Bit (Fakultas Teknologi Informasi Universitas Budi Luhur) p-ISSN: 1693-9166
Vol. 20, No. 1, April 2023, hlm. 44-49 e-ISSN: 2685-127X

IMPLEMENTASI ALGORITME KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256) UNTUK MENGAMANKAN DATABASE PENILAIAN KARYAWAN PADA KJPP NDR

Raka Febrianto[1*], Sejati Waluyo[2]

[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Email: 1rakafebrianto24@gmail.com, 2sejati.waluyo@budiluhur.ac.id

(Naskah masuk: 10 Maret 20223, diterima untuk diterbitkan: 30 Mei 2023)

Abstrak

Dalam menjalankan tugasnya, *Human Resources Develompment* (HRD) yang dibantu oleh staff dan admin KJPP NDR memiliki permasalahan yaitu menyangkut kerahasiaan dokumen penting atau laporan pekerjaan agar terjaga oleh pihak yang tidak berwenang. Karena tidak adanya informasi tentang cara mendapatkan dokumen dan untuk memudahkan seorang HRD melakukan tugasnya dengan memberikan penilaian untk para pegawai dengan sistem yang lebih baik, maka dibuatlah Aplikasi berbasis web Penilaian Karyawan Pada KJPP NDR. Tujuan dari penelitian ini adalah untuk membuat aplikasi berbasis web. Penerapan algoritme kriptografi AES 256 berfungsi sebagai pengaman dokumen penting berupa data penilaian yang dibuat ke dalam skor/angka yang diperoleh dari 6 Data Kriteria Penilaian Pegawai. Data-data kriteria tersebut berupa Tanggung jawab, Kemampuan Komunikasi, Kehadiran, Inisiatif, Kedisiplinan dan Kreatifitas. Selama proses enkripsi dan dekripsi 32 byte/karakter, digunakan algoritma kriptografi AES 256 dengan metode perbandingan dan kunci dengan panjang yang sama atau kunci simetris. Bahasa pemrograman PHP berbasis web digunakan untuk membuat aplikasi keamanan dokumen ini.

Kata kunci: *AES 256, dokumen, HRD, KJPP NDR, Kriptografi*

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD CRYPTOGRAPHIC ALGORITHM (AES-256) TO SECURE EMPLOYEE ASSESSMENT DATABASE AT KJPP NDR

Abstract

In carrying out their duties, the Human Resources Development (HRD) who is assisted by the KJPP NDR staff and admin has problems, namely regarding the confidentiality of important documents or work reports so that they are maintained by unauthorized parties. Due to the absence of information on how to obtain documents and to make it easier for an HRD to carry out their duties by providing an assessment of employees with a better system, a web-based application for Employee Assessment was made at KJPP NDR. The purpose of this research is to create a web-based application. The application of the AES 256 cryptographic algorithm serves as a safeguard for important documents in the form of assessment data that is made into scores/numbers obtained from 6 Employee Assessment Criteria Data. These criteria data are in the form of Responsibility, Communication Skills, Attendance, Initiative, Discipline and Creativity. During the 32 bytes/character encryption and decryption process, the AES 256 cryptographic algorithm is used with the comparison method and keys of the same length or symmetric keys. The web-based PHP programming language is used to create this document security application.

Keywords*: AES 256, document, HRD, KJPP NDR, Cryptography*

1. PENDAHULUAN

Teknologi informasi yang digunakan saat ini telah berkembang begitu pesat dan memerlukan wawasan yang lebih baik untuk menatap masa depan mengenai kemajuan teknologi komputer dan telekomunikasi. Perusahaan, perguruan tinggi, instansi pemerintah (birokrasi), dan individu (swasta) semuanya sangat bergantung pada kemampuan organisasi atau lembaga untuk memberi informasi dengan cepat dan akurat kepada semua orang.

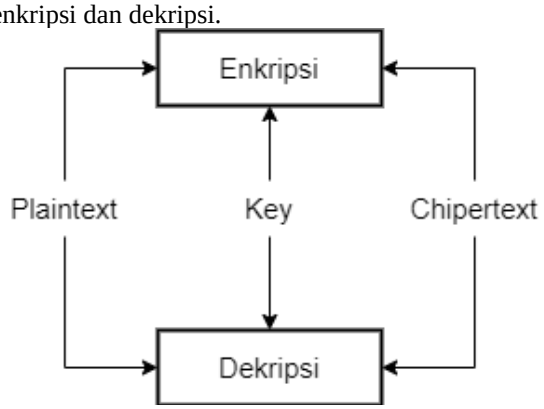
Pengguna yang kurang memahami keamanan data menjadi ancaman serius mengingat kecanggihan teknologi transmisi data dan penerapannya. Sistem enkripsi diperlukan untuk teknologi keamanan informasi untuk mencegah penyalahgunaan data.

Dengan pertumbuhan penyimpanan data berbasis komputer dan teknologi telekomunikasi, maka kami melakukan riset di salah satu Kantor Penilaian Properti dan Bisnis di Jakarta. Kami pun berterima kasih sudah diberikan kesempatan melakukan riset di

KJPP Nirboyo Adiputro, Dewi Apriyanti & Rekan (KJPP NDR). KJPP NDR adalah perusahaan yang memberikan jasa sesuai dengan bidang penilaian properti dan bisnis, penyimpanan data di KJPP NDR juga masih disimpan secara manual rentan terjadi penyadapan data. Sehingga permasalahan yang terjadi pada KJPP NDR adalah belum adanya keamanan yang mumpuni pada sistem penilaian pegawai sehingga rentan untuk terjadinya pencurian data. Dan untuk memproteksi pesan sehingga pihak-pihak yang tidak berkepentingan tidak dapat membacanya karena menyangkut Penilaian Pegawai secara menyeluruh dan menjadi opsi maupun evaluasi untuk KJPP NDR. Akibatnya, keamanan data melalui kriptografi sangat penting. Kriptografi adalah salah satu teknik yang sering digunakan untuk keamanan data. Enkripsi adalah proses dimana informasi dibuat sedemikian rupa sehingga tidak dapat dibaca atau diketahui oleh pihak yang tidak diinginkan.

Kriptografi merupakan kata yang berasal dari bahasa Yunani, tercipta dari dua kata yaitu kata crypto yang berarti rahasia dan graphia diartikan sebagai tulisan, ini berarti bahwa kriptografi dapat mudah dipahami sebagai "tulisan rahasia"[1]. Kriptografi merupakan keahlian atau ilmu dalam penyandian atau pengamanan sebuah data atau informasi yang bersifat *privacy* [2]. Kriptografi merupakan sebuah metode yang dapat mrngacak teks asli menjadi teks tidak dapat dibaca seperti aslinya [3]. Umumnya, kriptografi dapat diartikan sebagai bidang ilmu tentang penyandian untuk keamanan dan kerahasiaan suatu data atau dokumen. Namun, perlu diingat bahwa kriptografi bukan berarti hanya memberikan keamanan informasi, tapi lebih ke arah teknik – tekniknya [4]. Salah satu algoritma pada teknik kriptografi yang sangat terkenal adalah algoritma *Advance Encryption Standard* (AES). Dalam kriptografi, dikenal istilah enkripsi yaitu suatu proses pengubahan sebuah data menjadi kumpulan kode yang sulit dimengerti manusia (*ciphertext*). Sebaliknya, dekripsi yaitu pengubahan kumpulan kode enkripsi menjadi sekumpulan data yang sebenarnya sebelum data di enkripsi (*plaintext*) [5]. Proses dari kedua hal ini juga memerlukan komponen satu atau beberapa kunci kriptografi serta algoritma untuk memproses penyandian dokumen [6]. Alasan utama memilih AES Rijndael ini bukan karena algoritmanya paling aman di antara MARS, RC6, Serpent, Twofish, dan lain sebagainya, tetapi AES Rijndael memiliki keseimbangan antara keamanan dan fleksibelitas di berbagai platform perangkat lunak dan perangkat keras seperti PC / Laptop [7]. Komputer adalah suatu atau perangkat yang membutuhkan suatu keamanan penyimpanan database ataupun data-data informasi pribadi atau perusahaan yang sangat penting dan keamanan data tidak boleh dibiarkan begitu saja [8]. Proses pengamanan database dari ancaman disengaja atau tidak disengaja yang menimbulkan ancaman terhadap sistem dikenal sebagai keamanan database.

Berikut ini adalah Gambar 1 mengenai alur enkripsi dan dekripsi.



Gambar 1. Proses enkripsi dan dekripsi

Dengan menggunakan algoritma AES, keamanan data bisa ditingkatkan kepada jumlah bit yang tinggi seperti 64, 128, dan 256-bit, agar menjaga orisinalitas daripada isi data yang akan diamankan dari pihak yang tidak bertanggung jawab [9]. AES 256 juga digunakan untuk mengamankan beberapa informasi maupun data yang tidak dapat dibaca oleh pihak-pihak yang ingin merugikan perusahaan. Dikarenakan data-data yang sudah di enkripsi mempunyai kodenya sendiri [10].

Algoritma kriptografi atau sering disebut dengan cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*).

Algoritma simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok).

Kelebihan dari kriptografi simetris kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetris, karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real time*.

Kelemahan dari kriptografi simetris tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda pula, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut. Permasalahan dalam pengiriman kunci itu sendiri yang disebut "*key distribution problem*".

Algoritma kriptografi simetris dapat dikelompokkan menjadi dua kategori ***pertama*** Cipher aliran (*stream cipher*), Algoritma kriptografi beroperasi pada *plaintext* atau *ciphertext* dalam bentuk bit tunggal yang dalam hal ini rangkaian bit dienkripsikan atau didekripsikan bit per bit. *Cipher* aliran mengenkripsi satu bit setiap kali. Contoh

algoritma *stream cipher:* RC4, Panama dan Pike. ***Kedua*** *Cipher* blok (*block cipher*), Algoritma kriptografi beroperasi pada *plaintext* atau *ciphertext* dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. *Cipher* blok mengenkripsi satu blok bit setiap kali.

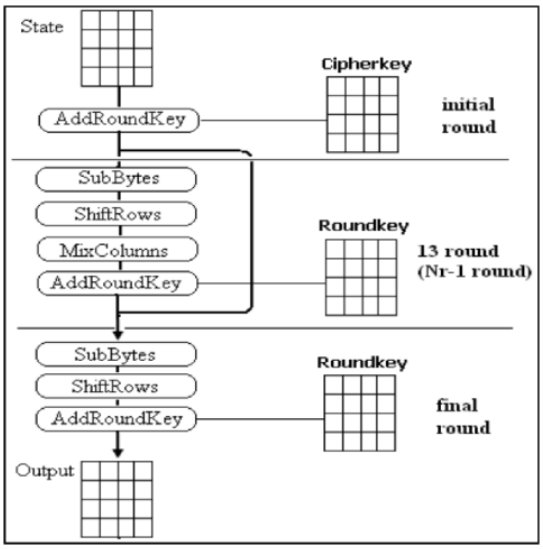
Algoritma asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci *private* untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

Kriptografi *public key* sering disebut dengan kriptografi asimetris. Kunci yang digunakan pada proses enkripsi dan proses dekripsi pada kriptografi kunci publik (*public key*) ini berbeda satu sama yang lain. Jadi dalam kriptografi kunci publik, suatu kunci *generator* akan menghasilkan dua kunci berbeda dimana satu kunci digunakan untuk melakukan proses enkripsi dan kunci yang lain digunakan untuk melakukan proses dekripsi.

Kunci yang digunakan untuk melakukan proses enkripsi akan dipublikasikan kepada umum untuk dipergunakan secara bebas. Oleh sebab itu, kunci yang digunakan untuk melakukan proses enkripsi disebut juga kunci *public*. Sedangkan kunci yang digunakan untuk melakukan dekripsi akan disimpan oleh pembuat kunci dan tidak akan dipublikasikan kepada umum. Kunci untuk melakukan dekripsi ini disebut dengan kunci pribadi (*private key*).

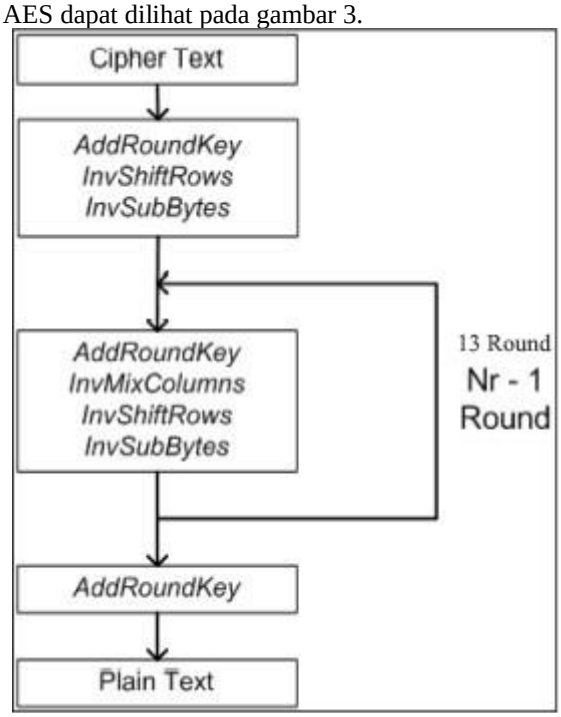
Dengan cara demikian, semua orang yang akan mengirimkan pesan kepada pembuat kunci dapat melakukan proses enkripsi terhadap pesan tersebut, sedangkan proses dekripsi hanya dapat dilakukan oleh pembuat atau pemilik kunci dekripsi. Dalam kenyataannya, kriptografi asimetris ini dipakai dalam SSH, suatu layanan untuk mengakses suatu server.

SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey adalah empat jenis *byte* transformasi yang digunakan pada tahap awal enkripsi AES. Saat input yang telah digandakan dalam status mengubah byte AddRoundKey di awal tahap enkripsi ini. Tahap ini, yang disebut sebagai round function, akan mengubah status menjadi Nr Repeatable SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Karena keadaan tidak mengalami transformasi MixColumns di final round, ini sedikit berbeda dari round sebelumnya. Tahapan enkripsi AES dapat dilihat pada gambar 2.



Gambar 2. Tahapan enkripsi AES

Transformasi *cipher* dapat dibalik dan diterapkan dalam berbagai arah selama fase dekripsi untuk menghasilkan cipher invers ramah algoritma AES. *Cipher* terbalik memanfaatkan InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey sebagai transformasi byte. Tahapan proses dekripsi AES dapat dilihat pada gambar 3.



Gambar 3. Tahapan dekripsi AES

2. METODE PENELITIAN

2.1 Pengumpulan Data

Langkah awal ini perlu dilaksanakan akumulasi data terkait penelitian yang menjadi fokus utama melalui observasi dan wawancara terlebih dahulu, dalam hal ini pada KJPP NDR yang sedang rentan akan keamanan data. Masalah yang terkumpul akan

dianalisa dan dirancang sebuah solusi termasuk perancangan aplikasi untuk keamanan data.

a. Wawancara

Untuk mempelajari lebih lanjut tentang aplikasi dan perangkat keamanan yang ada, pihak yang terlibat dalam pengembangan aplikasi dan program diwawancarai.

b. Observasi

Salah satu metode terbaik untuk mengumpulkan data untuk mempelajari dan mengamati suatu sistem adalah observasi. Pengamatan langsung dari prosedur sistem operasi digunakan untuk mencapai hal ini.

c. Studi Literatur

Tahapan selanjutnya yaitu melakukan studi terkait metode yang akan diterapkan pada penelitian ini. Mengobservasi dan menggali berbagai informasi juga diperlukan melalui berbagai macam media referensi seperti buku, diktat kuliah, jurnal dan karya ilmiah lain yang berkaitan dengan masalah inti dalam penelitian ini melalui implementasi kriptografi, terutama pada algoritma AES-256. Hal ini dilakukan agar penulis memiliki dasar yang kuat dan akurat untuk memilih strategi terbaik.

2.2 Perancangan

Tahapan ini dimulai perancangan aplikasi seperti pada hasil analisis sistem sebelumnya, terutama perancangan yang berhubungan dengan algoritma AES-256, dan metode pendukung lainnya yang akan dimasukkan ke dalam aplikasi dan desain *interface* yang akan dibangun. Metode *Waterfall* yang dalam model ini membutuhkan penyelesaian suatu tahapan secara keseluruhan sebelum melanjutkan ke tahapan selanjutnya digunakan untuk mengembangkan perangkat lunak ini. Output dari setiap tahapan harus dicatat dengan baik dalam sebuah dokumen.

2.3 Implementasi

Langkah ini, sangat diutamakan pada pembuatan modul - modul yang telah direncanakan dalam tahap perancangan ke dalam bahasa pemrograman. Aplikasi yang akan dibuat pada penelitian ini, menerapkan bahasa pemrograman PHP serta MySQL. Aplikasi ini diuji pada perangkat keras dengan spesifikasi Prosesor Intel Core i3, kapasitas RAM 2 GB, dan penyimpanan Harddisk sebesar 500 GB.

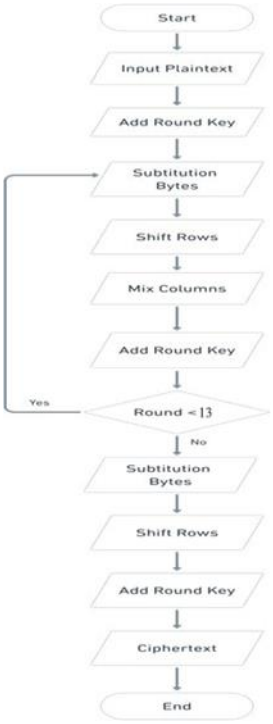
2.4 Pengujian

Tahapan terakhir yaitu pengujian yang dilakukan dengan tujuan sebagai penjamin jika aplikasi yang akan dibuat telah memenuhi hasil dari analisis dan perancangan yaitu menghasilkan satu kesimpulan, apakah aplikasi tersebut sesuai dengan yang diharapkan atau tidak. Maka, untuk menyimpulkan bahwa sistem tersebut memang telah beroperasi sesuai dengan tujuan yang diinginkan, diperlukan suatu metode pengujian yang akan digunakan sebagai ukuran atau parameter. Metode komparasi adalah salah satu yang digunakan dalam pengujian. Untuk membandingkan data yang digunakan untuk menarik kesimpulan baru metode ini digunakan. Kata "*compare*," berasal dari bahasa Inggris, yang secara harfiah diterjemahkan menjadi "untuk menemukan kesamaan antara dua konsep atau lebih,".

2.5 Flowchart

a. Flowchart Enkripsi AES

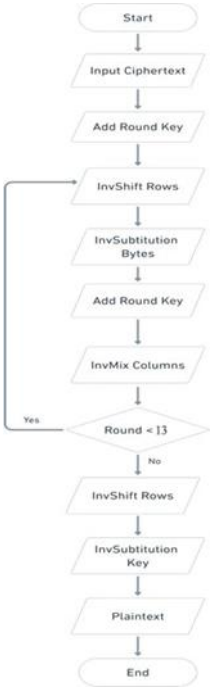
Berikut ini flowchart dari Enkripsi AES-256. Pada Flowchart Enkripsi AES dimulai dari memasukan *plaintext* dilanjutkan dengan proses *round key*. Selanjutnya dilanjutkan dengan proses substitution *bytes*, *shift row*, *mix column* dan *add round key*. Apabila telah mencapai 13 putaran maka dilanjutkan dengan proses *substitution bytes* dan diakhir dengan dihasilkannya *chipertext*. Flowchart Enkripsi AES dapat dilihat pada Gambar 4 dibawah ini.



Gambar 4. Flowchart Enkripsi AES

b. Flowchart Dekripsi AES

Berikut ini flowchart dari Dekripsi AES-256. Pada Flowchart Dekripsi AES dimulai dari memasukan *ciphertext* dilanjutkan dengan proses *round key*. Selanjutnya dilanjutkan dengan proses *invshiftrow*, *invsubtitution bytes*, *add round key* dan *invmix columns*. Apabila telah mencapai 13 putaran maka dilanjutkan dengan proses invshift row dan diakhir dengan dihasilkannya *plaintext*. Flowchart Dekripsi AES dapat dilihat pada Gambar 5 dibawah ini.



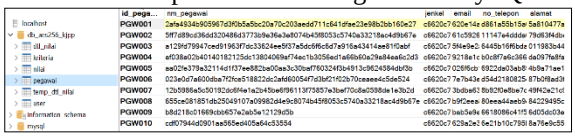
Gambar 5. Flowchart Dekripsi AES

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Enkripsi dan Dekripsi

3.1.1 Pengujian Proses Enkripsi

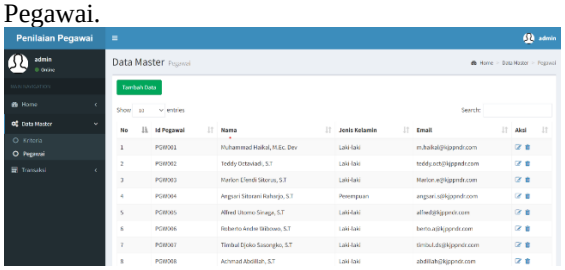
Pada gambar berikut ini adalah hasil enkripsi yang telah dilakukan pada database Pegawai di MySQL.



Gambar 6. Hasil Enkripsi Database Pegawai

3.1.2 Pengujian Proses Dekripsi

Pada gambar berikut ini adalah hasil dekripsi yang telah dilakukan pada Aplikasi Tampilan Menu Pegawai.



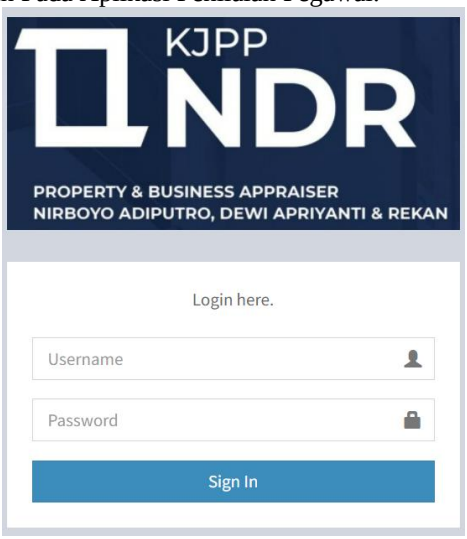
Gambar 7. Hasil Dekripsi Database Pegawai

3.2 Tampilan Layar Aplikasi Penilaian Pegawai KJPP NDR

Dari pertama kali aplikasi dijalankan hingga selesai, tampilan layar implementasi metode *Advanced Encryption Standard* (AES-256) dijelaskan pada bagian ini. Setiap tampilan pada aplikasi yang menggunakan metode *Advanced Encryption Standard* (AES-256) akan dijelaskan pada bagian selanjutnya.

3.2.1 Tampilan Layar Form Login

Berikut ini adalah Hasil Tampilan Layar Form Login Pada Aplikasi Penilaian Pegawai.



Gambar 8. Tampilan Layar Form Login

3.2.2 Tampilan Layar Menu Utama

Berikut ini adalah Hasil Tampilan Layar Menu Utama Pada Aplikasi Penilaian Pegawai.

Gambar 9. Tampilan Layar Menu Utama

3.2.3 Tampilan Layar Master Data Kriteria

Berikut ini adalah Hasil Tampilan Layar Master Data Kriteria Pada Aplikasi Penilaian Pegawai.

Gambar 10. Tampilan Layar Master Data Kriteria

3.2.4 Tampilan Layar Transaksi Penilaian

Berikut ini adalah Hasil Tampilan Layar Transaksi Pada Aplikasi Penilaian Pegawai.

Gambar 11. Tampilan Layar Transaksi Penilaian

4. KESIMPULAN

Berdasarkan analisa yang telah dilakukkan dalam upaya peerancangan, pembuatan, serangkaian uji coba dan analisis program Pengamanan Database Penilaian Pegawai Pada KJPP NDR menggunakan Algoritma AES 256. Beberapa kesimpulan dapat ditarik dari analisia permasalahan dan aplikasi yang dikembangkan berdasarkan permasalahan dan pemecahan masalah yang telah dijelaskan.

Penerapan algoritma AES-256 ini tentu masih memiliki beberapa keterbatasan. Dengan menggunakan algoritme *Advanced Encryption Standard* (AES-256) ini dapat meningkatkan keamanan data penilaian pegawai di KJPP NDR. Alangkah baiknya untuk pengembangan aplikasi ini secara bertahap dan berkelanjutan yang salah satunya membuat aplikasi ini agar dapat memproses enkripsi dan dekripsi data atau dokumen dengan format yang lebih variasi, serta dapat mencegah terjadinya pencurian data. Terjaga kerahasiaan internal sebuah perusahaan dari orang yang tidak bertanggung jawab, dan kecepatan enkripsi dan dekripsi juga tergantung pada *hardware*, *software* dan banyaknya data. Sehingga para pengguna yang terlibat pada dokumen rahasia suatu perusahaan tidak mengkhawatirkan akan kehilangan atau kerusakan dokumen.

DAFTAR PUSTAKA

[1] N. Anwar, M. Abduh, and N. B. Santosa, "Komparatif performance model keamanan menggunakan metode Algoritma AES 256 bit dan RSA," Jurnal Resti, vol. 2, no. 3, pp. 783–791, 2018, [Online]. Available: http://jurnal.iaii.or.id

[2] F. Ahmad Sitorus, N. Budi Nugroho, U. Fatimah Sari Sitorus Pane, P. Studi Mahasiswa, S. Triguna Dharma, and P. Studi Dosen Pembimbing, "Implementasi algoritma Advanced Encryption Standart (AES) 128-bit untuk keamanan data transaksi penjualan pada PT. Mitsubishi Electric Indonesia," Jurnal CyberTech, vol. 4, no. 5, pp. 1–15, 2021, [Online]. Available: https://ojs.trigunadharma.ac.id/

[3] A. Susilo et al., "Pengamanan File Video dengan Algoritma Advanced Encryption Standard (AES)," SYSTEMATICS, vol. 2, no. 1, pp. 28–32, 2020.

[4] Wahyu Pramusinto, Nugroho Wizaksono, and Ari Saputro, "Aplikasi pengamanan file dengan metode kriptografi AES 192, RC4 dan metode kompresi Huffman," Jurnal BIT, vol. 16, no. 2, pp. 47–53, 2019.

[5] Y. Wiharto and A. Irawan, "Enkripsi data menggunakan advanced encryption standard 256," Jurnal Kilat, vol. 7, no. 2, pp. 91–99, 2018.

[6] M. Dedi Irawan, "Implementasi kriptografi Vigenere cipher dengan php," 2017.

[7] Ade Rukmana and Irman Nurichsan, "Implementasi algoritma AES-Rijndael untuk enkripsi dan dekripsi data sms pada ponsel berbasis android," Jurnal Penelitian dan Pengembangan Teknik Elektro Telekomunikasi Indonesia, vol. 10, no. 2, pp. 48–53, 2019.

[8] D. Novianto and Y. Setiawan, "Aplikasi pengamanan informasi menggunakan metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES)," Jurnal Ilmiah Informatika Global, vol. 9, no. 2, pp. 83–89, 2018.

[9] D. Ardianta Sitepu and H. Khair MKom, "Implementasi pengamanan data menggunakan algoritma Advanced Encryption Standart (AES)," Jurnal Ilmiah Kaputama, vol. 6, no. 1, 2022.

[10] D. Nurnaningsih and A. A. Permana, "Rancangan aplikasi pengamanan data dengan Algoritma Advanced Encyption Standard (AES)," Jurnal Teknik Informatika, vol. 11, no. 2, pp. 177–186, Nov. 2018, doi: 10.15408/jti.v11i2.7811.