2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

PENERAPAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* 192 UNTUK MENGAMANKAN *DATABASE* PADA PT. PELITA INSAN ABADI

Teguh Apriyanto[1*], Hari Soetanto[2], Dolly Virgian Shaka Yudha Sakti[3], Rizky Pradana[4]

[1,2,3,]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia
[4]Sistem Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]teguhapriyanto.ta@gmail.com, [2]hari.soetanto@budiluhur.ac.id, [3]dolly.virgianshaka@budiluhur.ac.id, [4]rizky.pradana@budiluhur.ac.id
(* : corresponding author)

Abstrak-Penelitian ini dilakukan di PT. Pelita Insan Abadi dengan tujuan mengatasi permasalahan pencurian data penilaian pegawai dan memaksimalkan keamanan data dari oknum yang akan menyalahgunakan data ini. Maka sebagai upaya dari pengamanan data diperlukan perlindungan data dengan menggunakan metode kriptografi *Advanced Encryption Standard* 192, metode yang dilakukan pada penelitian ini adalah dengan di lakukannya implementasi rancangan *algoritme* kriptografi pada *database* dan dokumen penilaian pegawai di PT. Pelita Insan Abadi yang diharapkan dapat mencegah terjadinya pencurian data dan dengan menggunakan *algoritme Advanced Encryption Standard* (AES-192) dan meningkatkan keamanan data penilaian pegawai di PT. Pelita Insan Abadi. Hasil penelitian ini adalah dengan implementasi rancangan algoritme kriptografi pada *database* penilaian pegawai di PT Pelita Insan Abadi dapat mencegah terjadinya pencurian data dan meningkatkan keamanan data penilaian pegawai di PT Pelita Insan Abadi.

Kata Kunci: *Advanced Encryption Standard* 192, Meningkatkan Keamanan Data Penilaian Pegawai, Metode Kriptografi, Keamanan Basis Data.

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD-192 CRYPTOGRAPHY TO SECURE DATABASE AT PT. PELITA INSAN ABADI

Abstract- *This research was conducted at PT. Pelita Insan Abadi with the aim of overcoming the problem of theft of employee assessment data and maximizing data security from persons who will misuse this data. So as an effort to secure data, it is necessary to protect data using the Advanced Encryption Standard 192 cryptographic method. The method used in this research is to implement a cryptographic algorithm design on databases and employee assessment documents at PT. Pelita Insan Abadi which is expected to be able to prevent data theft and by using the Advanced Encryption Standard (AES-192) algorithm and improve the security of employee assessment data at PT. Pelita Insan Abadi. The results of this study are that by implementing a cryptographic algorithm design on the employee appraisal database at PT Pelita Insan Abadi it can prevent data theft and improve the security of employee appraisal data at PT Pelita Insan Abadi.*

Keywords*: Advanced Encryption Standard 192, Improving employee assessment data security, Cryptographic Methods, Data Security.*

1. PENDAHULUAN

Komputer adalah suatu alat yang perangkat yang membutuhkan suatu keamanan penyimpanan *database* ataupun data-data informasi pribadi atau perusahaan yang sangat penting dan tidak boleh dibiarkan begitu saja [1].

PT Pelita Insan Abadi mempunyai *database* dimana dokumen-dokumen yang penting, penyimpanan data tempat riset masih menggunakan sistem penyimpanannya secara manual yang mana rentan sekali terjadi *sabotase* data. Permasalahan pada PT Pelita Insan Abadi adalah belum adanya keamanan yang mumpuni pada sistem database pegawai sehingga rentan untuk terjadinya pencurian data. Kriptografi merupakan metode yang biasa digunakan untuk mengamankan beberapa data-data ataupun informasi untuk melindungi data perusahaan keamanan [2]. Maka penulis menggunakan metode ini untuk pengamanan data-data menggunakan Teknik algoritma kriptografi AES 192. Masing-masing penyamatan mengenkripsi dan mendekripsi data kedalam 128 bit menggunakan kripstografi 192, 128, 256 bit. [3]. AES 192 juga digunakan untuk mengamankan beberapa informasi maupun data yang tidak dapat dibaca oleh pihak pihak yang ingin merugikan perusahaan. Di karenakan data-data yang sudah di enkripsi mempunyai kodenya sendiri[4].

Pelita Insan Abadi membutuhkan pengamanan data khususnya pada *database* dan dokumen penilaian pegawai tersebut. Kriptografi memiliki proses enkripsi dan juga proses dekripsi yang dimana proses enkripsi itu ialah proses mengubah informasi jadi bentuk yang tidak akan dapat dimengerti (*Chipertext*). Proses dekripsi mengembalikkan informasi dari *chipertext* yang telah dienkripsi [5].

Sistem ini bisa digunakan untuk mengimplementasikan metode algoritma kriptografi AES-192 dan guna untuk memproteksi data-data penilaian pegawai dari berbagai ancaman dari sisi yang tidak berkepentingan dan tujuan berdasarkan rumusan masalah yang didapat. Penerapan kriptografi pada data-data yang di terima di PT pelita Insan Abadi Untuk mencegah terjadinya pencurian ataupun terjadinya halhal yang merugikan PT Pelita Insan Abadi dan dengan menggunakan Metode Algoritma ini bisa bermanfaat untuk mengamankan data-data yang akan dienkripsi dan dekripsi [6].

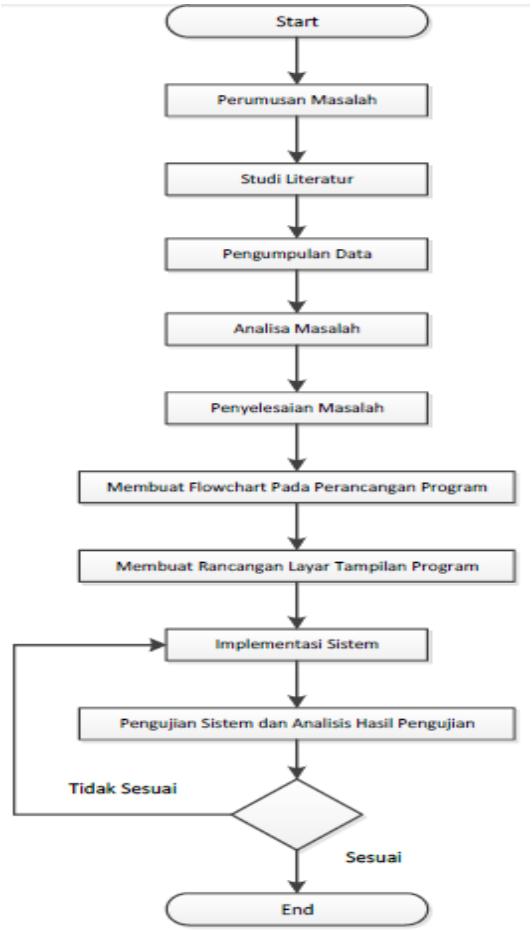
Kriptografi yang digunakan militer dapat diterapkan oleh bangsa Spartan berbentuk sepotong *papyrus* atau *parkamen* dan dibungkus dengan batang-batang kayu. Sistem ini disebut *Scytale* [7] Sistem *disk* digunakan secara luas selama perang sipil US. untuk mengkode dan mendekodekan sinyal-sinyal bendera diantara unit-unit [8].

Tujuan dari penelitian ini adalah melakukan implementasi rancangan *algoritme* kriptografi pada *database* penilaian pegawai di PT. Pelita Insan Abadi untuk mencegah terjadinya pencurian data dan meningkatkan keamanan data penilaian pegawai menggunakan *algoritme Advanced Encryption Standard* (AES-192).

Manfaat dari penelitian ini untuk perusahaan adalah memberikan keamanan data penting yang ada. Ada juga untuk manfaat di bidang ilmu Teknik Informatika yaitu menjadi referensi bagi penelitian selanjutnya di bidang keamanan data dengan Teknik *algoritme* kriptografi. Serta, manfaat untuk penulis sendiri yaitu menambah wawasan dan mengimplementasikan di bidang keamanan data dengan menggunakan Teknik kriptografi dan *algortime* AES 192.

2. METODE PENELITIAN

Metode *algorithm* ini ialah riset yang digunakan dalam pelaksanaan riset agar tujuan yang telah ditentukan tidak menyimpang [9].



Gambar 1. Tahapan Penelitian

a. Perumusan Masalah

Metode Algoritma ini biasanya dapat ditentukan dengan masalah-masalah yang akan dialami dan untuk menuntaskan dalam perumusan masalah metode ini metode AES 192

b. Studi Literatur

Pada studi kasus literatur ini dapat disimpulkan menggunakan alat bantu dan konsep yang digunakan dalam menggunakan penelitian ini. Studi ini biasa dapat dilakukan menggunakan alat bantu ataupun metode yang dapat digunakan oleh proses ini.

c. Pengumpulan data

Pada Metode Algoritma ini dapat disimpulkan untuk mengumpulkan data yang telah dijelaskan diatas. Segala tahapan untuk proses data pengumpulan dan di kumpulkan dari narasumber.

1. Wawancara

   Wawancara ialah pengumpulan data-data dengan narasumber yang mengalami terjadinya proses pembuatan aplikasi untuk mendapatkan informasi mengenai kemanan data untuk mendapatkan hasil yang lebih baik.

2. Observasi

   Observasi adalah satu cara Teknik pengambilan data-data yang cukup efisien untuk mempelajarkan dan mengamati suatu cara dalam *system* observasi. Dilakukan dengan cara pengamatan secara langsung.

d. Analisa Masalah & Penyelesaian Masalah

Setelah melakukan pengambilan data-data, Langkah selanjutnya ialah menganalisa masalah-masalah terkait dalam system yang akan dirancang sesuai kebutuhan yang telah ditentukan dalam proses ini:

1. Analisa Data

   Analisa data adalah salah satu tahap yang dilakukan untuk penyelesaian permasalahan keamanan ini, dalam analisa data dilakukan beberapa tindakan sebagai berikut :

   a) Pengumpulan data yang berfungsi untuk memperoleh data yang diperlukan dalam perancangan program.
   b) Pengelompokan data sesuai dengan jenis dan fungsinya.

e. Perancangan modul enkripsi, dekripsi, dan antarmuka serta integrasi dengan aplikasi dilakukan setelah analisis sistem. Metode *Waterfall* dipilih untuk pengembangan perangkat lunak dengan tuntutan penyelesaian tahap secara tuntas dan dokumentasi yang baik.

f. Pengujian sistem menggunakan metode *blackbox* untuk menjamin kesesuaian dengan hasil analisis dan perancangan. Metode ini digunakan untuk menemukan kesalahan dan mengevaluasi fungsional aplikasi saat dioperasikan.

2.1 *Advanced Encryption Standard*

a. *Algoritme* Enkripsi AES-192

Ringkasan proses algoritme enkripsi *Advanced Encryption Standard* 192 sebagai berikut :

1. *Key Expansion*: Kunci 192-bit di-*generate* menjadi 52 sub-kunci dengan panjang masing-masing 128-bit melalui proses *Key Expansion Algorithm*.
2. *AddRoundKey*: Blok *plaintext* (16-byte) dipadankan dengan sub-kunci pertama (128-bit) dengan melakukan operasi XOR antara kedua blok.
3. *SubBytes*: Setiap *byte* dalam blok di-substitusi dengan nilai lain menggunakan *S-Box*.
4. *ShiftRows*: Setiap baris dalam blok dipindahkan ke kiri sebanyak *byte* yang sesuai dengan nomor barisnya.
5. *MixColumns*: Setiap kolom dalam blok diubah dengan menggunakan operasi matematika tertentu yang melibatkan nilai-nilai di dalam kolom tersebut.
6. *Repeat Rounds*: Langkah 2-5 diulangi sebanyak 11 kali (total putaran enkripsi adalah 12) dengan blok *plaintext* dan sub-kunci yang diambil secara berurutan.
7. *Final Round*: Langkah 2-4 diulangi untuk putaran terakhir, tetapi tidak ada operasi *MixColumns* yang dilakukan.
8. *AddRoundKey*: Blok *ciphertext* dihasilkan dengan melakukan operasi *XOR* antara blok *plaintext* yang telah diproses dengan sub-kunci terakhir.

9. Blok *ciphertext* yang dihasilkan digabungkan menjadi satu data yang utuh.

Dalam proses enkripsi AES-192, setiap blok *plaintext* diolah secara terpisah menggunakan kunci yang berbeda pada setiap putaran enkripsi. Nilai-nilai dalam blok *plaintext* diubah dengan menggunakan operasi matematika tertentu yang membuat ketergantungan antara nilai-nilai tersebut semakin kompleks, sehingga membuat serangan pada enkripsi menjadi lebih sulit .

b. Algoritme Dekripsi AES-192

Proses *decryption* ialah pembalikkan dari proses enkripsi. Langkah-langkah proses *decryption* sebagai berikut:

1. *Key Expansion*: Kunci 192-bit di-*generate* menjadi 52 sub-kunci dengan panjang masing-masing 128-bit melalui proses *Key Expansion Algorithm*.
2. *AddRoundKey*: Blok *ciphertext* dipadankan dengan sub-kunci terakhir (128-bit) dengan melakukan operasi *XOR* antara kedua blok.
3. *InverseShiftRows*: Setiap baris dalam blok *ciphertext* dipindahkan ke kanan sebanyak *byte* yang sesuai dengan nomor barisnya.
4. *InverseSubBytes*: Setiap *byte* dalam blok di-*substitusi* kembali dengan nilai aslinya menggunakan *Inverse S-Box*.
5. *Repeat Rounds*: Langkah 2-4 diulangi sebanyak 11 kali (total putaran dekripsi adalah 12) dengan blok *ciphertext* dan sub-kunci yang diambil secara berurutan.
6. *Final Round*: Langkah 2-3 diulangi untuk putaran terakhir, tetapi tidak ada operasi *MixColumns* yang dilakukan.
7. *AddRoundKey*: Blok *plaintext* dihasilkan dengan melakukan operasi *XOR* antara blok *ciphertext* yang telah diproses dengan sub-kunci pertama.
8. Blok *plaintext* yang dihasilkan digabungkan menjadi satu data yang utuh.

Proses dekripsi AES-192 juga menggunakan setiap blok *ciphertext* secara terpisah dan menggunakan sub-kunci yang berbeda pada setiap putaran dekripsi. Setiap putaran dekripsi melibatkan operasi-*invers* dari langkah-langkah enkripsi. Dalam proses dekripsi AES-192, blok *ciphertext* diproses terbalik dari proses enkripsi, sehingga menghasilkan blok *plaintext* yang sesuai dengan blok plaintext yang digunakan dalam proses enkripsi [10].

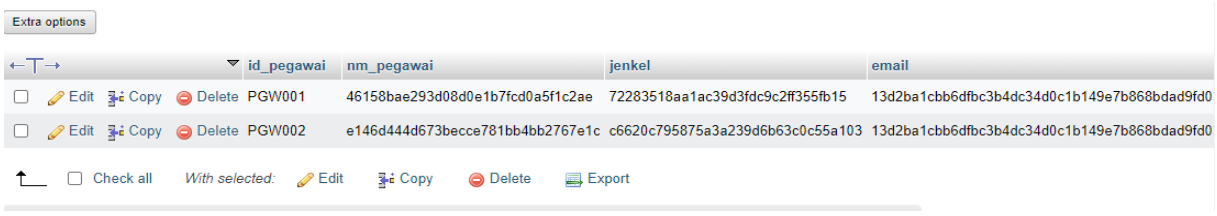
3. HASIL DAN PEMBAHASAN

Pada penelitian ini, dapat diperoleh hasil sebagai berikut :

3.1 Pengujian Enkripsi dan Dekripsi

3.1.1 Pengujian Proses Enkripsi

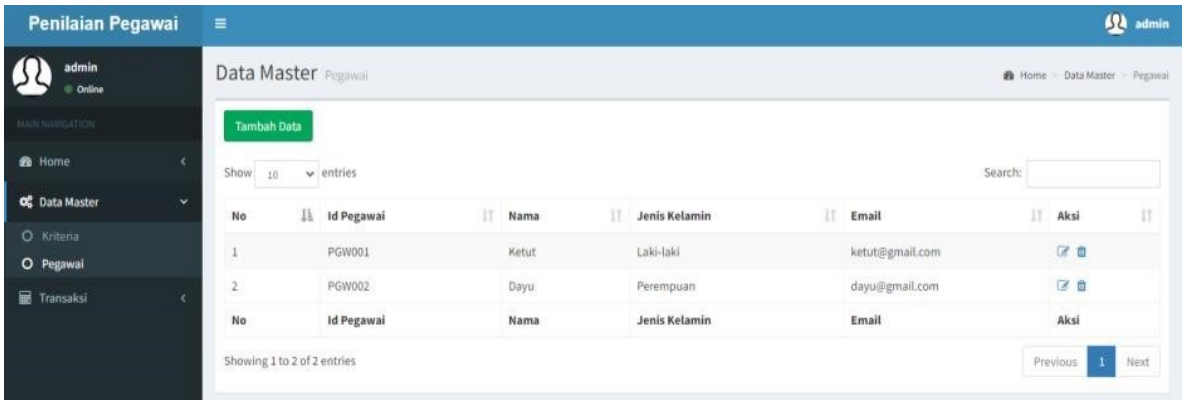
Pada Gambar 2 menampilkan hasil enkripsi yang telah dilakukan pada *database* pegawai, sebelumnya di*input*kan di aplikasi program tambah data pegawai.



Gambar 2. Enkripsi Pegawai

3.1.2 Pengujian Proses Dekripsi

Pada Gambar 3 menampilkan hasil dekripsi atau *output* yang telah dilakukan pada menu pegawai, sebelumnya diinputkan di aplikasi program tambah data pegawai.



Gambar 3. Dekripsi Pegawai

3.2 Pengujian Waktu Enkripsi

Pengujian waktu enkripsi ini adalah proses penelitian untuk mendapatkan informasi mengenai waktu yang dibutuhkan untuk enkripsi dokumen menggunakan kriptografi AES 192. Tabel 1 adalah hasil pengujian waktu enkripsi.

Tabel 1. Pengujian Waktu Enkripsi

No	Nama File Asli	Ukuran Asli File (Kb)	Nama File Setelah dienkripsi	Ukuran File setelah dienkripsi	Waktu enkripsi (detik)
1	CV_1.jpg	93 kb	CV_1.rda	93 kb	01 Detik
2	CV_2.jpg	65 kb	CV_2.rda	65 kb	01 Detik
3	CV_3.jpg	533 kb	CV_3.rda	533 kb	08 Detik
4	CV_4.jpg	88 kb	CV_4.rda	88 kb	01 Detik
5	CV_5.jpg	149 kb	CV_5.rda	149 kb	02 Detik

3.3 Pengujian Waktu Dekripsi

Pengujian waktu dekripsi ini adalah proses penelitian untuk mendapatkan informasi mengenai waktu yang dibutuhkan untuk dekripsi dokumen menggunakan kriptografi AES 192. Tabel 2 adalah hasil pengujian waktu dekripsi.

Tabel 2. Pengujian Waktu *Decryption*

No	Nama File Asli	Ukuran Asli File (Kb)	Nama File Setelah didekripsi	Ukuran File setelah di dekripsi	Waktu dekripsi (detik)
1	CV_1.rda	93 kb	CV_1.jpg	93 kb	01 Detik
2	CV_2.rda	65 kb	CV_2.jpg	65 kb	01 Detik
3	CV_3.rda	533 kb	CV_3.jpg	533 kb	09 Detik
4	CV_4.rda	88 kb	CV_4.jpg	88 kb	01 Detik
5	CV_5.rda	149 kb	CV_5.jpg	149 kb	02 Detik

3.4 Tampilan Layar

Penjelasan tampilan layar aplikasi implementasi metode AES-192 disajikan dari awal hingga selesai. berikut tampilan layar:

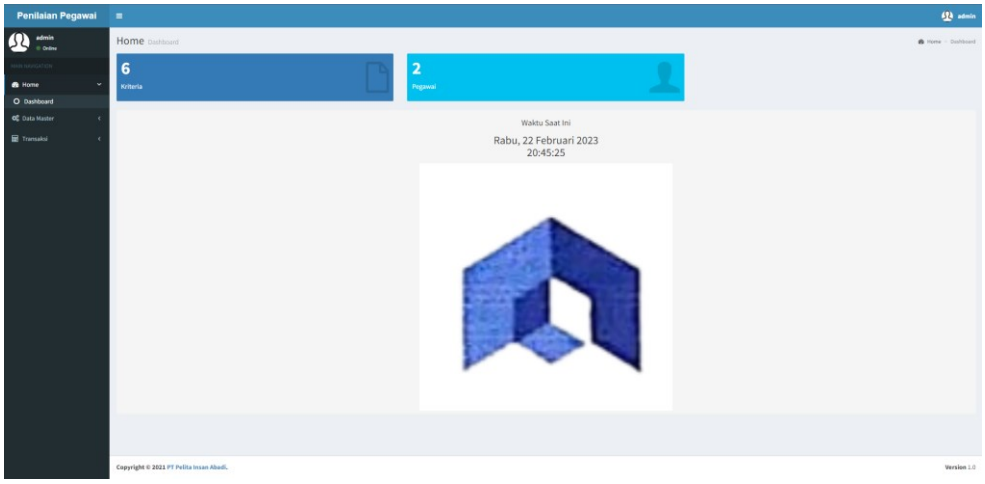
3.4.1 Tampilan Layar Form Login

Berikut adalah halaman login yang dimana pengguna wajib untuk mengisi login sesuai yang dimiliki.

Gambar 4. Tampilan Layar Form Login

3.4.2 Hasil Menu Utama Pelita Insan Abadi

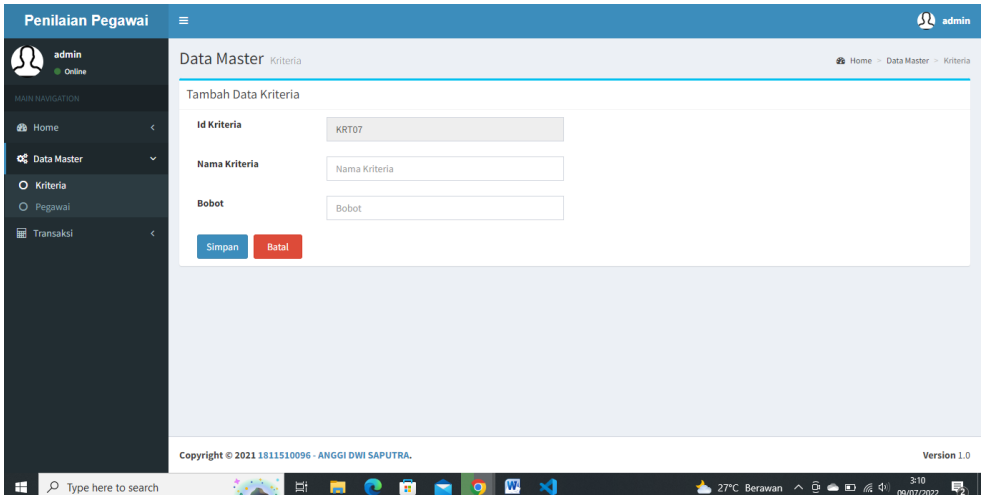
Tampilan Menu Utama memperlihatkan akses ke menu Data Master dan Transaksi. Menu Data Master memiliki sub menu Data Kriteria dan Data Pegawai, sedangkan sub menu Transaksi memiliki fitur Penilaian. Admin harus login terlebih dahulu untuk mengakses menu dan sub menu di Menu Utama. Gambar 5 menampilkan tampilan Menu Utama.



Gambar 5. Tampilan Menu Utama

3.4.3 Hasil Layar Master Kriteria

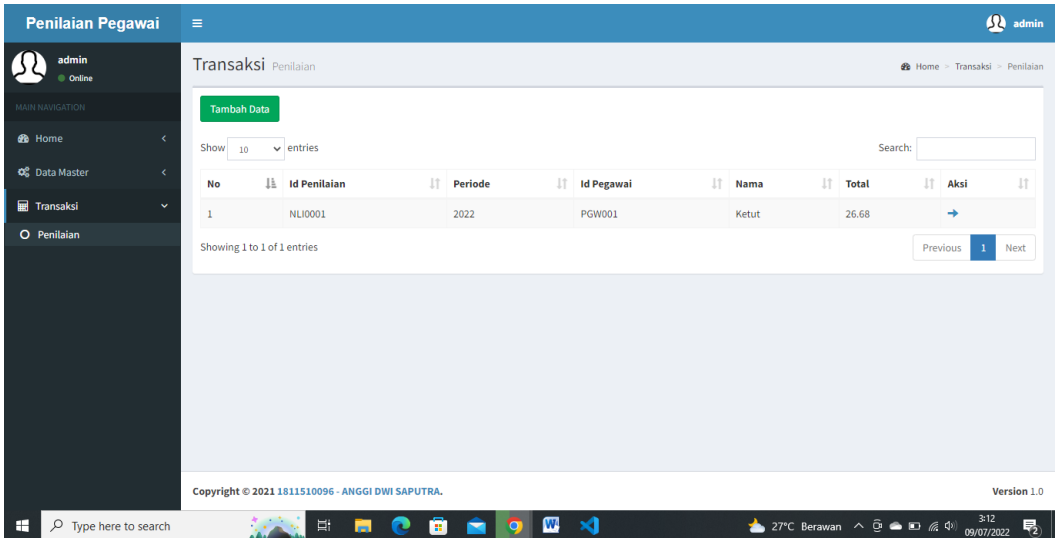
Tampilan Master Data Kriteria menampilkan tombol tambah data untuk menambahkan id kriteria, nama kriteria, dan bobot. Gambar 6 menunjukkan tampilan layar tambah data pada Master Data Kriteria.



Gambar 6. Hasil Layar Tambah Kriteria

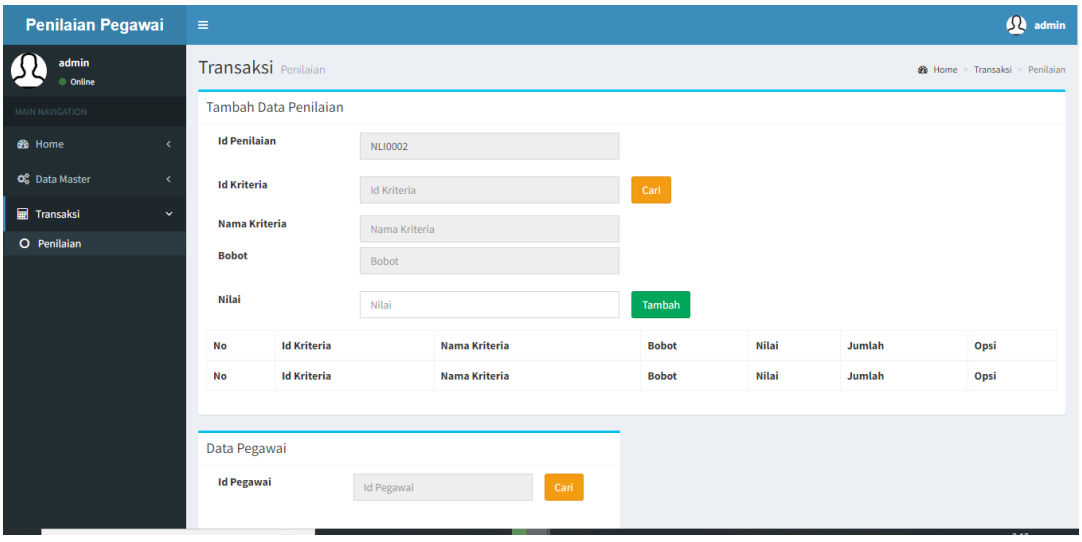
3.4.4 Hasil Transaksi Penilaian

Tampilan Form Transaksi Data Penilaian pada Gambar 7 menampilkan panel dengan id penilaian, periode, id pegawai, dan nama. Terdapat tombol tambah data untuk memasukkan informasi tersebut. Gambar 7 menunjukkan tampilan layar pada Transaksi Data Penilaian.



Gambar 7. Tampilan Layar Transaksi Data Penilaian

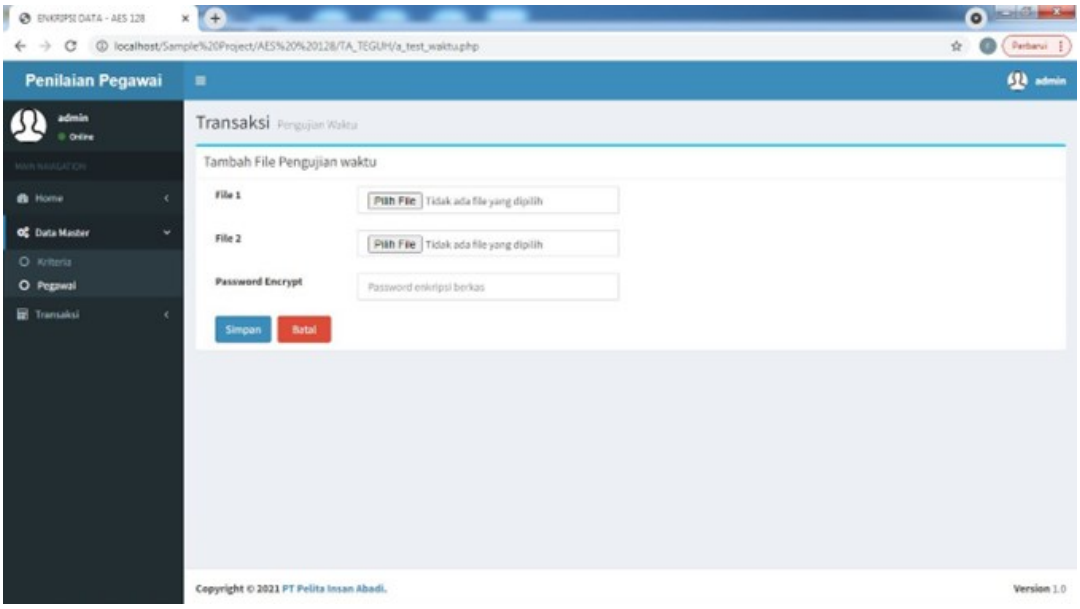
Tampilan Transaksi Data Penilaian pada Gambar 8 menunjukkan tombol tambah data untuk menambahkan informasi id penilaian, periode, id pegawai, dan nama. Gambar 8 menampilkan tampilan layar tambah data pada Transaksi Data Penilaian.



Gambar 8. Tampilan Layar Tambah Data Penilaian

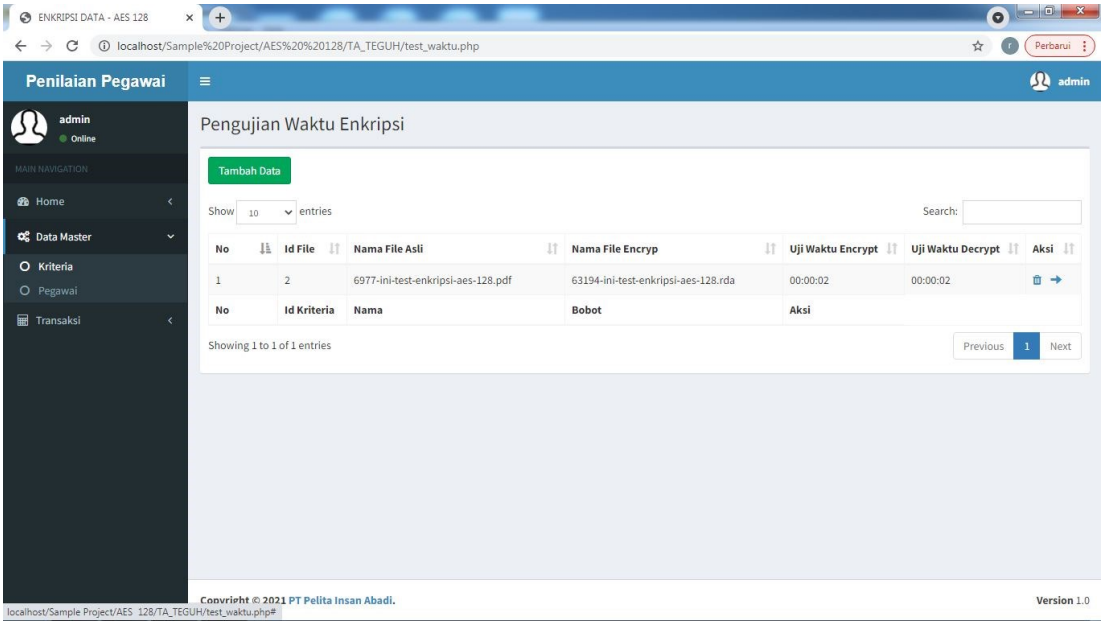
3.4.5 Hasil Layar Transaksi Data Pengujian Waktu

Gambar 9 menunjukkan Transaksi Data Pengujian Waktu dengan tombol tambah data untuk menambahkan informasi *file* 1, *file* 2, dan *password encrypt*. Gambar tersebut menampilkan tampilan layar tambah data pada Transaksi Data Pengujian Waktu.



Gambar 9. Tampilan Layar Tambah Data Pengujian Waktu

Gambar 10 menunjukkan Form Transaksi Data Pengujian Waktu, yang terdiri dari id *file*, nama *file* asli, nama *file encrypt*, uji waktu *encrypt*, dan uji waktu *decrypt*. Ada tombol tambah data untuk menambah data baru pada form tersebut.



Gambar 10. Tampilan Transaksi Data Pengujian Waktu

4. KESIMPULAN

Dengan dilakukannya implementasi rancangan algoritme kriptografi pada database penilaian pegawai menggunakan algoritme AES-192 dapat mengembangkan keamanan data penilaian pegawai serta mencegah terjadinya pencurian data di PT Pelita Insan Abadi. Algoritma Kriptografi ialah selalu ditingkatkan, karena berkembangnya ilmu pengatahuan *computer* di bidang kriptografi dan di dunia komputer, maka tidak dapat dilihat bahwa metode ini dapat berjalan dengan baik semestinya. Program ataupun metode enkripsi ini dapat membantu pekerjaan menjadi lebih baik. Dengan algoritma ini diharapkan dapat membantu mengamankan beberapa data yang akan di simpan dan dienkripsi dengan baik menggunakan Metode Algoritma AES- 192.

DAFTAR PUSTAKA

[1] D. Novianto and Y. Setiawan, "Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi *Advanced Encryption Standard* (AES)," *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jig.v9i2.561.

[2] Y. Wiharto and A. Irawan, "Enkripsi Data Menggunakan AES 256," vol. 7, no. 2, pp. 91–99, 2018.

[3] N. Anwar, M. Munawwar, M. Abduh, and N. B. Santosa, "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 3, pp. 783–791, 2018, doi: 10.29207/resti.v2i3.606.

[4] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma *Advanced Encyption Standard* (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[5] N. Cristy and F. Riandari, "Implementasi Metode *Advanced Encryption Standard* (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komput. dan Sist. Informasi]*, vol. 4, no. 2, pp. 75–85, 2021, [Online]. Available: https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

[6] M. Simanjuntak, T. Pasaribu, and S. Rahmadilla, "Implementasi Algoritma Merkle Hellman untuk Keamanan Database," *MEANS (Media Inf. Anal. dan Sist.*, vol. 4, no. 1, pp. 46–50, 2019, doi: 10.54367/means.v4i1.327.

[7] J. Prayudha, _ S., and _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode *Advanced Encryption Standard* (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.

[8] W. Pramusinto, N. Wizaksono, and A. Saputro, "Aplikasi Pengamanan File Berbasis Web Dengan Metode Kriptografi Aes 192, Rc4 Dan Metode Kompresi Huffman," *J. Bit*, vol. 16, no. 2, pp. 47–53, 2019, [Online]. Available: https://journal.budiluhur.ac.id/index.php/bit

[9] B. A. Wijaya, M. Harahap, and S. Aisyah, "Perancangan Aplikasi Enkripsi Data Menggunakan Algoritma XXTEA," *J. Sist. Inf. dan Ilmu Komput. Prima(JUSIKOM PRIMA)*, vol. 3, no. 2, pp. 7–12, 2020, doi: 10.34012/jusikom.v3i2.847.

[10] D. Saputra and D. Kusumaningsih, "Implementasi Keamanan Database Menggunakan Algoritma Aes-192 Pada Pt Gurita Lintas Samudera Berbasis Android," *J. Skanika*, vol. 1, no. `Vol 1 No 3 (2018): Jurnal SKANIKA Juli 2018, pp. 884–888, 2018, [Online]. Available: http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2501