Jurnal Cahaya Mandalika, Vol. 3, No. 3, 2022, e- ISSN: 2721-4796, p-ISSN: 2828-495X
Available online at: http://ojs.cahayamandalika.com/index.php/JCM

IMPLEMENTASI ALGORITMA AES UNTUK MENINGKATKAN KEAMANANDATA KARYAWAN PADA PT PNM CABANG KARAWANG BARAT MENGGUNAKAN PHP

Ajar Rohman[1], Yunita Ayu Ramdhani [2]
[1,2]Universitaspanca Sakti
e-mail : ajarrohmanu@gmail.com[1], ayu.yunita43@gmail.com-[2]

Abstrak: *Keamanan data merupakan hal yang sangat penting bagi pengguna jaringan internet saat ini. Kasus penyadapan informasi merupakan salah satu hal yang sangat merugikan, dengan adanya kemungkinan terjadinya kejadian ini, maka perlunya peningkatan dalam hal keamanan data menjadi penting. Pada saat ini, keamanan pertukaran informasi ini perlu mendapatkan perhatian khusus, maka penelitan ini akan membuat suatu implementasi kriptografi algoritma AES-128 untuk enkripsi dan deksripsi data yang berupa file dokumen). Algoritma Advanced Encryption Standarts (AES) dipilih karena memiliki suatu tingkat keamanan data yang baik.*
Kata kunci : AES-128, Keamanan, Enkripsi, Dekripsi

Abstracts: *Security of data or information is very important for internet network users today. The case of wiretapping messages or information is one of the things that is very detrimental, with the possibility of this happening, it is necessary to increase the security of information exchange to be important. At this time, the security of this information exchange needs special attention, so this research will create a cryptographic implementation of the AES-128 algorithm for encryption and decryption of data in the form of document files). The Advanced Encryption Standards (AES) algorithm was chosen because it has a fairly good.*
Keywords*:AES-128, Security, Encryption, Decryption*

PENDAHULUAN

Keamanan data atau informasi adalah hal yang sangat penting bagi pengguna jaringan internetsaat ini. Kasus penyadapan akan pesan atau informasi merupakan salah satu hal yang sangat merugikan, dengan adanya kemungkinan terjadinya kejadian ini, maka perlunya peningkatan dalam hal keamanan pertukaran informasi menjadi penting. Pada saat ini, keamanan pertukaran informasi ini perlu mendapatkan perhatian khusus, oleh sebab itu peneliti akan menjadikan penelitian ini suatu implementasi kriptografi algoritma AES-128 untuk enkripsi dan dekripsi data yang berupa file dokumen (PDF, DOC, TXT). Algoritma Advanced Encryption Standard (AES) dipilih karena memiliki suatu tingkat keamanan pertukaran informasi yang cukup bagus, dan pada penelitian ini diuji coba file dokumen untuk melihat kecepatan waktu yang dibutuhkan selama proses enkripsi dan dekripsi.

Berbanding terbalik dengan deskripsi yang merupakan teknik pengembalian ciphertext menjadi teks asli atau plaintext. Kriptografi sendiri dapat dikategori lebih lanjut berdasarkanjenis security key yang digunakan, yaitu menjadi symmetric key dan asymmetric key. Pemilihan pengguanaan juga mempengaruhi tingkat keamanan. Fakta tersebut berkaitan dengan semakin panjang kunci yang dipakai maka semakinlama pula waktu yang diperlukan pihak yang tidak bertanggung jawab untuk membuka dokumen tersebut dengan kata lain semakin rumit kunci yangdigunakan akan semakin aman.

PT Permodalan Nasional Madani mempunyai banyak cabang, salah satunya Cabang Karawang Barat. Sistem penyimpanan data karyawan dikantor Cabang Karawang Barat masih memnggunakan sistem yang lama berupa berkas yang dapat mengakibatkan kehilangan data. Perusahaan ini masih menyimpan data dalam file berbentuk berkas tanpa adanya pengamanan data. Perusahaan ini juga tidak memiliki media penyimpanan file dokumen, sehingga apabila para pegawai membutuhkan suatu file, mereka harus meminta kepada pegawai yang membutuhkan.

Jurnal Cahaya Mandalika, Vol. 3, No. 3, 2022, e- ISSN: 2721-4796, p-ISSN: 2828-495X
Available online at: http://ojs.cahayamandalika.com/index.php/JCM

METODE PENELITIAN

2.1 Tahapan Penelitian

Adapun tahapan yang penulis lakukan antaralain :

1. Wawancara

Pada tahapan wawancara penulis mengumpulkan informasi terkait permasalahan tentang proses penginputan data karyawan, kendala kendal pada sistem yang sedang berjalan seperti apa supaya bisa diteliti dan dicarikan solusinya.

2. Observasi

Diperlukan observasi untuk menkonfirmasi terkait permasalahan yang telah diwawancarai sehingga penulis mempunyai gambaran akan pemecahan masalahnya.

3. Studi Pustaka

Pengumpulan data data dengan mencari informasi dari sumber sumber membaca buku, jurnal dan laporan yang berhubungan dengan maalahpenelitian.

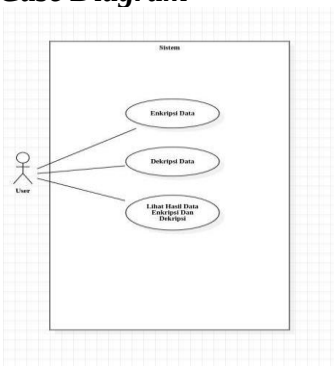
HASIL DAN PEMBAHASAN

Peneliti mengimplementasikan metode algoritma *Advanced Encryption Standard* (*AES*) sebagai enkripsi pada sistem informasi tersebut. Peneliti memilih metode algoritma *Advanced Encryption Standard* (*AES*) sebagai enkripsi dan deskripasi pada sistem tersebut. Peneliti akan menganalisis langkah-langkah yang akan dijalankan pada saat proses enkripsi dan deskripsi. Analisis ini bertujuan untuk menyusun langkah-langkah yang akan dijalankan program berdasarkan analisis awal.

3.1 Perancangan Sistem

Pada tahap ini perancangan sistem ini dilakukan pendekatan dengan UML *(Unified Modeling Language)* yaitu dengan membuat *use case diagram,sequence diagram,* dan *activity diagram* seperti pada gambar berikut ini:

3.1.1 Use Case Diagram

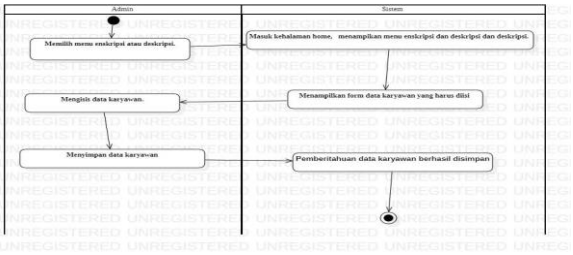


Gambar 3.1 Use Case Diagram

Penjelasan dari diagram diatas admin langsung admin menginput data yang akan di enskripsi dan di deskripsi, setelah admin selesai mengisi formulir datakaryawan sistem langsung menyimpan data.

Jurnal Cahaya Mandalika, Vol. 3, No. 3, 2022, e- ISSN: 2721-4796, p-ISSN: 2828-495X
Available online at: http://ojs.cahayamandalika.com/index.php/JCM

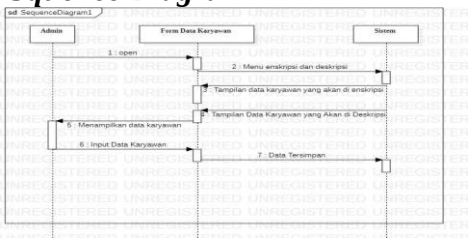
3.1.2 Activity Diagram



Gambar 3.2 Activity Diagram

Penjelasan dari gambar diatas dapat diuraikan sebagaiberikut. Admin langsung memasuki halaman *home*. Sistem langsung menampilkan menu enskripsi dandeskripsi, lalu admin memilih menu sesuai data yang akan di enskripsi atau dideskrips. Sistem menampikan formulir untuk diisi oleh admin, setelah admin selesai mengisi formulir data karyawan sistem langsung menyimpan data.

3.1.3 Squence Diagram



Gambar 3.3 Squence Diagram

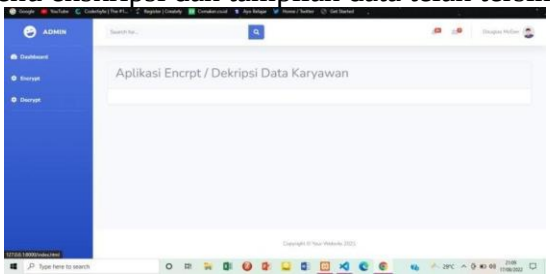
3.2 Implementasi Sistem

Implementasi sistem adalah sebuah tahapan dimana sistem dilakukan setelah perencanaan dan analisa perancangan sistem selesai dilakukan.

Tampilan antar muka sistem keamanan data karyaawan PT Permodalan Nasional Madani Cabang Karawang Barat adalah sebagai berikut :

3.2.1 Halaman Dashboard

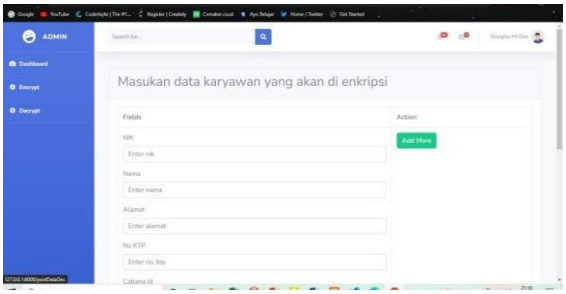
Tampilan ini adalah tampilan awalan dari sistemyang sudah dibuat. Dalam tampilan ini ada menu deskripsi, menu enskripsi dan tampilan data telah tersimpan.



Gambar 3.4 Halaman *Dashboard*

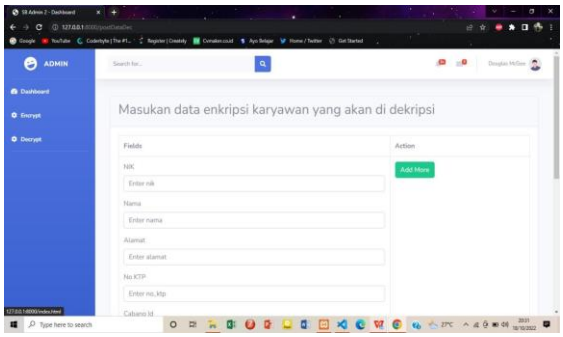
Jurnal Cahaya Mandalika, Vol. 3, No. 3, 2022, e- ISSN: 2721-4796, p-ISSN: 2828-495X
Available online at: http://ojs.cahayamandalika.com/index.php/JCM

3.2.2 Tampilan Menu Enskripsi



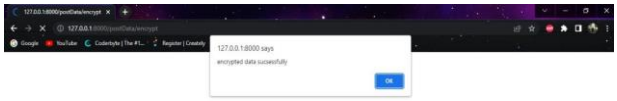
Gambar 3.5 Tampilan Menu Enskripsi

3.2.3 Tampilan Menu Deskripsi



Gambar 3.6 Tampilan Menu Deskripsi

3.2.4 Tampilan Informasi Data Tersimpan



Gambar 3.7 Tampilan Menu Informasi DataTersimpan

3.3 Pengujian Sistem

Pengujian sistem adalah tahapan untuk memastikan bahwa semua bagian berjalan dengan baik. Tahapan pengujian dilakukan setelah proses perancangan sistem dan proses implementasi selesai. Pada tahap ini dilakukan dengan metode algoritma *Advanced Encryption Standard* (*AES*). Pada penelitian ini proses enkripsi dan dekripsi yang dilakukan dalam perlindungan data informasi berbasiskan algoritma kriptografi yaitu Algoritma AES, Pada proses pembuatan aplikasi perlindungan enkripsi dekripsi ini akan menggunakan PHP sebagai bahasa pemrograman.

Setelah sistem dinyatakan layak/baik digunakan sebagai pengamanan pada sistem informasi, kemudian produk di uji coba dengan mengimplementasikan pada sistem informasi untuk mendapatkan hasil kesesuaian antara produk dengan sistem informasi. Adapun hasil uji coba produk algoritma *Advanced Encryption Standard* adalah sebagai berikut:

Butir Uji	Hasil yang diharapkan	Hasilyang diamati	Keterangan
Enkripsi *Password*	Data dapat dienkripsi sehingga menghasilkan *output*	Data berhasil dienkripsi	Sukses
Enkripsi *NIK*			
Enkripsi *Nama*			
Enkripsi *No KTP*			
Dekripsi *Password*	Data dapat didekripsi sehingga menghasilkan *output*	Data berhasil didekripsi	Sukses
Dekripsi *NIK*			
Dekripsi *Nama*			
Dekripsi *No KTP*			

Berdasarkan hasil uji diatas sistem berjalan sesuai dengan perintah dan sesuai dengan apa yangdiharapkan .

KESIMPULAN

Berdasadatarkan analisis yang telah dilakukan oleh peneliti, dapat diambil kesimpulan sebagai berikut :

1. Hasil dari enskripsi bisa menjamin keamanan data agar tidak mudah bocor ke pihak yang tidak bertanggung jawab.
2. Hasil dari penelitian perancangan sistem keamanan data karyawan ini bahwa sistem yang dibuat untuk mempermudah dan membantu kinerja pihak administrasi dalam mengelola data karyawan secara efesie.
3. Setelah pembuatan sistem selesai, peneliti melakukan pengujian sistem agar sistem yang berjalan sesuai dengan fungsinya

DAFTAR PUSTAKA

Ariyus, Dony. 2006. Kriptografi: Keamanan Data dan Komunikasi. Yogyakarta: Penerbit Graha Ilmu.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*: *Teori, Analisis, danImplementasinya*. Yogyakarta: Penerbit Andi.

Asriyanik. 2017. *Studi terhadap AdvancedEncryption Standard* (*AES*) *da5n Algoritma Knapsack dalam Pengamanan Data*. Jurnal SANTIKA : Jurnal Ilmiah Sains danTeknologi. Vol. 7 (1): 553-561.

Budianroto dan Nanan Rohman. 2010. *Implementasi Algoritma Enkripsi pada Pembuatan Kunci Lisensi Program Pengubah Atribut File*. Jurnal Computech & Bisnis. Vol. 4(2):59-69.

Chan, Arief Subrata. 2014. *Penerapan Kriptografi dalam Mengamankan File* Menggunakan Interface USB Flashdisk (Memori External). Pelita Informatika Budi Darma. Vol. 6 (3):11-15.

Dharmawan, Eka Adhitya, dkk. 2013. *Perlindungan Web pada Login Sistem Menggunakan Algoritma AES128*. Jurnal EECCIS. Vol. 7 (1): 77-84.

Handoyo, Joko dan Yulleo Muchti Subakti. 2020. *Keamanan Dokumen Menggunakan Algoritma AdvancedEncryption Standard* (*AES*). Jurnal SITECH. Vol. 3 (2): 144-152.

JB, R. Kristoforus dan Stefanus Aditya BP. 2012. *Implementasi Algoritma Rinjdael untuk enkripsi dan dekripsipada citra digital*. Seminar NasionalAplikasi Teknologi Informasi 2012 (SNATI 2912). Yogyakarta, 15-16, Juni 2012.

Pabokort, Fresly Nandar, dkk. 2015. *Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokunen, dan FileDokumen Menggunakan Algoritma Advanced Encryption Standard.* Jurnal Informatika Mulawarman. Vol. 10 (1): 20-31.

Permana, Angga Aditya dan Des Nurnaningsih. 2018. *Rancangan Aplikasi Pengamanan Data denganAlgoritma Advanced Encryption Standard (AES)*. Jurnal Teknik Informatika. Vol. 11 (2): 177-186.

Primartha, Rifkie. 2018. *Security JaringanKomputer Berbasis CEH*.Bandung: Penerbit Informatika.

Sadikin, Rifki. 2012. *Kriptografi untukKeamanan Jaringan* Yogyakarta: Penerbit Andi.

Sofana, Iwan dan Rifkie Primartha. 2019. *Network Security dan Cyber Security*: *Teori dan Praktik Cisco CCNA, Linux, Windows, Amazon AWS, Android*. Bandung: Penerbit Informatika.

Surian, Didi. 2006. *Algoritma Kriptografi AES* . TESLA, Jurnal Teknik Elektro. Vol. 8 (2): 97-101.

Tullah, Rahmat, dkk. 2016. *Perancangan Aplikasi Kriptografi File dengan Metode Algoritma Advanced Encryption Standard* (*AES*). Vol. 6 (2): 24-30.

Widyastuti, Susi, dkk. 2019. *Implementasi Kriptografi AES dalam Pengamanan Data Seleksi Peserta JAMKESMAS*. Jurnal INTECH. Vol. 1 (2): 13-22.