Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi
Penerbit ADM RUMAH PENGETAHUAN

Application of AES 256 Cryptography Algorithm OCB Mode on Student Data

Penerapan Algoritma Kriptografi AES 256 Mode OCB pada Data Mahasiswa

Nora Febitri [1]; Harry Witriyono [2]; Muntahanah [3]; Marhalim [4]
[1] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Bengkulu
Email: [1] norafebitri821@gmail.com ;[2] harrywitriyono@umb.ac.id ;[3] muntahanah@umb.ac.id ; [4] marhalim@umb.ac.id

How to Cite :
Febitri, N. Witriyono, H. Muntahanah, Marhalim. (2023). Penerapan Algoritma Kriptografi AES 256 Mode OCB pada Data Mahasiswa, Jurnal Komputer, Informasi dan Teknologi, 3 (2). DOI: https://doi.org/10.53697/jkomitek.v3i2

ARTICLE HISTORY
Received [16 November 2023]
Revised [16 Desember 2023]
Accepted [18 Desember 2023]

Keywords :
AES 256, Student Data, OCB.

ABSTRAK
Dalam era digital saat ini, data mahasiswa menjadi hal yang sangat penting dan harus dijaga keamanannya. Kriptografi merupakan suatu teknik untuk mengamankan data dari pihak yang tidak berwenang. AES 256 (*Advanced Encryption Standard 256*) adalah salah satu algoritma kriptografi yang digunakan untuk mengamankan data dengan kunci simetris dan menggunakan mode OCB (*Offset Codebook Mode*). Penerapan algoritma kriptografi AES 256 mode OCB pada data mahasiswa akan memberikan perlindungan yang lebih baik terhadap akses yang tidak sah atau manipulasi data. Hal ini akan sangat penting untuk menjaga kerahasiaan dan integritas data mahasiswa yang bersifat rahasia dan privasi seperti data pribadi, nilai, dan rekam jejak akademik. Pada penelitian ini dapat disimpulkan bahwa penggunaan AES-256 pada mode OCB adalah pilihan yang baik untuk melindungi data mahasiswa dengan tingkat keamanan yang tinggi. Kombinasi AES-256 dan OCB memberikan tingkat keamanan yang sangat tinggi untuk pengiriman data yang sensitif melalui jaringan. Mode OCB menggunakan pengkodean pesan dengan offset, yang memungkinkan penggunaan kunci yang lebih pendek, membuatnya lebih efisien daripada mode operasi enkripsi lainnya.

ABSTRACT
In today's digital era, student data is very important and must be kept secure. Cryptography is a technique for securing data from unauthorized parties. AES 256 (Advanced Encryption Standard 256) is a cryptographic algorithm used to secure data with a symmetric key and uses OCB (Offset Codebook Mode) mode. The application of the OCB mode AES 256 cryptographic algorithm to student data will provide better protection against unauthorized access or data manipulation. This will be very important to maintain the confidentiality and integrity of confidential and private student data such as personal data, grades, and academic track records. In this study it can be concluded that the use of AES-256 in OCB mode is a good choice to protect student data with a high level of security. The combination of AES-256 and OCB provides a very high level of security for sending sensitive data over the network. OCB mode uses message encoding with offset, which allows use of shorter keys, making it more efficient than other modes of encryption operation.

PENDAHULUAN

Era globalisasi modern membawa kemajuan yang sangat pesat dalam teknologi informasi dan telekomunikasi, mempermudah manusia untuk mengakses informasi dari berbagai sumber. Penggunaan komputer dalam bidang pendidikan antara lain untuk media pembelajaran berbantuan komputer termasuk e-learning, alat bantu pengolahan data akademik, dan media penyampaian informasi [1]. Namun, penggunaan teknologi informasi dan telekomunikasi juga memiliki beberapa dampak negatif seperti penyalahgunaan informasi, dan kekhawatiran tentang privasi dan keamanan data.

Data mahasiswa adalah informasi pribadi dan rahasia yang terkait dengan identitas, akademik, dan riwayat kehidupan mahasiswa yang disimpan oleh universitas atau institusi pendidikan. Dalam

pengelolaan data mahasiswa, terdapat informasi sensitif seperti identitas pribadi, dan informasi keluarga yang perlu dijaga kerahasiaannya [2].

Keamanan data yang tidak aman dapat mengakibatkan masalah serius, seperti pencurian identitas, kebocoran informasi rahasia, atau manipulasi data. Keamanan sistem informasi meliputi keamanan dari perangkat lunak, perangkat keras, kemanan jaringan, keamanan program dan keamana data yang tersimpan di dalam database. Dengan menggunakan bahasa pemrograman, dapat meningkatkan kinerja dari sebuah sistem yang dibuat. Pembuatan website ini ditujukan untuk perguruan tinggi agar memudahkan dalam penginputan data mahasiswa. Sehingga berkas-berkas yang disimpan menjadi lebih efektif dan efisien [3].

AES (Advanced Encryption Standard) 256 adalah salah satu algoritma kriptografi yang digunakan untuk mengamankan data dengan kunci simetris dan menggunakan mode OCB (Offset Codebook Mode), OCB adalah mode pengoperasian yang menggunakan kode buku offset sehingga dapat mengenkripsi dan mendekripsi data dengan efisien dan cepat [4]. OCB juga memungkinkan untuk dilakukan proses autentikasi dan integritas data sehingga dapat memastikan bahwa data yang diterima adalah data asli yang belum diubah oleh pihak yang tidak berwenang. Penerapan algoritma kriptografi AES 256 mode OCB pada data mahasiswa akan memberikan perlindungan yang lebih baik terhadap akses yang tidak sah atau manipulasi data. Hal ini akan sangat penting untuk menjaga kerahasiaan dan integritas data mahasiswa yang bersifat rahasia dan privasi seperti data pribadi dan lainnya.

kriptografi AES 256 mode OCB harus diikuti dengan kebijakan dan prosedur yang tepat untuk memastikan bahwa penggunaannya tidak menimbulkan risiko keamanan. Melihat permasalahan tersebut, maka menjaga Kemanan yang tepat dengan menggunakan Algoritma kriptografi AES 256 Mode OCB merupakan suatu teknik untuk mengamankan data dari pihak yang tidak berwenang dapat digunakan sebagai upaya meningkatkan tingkat keamanan terhadap data yang ada di dalam basis data sehingga meminimalisir terjadi pencurian data.

LANDASAN TEORI

Penelitian Terkait

Dalam penelitian ini, penulis sedikit banyak mengambil referensi dari penelitian-penelitian sebelumnya yang berkaitan dengan topik pada penelitian ini. Penelitian ini yang dilakukan oleh Rinaldi Munir pada tahun 2019 yang berjudul Kriptografi *ADVANCED ENCRYPTION STANDARD (AES*). Penelitian tersebut menghasilkan kesimpulan bahwa kriptografi menggunakan metode klasik dan modern dapat membantu para programer agar dapat menjaga keamanan data. Keamanan informasi meliputi banyak aspek, pencegahan dari pengaksesan informasi oleh pihak-pihak yang tidak berhak, melindungi kerahasiaan informasi yang bersifat privasi, pencegahan dari usaha untuk mengubah informasi.

Penelitian yang dilalukan oleh Voni Yunianti, Gani Indriyanta dan Antonius Rachmat pada tahun 2009 yang berjudul Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File. Penelitian ini menghasilkan kesimpulan sebagai berikut, dalam penelitian ini, file dekripsi dapat kembali seperti ekstensi file sumber karena saat sistem melakukan proses enkripsi ditambahkan header untuk menyimpan informasi ekstensi file sumber. Oleh karena itu, ukuran file enkripsi akan bertambah 11 byte dari ukuran file asli. Sedangkan ukuran file dekripsi akan kembali ke ukuran file asli.Waktu yang diperlukan untuk proses enkripsi pada penelitian ini tidak sama dengan waktu proses dekripsi yang dikarenakan adanya pemakaian *resource* komputer.

Penelitian yang dilakukan oleh Hyo-Won Kim, Su-Hyun-Kim, Sun Kang dan Taejoo Chang.Pada tahun 2008 yang berjudul ***Fast Implementation of a 128bit AES Blok Chiper Algoritm OCB Mode Using a High Performance DSP***.Arti(Implementasi Cepat Mode OCB Algoritma Cipher Blok AES 128 bit Menggunakan DSP Kinerja Tinggi), Penelitian tersebut menghasilkan kesimpulan Dalam makalah ini, metode yang efisien untuk mengoptimalkan algoritma cipher blok AES 128bit mode OCB menggunakan DSP kinerja tinggi diusulkan. Di antara skema enkripsi yang diautentikasi, diketahui bahwa mode OCB kira-kira dua kali lebih cepat daripada mode CBC-MAC. Proses optimisasi dilakukan dengan membuka kode sumber AES OCB yang didesain dalam bahasa C menggunakan DSP c-compiler.Sebagai hasil simulasi, kinerja enkripsi/dekripsi dari cipher blok yang diimplementasikan adalah 401Mbps, masing-masing 406Mbps pada kecepatan clock 1GHz. Hasil ini sesuai dengan 50% lebih cepat dari implementasi umum dengan penggunaan memori 3,5% lebih banyak.

Penelitian ini dilakukan oleh Harry Witriyono dan Sandhy Fernandez pada tahun 2021 yang berjudul Enkripsi Base 64, Hashing SHA1 dan MD5 pada QR Code Presensi Kuliah**.** Penelitian tersebut menghasilkan kesimpulan bahwa Penelitian berhasil menerapkan enkripsi Base 64 dan hasing SHA1 dan MD5 sehingga terbentuk kode QR yang hasil uraian isinya lebih aman karena terenkripsi dan menjadi tulisan yang berisi kode yang tidak dapat langsung dimengerti oleh manusia. Pengurangan kecurangan

mahasiswa dalam prosesnya dapat dilakukan dengan penguncian IP address ter-hashing yang tidak dapat langsung diartikan oleh manusia Penggunaan presensi kode QR membantu memberikan solusi bagi kebutuhan proses presensi perkuliahan sebaga indikator kinerja dosen dan mahasiswa baik pada perkuliahan luring ataupun perkuliahan daring yang menggunakan Learning Management System seperti Moode dan Google Classroom, dan aplikasi media sosial seperti Whatsapp dan Telegram.

1. ***Kriptografi***

Penggunaan kriptografi sangat penting dalam melindungi informasi sensitif dan data pribadi dari pihak yang tidak berhak. Kriptografi adalah salah satu cara untuk mencegah kebocoran data yang bersifat rahasia [5]. Kunci rahasia tersebut harus diamankan dan tidak dapat diakses oleh pihak yang tidak berhak. Data mahasiswa menjadi aman dan sekaligus memberikan kemudahan dalam prosesnya serta terjaganya otentikasi asal datanya[6].

2. ***AES (Advance Encryption Standard)***

Advanced Encryption Standard metode yang sangat tepat digunakan untuk mengamankan data-data yang penting , Advanced Encryption Standard adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini [7]. Inilah ukuran blok dan kunciyang ditetapkan secara independen Advanced Encryption Standard memiliki panjang kunci variasi dari AES128, AES192 dan AES256 [8].

3. **OCB (*Operasi Cipher Blok*)**

Operasi Cipher Blok yang menggunakan teknik enkripsi untuk mengamanankan data dengan memecah pesan menjadi blok-blok yang sama ukurannya, dan setiap blok akan dienkripsi secara terpisah dengan menggunakan kunci enkripsi yang sama. Tujuan dari operasi Cipher Blok adalah untuk menjaga kerahasiaan data dan kunci enkripsi, serta membuat pola data menjadi lebih sulit untuk dibaca atau diretas. Mode *Operasi Block-Cipher* (OCB) adalah dalam pengaturan keamanan yang santai sehingga bahwa keamanan mereka diyakini secara luas bertahan memberikan privasi dan keaslian dengan tujuan ini disebut skema enkripsi-autentikasi OCB dirancang sebagiaan besar sebagai tanggapan terhadap aktivitas mode operasi *National Institute of Standards and Technology* (NIST)[4].

4. **Flowchart**

Representasi secara simbolik dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, pengembangan perangkat lunak atau sistem informasi dan menemukan solusi yang tepat. Dengan menggunakan *flowchart* akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisis masalah, disamping itu *flowchart* juga berguna sebagai fasilitas untuk berkomunikasi antara pemrogram yang bekerja dalam tim suatu proyek [9].

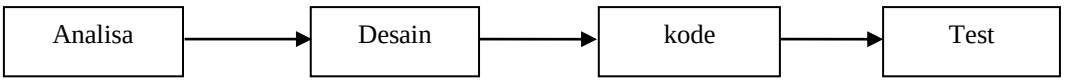
5. ***Data Flow Diagram (DFD)***

DFD dapat membantu dalam memvisualisasikan alur data atau informasi dari sumber data hingga output data yang dihasilkan, sehingga dapat membantu dalam memahami bagaimana data bergerak dalam suatu sistem atau proses bisnis. Menurut Hartono (1999). Data Flow Diagram (DFD) adalah diagram yang menggunakan notasi simbol untuk menggambarkan arus data sistem. Kita dapat menggunakan DFD untuk dua hal utama yaitu untuk membuat dokumentasi dari sistem informasi yang ada, atau untuk menyusun dokumentasi untuk sistem informasi yang baru [10].

METODE PENELITIAN

Metode pengembangan sistem yang akan penulis gunakan adalah metode incremental. Metode Incremental akan menerapkan rekayasa perangkat lunak yang akan membagi tugas hingga menghasilkan perangkat lunak yang lengkap. Proses akan berhenti jika sudah mencapai seluruh fungsi yang diharapkan. Tahapan-tahapannya adalah sebagai berikut:

Gambar 1 Metode Incremental



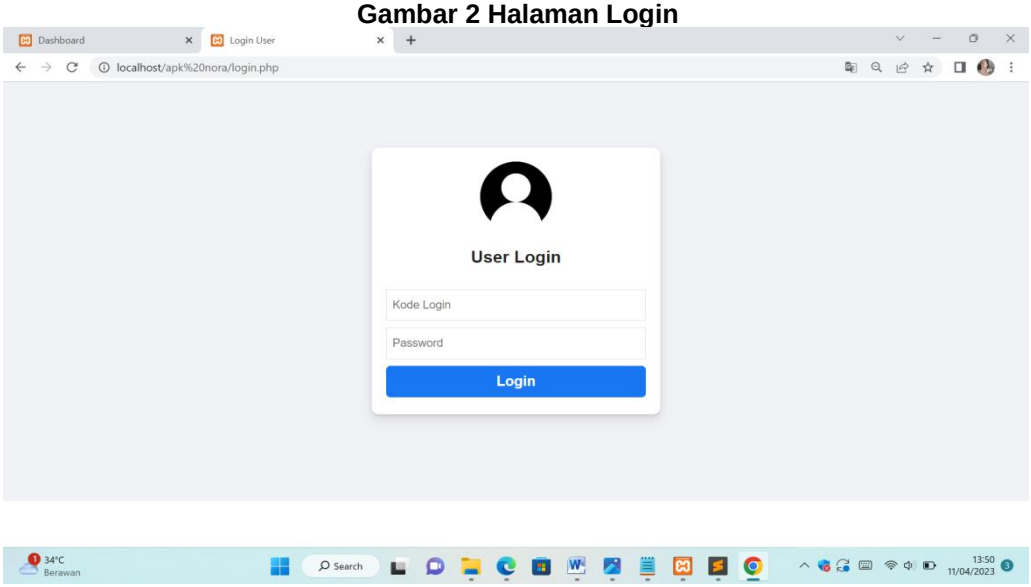
HASIL DAN PEMBAHASAN

Aplikasi penerapan kriptografi AES-256 mode OCB pada data mahasiswa dalam mengamankan data mahasiswa telah berhasil penulis bangun menggunakan Bahasa pemrograman php dan database MySQL. Aplikasi terdiri dari beberapa halaman, yaitu halaman login, halaman dashboard, halaman input, halaman angkatan.

Halaman Menu Login

Menu login digunakan untuk mengakses sistem. From login tersebut terdiri dari dua field, yaitu kode login dan password, dimana pengguna dapat memasukkan informasi yang diminta. Terdapat juga tombol Login, yang memungkinkan pengguna untuk melakukan aksi terkait login. Menu Login dapat dilihat pada gambar di bawah ini sebagai berikut.

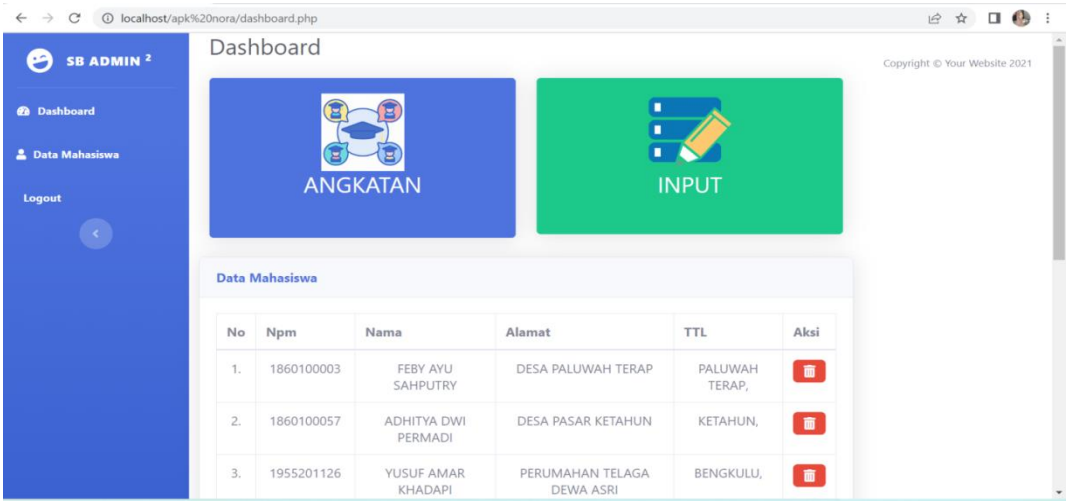
Gambar 2 Halaman Login



Halaman Menu Dashboard

Pada menu tampilan awal dilengkapi dengan fitur-fitur menu yaitu terdapat 2 pilihan, yaitu halaman angkatan dan halaman input. Pada menu dashboard menampilkan beberapa tabel data mahasiswa yang di simpan dari proses input data yang telah dilakukan oleh admin. Dengan adanya menu dashboard, pengguna dapat dengan mudah memantau dan mengelola kinerja aplikasi atau sistus web, serta membuat keputusan yang tepat dan akurat berdasarkan informasi yang tersaji di dalamnya.

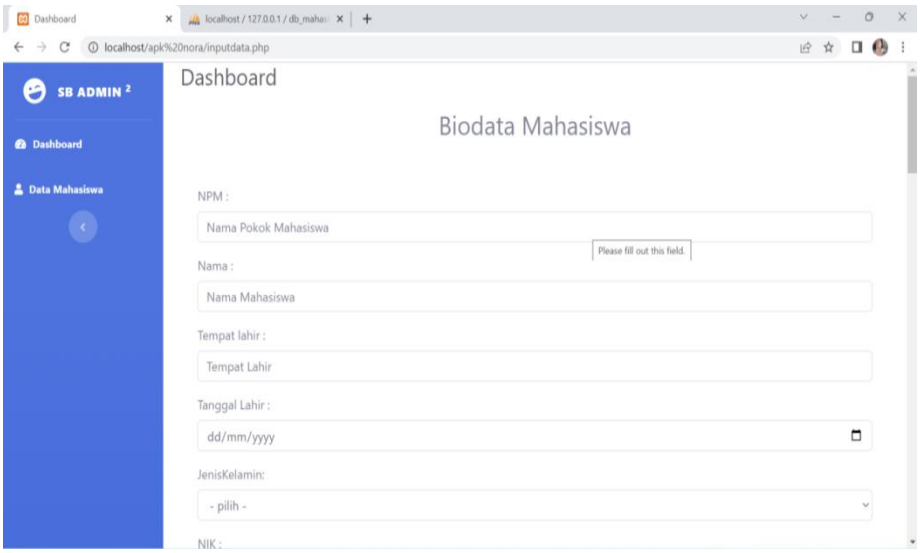
Gambar 3 halaman menu dashboard



Halaman Menu Input

Pada halaman menu input yang digunakan untuk memasukkan atau menginput ke dalam sebuah sistem atau aplikasi, seperti pembuatan data mahasiswa, data yang telah diinput oleh pengguna melalui form penginputan. Dalam proses menyimpanan data, data-data tersebut akan melalui proses enkripsi terlebih dahulu menggunakan algoritma AES-256 Mode OCB. Setelah dienkripsi data tersebut akan disimpan kedalam database sistem, dalam bentuk chipertext.

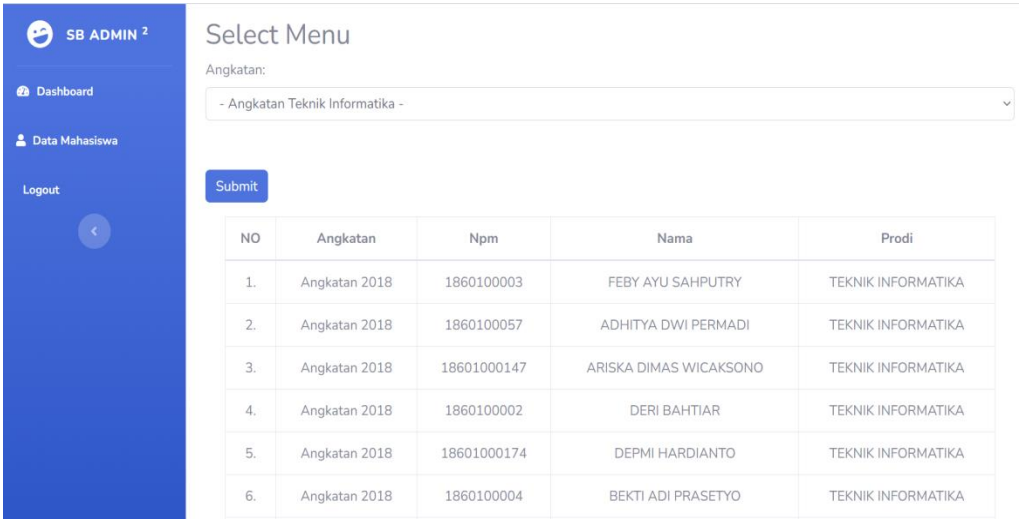
Gambar 4 Halaman input data



Halaman Menu Angkatan

Pada halaman ini ada beberapa angkatan yang sudah diinput, data-data tersebut akan tersusun sesuain angkatan menghindari tergabungnya semua angkatan yang membuat resiko tidak rapi dan susah mencari sesuai angkatan

Gambar 5 Halaman menu angkatan

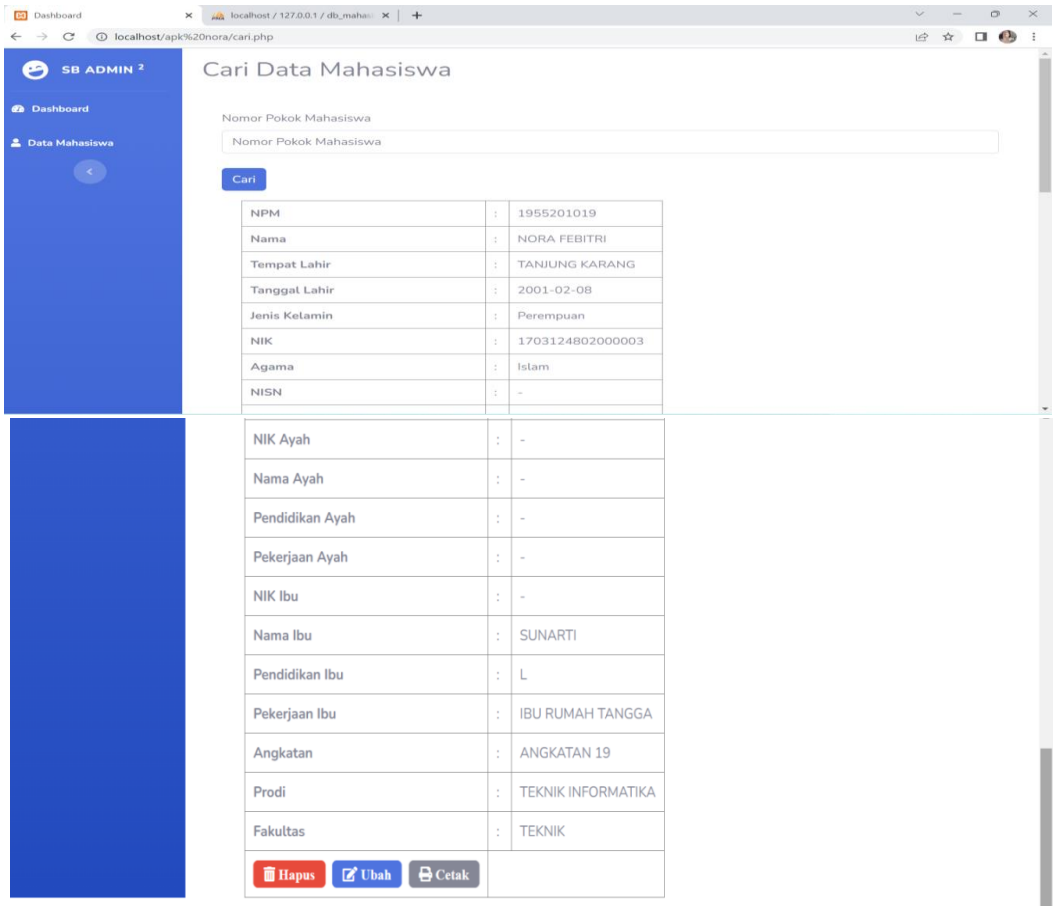


NO	Angkatan	Npm	Nama	Prodi
1.	Angkatan 2018	1860100003	FEBY AYU SAHPUTRY	TEKNIK INFORMATIKA
2.	Angkatan 2018	1860100057	ADHITYA DWI PERMADI	TEKNIK INFORMATIKA
3.	Angkatan 2018	18601000147	ARISKA DIMAS WICAKSONO	TEKNIK INFORMATIKA
4.	Angkatan 2018	1860100002	DERI BAHTIAR	TEKNIK INFORMATIKA
5.	Angkatan 2018	18601000174	DEPMI HARDIANTO	TEKNIK INFORMATIKA
6.	Angkatan 2018	1860100004	BEKTI ADI PRASETYO	TEKNIK INFORMATIKA

Halaman Cari Data Mahasiswa

Pada halaman ini mempermudah pencarian data mahasiswa yang sulit dijangkau, ada fitur ngprint data,memperbarui atau mengubah data-data dan hapus data yang terkait dengan mahasiswa yang terdaftar dalam suatu sistem informasi. Didalam menu ini terdapat beberapa kolom-kolom yang wajib diisi dengan data yang baru atau data yang telah diperbarui.

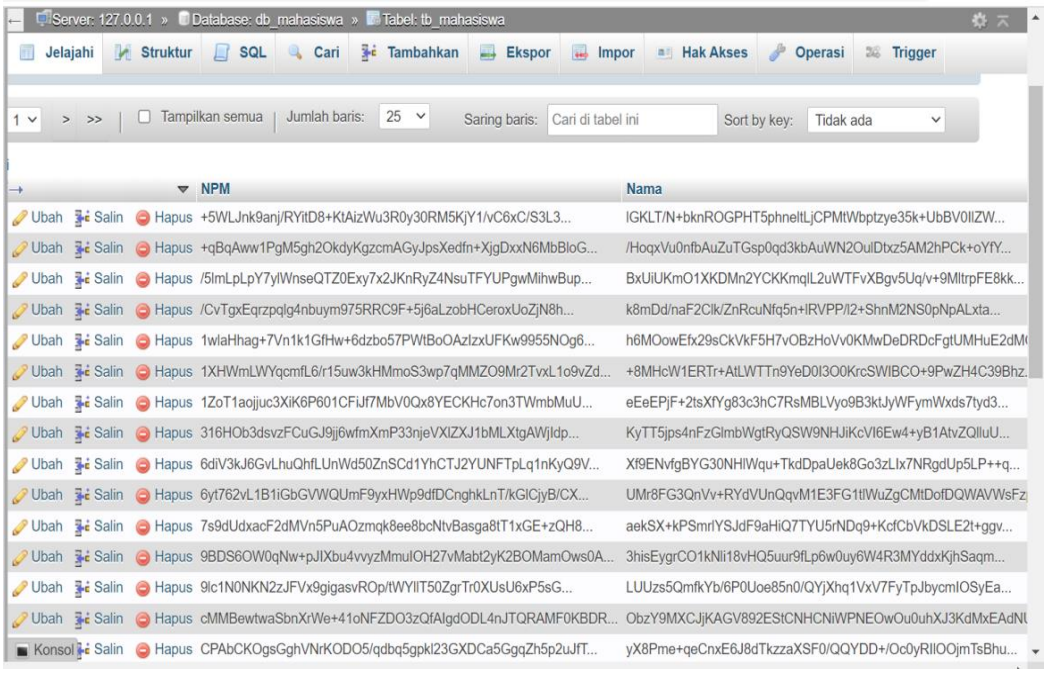
Gambar 6 Halaman menu cari data

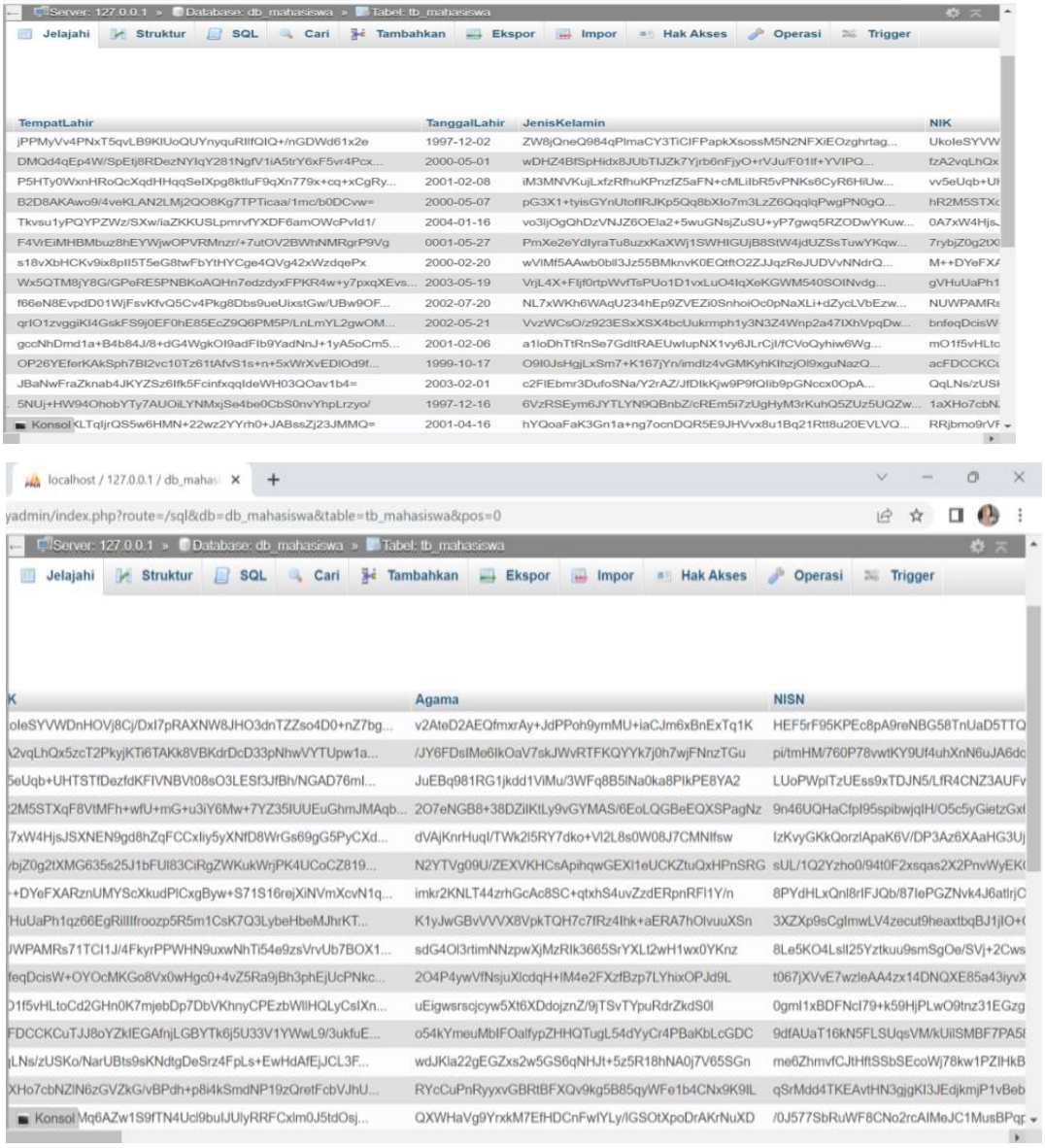


Pengujian Algoritma Pada Database

Penerapan keamanan menggunakan algoritma AES-256 Mode OCB pada *database* dapat dilihat pada gambar berikut:

Gambar 7 Halaman Pengujian Algoritma Pada Database





Gambar diatas merupakan hasil menggunakan dengan algoritma AES 256 Mode OCB. Keuntungan dari menggunakan mode OCB adalah memperkenalkan efek domino pada enksipsi dan deskripsi blok. Efek ini membuat perubahan pada satu bit suatu blok mempengaruhi blok-blok selanjutnya. Hal ini membuat hasil enkripsi lebih sulit dipecahkan dengan teknik kriptanalis tertentu. Efek domino juga membuat OCB lebih aman terhadap serangan *ciphertext-only* dan *know-plaimtext attack*. Dalam proses deskripsi jika ada satu blok data yang rusak atau diubah, hal ini akan mempengaruhi seluruh blok data yang berada setelahnya dalam rantai blok yang terenkripsi. Ini dapat memyembabkan data yang telah dienkripsi menjadi tidak dapat dibaca atau bahkan menjadi tidak valid.

Pengujian algoritma pada database adalah proses untuk menguji keandalan dan kinerja suatu algoritma kriptografi AES 256 mode OCB yang digunakan dalam sistem database. Algoritma pada database digunakan untuk mengoptimalkan proses akses data, penyimpanan, dan pengolahan data dalam database.

Pengujian algoritma pada database dapat dilakukan dalam beberapa tahapan, antara lain:

1. Pengujian fungsional: Pengujian ini bertujuan untuk menguji apakah algoritma yang digunakan dalam database dapat berfungsi sesuai dengan yang diharapkan. Contohnya adalah menguji kemampuan algoritma untuk melakukan pencarian data, penyimpanan data, atau mengubah data.

2. Pengujian keamanan: Pengujian ini bertujuan untuk menguji keamanan algoritma dalam melindungi data di dalam database dari ancaman keamanan, seperti serangan hacker atau akses yang tidak sah.
3. Pengujian skalabilitas: Pengujian ini bertujuan untuk menguji kemampuan algoritma dalam menangani penambahan data atau perubahan struktur database dengan jumlah data yang semakin besar.

Dalam melakukan pengujian algoritma pada database, diperlukan spesifikasi dan kriteria pengujian yang jelas dan terdefinisi dengan baik. Hal ini bertujuan untuk menghindari terjadinya kesalahan dalam proses pengujian dan memastikan bahwa hasil pengujian dapat diinterpretasikan dengan benar.

Selain itu, pengujian algoritma pada database juga harus dilakukan dalam lingkungan yang representatif dengan penggunaan yang realistis. Hal ini akan memastikan bahwa pengujian dapat memberikan hasil yang valid dan dapat diterapkan dalam penggunaan sehari-hari. Penggunaan IV pada AES 256 OCB dapat menghasilkan ciphertext yang aman dan tidak dapat dipecahkan bahkan jika serangan terdapat kunci dilakukan. Oleh karena itu, IV sangat penting dalam memastikan keamanan.

Pengujian Kecepatan Hasil Enkripsi Dan Dekripsi

Pengujian selanjutnya yang dilakukan dengan memfokuskan terhadap sisi kecapatan dan hasil enkripsi yang berupa banyak karakter sebelum dan sesudah dienkripsi menggunakan algoritma kriptografi AES-256-OCB.

Tabel 1 Pengujian Kecepatan Hasil

Pengujian CRUD	Jumlah data	Kecepatan	Keterangan
Input Data	31 data diinput	1.5974 ms	Enkripsi data
Cari data	2 data ditampilkan	0.0037 ms	Dekripsi data
Edit Data	31 data diedit	1.4066 ms	Dekripsi data

Dari pengujian pada tabel diatas diketahui bahwa kecepatan enkripsi dan dekripsi tidak selalu sama di setiap melakukan proses enkripsi, akan tetapi bergantung dengan spesifikasi *hardware* atau alat yang digunakan. Hasil pengujian kecepatan AES 256 Mode OCB digunakan untuk menentukan apakah algoritma ini cocok untuk digunakan dalam aplikasi yang membutuhkan keamanan yang tinggi dan pemrosesan data yang cepat.

Namun, perlu diingat bahwa keamanan data adalah faktor yang lebih penting daripada kecepatan pemrosesan data, sehingga pilihan algoritma kriptografi harus didasarkan pada keamanan yang diinginkan terlebih dahulu, baru kemudian dipertimbangkan faktor kecepatannya.

KESIMPULAN DAN SARAN

Kesimpulan

Penggunaan AES-256 pada mode OCB adalah pilihan yang baik untuk melindungi data mahasiswa dengan tingkat keamanan yang tinggi. Kombinasi AES-256 dan OCB memberikan tingkat keamanan yang sangat tinggi untuk pengiriman data yang sensitif melalui jaringan.Mode OCB menggunakan pengkodean pesan dengan offset, yang memungkinkan penggunaan kunci yang lebih pendek, membuatnya lebih efisien daripada mode operasi enkripsi lainnya.

Namun, penting untuk diingat bahwa meskipun enkripsi AES-256 pada mode OCB memberikan tingkat keamanan yang sangat tinggi, tidak ada sistem keamanan yang sepenuhnya tidak dapat ditembus. Oleh karena itu, selalu penting untuk menggunakan lapisan keamanan tambahan dan mengikuti praktik keamanan terbaik saat mengirimkan data yang sensitif. Pastikan bahwa data mahasiswa dapat diakses oleh pihak yang berwenang dengan cara yang aman dan mudah diakses.pastikan bahwa deskripsi mudah diggunakan danaman bagi pengguna yang berhak mengakses data.

Saran

1. Pastikan kunci enkripsi Anda aman dan disimpan dengan baik. Memilih kunci yang kuat dan menghindari penggunaan kunci yang sama untuk semua data penting. Selain itu, pastikan kunci disimpan dengan aman dan hanya diakses oleh orang yang memiliki hak akses yang tepat.
2. Pastikan bahwa sistem enkripsi Anda memenuhi standar keamanan yang tepat. Pastikan bahwa sistem enkripsi yang digunakan diatur dan dikonfigurasi dengan benar dan memenuhi standar keamanan yang disarankan. Anda juga dapat melakukan tes keamanan untuk memastikan bahwa sistem enkripsi Anda berfungsi dengan baik dan tidak rentan terhadap serangan.
3. Jangan mengandalkan enkripsi sebagai satu-satunya lapisan keamanan. Pastikan bahwa data mahasiswa juga dilindungi oleh tindakan keamanan lainnya, seperti autentikasi pengguna, firewall, dan sistem deteksi intrusi. Menggabungkan lapisan keamanan yang berbeda dapat meningkatkan tingkat keamanan secara keseluruhan.

DAFTAR PUSTAKA

Y. Utama, “Sistem Informasi Berbasis Web Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Sriwijaya,” *J. Sist. Inf.*, vol. 3, no. 2, pp. 359–370, 2011.

M. Alfan Rosid and S. Sumarno, “Rancangan Sistem Presensi Mahasiswa Menggunakan Qr Code Dengan Fitur Geolocation Dan Enkripsi Aes,” *JIKA (Jurnal Inform.*, vol. 5, no. 2, p. 167, 2021, doi: 10.31000/jika.v5i2.4052.

I. P. Sari, A. Jannah, A. M. Meuraxa, A. Syahfitri, and R. Omar, “Perancangan Sistem Informasi Penginputan Database Mahasiswa Berbasis Web,” *Hello World J. Ilmu Komput.*, vol. 1, no. 2, pp. 106–110, 2022, doi: 10.56211/helloworld.v1i2.57.

P. Rogaway, M. Bellare, and J. Black, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption,” *ACM Trans. Inf. Syst. Secur.*, vol. 6, no. 3, pp. 365–403, 2003, doi: 10.1145/937527.937529.

M. Metode Blowfish Dengan Bahasa Pemrograman Java Mohamad Natsir, K. Kunci, K. Simetris, and A. Blowfish, “Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office,” *Jurnal*, vol. 6, pp. 2089–5615, 2016.

H. Witriyono and S. Fernandez, “Enkripsi Base 64, Hashing SHA1 dan MD5 pada QR Code Presensi Kuliah,” *JSAI (Journal Sci. Appl. Informatics)*, vol. 4, no. 2, pp. 263–272, 2021, doi: 10.36085/jsai.v4i2.1680.

F. Muharram, H. Azis, and A. R. Manga, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES),” *Proc. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

Asiyanik, “Studi Terhadap Advanced Encryption Standard (Aes) DanAlgoritma Knapsack Dalam Pengamanan Data,” *Santika*, vol. 7, no. Jurnal Ilmiah Sains dan Teknologi, pp. 553–561, 2017.

M. I. Suri and A. S. Puspaningrum, “Sistem Informasi Manajemen Berita Berbasis Web,” *J. Teknol. dan Sist. Inf.*, vol. 1, no. 1, pp. 8–14, 2020, doi: 10.33365/jtsi.v1i1.128.

Rina Noviana, “Pembuatan Aplikasi Penjualan Berbasis Web Monja Store Menggunakan Php Dan Mysql,” *J. Tek. dan Sci.*, vol. 1, no. 2, pp. 112–124, 2022, doi: 10.56127/jts.v1i2.128.

“MEMBANGUN APLIKASI E-LIBRARY MENGGUNAKAN HTML, PHP SCRIPT, DAN MYSQL DATABASE Rini Sovia dan Jimmy Febio,” vol. 6, no. 2, pp. 38–54, 2011.

S. Santoso and R. Nurmalina, “Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas,” *J. Integr.*, vol. 9, no. 1, p. 84, 2017, doi: 10.30871/ji.v9i1.288.

Fatimah and Samsudin, “Perancangan Sistem Informasi E-Jurnal Pada Prodi Sistem Informasi Diuniversitas Islam Indragiri,” *J. Perangkat Lunak*, vol. 1, no. 1, pp. 33–49, 2019, doi: 10.32520/jupel.v1i1.782.

Santoso and R. Nurmalina, “Pelatihan Desain Web Bagi Umkm Menggunakan,” vol. 3, no. 3, pp. 1466–1472, 2022.

B. A. B. Ii and A. P. Aplikasi, “No Title,” pp. 5–42, 2008.