IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE *ADVANCED ENCRYPTION STANDART* (AES 128) PADA APLIKASI INISIASI *PROJECT* BERBASIS WEB DI PT PINS INDONESIA

Sandy Andreas[1*], Purwanto Purwanto[2]

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

Email: [1*]sndya04@email.com, [2]purwanto@budiluhur.ac.id
(* : corresponding author)

Abstrak -Perusahaan Pins Indonesia tempat dimana dilakukan penelitian memiliki data yang sangat rahasia untuk diamankan. Jika data tersebut disimpan dengan tidak baik kerahasiaannya, data tersebut dapat disalahgunakan oleh pihak atau orang tertentu yang dapat merugikan perusahaan. Agar tidak tidak dapat dicuri ,disalah gunakan, diubah oleh pihak atau orang tertentu, maka dibutuhkan suatu metode untuk dapat mengamankan data. Proses dokumen inisiasi project yang dilakukan secara hardcopy kerahasiaan dokumen atau file jadi tidak terjamin, karena proses ini dilakuakan secara hardcopy dan belum ada keamanan data didalamnya. Dengan demikian perlu dibuat suatu aplikasi yang dapat mengamankan proses dokumen inisiasi project tersebut. Metode yang dipakai untuk mengamankan data tersebut yaitu dengan enkripsi AES 128 dengan menggunakan metode kunci yang simetris yaitu metode yang menggunakan kunci enkripsi dan deskripsi yang sama. Penelitian ini diharapkan proses dokumen inisiasi project kerahasiaannya terjaga dengan baik. Hasil penelitian dapat membuat sistem yang sebelumnya dilakukan secara manual dan hardcopy, dokumen atau file dapat tersimpan dengan baik dan aman didalam sistem yang dibuat.

Kata Kunci: kriptografi, keamanan, *algoritme AES-12*, deskripsi, enkripsi

CRYPTOGRAPHIC IMPLEMENTATION USING THE ADVANCE ENCRYPTION STANDART METHOD (AES 128) IN A WEB-BASED PROJECT INITIATION APPLICATION AT PT PINS INDONESIA

Abstract-PT Pins Indonesia *company where the research is conducted has very confidential data to be secured. If the data is stored incorrectly confidential, it may be misused by certain parties or people who can harm the company. In order not to be stolen, misused, changed by certain parties or people, a method is needed to be able to secure data. The project initiation document process which is carried out by hardcopy confidentiality of documents or files is not guaranteed, because this process is carried out in hardcopy and there is no data security in it. Thus, it is necessary to create an application that can secure the process of initiating the project. The method used to secure the data is AES 128 encryption using a symmetric key method, which is a method that uses the same encryption key and description. This research is expected to maintain the confidentiality of the project initiation document process properly. The results of the study can make the system that was previously done manually and hardcopy, documents or files can be stored properly and safely in the system created.*

Keywords*:Cryptograpic, Security, Algoritme AES-128, Description, Encryption.*

1. PENDAHULUAN

PT PINS Indonesia saat ini proses bisnis dalam inisiasi project penyimpanan dokumen masih dalam bentuk *hardcopy*. Dokumen tersebut jika dilakukan penyimpanan yang tidak baik, dokumen tersebut dapat disalah gunakan oleh pihak atau orang terentu yang dapat merugikan perusahaan PT PINS Indonesia. Agar tidak tidak dapat dicuri ,disalah gunakan, diubah oleh pihak atau orang tertentu, maka dibutuhkan suatu metode untuk dapat mengamankan data. *Enterprise Bussiness* adalah salah satu unit bisnis pada PT PINS Indonesia yang dimana tugasnya adalah mencari dan mendapatkan project untuk perusahaan. Unit bisnis dipimpin oleh seorang *general manager*, satu orang *manager*, dan beberapa *account manager*. Dokumen yang dibuat oleh account manager dalam inisiasi project sampai dengan mendapatkan project masih dalam bentuk hardcopy dan bersifat rahasia, oleh karena itu diperlukan suatu aplikasi penyimpanan selain hardcopy agar kemanan file dokumen dalam hal-hal yang tidak di inginkan. Dalam aplikasi dibuat ini, diharapkan agar file dokumen tidak disalah gunakan, diubah oleh pihak atau orang terentu.

Metode yang digunakan dalam penelitian ini menggunakan metode enkripsi AES 128, dimana enkripsi ini dalam enkripsi dan deskripsinya menggunakan kata kunci yang sama. Didalam enkripsi memiliki proses antara lain *addroundkey*, *subbytes*, *shiftrows*, serta *mixcolumn*. Dan dalam proses deskripsi memiliki proses antara lain *invshiftrows*, *invsubbyte*, dan *invmiccolumn*.

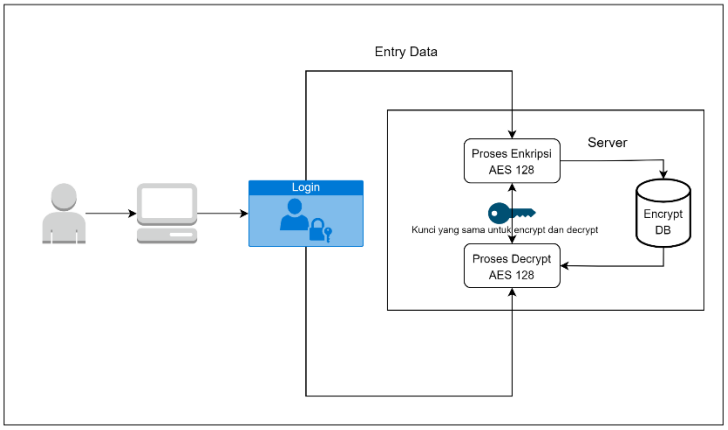
Manfaat dalam penelitian ini, data yang tersimpan dapat dijaga keamanannya dengan baik, serta perusahaan tempat dilakukan penelitian ini dapat terbantu dengan baik dalam pengelolahan, penyimpanan, dan keamanan file dokumen yang terjaga dengan baik.

2. METODE PENELITIAN

2.1 Data Penelitian

Account manager (AM) menjalani bisnis proses inisiasi project dan memenangkannya memiliki dokumen-dokumen yang harus didokumentasikan. Pada saat project menang atau win, dokumen-dokumen tersebut masih disimpan dalam bentuk hardcopy dan sebagai dokumentasi masih dalam bentuk scan dan disimpan manual.

Data file yang dipergunakan dalam penelitian ini tentang data dokumen inisiasi proyek bisnis di PT Pins Indonesia.



Gambar 1. Arsitektur Sistem

2.2 Teknik Pembanding

Teknik pembanding yang dipakai di di PT Pins Indonesia, masih menggunakan metode manual yaitu dokumen hardcopy discan diprinter lalu didownload manual.

Pada aplikasi ini, penulis menggunakan Algoritme advanced encryption standar -128 (AES-128) sebagai metode kriptografi. Algoritme AES-128 merupakan teknik kriptografi dengan menggunakan kunci yang sama dalam enkripsi atau dekripsikan suatu data ataupun file. Agar file dokumen inisiasi proyek di dalam database dapat terenkripsi menjadi data ciphertext dan dikembalikan kedata semula, data di dalam database akan di enkripsi dan text di dalam database menjadi *plaintext* pada saat dilakukan dekripsi. Dalam membuat sistem aplikasi, bahasa pemrograman menggunakan PHP dan memakai mysql sebagai pendukungnya.

2.3 Metode Penelitian

Berikut metode penelitian yang dipakai dalam penelitian ini antara lain:

a. Penilitan Yang Dilakukan
   Penelitian dimulai dengan studi ke perpustakaan, mengumpulkan data yang dapat membantu penyusunan tugas akhir.
b. Wawancara
   Setelah dilakukan studi litelatur dilanjutkan dengan wawancara terkait masalah yang ada di PT Pins Indonesia
c. Analisis kebutuhan
   Melakukan analisa masalah dan kebutuhan aplikasi yang nantinya akan buatkan kedalam sistem.
d. Desain
   Menentukan spesifikasi detail dari program serta membuat rancangan *input* dan *output*.

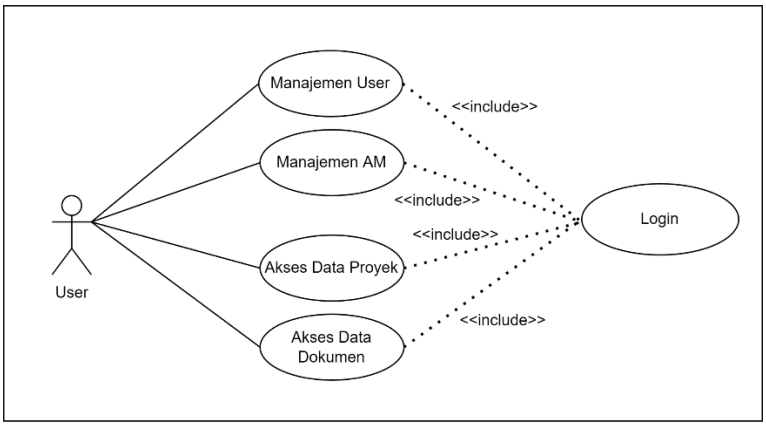
e. Implementasi
Meimplementasikan seluruh sistem yang telah buat dan didesign sebelumnya menjadi program yang nantiinya akan diitegrasikan menajadi sebuah sistem sesuai dengan kebutuhan.

f. Integrasi dan Testing
Sistem yang sudah dibuat akan ditest dan diintegrasikan untuk mengetahui apakah sistem tersebut telah berfungsi sesuai dengan design dan sistem yang telah dibuat atau tidak.

g. Pemeliharaan
Melakukan pemeliaharaan setiap bulan atau dan per periode agar mengetahui sistem aplikasi ini tedapat bug atau tidak, dan memastikan sistem aplikasi ini berjalan dengan baik.

3. HASIL DAN PEMBAHASAN

Pada Berikut adalah rancangan rancangan yang dibuat dari hasil penelitian terkait keamanan data di perusahaan PT Pins Indonesia yang tediri dari menu *login*, *home*, *user*, proyek dan laporan proyek. Berikut use case diagram yang dibuat didalam penelitian ini dapat dilihat pada gambar 2.



Gambar 2. Gambar *Use Case* Diagram

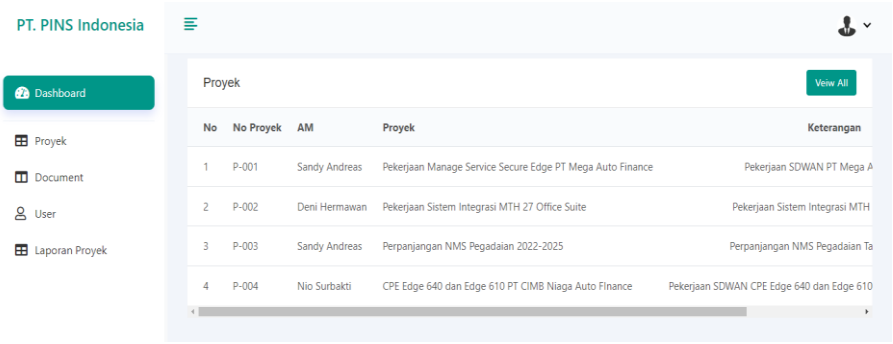
3.1 Menu Login

Didalam menu login ini, user dapat menginput username dan password yang telah dimasukan kedalam database. Berikut tampilan menu login pada gambar 3.

Gambar 3. Menu Tampilan Login

3.2 Menu Home

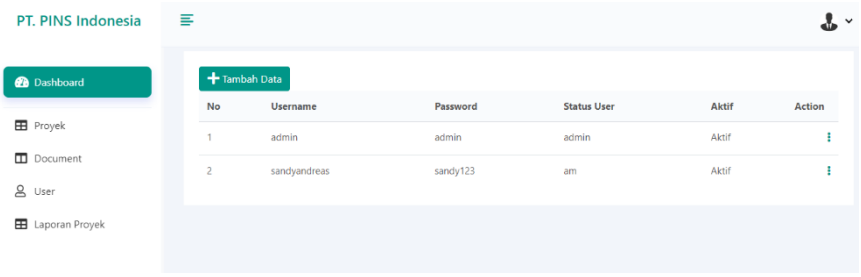
Didalam menu home, user dapat melihat submenu proyek, dokumen, *user*, serta lamporan proyek yang terlihat pada gambar 4.



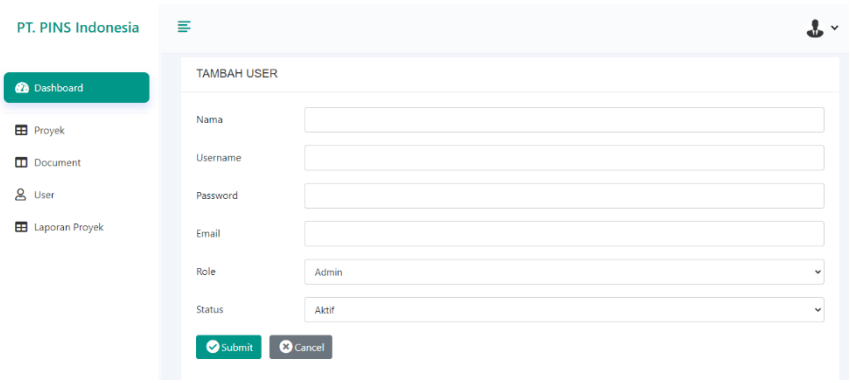
Gambar 4. Tampilan Menu Home

3.3 Menu User

Pada tampilan didalam menu user ini, kita dapat melihat siapa saya yang dapat *login* ke aplikasi ini beserta status dari *user-user* tersebut sepeti admin atau bukan seperti pada gambar 5. Serta dimenu ini kita dapat menambah *login user* dan dapat memilih user tersebut dapat sebagai admin atau bukan pada gambar 6.



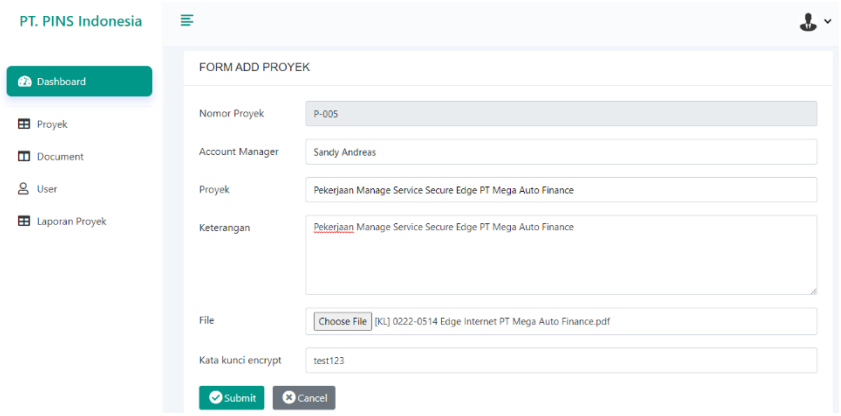
Gambar 5. Tampilan Menu User



Gambar 6. Tampilan Tambah User

3.4 Menu Proyek

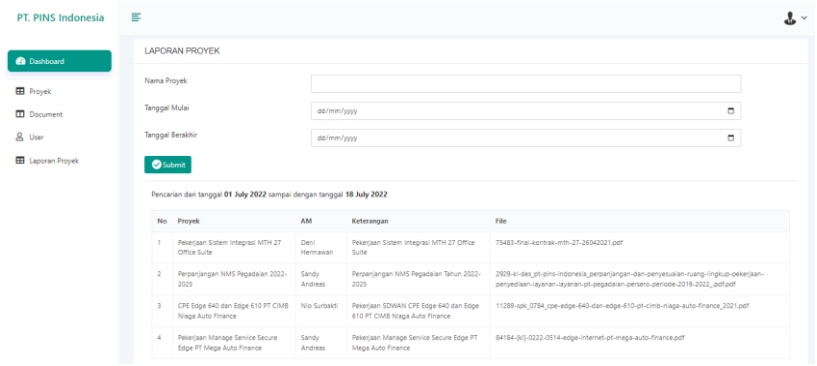
Didalam menu ini kita dapat menambah proyek serta disini kita melakukan enkripsi dalam penyimpanan datanya yang dapat dilihat pada gambar 7. Dan dimenu ini kita juga dapat deskripsi file yang sudah disimpan sebelumnya didalam database.



Gambar 7. Tampilan Menu Tambah Proyek

3.5 Menu Laporan Proyek

Didalam menu ini *user* atau pengguna dapat melihat data-data proyek yang telah di input sebelumnya, dan dapat di *filter* dengan nama proyek, tanggal mulai proyek, atau tanggal berakhir proyek yang dapat terlihat pada gambar 8.



Gambar 8. Gambar Tampilan Laporan Proyek

3.6 Rancangan Pengujian

Rancangan pengujian dilakukan pengujian dari sistem yang bertujuan untuk mengetahui fungsi utama dari algoritma ini.

3.6.1 Rancangan Pengujian Enkripsi

Berikut adalah rancangan pengujian dalam melakukan enkripsi data yang dapat dilihat pada tabel 1 menyajikan hasil pengujian enkripsi.

Table 1. Hasil Pengujian Enkripsi

Judul *File* Asli	*Size File* Asli	*Size File* Hasil Enkripsi	Lamanya Enkripsi (detik)
NamaDokumen1.pdf	502 kb	501 kb	16,62
NamaDokumen2.pdf	484 kb	483 kb	15,93
NamaDokumen3.pdf	1.771 kb	1.771 kb	56,78

3.6.2 Rancangan Pengujuan Deskripsi

Berikut adalah rancangan pengujian dalam melakukan deskripsi data yang dapat dilihat pada tabel 2 menyajikan hasil pengujian deskripsi.

Table 2. Hasil Pengujian Deskripsi

Judul *File* Asli	*Size File* Asli	*Size File* Hasil Deskripsi	Lamanya Deskripsi (detik)
NamaDokumen1.rda	501 kb	502 kb	51,1
NamaDokumen2.rda	483 kb	484 kb	49,5
NamaDokumen3.rda	1.771 kb	1.771 kb	139,79

3.6.2 Metode Testing

Pengujian dengan metode black box adalah pengujian fungsi input dan output dari aplikasi yang dibuat. Peneliti mengartikan pengekelompokan kondisi input kemudian tampilan yang diharapkan dan hasil serta keterangan hasil pengujiannya.

No	Proses	Tampilan	Hasil	Keterangan
1.	Isi Form *Login*	Muncul Tampilan Dashboard	Pass	Kondisi benar
2.	Klik Menu Proyek	Masuk ke Halaman List Proyek	Pass	Jika ke Halaman List Data Proyek
3.	Klik Button Tambah Proyek	Masuk ke Form Tambah Proyek	Pass	Ke Form Tambah Proyek
4.	Mengisi Form Tambah Tambah Proyek	Input Data Proyek	Pass	Jika di Input Benar
5.	Klik Link Download *File* Encrypt	*File* Encrypt langsung terdownload	Pass	Jika Langsung Ke *File* Download
6.	Klik Link Download *File* Decrypt	Masukan Kata Kunci	Pass	Jika di Input Benar
7.	Klik Link Hapus	Data setelah di klik akan terhapus	Pass	Jika di Klik
8.	Klik Menu Dokumen	Masuk ke Halaman List Daftar Dokumen	Pass	Jika ke Halaman Daftar Dokumen
9.	Klik Menu User	Masuk ke Halaman List User	Pass	Jika ke Halaman List User
10.	Klik Button Tambah User	Masuk ke Halaman Tambah User	Pass	Jika ke Halaman Tambah User
11.	Mengisi Form Tambah Tambah User	Input Data User	Pass	Jika di Input Benar
12.	Klik Menu Laporan Proyek	Masuk ke Halaman Laporan proyek	Pass	Jika ke Halaman Laporan Proyek
13.	Klik Nama Proyek dan Tanggal Proyek	Masuk ke Dalam List Proyek	Pass	Jika Input Benar
14.	Klik Logout	Keluar Halaman *Login*	Pass	Jika ke Halaman *Login*

4. KESIMPULAN

Pada pembahasan diatas sebelumnya, dapat temu kenali bahwa sistem informasi inisiasi proyek berbasi web menggunakan keamanan metode AES-128 diperlukan, karena aplikasi ini dapat mudah dimengerti oleh pengguna, dapat di implementasikan pada keamanan data. Dalam pengembangan lebih lanjut aplikasi ini dapat menjadi lebih baik lagi dengan dikembangkan kedalam aplikasi berbasis *mobile.*

DAFTAR PUSTAKA

[1] R. Nuari, N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *Journal Of Artificial Intelligence And Innovative Applications*", vol. 1, no.2, pp. 37-44, 2020.

[2] A. R. Tulloh, Y. Permanasari and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika INISBA*, vol. 15, no. 1, pp 1-14, 2016.

[3] A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, "*Handbook of Applied Cryptografi*," 5th printing, 2001.

[4] R. Primartha, "Penerapan Enkripsi Dan Dekripsi File menggunakan *Algoritme Advanced Encryption Standard* (AES)," *Journal of Research in Computer Science and Applications Informatics Engineering Department*, vol.1 no. 01, pp. 1-19, 2013.

[5] A. Widarma, "Kombinasi Algoritme AES, RC4 dan ELGAMAL dalam Skema Hybrid Untuk Keamanan Data," CESS (*Journal of Computer Engineering System and Science*), vol. 1, no. 1, pp. 1-8, 2016.

[6] R. Primartha, "Penerapan Enkripsi Dan Dekripsi File menggunakan *Algoritme Advanced Encryption Standard* (AES)," *Journal of Research in Computer Science and Applications Informatics Engineering Department*, vol.1 no. 01, pp. 1-19, 2013.

[7] R. T. Shita and L. Li Hin, "Implementasi Algoritma Kriptografi AES 128BIT Dan Elgamal Untuk Pengamanan E-Mail Pada Bandara International Sultan Mahmud Baharuddin II Palembang," Jurnal BIT, vol. 15, no. 1, pp. 1-11, 2018.

[8] F. A. Sianturi, "Perancangan Aplikasi Pengamanan Data dengan Kriptografi *Advanced Encryption Standard* (AES), *Jurnal Pelita Informatika Budi Darma*, vol. 4, no. 1, pp.42–46, 2013.