PELITA TEKNOLOGI
Journal homepage: jurnal.pelitabangsa.ac.id, p-ISSN: 2301-475X, e-ISSN: 2656-7059

Penerapan Algoritma AES (*Advanced Encryption Standard*) Untuk Meningkatkan Keamanan Data Pribadi

Wahyu Rahadian Seto

Program Studi Informatika, Universitas Bhayangkara Jakarta Raya
Jl. Raya Perjuangan No.81, RT.003/RW.002, Marga Mulya, Kec. Bekasi Utara, Kota Bks, Jawa Barat 17143
Korespondensi email: akuwahyu009@gmail.com

Abstrak

Data security is one of the most crucial aspects in today's digital era. When it comes to storing and transmitting personal data, it is highly sensitive, and proper protection is necessary to prevent unauthorized access and potential misuse of information. One effective method to ensure data confidentiality is through the use of strong encryption algorithms, and one internationally recognized encryption algorithm is the Advanced Encryption Standard (AES). The aim of this research is to implement the AES algorithm to enhance the security of personal data. This study will examine and analyze the implementation of AES in an application involving the transmission and storage of personal data. Furthermore, it will involve testing and evaluating the security of the applied AES algorithm. The research methodology employed in this study is research and development.

Informasi Artikel

Diterima: 07 Desember 2024
Direvisi: 07 Februari 2024
Dipublikasikan: 27 Maret 2024

Keywords

Data Encryption, Data Security, Advanced Encryption Standard Algorithm.

I. Pendahuluan

Perkembangan teknologi informasi telah membawa perubahan dalam banyak aspek kehidupan seiring dengan kemajuan teknologi dalam era digital ini, pertukaran data dan informasi melalui komputer dan jaringan telah menjadi sangat umum. Namun, semakin banyaknya serangan siber dan pelanggaran keamanan yang dilaporkan menunjukkan bahwa perlindungan data sangat penting dalam memastikan kerahasiaan dan integritas informasi yang kita kirim dan terima. Pengamanan data pribadi merupakan salah satu aspek yang paling penting. Banyak organisasi dan individu mengabaikan pengamanan data pribadi sehingga keamanan suatu data dalam organisasi atau individu masih lemah. Suatu organisasi ataupun individu seringkali menyimpan dan mentransfer data

yang sensitif, seperti informasi pribadi, keuangan, atau bisnis yang tidak terproteksi. Oleh karena itu, diperlukan langkah-langkah yang efektif untuk melindungi data tersebut dari akses yang tidak sah. Untuk mengatasi masalah tersebut salah satu metode yang telah terbukti sangat aman dalam mengamankan data adalah dengan menggunakan algoritma enkripsi. Enkripsi adalah proses mengubah data asli menjadi bentuk yang tidak terbaca, yang hanya dapat diubah kembali menjadi bentuk semula oleh pihak yang memiliki kunci enkripsi yang sesuai.

Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunkan untuk mengamankan data. Algoritma AES adalah *block chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*; sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext* [6] Berdasarkan penelitian sebelumnya [5] .Penelitian tersebut menghasilkan kesimpulan bahwa algoritma *Caesar Cipher* dan AES-128 CBC menjadi algoritma yang bagus untuk mengamankan data dengan korelasi sebesar 0,257 dan *entropy* 5,75. Namun nilai *avalanche effect* yang kecil yakni 11,30%.[5]

II. Metodologi

Dalam penelitian ini, digunakan metode penelitian pengembangan *atau Research & Development* (R&D), Dengan metode *Waterfall* yang terdiri dari:

1. Analisis Kebutuhan (*Requirements Analysis*):

   Pada tahap ini, kebutuhan pengguna dan persyaratan sistem yang diinginkan dikumpulkan dan dianalisis secara menyeluruh.

2. Perancangan (*Design*):

   Tahap perancangan melibatkan merancang struktur dan arsitektur sistem berdasarkan kebutuhan yang telah dianalisis. Desain meliputi desain sistem secara keseluruhan, desain antarmuka pengguna, desain basis data, dan desain modul atau komponen perangkat lunak.

3. Implementasi (*Implementation*):

   Tahap implementasi melibatkan pembuatan dan pengkodean perangkat lunak berdasarkan desain yang telah dibuat sebelumnya. Kode program ditulis, modul atau komponen perangkat lunak dibangun, dan integrasi antara modul-modul dilakukan.

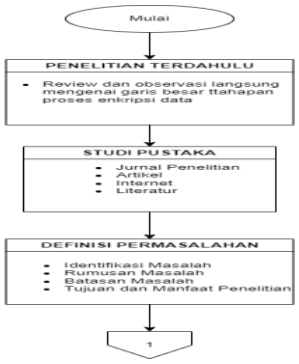
4. Pengujian (*Testing*):

   Pada tahap pengujian, perangkat lunak diuji untuk memastikan bahwa ia berfungsi dengan benar dan sesuai dengan kebutuhan yang telah ditentukan. Tes dilakukan untuk mendeteksi bug, kesalahan logika, dan memverifikasi bahwa sistem memenuhi persyaratan fungsional dan non-fungsional.

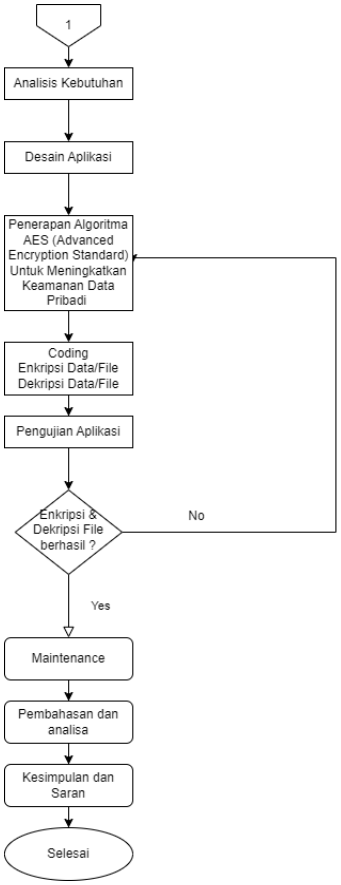
5. Pemeliharaan (*Maintenance*):

   Setelah perangkat lunak telah selesai dan dirilis, tahap pemeliharaan dimulai. Pemeliharaan meliputi perbaikan bug, pembaruan perangkat lunak, dan peningkatan fungsionalitas berdasarkan umpan balik pengguna.

Penelitian dilakukan dengan mengikuti alur peneltian sebagai berikut:

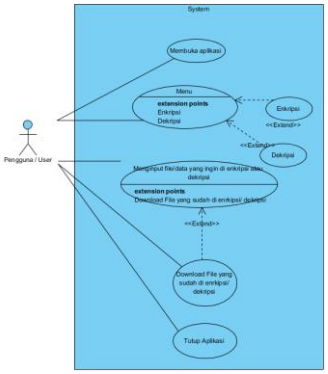


Gambar 1 Kerangka Penelitian



Gambar 2 Kerangka Penelitian Lanjutan

Desain sistem adalah tahap awal dalam melakukan pada pembuatan aplikasi. Pada tahap ini Fungsi fungsi dalam sistem aplikasi yang dikembangkan. Disajikan pada usecase gambar. Desain sistem akan menjadi acuan dalam pembuatan aplikasi



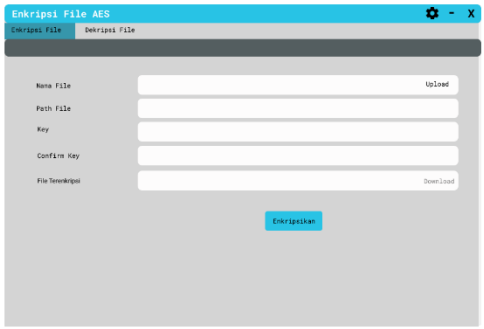
Gambar 1 *Use Case* Aplikasi

III. Hasil dan Pembahasan

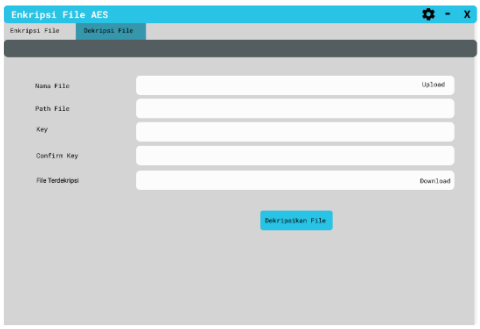
Data yang digunakan dalam penelitian ini adalah sejumlah data pribadi yang beragam, termasuk informasi pribadi seperti nama ,tanggal lahir, nomor identitas, nomor telepon, dan data sensitif lainnya. Data ini merupakan representasi data pribadi yang umumnya harus dijaga kerahasiaannya, baik dalam konteks organisasi maupun individu.

Pada tahap ini, algoritma AES diimplementasikan pada data pribadi yang telah dikumpulkan. Implementasi dilakukan dengan menggunakan perangkat lunak atau bahasa pemrograman yang mendukung algoritma AES. Dalam implementasi, data pribadi dienkripsi menggunakan algoritma AES dengan kunci yang relevan.

Gambar 2 Tampilan Antarmuka Awal Aplikasi



Gambar 3 Tampilan Antarmuka Menu Enkripsi *File*



Gambar 4 Tampilan Antarmuka Menu Dekripsi *File*

Setelah data pribadi dienkripsi menggunakan algoritma AES, dilakukan analisis untuk mengevaluasi tingkat keamanan yang dihasilkan. Analisis ini melibatkan pengujian terhadap data terenkripsi untuk memastikan bahwa data tersebut tidak dapat diakses atau dipahami tanpa kunci yang benar dan juga dilakukan pengujian integritas data. Melalui uji coba, dilakukan pengecekan apakah data terenkripsi tetap utuh dan tidak mengalami perubahan atau manipulasi yang tidak sah. Modifikasi atau perubahan data yang terjadi harus terdeteksi dan dianggap sebagai kegagalan dalam menjaga integritas data berikut adalah contoh data yang diuji :

Tabel 1 Tabel Plainteks Data Pribadi

NAMA	: WAHYU ETO
TTL	: BEKASI 4 JUNI 1940
EMAIL	: WWW.TEST@GMAIL.COM
PEKERJAAN	: KARYAWAN SWASTA
NO HP	: 088211019241
INSTITUT	: UNIVERSITAS BHAYANGKARA JAKARTA RAYA
NIK	: 32101205015915152
NPWP	: 8200.125.1-05125.00
NO REK	: 3150022151
STATUS	: AKTIF

Dilakukan pengujian enkripsi file berupa data pribadi dengan hasil berupa *ciperteks.*

Tabel 2 Tabel *Ciperteks* Hasil Enkripsi

O2ErOqqVZMTdYKBw6+fGDN
EicmjsAp/+L9aJoV54+NcyxpUjx
v3kivV3Ay5NTo5Q4wJVoo0gO3
awvZIJ/kdiSRqK2b9k9nhNIRg2H
gxf1aUGrnsfs5A8qnZ/rQ4xivnxw
rdeghZvzch5iziJqnmSjlRtRwxwd
12Vf/x67bYIwldphvpiSJX/rCO8j
XLGWx6f8/7X2xR8n0Wg5fLmP
ZFv2xJNfXGi5s3W2e2p/USY4g
UVslyZS/Ua8p4m5vJEJu08WCyx
eCeInOU6odRR/maRa1mks0xLP
KJ1SN6HVIErDcs9PyBtkbeWeW
L8PDjHsDiaZj5+PEn1BzpRvI+un
Sao32hrM9frCNlrEvKIw4YywF0
=

Setelah pengujian enkripsi file selesai, dilakukan beberapa uji lainnya untuk membandingkan ukuran file awal dengan file yang terenkripsi.

Tabel 3 Perbandingan Ukuran File

Nama File	Ukuran File Awal	Ukuran File Sesudah Enkripsi
DATA PRIBADI WAHYU	293 bytes	364 bytes
DATA PRIBADI REZA	298 bytes	384 bytes
DATA PRIBADI SETO	298 bytes	384 bytes
DATA PRIBADI RETNO	234 bytes	320 bytes

Hasil dari analisis keamanan data akan dievaluasi untuk mengevaluasi keefektifan algoritma AES dalam menjaga kerahasiaan data pribadi adalah cukup baik. Pengujian integritas data telah dilakukan dan mendapatkan hasil bahwa data yang telah terenkripsi masih tetap sama setelah dikembalikan seperti semula . Selanjutkan

Evaluasi dilakukan dengan membandingkan tingkat keamanan yang diperoleh dengan standar keamanan yang telah ditentukan sebelumnya. Algoritma AES mempunyai keamanan yang kuat namun ukuran data menjadi sedikit lebih besar dibandingkan dengan enkripsi algoritma BASE64

IV. Kesimpulan

Penelitian ini bertujuan untuk menerapkan algoritma AES (*Advanced Encryption Standard*) dalam meningkatkan keamanan data pribadi. Dalam melakukan penerapan, data pribadi dienkripsi menggunakan algoritma AES dengan kunci yang relevan. Setelah itu, dilakukan analisis terhadap keamanan data yang terenkripsi, meliputi kerahasiaan, integritas, dan kekuatan kunci. Hasil evaluasi menunjukkan bahwa penggunaan algoritma AES efektif dalam menjaga kerahasiaan data pribadi dengan tingkat keamanan yang tinggi. Berdasarkan hasil dari Penerapan Algoritma AES (*Advanced Encryption Standard*) Untuk Meningkatkan Keamanan Data Pribadi ini dapat disimpulkan bahwa pengamanan data pribadi menggunakan enkripsi data yang disimpan tidak akan dapat terbaca secara langsung yang mana enkripsi data efektif dalam meningkatkan keamanan data pribadi. Perubahan ukuran file awal dan sesudah enkripsi tidak terlalu signifikan sehingga data yang tersimpan tidak memenuhi tempat.

Daftar Pustaka

[1] C Aulia, R., Zakir, A., & Purwanto, D. A. "Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem". InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 2(2), 146-15111.2. 2018

[2] A., Azlin, F., Musadat, & Nur, J. "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64". Jurnal Informatika, 7(2). 2018

[3] Lovian, T., & Fitri, I. "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang". Jurnal Media Informatika Budidarma, 6(1), 692-700. 2022

[4] Meko, D. A. "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data". Jurnal Teknologi Terpadu (JTT), 4(1). 2018

[5] Nuraeni, F., & Agustin, Y. H. (2020). "The Implementasi Caesar Cipher & Advanced Encryption Standar (AES) Pada Pengamanan Data Pajak Bumi Bangunan". Jurnal Ilmiah MATRIK, 22(2), 187-194. 2020

[6] Nurnaningsih, D., & Permana, A. A. "Rancangan aplikasi Pengamanan Data dengan Algoritma advanced encyption standard (AES)". JURNAL TEKNIK INFORMATIKA, 11(2), 177–186. 2018. doi:10.15408/jti.v11i2.7811

[7] Panjaitan, Z., Ginting, E. F., & Yusnidah, Y. "Modifikasi SHA-256 dengan Algoritma Hill Cipher untuk Pengamanan Fungsi Hash dari Upaya Decode Hash". Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), 19(1), 53-61. 2020

[8] Prameshwari, A., & Sastra, N. P. "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen". Jurnal Eksplora Informatika, 8(1), 52-58. 2018

[9] Rahmawati, A., & Rahman, A. "Sistem Pengamanan Keaslian Ijasah Menggunakan QRCode dan Algoritma Base64". Program Studi Sistem Informasi, Universitas Ahmad Dahlan, 1(2). 2011

[10] Sari, M. P. "Analisis Algoritma SHA-3 Keamanan pada Data Pribadi". JURNAL TECNOSCIENZA, 5(2), 231-242. 2021

[11] R., Siringoringo. "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File". KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak, 2(01), 31-42. 2020