademik adalah SQL *Injection*, di mana peretas menyisipkan perintah SQL berbahaya ke dalam sistem dengan tujuan mendapatkan akses tidak sah terhadap basis data. Studi oleh Idfiana & Jakaria (2024) menunjukkan bahwa sistem pendaftaran mahasiswa baru yang memiliki celah keamanan dapat dieksploitasi melalui serangan SQL *Injection*, menyebabkan kebocoran data pribadi mahasiswa. Pengujian pada dua sistem yang berbeda mengungkapkan bahwa salah satu sistem mengalami kebocoran data dengan tingkat risiko *medium* (5,76 dari 10) berdasarkan CVSS (*Common Vulnerability Scoring System*), menegaskan bahwa keamanan SIAKAD di lingkungan akademik masih perlu ditingkatkan (Idfiana dan Jakaria, 2024).

Menurut penelitian Prajna Deshanta Ibnugraha (2021), analisis risiko terhadap sistem informasi akademik dapat dilakukan menggunakan metode CVSS (*Common Vulnerability Scoring System*) untuk mengukur tingkat ancaman dari serangan siber. Sistem pendaftaran mahasiswa baru sering kali mengandung informasi sensitif yang harus dijaga agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, perlindungan keamanan berbasis enkripsi menjadi solusi utama dalam mencegah

kebocoran data (Ibnugraha et al. 2021).

Advanced Encryption Standard (AES) merupakan salah satu algoritma enkripsi yang telah terbukti efektif dalam menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), autentikasi (*authentication*), dan *non-repudiation* dalam sistem informasi akademik (Abdullah dan Aziz, 2016).

Dengan menerapkan AES, data dalam SIAKAD dapat dienkripsi sebelum disimpan atau ditransmisikan, sehingga meskipun terjadi kebocoran, informasi yang tersimpan tetap terlindungi dari penyalahgunaan. Sebagai bagian dari penelitian ini, akan dikembangkan prototipe aplikasi mobile yang mengimplementasikan algoritma AES untuk melindungi data akademik di SIAKAD Poltekad. Prototipe ini akan menampilkan fitur dasar, seperti login aman, akses nilai, dan input data mahasiswa, untuk mendemonstrasikan bagaimana enkripsi dapat meningkatkan perlindungan terhadap informasi akademik yang sensitif. Dengan meningkatnya ancaman kebocoran data dalam sistem akademik, penelitian ini diharapkan dapat berkontribusi dalam memberikan solusi keamanan berbasis enkripsi untuk menjaga kepercayaan pengguna terhadap sistem informasi akademik, serta memastikan kepatuhan terhadap regulasi perlindungan data mahasiswa seperti FERPA (*Family Educational Rights and Privacy Act*).

RANCANGAN PENELITIAN

Dalam penelitian ini, penulis memakai metode *Research and Development* (R&D) dengan tujuan memperbarui sistem yang telah ada sebelumnya dengan beberapa inovasi yang kemudian bisa di pakai untuk meningkatkan keamanan data. Mencari sebuah masalah, pengumpulan informasi data, konfigurasi sistem, tahapan uji coba, dan penilaian sistem adalah beberapa tahapan penelitian yang dilaksanakan dengan metode penelitian dan pengembangan ini.

Sugiyono (2015) menyatakan bahwa tujuan dari pendekatan penelitian dan pengembangan adalah untuk membuat *project* atau *update project* yang dulu pernah di buat lewat uji coba yang kontinyu. Penelitian ini, keseluruhan tahapan tersebut di masukan melalui proses perancangan sistem keamanan data dengan menguji keamanan data pada aplikasi android tersebut menggunakan metode AES.

POPULASI DAN SAMPEL

Dalam penelitian ini, populasi mencakup keseluruhan sistem keamanan data yang menggunakan enkripsi AES (*Advanced Encryption Standard*) dalam aplikasi siakad poltekad berbasis Android. Populasi ini mencakup berbagai aspek sistem yang berperan dalam menjaga keamanan dan integritas data, di antaranya perangkat lunak untuk pemantauan realtime, pengolahan data untuk ditampilkan dalam aplikasi, Mekanisme ekspor data yang efektif. sampel penelitian yang digunakan dalam proses penelitian ini adalah aplikasi yang

berisi server database, keamanan data, metode keamanan data. Adapun hal lain yang menjadi fokus adalah metode keamanan data enkripsi AES yang di implementasikan pada aplikasi siakad poltekad berbasis android.

TEKNIK PENGUMPULAN DATA

Pada teknik pengumpulan data pada penelitian ini, keseluruhan data dikumpulkan melalui beberapa langkah berikut:

1. **Observasi Langsung**:Observasi dilakukan dengan pengamatan langsung terhadap implementasi sistem keamanan data menggunakan enkripsi AES dalam aplikasi siakad poltekad berbasis Android. dengan melihat cara kerja sistem, kinerja aplikasi, efektivitas enkripsi AES, potensi celah keamanan. yang nantinya data tersebut dapat dijadikan evaluasi dan pembelajaran.
2. **Studi Pustaka**: Studi pustaka dilakukan untuk mengumpulkan referensi terkait sistem keamanan data dalam aplikasi berbasis android, khususnya implementasi enkripsi AES. pada penelitian terdahulu mengenai rancang bangun prototipe aplikasi siakad poltekad berbasis android dengan implementasi keamanan data menggunakan enkripsi AES.
3. **Pengujian Sistem**: Pengujian sistem dilakukan untuk mengevaluasi performa dan keamanan enkripsi AES yang diterapkan dalam aplikasi siakad poltekad seperti keamanan data, kinerja aplikasi, ketahanan sistem enkripsi.

PENGEMBANGAN INSTRUMEN

Pengembangan instrumen dalam penelitian ini bertujuan untuk memastikan bahwa data yang dikumpulkan akurat, valid, dan dapat digunakan untuk mengevaluasi efektivitas sistem keamanan data menggunakan enkripsi AES dalam aplikasi siakad poltekad berbasis android. Data tersebut adalah data tentang kinerja sistem, potensi celah keamanan, kecepatan, dan efesiensi.

TEKNIK ANALISIS DATA

Penelitian ini menggunakan metode analisis deskriptif kuantitatif untuk mengevaluasi kinerja sistem aplikasi SIAKAD POLTEKAD dalam mengolah dan menyajikan data akademik secara real-time dengan implementasi keamanan data menggunakan enkripsi AES. Tujuan dari analisis ini adalah untuk menilai efektivitas, keandalan, dan performa sistem dalam menangani data akademik, seperti nilai mahasiswa, jadwal kuliah, serta informasi administrasi lainnya.

Ghozali (2016) menyatakan bahwa analisis deskriptif kuantitatif merupakan suatu pendekatan yang tepat untuk

mengilustrasikan proses pengerjaan suatu sistem berdasarkan pada hasil data yang bisa di perhitungkan semua yang tidak bias.mengimplementasikan tahapan analisis ini, penggunaan keamanan data menggunakan enkripsi AES yang di terapkan di aplikasi siakad poltekad berbasis android ini dapat ditinjau sebagai refleksi dan evaluasi untuk memastikan bahwa teknologi yang diintegrasikan pada sistem aplikasi bisa menghasilkan keamanan yang kuat.

HASIL PENELITIAN

Penelitian ini memiliki hasil berupa Rancang Bangun Prototipe Aplikasi Siakad Poltekad Berbasis Android Dengan Implementasi Keamanan Data Menggunakan Enkripsi AES yang telah diprogram dan di uji beberapa kali. Proses dimulai saat pengguna memasukkan data melalui aplikasi mobile SIAKAD. Sebelum dikirim ke server, data dienkripsi menggunakan AES untuk melindungi informasi sensitif, seperti autentikasi pengguna, nilai akademik, dan data mahasiswa. Data terenkripsi dikirim ke REST API melalui protokol aman. Di sisi server, data didekripsi untuk diproses, lalu dienkripsi kembali sebelum disimpan ke database, memastikan keamanan selama penyimpanan. Saat pengguna mengakses kembali data, REST API mengambil informasi terenkripsi dari database, lalu mendekripsi jika diperlukan atau tetap dalam bentuk terenkripsi selama transmisi. Di perangkat pengguna, data didekripsi kembali agar hanya pengguna berwenang yang dapat membaca informasi tersebut. AES menjamin keamanan data di setiap tahap, baik saat penyimpanan maupun transmisi, mencegah akses tidak sah dan melindungi informasi akademik secara optimal. Seperti yang di jelaskan prameshwari dan sastra bahwa algoritma enkripsi AES dapat diterapkan pada aplikasi mobile untuk menjaga keamanan data, khususnya dalam proses enkripsi dan dekripsi file dokumen. Studi ini menekankan bahwa AES merupakan algoritma yang tepat untuk memastikan keamanan data pada aplikasi mobile yang memerlukan perlindungan tinggi, seperti halnya aplikasi Sistem Informasi Akademik Politeknik Angkatan Darat (Prameshwari dan Sastra, 2018).

PEMBAHASAN

Dengan menerapkan AES, data dalam siakad dapat dienkripsi sebelum disimpan atau ditransmisikan, sehingga meskipun terjadi kebocoran, informasi yang tersimpan tetap terlindungi dari penyalahgunaan. Sebagai bagian dari penelitian ini, akan dikembangkan prototipe aplikasi mobile yang mengimplementasikan algoritma AES untuk melindungi data akademik di siakad Poltekad. Prototipe ini akan menampilkan fitur dasar, seperti login aman, akses nilai, dan input data mahasiswa, untuk mendemonstrasikan bagaimana enkripsi dapat meningkatkan

perlindungan terhadap informasi akademik yang sensitif. Dengan meningkatnya ancaman kebocoran data dalam sistem akademik, penelitian ini diharapkan dapat berkontribusi dalam memberikan solusi keamanan berbasis enkripsi untuk menjaga kepercayaan pengguna terhadap sistem informasi akademik, serta memastikan kepatuhan terhadap regulasi perlindungan data mahasiswa seperti FERPA (*Family Educational Rights and Privacy Act*).

PENUTUP

Penelitian ini sudah bisa menaikan dan menerapkan rancang bangun prototipe aplikasi siakad poltekad berbasis android dengan implementasi keamanan data menggunakan enkripsi AES oleh poltekad kodiklatad. Dengan memanfaatkan teknologi Keamanan Data Menggunakan Enkripsi AES, aplikasi ini tidak hanya untuk memenuhi kebutuhan akademik, tetapi juga untuk memberikan keamanan yang optimal dalam pengelolaan data sensitif. Enkripsi data menjadi elemen penting dalam menjaga kerahasiaan dan integritas data di dalam sistem informasi ini.

Pengembangan sistem keamanan data menggunakan enkripsi AES ini memberikan solusi yang praktis dan berdaya guna untuk keamanan aplikasi siakad berbasis android, sistem keamanan ini mengambil informasi terenkripsi dari database, lalu mendekripsi jika diperlukan atau tetap dalam bentuk terenkripsi selama transmisi. Di perangkat pengguna, data didekripsi kembali agar hanya pengguna berwenang yang dapat membaca informasi tersebut. AES menjamin keamanan data di setiap tahap, baik saat penyimpanan maupun transmisi, mencegah akses tidak sah dan melindungi informasi akademik secara optimal.

. Fitur *enkripsi* di aplikasi ini terbukti memberikan dampak yang signifikan kepada peneliti sehingga ketika aplikasi siakad digunakan tidak khawatir dengan keamanan data yang rawan akan di curi atau di salahgunakan.

Sistem keamanan ini menunjukkan hasil yang baik, namun tetap diperlukan penelitian lebih lanjut untuk meningkatkan keamanan. Oleh karena itu, sistem ini dapat diimplementasikan dan dioptimalkan pada setiap satuan Angkatan Darat, khususnya di satuan poltekad kodiklatad guna untuk meningkatkan daya belajar dan kemajuan tiap satuan tersebut.

Contoh dipenelitian sebelumnya oleh Irawan dan kawan-kawan (2024) yang berjudul pengembangan aplikasi berbasis Android menekankan aspek keamanan data dengan menerapkan algoritma enkripsi AES256. Enkripsi ini bertujuan untuk melindungi kode voucher dari potensi penyalahgunaan, memastikan bahwa data sensitif tidak mudah diakses oleh pihak yang tidak berwenang.

DAFTAR PUSTAKA

Safrizal and M. A. Afkar, “SIAKAD revitalization: The latest solution in answering the challenges of digitizing education,” International Journal Software Engineering and Computer Science (IJSECS), vol. 3, no. 1, pp. 40–49, 2023, doi: 10.35870/ijsecs.v3i1.1160.

Idfiana, I. and Jakaria, D.A., 2024. Analisis Kebocoran Data Sistem Informasi Pendaftaran Mahasiswa Baru Dari Serangan SQL Injection. Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 13(1), pp.259-267.

Ibnugraha, P.D., Nugroho, L.E. and Santosa, P.I., 2021. Risk model development for information security in organization environment based on business perspectives. International Journal of Information Security, 20(1), pp.113-126

A. Prameshwari and N. P. Sastra, “Implementasi algoritma Advanced Encryption Standard (AES) 128 untuk enkripsi dan dekripsi file dokumen,” Jurnal Eksplora Informatika, vol. 8, no. 1, pp. 52–58, 2018.

A. M. Abdullah and R. H. H. Aziz, “New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm,” International Journal of Computer Applications, vol. 143, no. 4, pp. 11–17, Jun. 2016.

R. H. Irawan, U. Mahdiyah, and R. D. Kurniawan, “Implementasi algoritma AES pada aplikasi pembelian voucher hotspot berbasis Android,” Generation Journal, vol. 8, no. 1, pp. 18–26, 2024.