JURNAL TEKNIK INFORMATIKA

Vol.2 No.2 Tahun.2022

Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data

Aprizaldi *[1], Mhd Arief Hasan[2], Debi setiawan[3]
[1,2]Informatic Enginering Program Study, Faculty of Computer Science, Universitas Lancang Kuning
[3] Universitas Abdurab
e-mail: *[1] aprizaldialdi09@gmail.com, [2]m.arif@unilak.ac.id, [3]debisetiawan@univrab.ac.id

***Abstract* – Cryptography is a science that studies mathematical techniques related to aspects of information security. So far, notification of information to staff or assistants is still manual, because the information is provided in paper form and is easy for others to read. This of course will be a matter of privacy which will be conveyed later. For this reason, the authors are interested in building a Message Cryptography Application in the Folio Sheet Paper division of PT Indah Kiat using the AES 128 algorithm to encrypt and decrypt data so that the process and production results in the form of data can be maintained. The author takes the AES 128 algorithm as the encryptor because the AES 128 encryption process uses 4 stages in carrying out the transformation using the following steps: subbyte transformation, shiftrows, mixcolumns, and addroundkey. While the decryption process flow uses the inverse for all transformations in the AES algorithm except addroundkey with the following steps changing invshiftrows, invsubbytes, addroundkey, and invmixcolumns, so the data will be safe and stored in the database.**

***Abstrak* – Kriptografi merupakan ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi. Selama ini pemberitahuan informasi kepada staf atau asisten masih bersifat manual, karena informasi diberikan dalam bentuk kertas dan mudah dibaca oleh orang lain. Hal ini tentunya akan menjadi masalah akan privasi yang akan disampaikan nantinya. Untuk itu penulis tertarik membangun Aplikasi Kriptograsi Pesan pada divisi Folio Sheet Paper PT Indah Kiat menggunakan algoritma AES 128 untuk mengenkripsi dan mendekripsi data agar proses dan hasil produksi berupa data dapat terjaga. Penulis mengambil algoritma AES 128 sebagai encryptor karena proses enkripsi AES 128 menggunakan 4 tahapan dalam melakukan transformasi dengan menggunakan langkah-langkah : transformasi subbyte, shiftrows, mixcolumns, dan addroundkey. Sedangkan alur proses dekripsi menggunakan invers untuk semua transformasi pada algoritma AES kecuali addroundkey dengan langkah berikut mengubah invshiftrows, invsubbytes, addroundkey, dan invmixcolumns, sehingga data akan aman dan tersimpan di database.**

***Kata Kunci* – Aplikasi, Algoritma AES 128, Keamanan Data, PHP, MySQL.**

I. PENDAHULUAN

Perkembangan zaman di dunia teknologi sangat pesat, terutama di bidang aplikasi yang begitu besar pengaruhnya terhadap pekerjaan manusia, yang menggunakan komputer, handphone dan lain sebagainya untuk mempermudah pekerjaan dalam mengintegrasikan data yang dikelola. Teknologi informasi yang dikemas dalam aplikasi online sangat memberikan nilai tambah bagi perusahaan yang dapat mempercepat akses data dan dapat memberikan informasi yang up to date.

Setiap hasil produksi, pengawas akan menginformasikan kepada asisten tentang kombinasi campuran bahan produksi yang akan diproses untuk melakukan produksi sesuai dengan yang diinginkan konsumen. Dari pengamatan penulis di tempat penelitian bahwa informasi yang dibagikan supervisor dapat dibaca oleh seluruh karyawan atau staf, informasi ini dapat dilihat dengan jelas oleh pengguna atau staf yang tidak berkepentingan sehingga data produksi dan proses dapat diketahui oleh staf lain. yang tidak berkepentingan, sehingga tidak

menutup kemungkinan data tersebut dapat diberikan kepada pihak yang tidak bertanggung jawab. Jenis data atau file yang ada berupa record data dan file dokumen pendukung seperti doc, xls dan pdf.

Kata kriptografi atau cryptography diketahui berasal dari bahasa Yunani, crypto dan graphia. Dimana crypto artinya bersembunyi, sedangkan graphia artinya menulis. Sehingga dapat diuraikan kriptografi merupakan ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi[1]. Data produksi akan dienkripsi dengan teknik kriptografi sehingga data produksi tidak dapat dilihat oleh orang lain kecuali pengguna itu sendiri atau pengguna yang diperbolehkan setelah data tersebut di deskripsikan kembali[2].

Kriptografi memiliki empat tujuan utama yakni, **Kerahasiaan** : Informasi yang disajikan hanya bisa diakses oleh pihak yang berwenang[3]. **Integritas**: Kondisi ini dimana memastikan bahwa informasi yang disajikan tidak dirubah atau dimanipulasi.**Autentikasi**: Memastikan bahwasanya Informasi yang disajikan pengguna adalah asli.**Antipenyangkalan:** Mencegah penerima bahwasanya bukan dirinya yang menerima informasi[4].

Selama ini pemberitahuan informasi kepada staf atau asisten masih bersifat manual, karena informasi diberikan dalam bentuk kertas dan mudah dibaca oleh orang lain. Hal ini tentunya akan menjadi masalah akan privasi yang akan disampaikan nantinya. Untuk itu penulis tertarik membangun Aplikasi Kriptograsi Pesan pada divisi Folio Sheet Paper PT Indah Kiat menggunakan algoritma AES 128 untuk mengenkripsi dan mendekripsi data agar proses dan hasil produksi berupa data dapat terjaga. Penulis mengambil algoritma AES 128 sebagai encryptor karena proses enkripsi AES 128 menggunakan 4 tahapan dalam melakukan transformasi dengan menggunakan langkah-langkah : transformasi subbyte, shiftrows, mixcolumns, dan addroundkey[5]. Sedangkan alur proses dekripsi menggunakan invers untuk semua transformasi pada algoritma AES kecuali addroundkey dengan langkah berikut mengubah invshiftrows, invsubbytes, addroundkey, dan invmixcolumns, sehingga data akan aman dan tersimpan di database [6], [7].

II. PENELITIAN YANG TERKAIT

Kata kriptografi atau cryptography diketahui berasal dari bahasa Yunani, crypto dan graphia. Dimana crypto artinya tersembunyi, sedangkan graphia artinya tulisan. Sehingga dapat dijelaskan bahwa kriptografi merupakan ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi. Contohnya termasuk validitas data, kerahasiaan data, kredibilitas data, integritas data, dan otentikasi data. Namun, tidak semua aspek keamanan informasi dapat diatasi dengan kriptografi [8][9].

Dalam kriptografi, Advanced Encryption Standard (bahasa Inggris: Advanced Encryption Standard, disingkat AES) adalah standar enkripsi dengan kunci simetris yang diadopsi oleh Pemerintah Amerika Serikat. Standar tersebut terdiri dari tiga blok pengkodean, yaitu AES-128, AES-192 , dan AES-256, diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Setiap pengkodean memiliki ukuran blok 128 bit dengan ukuran kunci masing-masing 128, 192 dan 256 bit. AES telah dianalisis secara ekstensif dan sekarang digunakan di seluruh dunia, seperti halnya pendahulunya [10].

AES menggunakan matriks 4×4 dengan urutan byte dalam urutan kolom-lalu-baris (bawah, lalu kanan). Matriks ini disebut "status" (keadaan).

Misalnya, 16 byte data $b_0, b_1, \dots, b_{15}$, dijelaskan dalam matriks dua dimensi sebagai berikut.

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix} \quad (1)$$

Jumlah putaran yang dilakukan dalam AES bergantung pada ukuran kunci yang digunakan.

TABEL I
PERBANDINGAN UKURAN KUNCI DAN JUMLAH PUTARAN

Block Size	Key Size	Number of Rounds
128 bit	128 bit	10 putaran
	192 bit	12 putaran
	256 bit	14 putaran
	128 bit	10 putaran

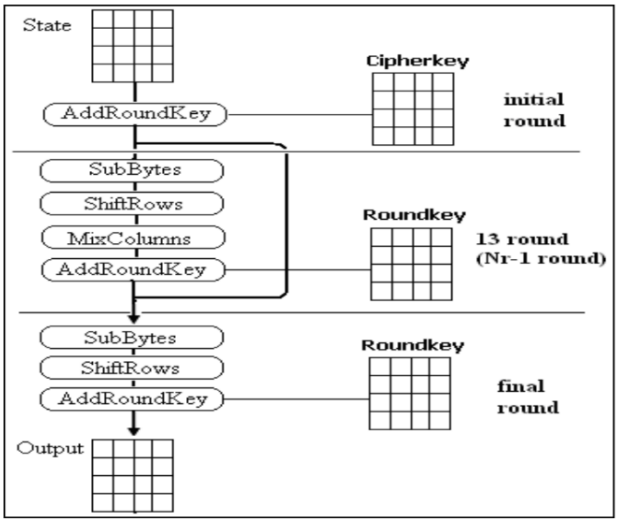
Setiap putaran terdiri dari beberapa langkah, termasuk yang menggunakan kunci enkripsi. Langkah inversi (mundur) digunakan untuk melakukan dekripsi dengan kunci (simetris) yang sama.

Gambaran umum algoritma

1. KeyExpansion, kunci bulat diturunkan dari kunci enkripsi melalui penjadwalan kunci AES. AES membutuhkan kunci bulat 128 bit untuk setiap putaran plus satu.
2. Penambahan kunci bulat awalan: AddRoundKey, setiap byte digabungkan dengan satu byte kunci bulat dengan operasi XOR.
3. Selama 9, 11, atau 13 putaran:
    1. SubBytes, substitusi nonlinear dimana setiap byte dipertukarkan dengan yang lain sesuai tabel referensi.
    2. ShiftRows, tukar posisi dimana tiga baris terakhir digeser beberapa kali.
    3. MixColumns, linear mixing yang bekerja pada setiap kolom “status”, yaitu kombinasi dari empat byte pada setiap kolom.
    4. AddRoundKey
4. Putaran terakhir (putaran ke-10, ke-12, atau ke-14):
    1. SubByte
    2. MoveRow
    3. AddRound Key

III. METODE PENELITIAN

Dari proses enkripsi, terdapat transformasi 4 byte yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Langkah pertama untuk melakukan proses enkripsi, input yang telah disalin menjadi state sehingga menjadi transformasi byte AddRoundKey. Setelah itu, status transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara iteratif adalah Nr [11], [12]. Proses dan aliran dalam algoritma AES ini disebut fungsi bulat. Putaran terakhir ini berbeda dengan putaran sebelumnya dimana pada putaran terakhir ini state tidak akan mengalami transformasi MixColumns. Ilustrasi dari setiap proses enkripsi AES 128 dapat dilihat pada gambar di bawah ini:



Gbr. 1 Ilustrasi AES 128 . Proses Enkripsi

Pada ilustrasi diatas menjelaskan alur dari setiap proses enkripsi yang dilakukan dengan menggunakan Algoritma AES 128.

IV. HASIL DAN PEMBAHASAN

A. Use Case Diagram

Use case diagram yang merupakan bagian dari jenis diagram di UML yang menggambarkan interaksi antara sistem dengan sistem dan aktor, use case diagram juga dapat menggambarkan jenis interaksi antara pengguna sistem dengan sistem itu sendiri. Use case diagram adalah model peworking untuk layanan sistem. Berikut ilustrasi usulan use case diagram untuk:enkripsi atau dekripsi formula campuran pengolahan data dan hasil produksi.

Gbr. 2 Use Case Diagram Aplikasi Keamanan Data Menggunakan Algoritma AES 128

TABEL II
LOGIN USE CASE SCENARIOS

Use Case Title	Login Dalam Keamanan Data Dengan Algoritma AES 128
Actor	Admin, Pegawai and Supervisor
Purpose	Untuk keamanan akun pengguna
Description	Pengguna sebelum melakukan aktivitas pada sistem, pengguna harus melakukan login pada aplikasi
Actor Action	**System Response**
1. Pengguna masuk dengan nama pengguna dan kata sandi 3. Pengguna dapat menginput kebutuhan sistem seperti input data pegawai, generate kode dan hasil produksi.	2. Proses Sistem Login 4. Sistem memverifikasi permintaan pengguna.

TABEL II
GUNAKAN SKENARIO KASUS MENGELOLA DATA PROSES DAN HASIL PRODUKSI

Use Case Title	Implementasi Algoritma AES 128 pada Aplikasi
Actor	Admin
Purpose	Untuk memudahka pengguna mengenkripsi dan mendekripsi data
Description	Enkripsi dan dekripsi data formulasi campuran produksi
Actor Action	**System Response**

1. User login di website 3. Memilih data/file	2. Login sistem dan proses autentikasi 4. Sistem pengolah data atau file 5. Data/File ditampilkan

TABEL III
SKENARIO KASUS PENGGUNAAN ENKRIPSI DATA

Use Case Title	Enkripsi Data
Actor	Admin
Purpose	Enkrip Data
Description	Data atau file tersebut akan diinput dan sistem akan menyimpan data tersebut dalam bentuk file terenkripsi.
Actor Action 1. Admin login di Website 3. Entri Data	**System Response** 2. Login sistem dan proses autentikasi 4. Data or file confirmation system 5. Data processing system for encryption 6. System displays encrypted data

TABEL IV
USE CASE SCENARIO IMPLEMENTASI ALGORITMA AES 128

Use Case Title	Implementasi Algoritma AES 128 pada Aplikasi
Actor	Admin
Purpose	Untuk memudahkan pengguna mengenkripsi dan mendekripsi data
Description	Enkripsi dan dekripsi data formulasi campuran produksi
Actor Action 2. User login di website 6. Memilih Data/File	**System Response** 3. Login Sistem dan autentifikasi proses 7. Sistem pengolah data atau file 8. Data/Files ditampilkan

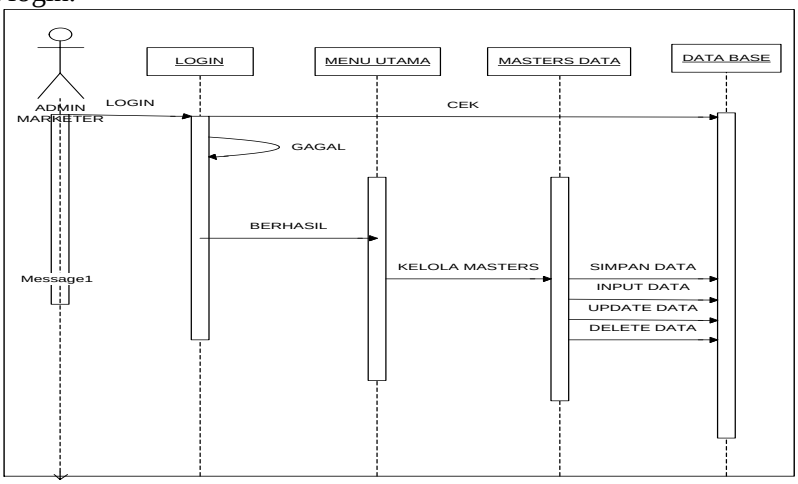
TABEL IV
LOGOUT USE CASE SCENARIOS

Use Case Title	Logout Dari Sistem
Actor	Admin, Employee and Supervisor
Purpose	Untuk exit aplikasi
Description	Jika pengguna mengklik menu ini, berarti pengguna telah menghentikan semua aktivitas di aplikasi.
Actor Action 1. User menekan tombol logout	**System Response** 2. Proses Logout di Sistem 3. Sistem memverifikasi permintaan pengguna, dan pengguna tidak terdaftar dari sesi aplikasi.

Sequence diagram adalah pola diagram yang dapat berinteraksi antar objek dan berkomunikasi antar objek pada setiap diagramnya. Diagram ini juga menunjukkan rangkaian pesan yang ditransfer oleh setiap objek yang melakukan aktivitas atau tugas untuk akses dan tindakan tertentu. Berikut ini menjelaskan diagram urutan yang diusulkan.

B. Sequence Diagram Login

Diagram urutan login ini menggambarkan proses-proses yang terjadi pada sistem pada saat aktor atau pengguna melakukan login.



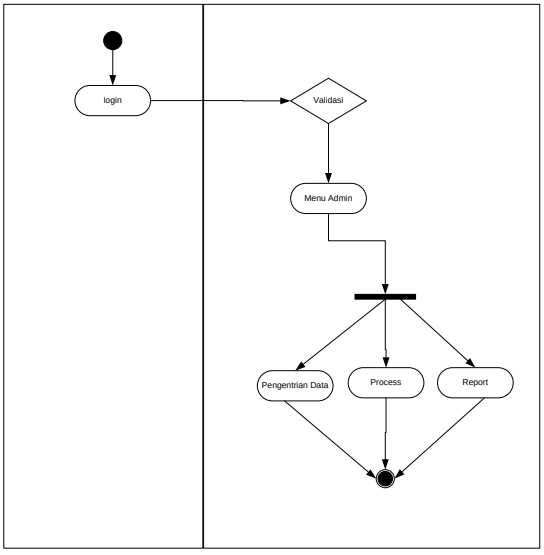
Gbr. 3 Sequence Diagram Login.

Sequence diagram ini menggambarkan alur proses login user pada database pada aplikasi yang penulis buat. Dimana aktor diharuskan memasukkan username dan password sebelum masuk ke menu utama. Sistem akan mencocokkan dengan data yang ada di sistem. Jika sudah benar maka sistem akan menampilkan halaman utama.

C. *Activity diagrams*

Activity diagram atau diagram aktivitas merupakan salah satu jenis diagram dalam UML yang dapat memodelkan setiap proses yang terjadi pada sistem. Pada aplikasi ini terdapat 3 pengguna aplikasi yaitu Admin, Supervisor dan Pegawai..

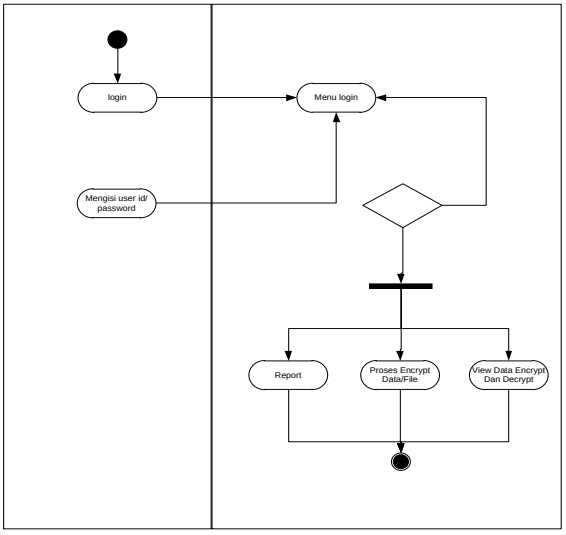
1. User Admin (Admin Activity Diagram)



Gbr. 4 Activity Diagram of User Admin

Pada Activity Diagram Pada menu Login ini admin dapat mengisi user id dan password sehingga dapat dilakukan dengan mudah mengakses menu admin dan mengisi data sesuai kebutuhan pada menu admin.

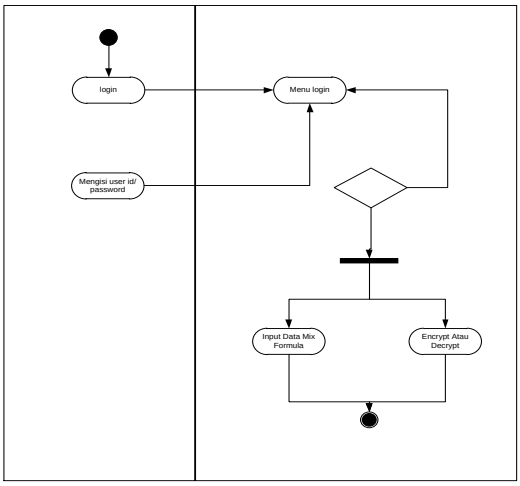
2. *Activity Diagram Supervisor*



Gbr. 5 Supervisor Activity Diagram

Pada diagram aktivitas Supervisor dapat melihat hasil data yang dienkripsi atau didekripsi oleh user pada input data awal. Dimana supervisor bisa mengenkripsi dokumen, kemudian dokumen yang sudah di enkripsi bisa di dekripsikan kembali.

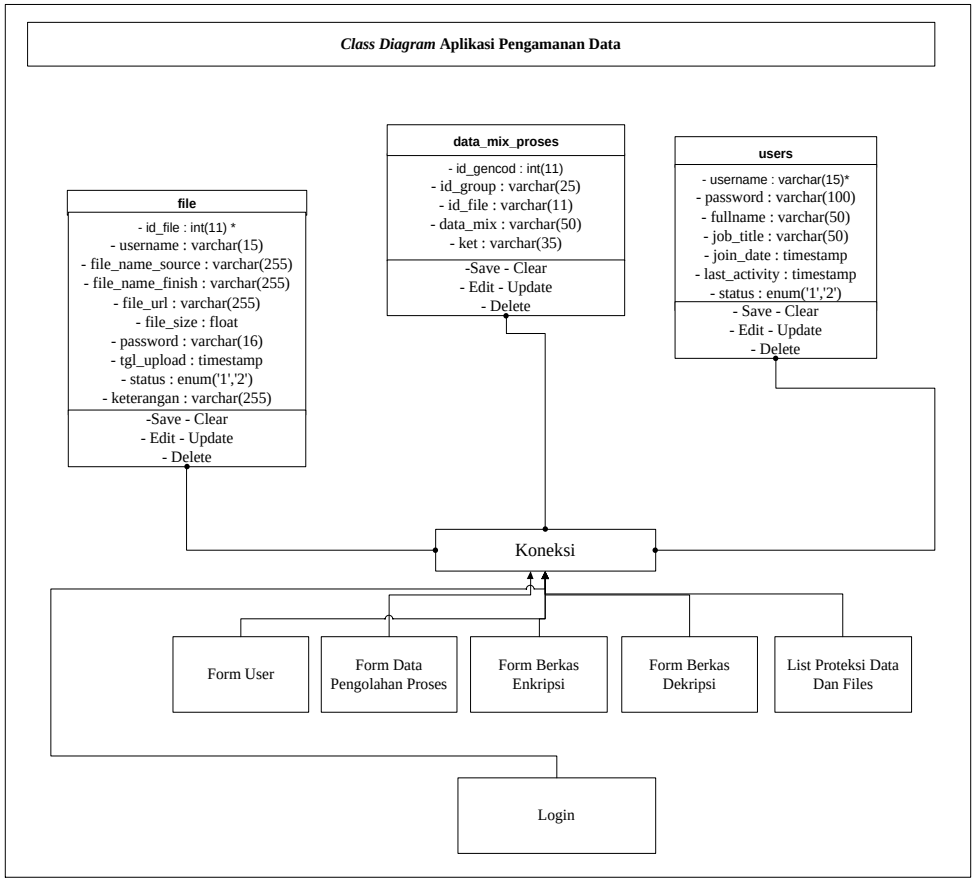
3. *Activity Diagram Pegawai*



Gbr. 6 Activity Diagram Pegawai

Pada diagram aktivitas, pengguna dapat menginputkan mix formula dan melihat hasil inputan berupa enkripsi dan dekripsi data atau file.

D. *Class Diagram*



Gbr. 7 Class Diagram

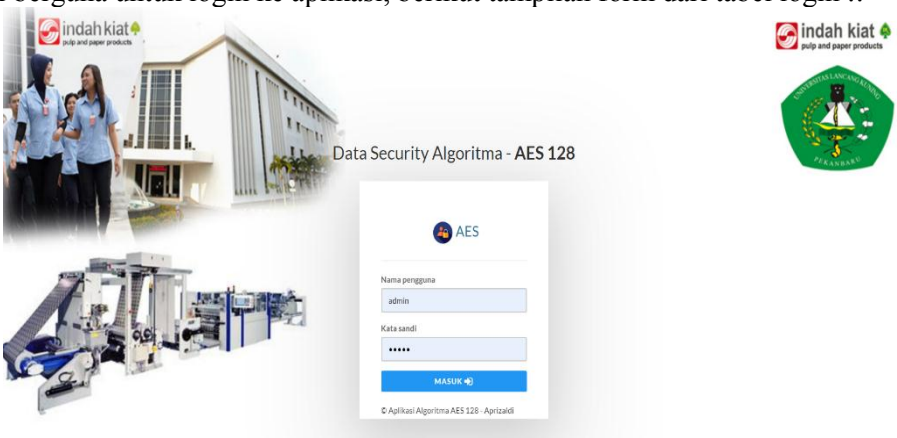
Class diagram pada dasarnya adalah representasi grafis dari tampilan statis sistem dan mewakili berbagai aspek aplikasi. Kumpulan diagram kelas mewakili keseluruhan sistem. Nama class diagram harus bermakna untuk menggambarkan aspek dari sistem.*Class Diagram* yang penulis rancang meliputi form user, pengolahan data, enkripsi file, dekripsi dan daftar file data, dari kelima form yang saling berhubungan antar tabel dalam database.

E. Implementasi

Implementasi adalah pelaksanaan rencana atau sistem yang telah disusun secara matang. Berikut adalah implementasi dari sistem yang dibuat.

1. Login Form

Form ini berguna untuk login ke aplikasi, berikut tampilan form dari tabel login ::



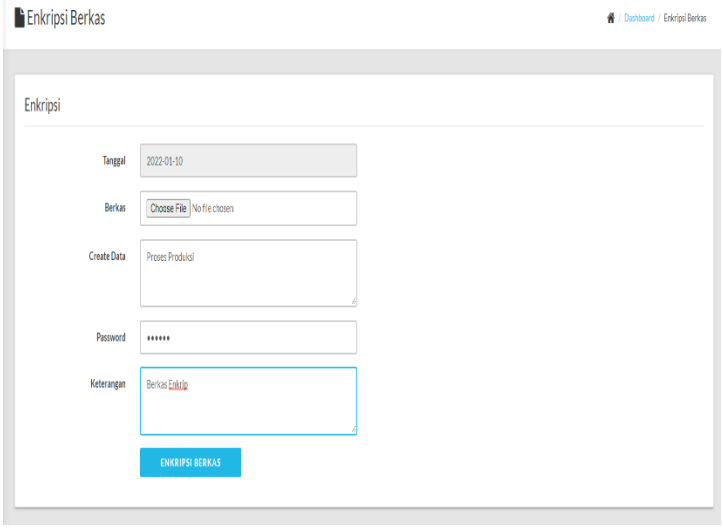
Gbr.8 Login Form

Form ini berguna untuk login ke aplikasi, setiap user berhak login untuk menggunakan aplikasi

ini.

2. Formulir Enkripsi Data Atau File

Form ini berguna untuk menginput data hasil enkripsi dan proses produksi, berikut tampilan form Enkripsi Data Atau File:

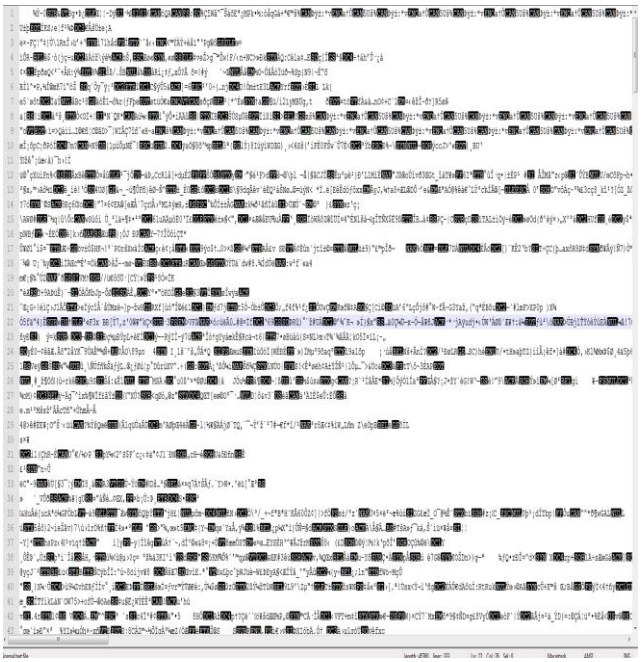


Gbr. 9 Data or File Encryption Form

Form ini berguna untuk mengenkripsi file, form ini hanya dapat diakses oleh user khusus yang ditunjuk oleh admin dan akses lock tergantung user yang melakukan key pada awal enkripsi.

3. Formulir Hasil Enkripsi

Form ini berguna untuk melihat hasil enkripsi dari algoritma AES 128, berikut tampilan form Hasil Enkripsi:

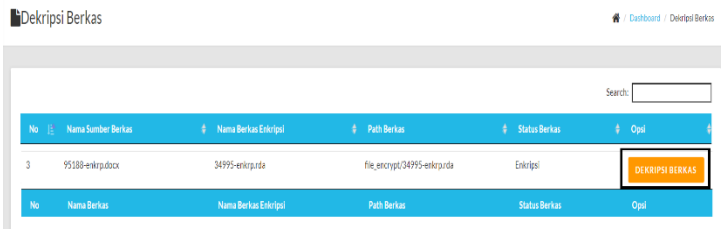


Gbr. 11 Form Hasil Enkripsi

Form ini menampilkan file yang diproteksi oleh user kemudian dibuka menggunakan notepad, sehingga user lain tidak dapat melihatnya, form ini hanya dapat diakses oleh user khusus yang ditunjuk oleh admin dan akses lock tergantung user yang melakukan key pada awal enkripsi.

4. Formulir Dekripsi Data Atau File

Form ini berguna untuk mengenkripsi data hasil dan proses produksi, berikut tampilan form dekripsi data atau file:

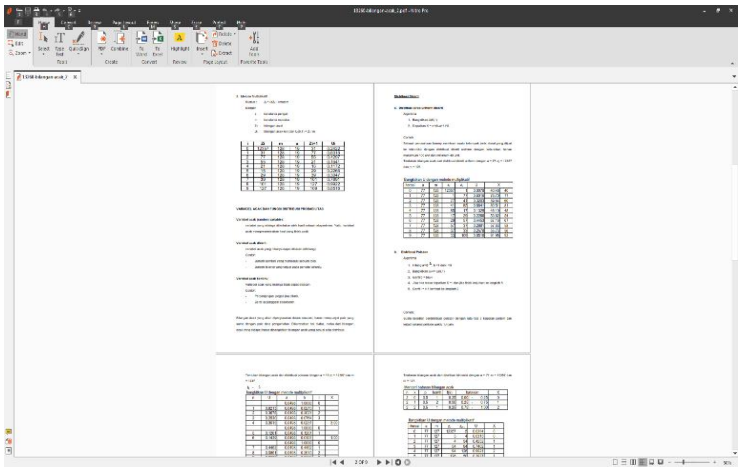


Gbr. 12 View Decryption of Data or Files

Formulir ini melihat file didekripsi oleh pengguna, sehingga pengguna yang mendapatkan kunci dapat membuka file tersebut, formulir ini hanya dapat diakses oleh pengguna yang memegang kunci.

5. Form Hasil Dekripsi

Form ini berguna untuk melihat hasil dekripsi algoritma AES 128, berikut tampilan form Hasil Enkripsi:



Gbr. 13 Tampilan Hasil Form Dekripsi

Form ini berguna untuk membuka file atau mereview file yang diproteksi, form ini dapat diakses oleh user yang mengunci file tersebut.

V. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian Keamanan Data dengan Algoritma AES 128 di PT. Indah Kiat Pulp And Paper yang telah dilakukan, dapat disimpulkan sebagai berikut:

1. Dengan adanya sistem keamanan dalam penguncian data dan file yang bertujuan untuk menghindari terjadinya penipuan dalam pembocoran data proses dan produksi.
2. Mengenkripsi file dan menyimpannya dalam database dalam suatu program dapat membantu melindungi program dari pengguna yang tidak bertanggung jawab.
3. Melakukan upaya pengamanan file dalam menggunakan Algoritma AES 128.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada Fakultas Ilmu Komputer Universitas Lancang Kuning yang sudah membantu dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

[1] G. Rahmi Fajri *et al.*, “KEAMANAN DATA PADA PENGARSIPAN SURAT MENGGUNAKAN METODE KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN SHIFT CIPHER,” 2020. doi: https://doi.org/10.31849/zn.v2i1.6220.

[2] S. Widiyanto, G. Adnan, M. Fatkuroji, D. W. Handoyo, and M. A. Hasan, “Pengamanan Pesan Text dengan menggunakan Kriptografi Klasik Metode Shift Chipper dan Metode Substitution Chipper,” 2021. doi: https://doi.org/10.30606/rjocs.v7i1.2090.

[3] R. Feraldi *et al.*, “KOMBINASI ALGORITMA KRIFTOGRAFI CAESAR CIPHER DAN PERMUTATION CIPHER UNTUK PESAN TEKS MENGGUNAKAN PYTHON,” *Riau Journal of Empowerment*, vol. 7, no. 01, pp. 76–86, 2021, doi: https://doi.org/10.30606/rjocs.v7i1.2095.

[4] Megawati, Muhammad Fitra Hamidy, Sasqia Ismi Aulia, Yuhendri Putra, and Mhd Arief Hasan, "Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python," *SATIN - Sains dan Teknologi Informasi*, vol. 7, no. 1, pp. 102–111, Jun. 2021, doi: 10.33372/stn.v7i1.686.

[5] J. Simorangkir and M. Arief, "Sistem Verifikasi Dokumen Menggunakan QR-Code di Prodi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning," *Sistem dan Teknologi Informasi*, vol. 8, no. 4, pp. 369–375, 2020, doi: 10.26418/justin.v8i4.42315.

[6] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.

[7] L. Thulasimani and M. Madheswaran, "A SINGLE CHIP DESIGN AND IMPLEMENTATION OF AES-128/192/256 ENCRYPTION ALGORITHMS," 2010.

[8] J. H. Penelitian and H. Wijaya, "JURNAL AKADEMIKA PENERBIT IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN URL (UNIFORM RESOURCE LOCATOR) DARI SQL INJECTION," vol. 17, no. 1, 2020, [Online]. Available: https://www.

[9] F. Brandt, "Efficient cryptographic protocol design based on distributed El Gamal encryption," in *International Conference on Information Security and Cryptology*, 2005, pp. 32–47.

[10] K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, Y. L. Huang, and C. H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," *IEEE Access*, vol. 6, pp. 45325–45334, Jul. 2018, doi: 10.1109/ACCESS.2018.2852563.

[11] A. Arif, P. Mandarani, and M. Tenik Informatika, "REKAYASA PERANGKAT LUNAK KRIPTOGRAFI MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) 128 BIT PADA SISTEM KEAMANAN SHORT MESSAGE SERVICE (SMS) BERBASIS ANDROID," vol. 4, no. 1, 2016.