Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
Jakarta – Indonesia, 06 September 2022

ALGORITME AES-256 UNTUK KEAMANAN BASIS DATA PENILAIAN PEGAWAI PADA PT. BUANA JAYA KORINDO

Anggi Dwi Saputra[1*], Mohammad Syafrullah[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]anggidwisaputra2510@gmail.com, [2]mohammad.syafrullah@budiluhur.ac.id
(* : corresponding author)

Abstrak-Perkembangan ilmu pengetahuan teknologi sangatlah pesat dan telah merambah pada segala aspek yang menyangkut hampir semua kebutuhan pekerjaan manusia. Begitu pesatnya teknologi ini memungkinkan manusia untuk berkomunikasi, bertukar informasi, maupun bertukar data. Data atau dokumen selalu menjadi perhatian di setiap organisasi, instansi pemerintah atau dunia bisnis. PT. Buana Jaya Korindo yang menjadi salah satu perusahaan yang memiliki data atau dokumen berupa arsip penting. Problematika yang dihadapi oleh perusahaan ini ialah terjadinya pencurian data penilaian pegawai dan kurangnya keamanan data dari oknum yang akan menyalahgunakan data ini. Oleh karena itu, penelitian ini berupaya mengamankan data dengan mengimplementasikan teknik kriptografi melalui proses enkripsi dan dekripsi di dalamnya. Salah satu algoritma kriptografi yang populer adalah AES (*Advanced Encryption Standard*) 256, dimana algoritme ini memiliki 14 blok putaran yang cukup rumit sehingga dapat membantu proses pengamanan data di PT. Buana Jaya Korindo. Hasil dari penelitian ini mampu mencegah terjadinya pencurian data karena peningkatan keamanan data penilaian pegawai di PT. Buana Jaya Korindo.

Kata Kunci: AES-256, basis data, kriptografi

AES-256 ALGORITHM FOR EMPLOYEE ASSESSMENT DATABASE SECURITY AT PT. BUANA JAYA KORINDO

Abstract-*The development of science and technology is very rapid and has penetrated in all aspects concerning almost all the needs of human work. So rapidly this technology allows humans to communicate, exchange information, and exchange data. Data or documents are always a concern in every organization, government agency or business world. PT. Buana Jaya Korindo, which is one of the companies that has data or documents in the form of important archives. The problems faced by this company are the theft of employee assessment data and the lack of data security from individuals who will misuse this data. Therefore, this study seeks to secure data by implementing cryptographic techniques through the encryption and decryption processes in it. One of the popular cryptographic algorithms is AES (Advanced Encryption Standard) 256, where this algorithm has 14 round blocks which are quite complicated so that it can help the process of securing data at PT. Buana Jaya Korindo. The results of this study were able to prevent the occurrence of data theft due to increased security of employee assessment data at PT. Buana Jaya Korindo.*

Keywords*: AES-256, database, cryptography*

1. PENDAHULUAN

Ilmu pengetahuan bidang teknologi informasi telah berkembang luar biasa pesat. Hal ini ditandai dengan merambah ke berbagai aspek menyangkut kebutuhan pekerjaan manusia. Pesatnya teknologi memungkinkan manusia untuk mampu memberi maupun menerima informasi dengan kecepatan tinggi. Keamanan dalam suatu penyimpanan dokumen atau data merupakan urgensi yang tidak bisa dilewatkan. Tingginya tingkatan teknologi komputer berbanding lurus terhadap tingkat ancaman keamanan data pada komputer. Data atau dokumen selalu menjadi perhatian di setiap organisasi, instansi pemerintah atau dunia bisnis. Berbagai celah yang ditemukan di suatu sistem keamanan data selalu membuat sebagian pihak berusaha untuk meretas data atau dokumen. Bahkan, tanpa ada alasan jelas mengapa mereka mengubah atau merusaknya. Apabila hal demikian dibiarkan, maka akan merugikan bagi perusahaan, instansi atau *stakeholder*. Melihat betapa urgensi sebuah data atau dokumen, perlu diwujudkan suatu langkah dimana data atau dokumen yang dimiliki selalu terjaga kerahasiaannya. Satu dari sekian cara yang bisa diterapkan ialah menjadikan isi informasi dari suatu data atau dokumen penting menjadi suatu kode atau sandi yang sukar dimengerti.

PT. Buana Jaya Korindo termasuk perusahaan yang mempunyai data atau dokumen berupa arsip yang penting. Penyimpanan data yang dimiliki perusahaan ini masih disimpan secara manual dan rentan sekali terjadi peretasan data. Perusahaan ini belum menerapkan keamanan yang mumpuni pada sistem penilaian pegawai sehingga rentan

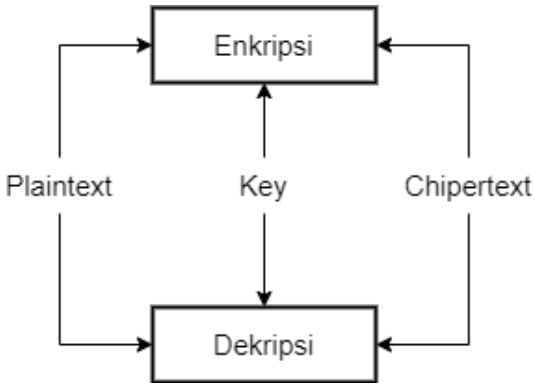
untuk terjadinya pencurian data. Dalam hal ini, diperlukan perlindungan data dengan menggunakan teknik kriptografi.

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*) [1].

Ada banyak penelitian yang terkait dengan penelitian ini yang diantaranya penelitian [2] mengenai penerapan sekuritas basis data penilaian pegawai pada PT. Capella Medan menggunakan AES. ada pula penelitian yang menerapkan algoritma *Merkle Hellman* untuk keamanan basis data oleh [3]. Algoritma AES juga telah diterapkan pada pengembangan aplikasi *chat messenger* oleh [4] agar aman dari penyadapan atau manipulasi. Terakhir, penggunaan AES untuk keamanan data keuangan oleh [5] pada SMK Harapan Bangsa agar aman dari pencurian data.

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" [6]. 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 [7].

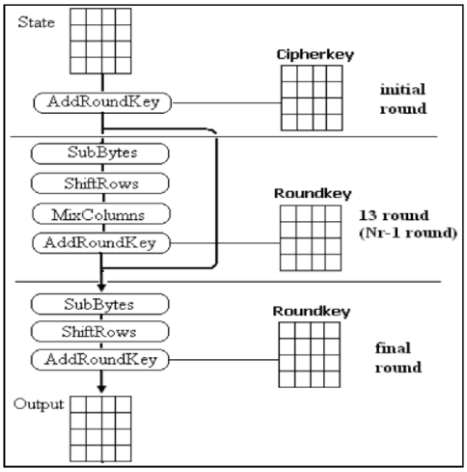
Konsep dasar kriptografi berkaitan erat dengan enkripsi dan dekripsi seperti yang telah dijelaskan sebelumnya. Enkripsi bertujuan untuk mengkonversikan pesan jelas (*plaintext*) ke pesan yang telah disandikan (*ciphertext*) dengan sedikit penambahan ukuran berkas. Sebaliknya, menerjemahkan *ciphertext* menjadi *plaintext* disebut dengan dekripsi. Proses dari kedua hal ini juga memerlukan komponen satu atau beberapa kunci kriptografi serta algoritma untuk memproses penyandian dokumen [8]. Alur enkripsi dan dekripsi bisa diamati pada gambar 1.



Gambar 1. Proses enkripsi dan dekripsi

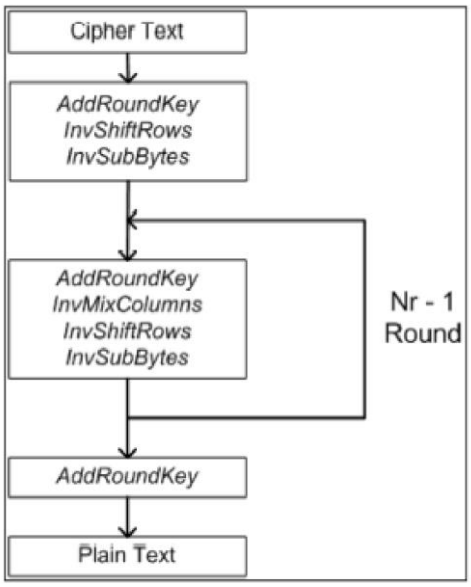
Advanced Encryption Standard (AES) menjadi salah satu algoritma kriptografi yang dapat digunakan untuk mengamankan data dengan blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi [9]. Dengan menggunakan algoritma AES, keamanan data bisa ditingkatkan kepada 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 [10].

Tahapan awal enkripsi pada AES terdiri dari 4 macam transformasi *bytes* yang diantaranya *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Permulaan tahapan enkripsi ini, ketika input yang telah diduplikasi pada *state* akan mengalami perubahan *byte AddRoundKey*. *State* akan bertransformasi menjadi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara *repeatable* sebanyak Nr, tahapan ini disebut sebagai *round function*. *Round* yang terakhir sedikit berbeda dengan *round* sebelumnya karena terletak pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns*. Tahapan enkripsi AES dapat dilihat pada gambar 2.



Gambar 2. Tahapan enkripsi AES

Pada tahap dekripsi, transformasi *cipher* dapat dibalikkan dan diterapkan dalam arah yang berbeda untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*. Tahapan proses dekripsi AES dapat dilihat pada gambar 3.



Gambar 3. Tahapan dekripsi AES

2. METODE PENELITIAN

2.1 Identifikasi Masalah

Langkah awal ini perlu dilaksanakan akumulasi data terkait penelitian yang menjadi fokus utama melalui observasi dan wawancara terlebih dahulu, dalam hal ini pada PT. Buana Jaya Korindo yang sedang rentan akan keamanan data. Masalah yang terkumpul akan dianalisa dan dirancang sebuah solusi termasuk perancangan aplikasi untuk keamanan data.

2.2 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-25. Sehingga, didapatkan pondasi rujukan yang mendukung dan akurat dalam menentukan metode yang tepat untuk menyelesaikan permasalahan yang akan diteliti dalam penelitian ini.

2.3 Perancangan

Tahapan ini dimulai perancangan aplikasi seperti pada hasil analisis sistem sebelumnya, terutama perancangan yang berhubungan dengan algoritma AES-256, dan metode pendukung lain yang akan diintegrasikan dengan aplikasi, serta perancangan antarmuka yang akan dibangun.

Pada pengembangan perangkat lunak ini, digunakan metode konvensional yaitu dengan menggunakan metode *Waterfall* yang Model ini mensyaratkan penyelesaian suatu tahap secara menyeluruh sebelum berpindah kepada tahap berikutnya dan *output* dari setiap tahap harus terekam dengan baik pada suatu dokumen.

2.4 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.

2.5 Pengujian

Tahapan terakhir yaitu pengujian yang dilakukan dengan tujuan untuk menjamin jika aplikasi yang akan dibuat telah memenuhi hasil dari analisis dan perancangan serta menghasilkan satu kesimpulan yaitu, apakah aplikasi tersebut sesuai dengan yang diharapkan atau tidak. Maka, diperlukan sebuah model pengujian yang akan dijadikan tolak ukur sehingga dapat disimpulkan bahwa aplikasi telah berjalan semestinya dengan tujuan yang telah direncanakan. Model pengujian yang dipakai yaitu *blackbox*, suatu metode untuk mengetahui *error system* dan melakukan demonstrasi fungsionalitas saat aplikasi tersebut dioperasikan, apakah input dan *ouput* diterima dan dihasilkan telah sesuai persis dengan yang diharapkan atau menyimpang.

3. HASIL DAN PEMBAHASAN

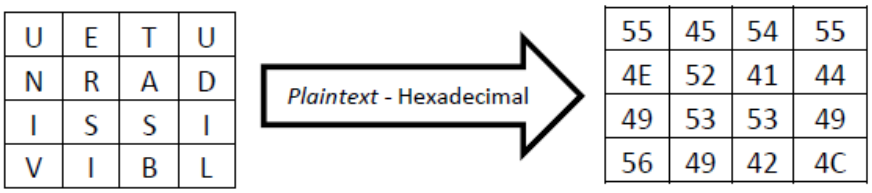
3.1 Algoritma Aplikasi

Pada algoritma AES-256 untuk proses enkripsi dan dekripsi yang telah diterapkan pada aplikasi, diambil kata kunci “UNIVERSITASBUDIL” pada contoh kasus ini. Kemudian, dibuat sebuah *key* yang mewakili setiap karakter dari kata kunci tersebut. Kedua dari ini diperlukan untuk alur enkripsi dan dekripsi menggunakan algoritma AES-256. Kata kunci dan *key* yang dimaksudkan sebelumnya dapat dilihat pada gambar 4.

Plaintext	U	N	I	V	E	R	S	I	T	A	S	B	U	D	I	L
Key	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6

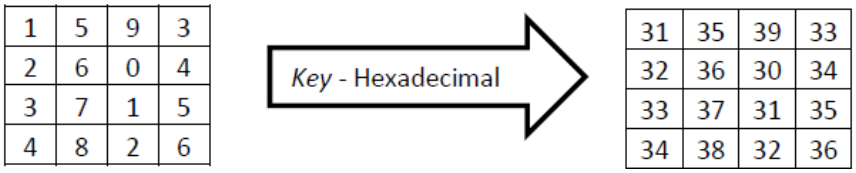
Gambar 4. Tabel *plaintext* dan *key*

a. Pertama, mengubah karakter di setiap kata kunci “UNIVERSITASBUDIL” menjadi bilangan Hexadesimal. Ilustrasi pengubahan karakter ini dapat diamati pada gambar 5.



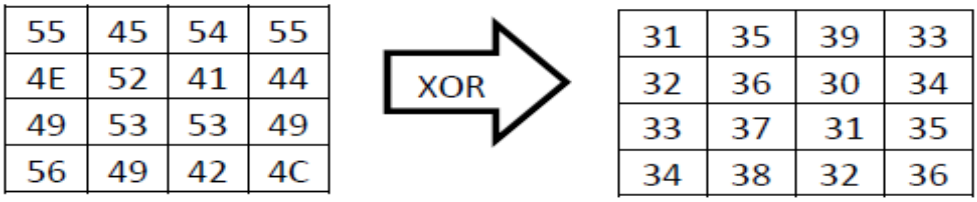
Gambar 5. *Plaintext to hexadecimal*

b. Kemudian, mengubah *key* pada kata kunci "UNIVERSITASBUDIL" menjadi bilangan Hexadesimal seperti tahapan pertama. Ilustrasi pengubahan *key* ini dapat diamati pada gambar 6.

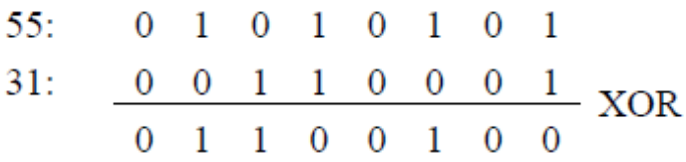


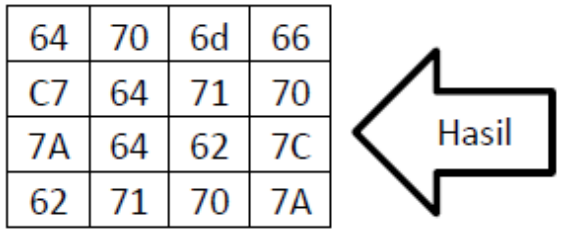
Gambar 6. *Key to hexadecimal*

c. Setelah itu, gabungkan Hexadesimal dari *plaintext* dengan *chiperkey* dengan fungsi XOR, ini yang dinamakan proses Add *RoundKey*. Perhatikan gambar 7 dan gambar 8 untuk ilustrasi proses dan hasil *Add RoundKey*.



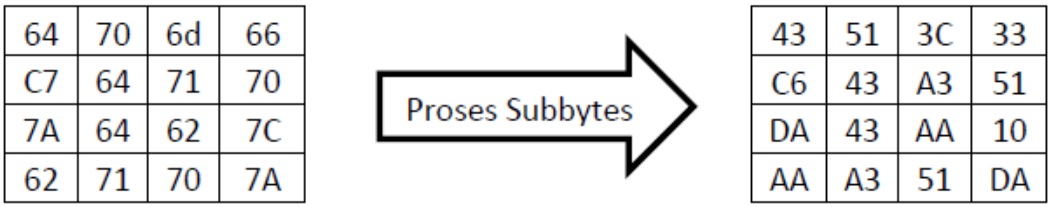
Gambar 7. Proses *Add RoundKey*





Gambar 8. Hasil *Add RoundKey*

d. Amatilah tabel S-Box untuk melakukan proses *SubBytes* pada gambar 9.



Gambar 9. Proses *SubBytes*

e. Lakukan proses *Shiftrow*, pada barisan pertama tidak ada pergeseran elemen blok, pada barisan kedua terjadi 1 kali pergeseran, pada baris ketiga terjadi 2 kali pergeseran, dan pada baris keempat terjadi 3 kali pergeseran. Perhatikan gambar 10.

43	51	3C	33	*No Change*
C6	43	A3	51	
DA	43	AA	10	
AA	A3	51	DA	
43	51	3C	33	
43	A3	51	C6	1 *ShiftRows*
DA	43	AA	10	
AA	A3	51	DA	
43	51	3C	33	
43	A3	51	C6	
AA	10	DA	43	2 *ShiftRows*
AA	A3	51	DA	
43	51	3C	33	
43	A3	51	C6	
AA	10	DA	43	
DA	AA	A3	51	3 *ShiftRows*

Gambar 10. Proses *Shiftrow*

f. Lakukan proses kali dari hasil *Shiftrow* dengan matriks *Mix Columns*. Ilustrasi pengubahan *key* ini dapat dilihat pada gambar 11.

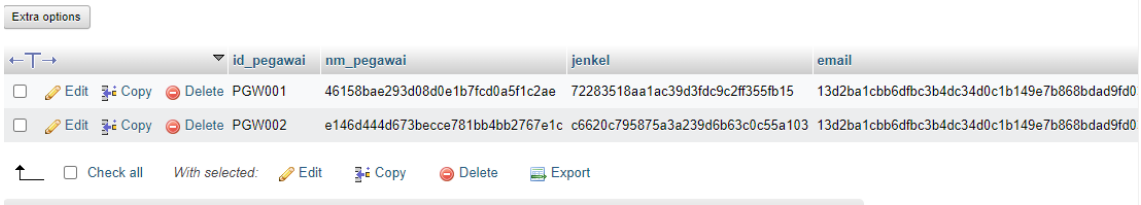
C1	85	51	40
F5	85	21	F5
43	A3	F3	8F
F5	FF	58	FF

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

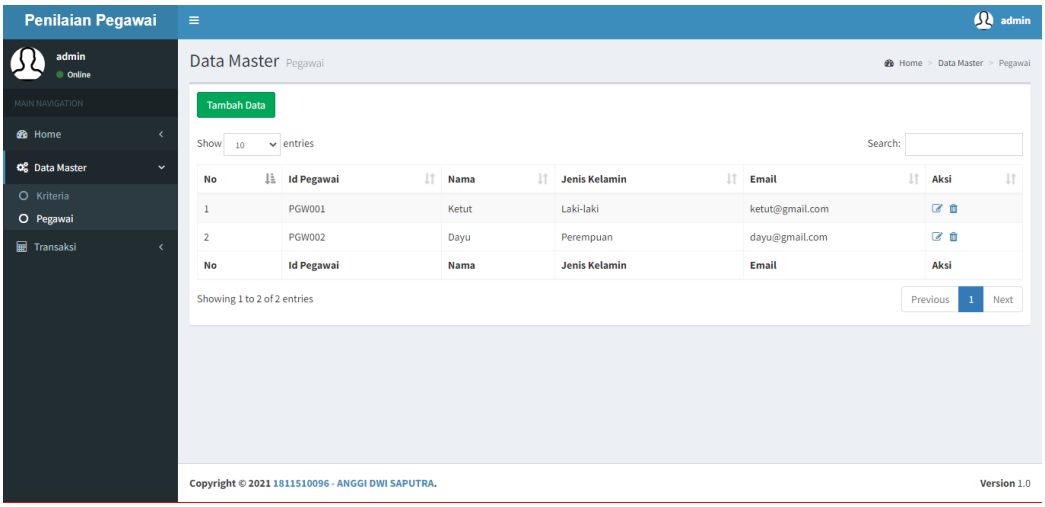
Gambar 11. Proses *Mix Columns*

3.2 Pengujian Aplikasi

Memastikan keberhasilan aplikasi yang dibuat, perlu dilakukan pengujian terhadap aplikasi yang menggunakan algoritma AES-256. Model pengujian diikuti oleh pihak PT. Buana Jaya Korindo dengan metode *Blackbox Testing*. Hal ini bertujuan untuk memastikan bahwa *output* yang didapat sesuai dengan tujuan yang akan diinginkan pada perspektif pekerja di perusahaan tersebut. Pengujian aplikasi sebanyak 5 kali yang terdiri dari pengujian halaman *login*, halaman pegawai, halaman kriteria dan halaman penilaian mendapat persentase keberhasilan sebanyak 100%. Proses algoritma AES-256 pada basis data pegawai berjalan dengan baik, hasil tangkapan layar proses enkripsi dan dekripsi bisa diamati pada gambar 12 dan gambar 13.



Gambar 12. Enkripsi pada basis data pegawai



Gambar 13. Dekripsi pada menu pegawai

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mulai dari identifikasi masalah, perancangan hingga pengembangan aplikasi ini, maka dapat diambil kesimpulan bahwa dengan dilakukannya implementasi rancangan algoritma AES-256 pada basis data penilaian pegawai di PT. Buana Jaya Korindo dapat mencegah terjadinya pencurian data. Dan juga penggunaan algoritma AES-256 dapat meningkatkan keamanan data penilaian pegawai di PT. Buana Jaya Korindo.

Penerapan algoritma AES-256 ini tentu masih memiliki beberapa keterbatasan. 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 menangani ukuran berkas yang lebih besar dengan jumlah kunci enkripsi yang lebih banyak demi keamanan dan kerahasiaan data tersebut sehingga para pengguna yang terlibat pada dokumen rahasia suatu perusahaan tidak mengkhawatirkan akan kehilangan atau kerusakan dokumen.

DAFTAR PUSTAKA

[1] Y. Wiharto, dan A. Irawan, "*Enkripsi Data Menggunakan Advanced Encryption Standard 256*", Jurnal Kilat, vol. 7, no.2, pp. 91-99, 2018.

[2] J. Prayudha, Saniman dan Ishak, "*Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)*", Sains dan Komputer (SAINTIKOM), vol. 18, no.2, pp. 119-129, 2019.

[3] M. Simanjuntak, "*Implementasi Algoritma Merkle Hellman untuk Keamanan Database*", M EANS (Media Informasi Analisa dan Sistem), vol. 4, no.1, pp. 46-50, 2019.

[4] J. Prayudha, Saniman dan Ishak, "*Pengembangan Aplikasi Chat Messenger Dengan Metode Advanced Encryption Standard (AES) Pada Smartphone*", Jurnal Coding Sistem Komputer Untan, vol. 5, no.2, pp. 1-12, 2017.

[5] N. Cristy dan F. Riandari, "*Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan*", JIKOMSI (Jurnal Ilmu Komputer dan Sistem Informasi), vol. 4, no.2, pp. 75-85, 2021.

[6] N. Anwar, Munawwar, M. Abduh dan N. B. Santosa, "*Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA*", Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 2, no.3, pp. 783-791, 2018.

[7] W. Pramusinto, N. Wizaksono dan A. Saputro, "*Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman*", Jurnal BIT (Budi Luhur Information Technology), vol. 16, no.2, pp. 47-53, 2019.

[8] M. Dedi Irawan, "*Implementasi Kriptografi Vigenere Cipher Dengan PHP*", Jurnal Teknologi Informasi (JurTI), vol. 1, no.1, pp. 11-21, 2017.

[9] D. Novianto dan Y. Setiawan, "*Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)*", Jurnal Ilmiah Informatika, vol. 9, no.2, 2018.

[10] D. A. Sitepu, Nurhayati, H. Khair, "*Implementasi Pengamanan Data Menggunakan Algoritma Advanced Encryption Standart (AES)*", Jurnal Ilmiah Kaputama (JIKA), vol. 6, no.1, 2022.