Volume 19 No.2 September 2022

Jurnal Ilmiah Fakultas Teknik
LIMIT'S

JURNAL ILMIAH FAKULTAS TEKNIK
LIMIT'S

ISSN 0216-1184

AlamatRedaksiPublikasiIlmiah:
FakultasTeknik – UniversitasSatya Negara Indonesia
Jl. ArteriPondok Indah No. 11 Jakarta Selatan 12240 Indonesia
Telp. (021) - 7398393, Fax. (021) - 77200352
http://www.usni.ac.id

ISSN 0216-1184

Jurnal Ilmiah Fakultas Teknik
LIMIT'S

Volume 19 September 2022 Nomor 2

ANALISA DAN PERANCANGAN SISTEM ENKRIPSI DAN DEKRIPSI DOKUMEN BERBASIS ANDROID MENGGUNAKAN METODE *ADVANCED ENCRYPTION STANDARD* – 128 (STUDI KASUS: PT. KELAB 21 RETAIL)

Teguh Budi Santoso [1],Fildan Hadika Rahman [2]
Fakultas Teknik Informatika Program Studi Teknik Informatika
Universitas Satya Negara Indonesia
teguh.santos12@gmail.com, ,fildanhadika@gmail.com,

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat memberi pengaruh yang besar hampir diserluruh aspek kehidupan manusia. Tentunya tingkat keamanan yang tinggi sangat diperlukan agar informasi tersebut tidak dapat diakses oleh orang yang tidak berkepentingan. Kriptografi banyak digunakan untuk menjaga aspek keamanan informasi. Kriptografi adalah ilmu mengenai teknik enkripsi dimana naskah asli (plaintext) diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit dibaca (ciphertext) oleh seseorang yang tidakmemiliki kunci dekripsi. salah satu metode kriptografi modern yang dikembangkan adalah algoritma Advanced Encryption Standard (AES). Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES 128, 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Pada proses state enkripsi akan melalui beberapa tahapan yakni Addroaundkey, Subbyte, Shiftrows, dan Mixcolumns sebanyak 10 kali putaran. Namun pada putaran terakhir tidak dilakukan lagi proses Mixcolumns langsung ke proses Addraoundkey, dan untuk proses dekripsi merupakan proses kebalikan dari proses enkripsi yakni InvAddrows, InvShiftrows, InvSubbyte, dan InvMixcolumns menggunakan kunci round yang sama dengan proses enkripsi. Algoritma Advanced Encryption Standard (AES) dipilih karena memiliki suatu tingkatan keamanan pertukaran informasi yang cukup bagus. Dan dari hasil implementasi algoritma AES dapat disimpulkan bahwa aplikasi ini dapat mengekripsi semua jenis karakter berupa string, huruf, angka, dan symbol.

Kata Kunci: Enkripsi, Dekripsi, Advanced Encryption Standard (AES) – 128

ABSTRACT

The quick development of information technology has had a major influence in almost humans' life aspects. Of course, a high level of security is needed so it cannot be accessed by unauthorized people. The usage of cryptography is to keep the aspects of information's security. Cryptography is a science of encryption techniques where the originao text (plain text) is scrambled by using an encryption key which transforms into scrambled text that is hard to be read (chiper text) by someone who does not have thr description key. One of the modern cryptography methods which is being developed is Advanced Encryption Standard (AES) algorithms. Advanced Encryption Standard (AES) is a cryptographic algorithm which is currently the standard for symmetric key encryption algorithms. In the AES 128 cryptographic algorithm, 1 128-bit plaintext block is first converted into a 4x4 hexadecimal matrix called state. In the state encryption process, it will go through several stages, namely Addroaundkey, Subbyte, Shiftrows, and Mixcolumns for 10 rounds. However, in the last round, the Mixcolumns process was not carried out directly to the Addraoundkey process, and the decryption process was the opposite of the encryption process, namely InvAddrows, InvShiftrows, InvSubbyte, and InvMixcolumns using the same round key as the encryption process. The Advanced Encryption Standard (AES) algorithm was chosen because it has a pretty good level of information exchange security. From the implementation of the AES algorithm, it can be concluded that this application can encrypt all types of characters in the form of strings, letters, numbers, and symbols.

Keywords*: Encryption, Decryption, Advanced Encryption Standard (AES) – 128.*

PENDAHULUAN

Latar Belakang

Pada era globalisasi sekarang ini tingkat informasi dan teknologi semakin maju dan modern, pertukaran data melalui jaringan internet sangat mungkin dilakukan karena tentunya akan mempercepat dan memudahkan proses pertukaran data terutama dengan jarak yang jauh. Kemudahan ini tentunya berdampak pada munculnya resiko dan ancaman keamanan data, misalnya penduplikasian atau bahkan perusakan informasi itu sendiri.

PT. Kelab 21 Retail juga pernah mendapatkan masalah dalam hal informasi. Dimana dokumen atau laporan keuangan yang tersimpan di dalam server diambil kemudian diubah informasi yang ada didalamnya oleh pihak yang tidak bertanggung jawab. Sehingga dengan kejadian seperti itu, PT. Kelab 21 Retail mengalami kerugian karna informasi yang ada tidak sesuai. Untuk itu diperlukan suatu metode keamanan yang dapat melindungi dokumen-dokumen tersebut.

Rumusan Masalah

Bagaimana cara mengimplementasikan *Advanced Encryption Standard* (AES) – 128 untuk menjaga keamanan dokumen pada PT. Kelab 21 Retail?

Tujuan dan Manfaat Penelitian

1. Tujuan dari penelitian ini adalah:
   Membangun sebuah sistem yang dapat melakukan enkripsi dan dekripsi dokumen menggunakan algoritma AES
2. Manfaat Penelitian adalah:
   a. Meningkatkan dan menjaga keamanan informasi yang ada pada sebuah dokumen
   b. Memperkecil terjadinya kebocoran dan penduplikasian dokumen

DASAR TEORI

Penelitian Terdahulu

Dalam penelitian Ashri Prameshwari, Nyoman Putra Sastra pada tahun 2018, dengan judul "Implementasi Algoritma *Advanced Encryption Standard* (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen" [1]. Dalam penelitian Gilang Gumira P.U.K pada tahun 2016, dengan judul "Implementasi Metode *Advanced Encryption Standard* (AES) Dan *Message Digest* 5 (MD5) Pada Enkripsi Dokumen" [2]. Dalam penelitian Sheila Maulida Intani, Fadilah Salsabila pada tahun 2019, dengan judul "Implementasi Kriptografi AES pada File Dokumen" [3].

Teori-teori Penelitian

1. Kriptografi

Kriptografi *(cryptography)* berhasal dari bahasa Yunani: *"cryptos"* artinya tersembunyi, sedangkan *"graphen"* artinya tulisan. Jadi, kriptografi berarti penulisan tersembunyi. (Janner Simarmata. Dkk, 2019).

2. *Advanced Encryption Standard* (AES)

Pertama kali diluncurkan pada tahun 1998 dan tergolong *block cipher*, AES dikenal juga bernama Rijndael. AES merupakan salah satu dari banyak rancangan yang lolos seleksi dan akhirnya diadopsi oleh NIST (*National Institure of Standards and Technology)* menjadi standar untuk Amerika pada tahun 2001 (Janner Simarmata.Dkk, 2019).

3. Sistem

Menurut Abdul Kadir (2014:61), sistem adalah sekumpulan elemen yang saling terkait atau terpadu yang dimaksudkan untuk mencapai suatu tujuan. Sebagai gambaran jika dalam sebuah sistem terdapat sebuah elemen yang tidak memberikan manfaat dalam mencapai tujuan yang sama, maka elemen tersebut dapat dipastikan bukanlah bagian dari sistem. Ada 3 elemen yang membentuk sebuah sistem yaitu:

1. Input Segala sesuatu yang masuk ke dalam sistem dan selanjutnya menjadi bahan untuk di proses
2. Proses Bagian yang melakukan perubahan dari input menjadi output yang berguna, misalnya berupda informasi dan produk, tetapi juga bisa berupa hal-hal yang tidak berguna, misalnya sisa pembuangan atau limbah

3. Output Hasil dari pemrosesan, misalnya berupa suatu informasi, saran, cetakan laporan, dll. Berdasarkan pengertian diatas dapat disimpulkan bahwa sistem adalah cara yang kita lakukan untuk mencapai tujuan yang telah kita buat mulai dari menginput sesuatu memprosesnya kemudian menghasilkan output.

4. Informasi

Menurut Rommey dan Steinbart (2015:4), informasi adalah data yang telah dikelola dan di proses untuk memberikan arti dan memperbaiki proses pengambilan keputusan

5. Flowchart

Indrajani (2015:36), "Flow chart adalah penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program."

METODE PENELITIAN

Metode Pengambilan Data

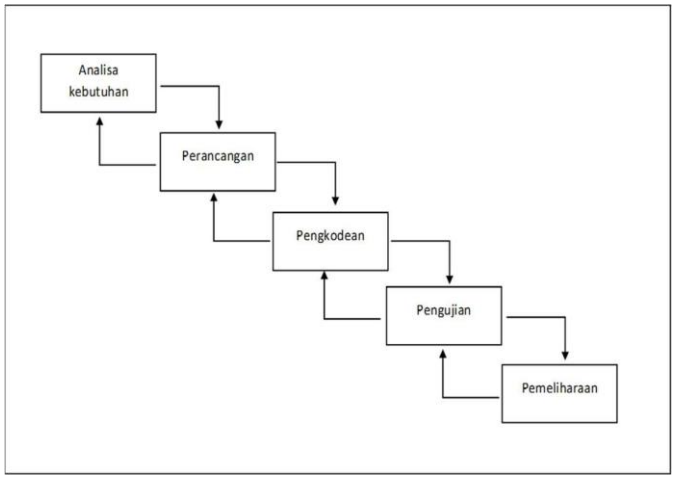
Dalam tahap pengumpulan data sebagai media untuk menyelesaikan tugas akhir ini, maka penulis mengambil sumber data primer dan sekunder. Adapun metode pengumpulan data yang akan dipakai adalah:

1. Pengamatan / observasi
2. Studi pustaka
3. Wawancara / *interview*

Metode Pengembangan Sistem

Model proses pengembangan perangkat lunak yang digunakan dalam penelitian ini yaitu menggunakan metode *waterfall* yang terdiri dari tahap analisa kebutuhan, tahap perancangan dan tahap pembuatan program serta tahap pengujian.

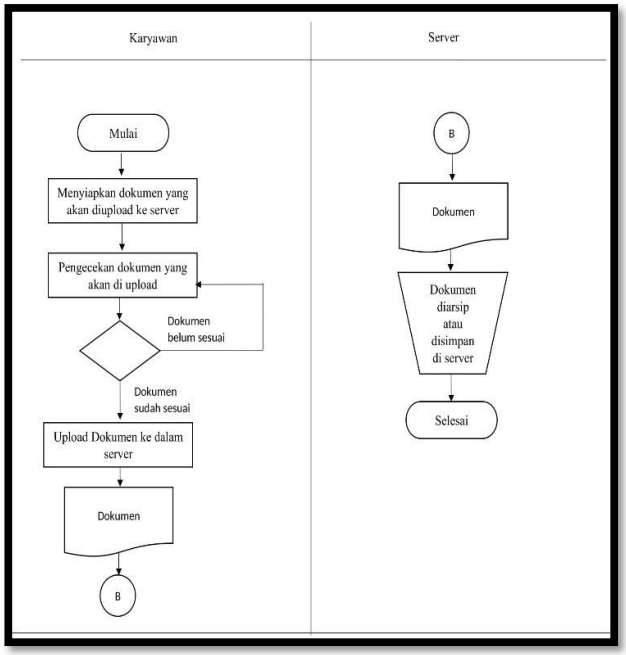
Model Waterfall adalah sebuah model pengembangan perangkat lunak yang membutuhkan pendekatan sistematis dan sekuensial, dimana satu tahap dilakukan setelah tahap sebelumnya selesai dilakukan, biasanya model ini disebut alur hidup klasik (*classic life cycle*)



Gambar 1. Metode Waterfall

Analisa Sistem Berjalan

Analisa sistem berjalan diperlukan untuk mengetahui proses yang biasa dilakukan oleh karyawan. Dari proses tersebut kita dapat mengetahui kelemahan-kelemahannya. Kemudian kita dapat mengusulkan sistem yang tepat untuk memperbaiki proses tersebut. Berikut adalah analisa sistem yang berjalan yang didapat dari metode pengumpulan data observasi:



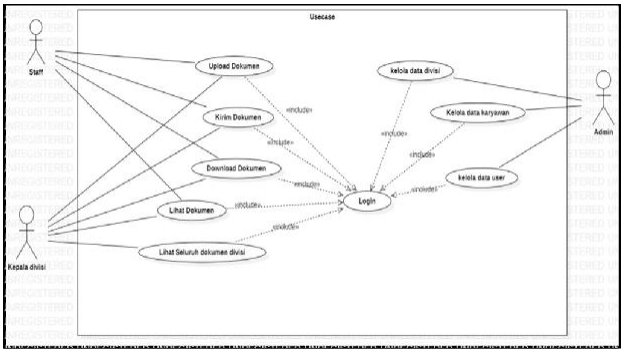
Gambar 2. *Flowchart* Sistem Berjalan

Berdasarkan *flowchat* diatas, dapat dideskripsikan seperti berikut:

1. Ketika karyawan ingin melakukan pengunggahan dokumen, karyawan tersebut harus mengakses server terlebih dahulu
2. Sebelum melakukan pengunggahan, karyawan perlu melakukan pemeriksaan terhadap file tersebut
3. Setelah melakukan pengecekan, maka karyawan perlu mengakses server dan membuka folder divisi karyawan tersebut
4. *Copy* dokumen yang ingin diunggah lalu*paste* kedalah folder server tersebut
5. Dan dokumen terarsip dan tersimpan di server.

Rancangan Sistem Usulan

Untuk memecahkan masalah yang ada, penulis mengusulkan untuk membuat sebuah aplikasi yang dapat mengenkripsi dokumen ketika dokumen diunggah.Selain itu ada beberapa poin tambahan dari hasil *interview* atau wawancara kepada beberapa karyawan tertentu. Berikut adalah *usecase* dari rancangan sistem usulan yang akan dibangun



Gambar 3. *Usecase* Sistem Usulan

Usecase diatas mendeskripsikan bahwa karyawan dapat mengunggah, mendownload, melihat, dan mengirim dokumen melalui aplikasi android. Namun sebelum melakukan proses tersebut, karyawan perlu login terlebih dahulu. Jika karyawan tesebut sebagai atasan dalam suatu divisi, maka dapat melihat semua dokumen yang terunggah oleh divisi tersebut

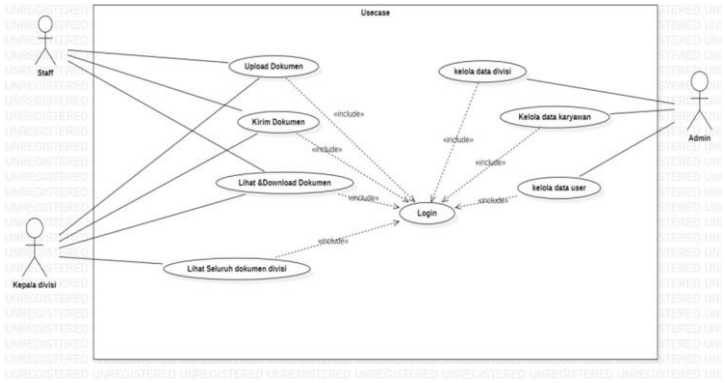
PEMBAHASAN

Perancangan Sistem

Pada tahapan iniakan menjelaskan perancangan sistem yang dapat menyelesaikan permasalahan yang diangkat dalam penelitian. Dalam perancangan sistem memuat *Use Case Diagram*, *Activity Diagram*, *Sequence Diagram* dan *Class Diagram.*

1. *Usecase* Diagram

Usecase diagram system menggambarkan fungsional dari sebuah sistem. Berikut adalah usecase dari rancangan sistem yang akan dibangun:

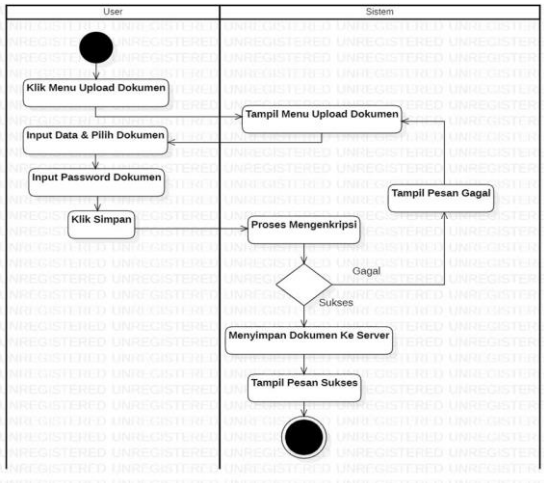


Gambar 4. Use Case Diagram

Usecase diatas merupakan gambaran umum rancangan sistem yang akan dibangun. Dimana didalam sistem ini memliki 3 aktor yang berperan, diantaranya yaitu staff, kepala divisi dan admin

2. *Activity* Diagram

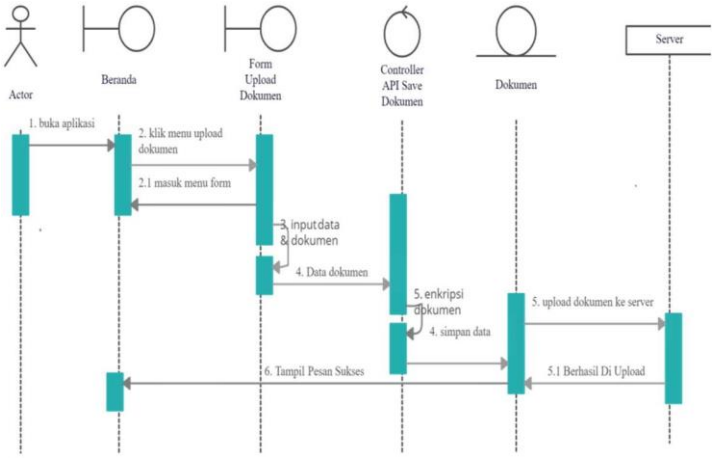
Activity diagram merupakan penjelasan tentang aktivitas antar aktor dengan program dalam menjalankan sistem tersebut. Berikut adalah activity diagram dari perancangan sistem yang akan dibangun.



Gambar 5. Activity Diagram

3. Sequence Diagram

Sequence Diagram adalah suatu diagram yang menjelaskan interaksi objek dan menunjukkan (memberi tanda atau petunjuk) komunikasi diantara objek-objek tersebut

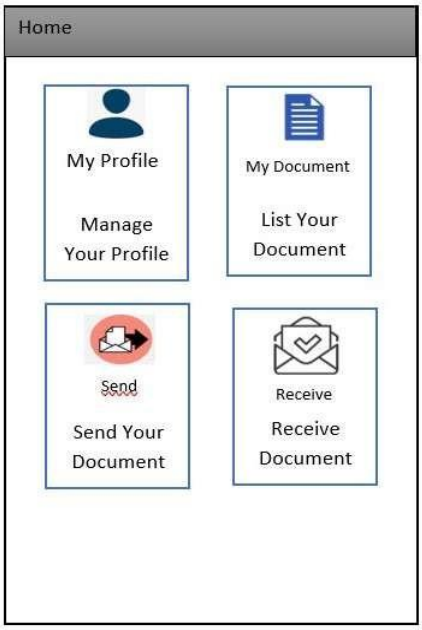


Gambar 6. Sequence Diagram

4. Rancangan Layar Tampilan

.

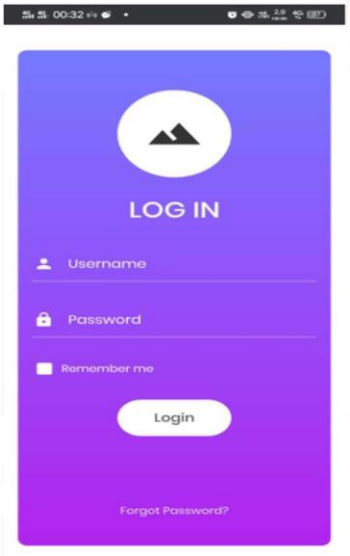
Gambar 7. Rancangan Layar Tampilan Login



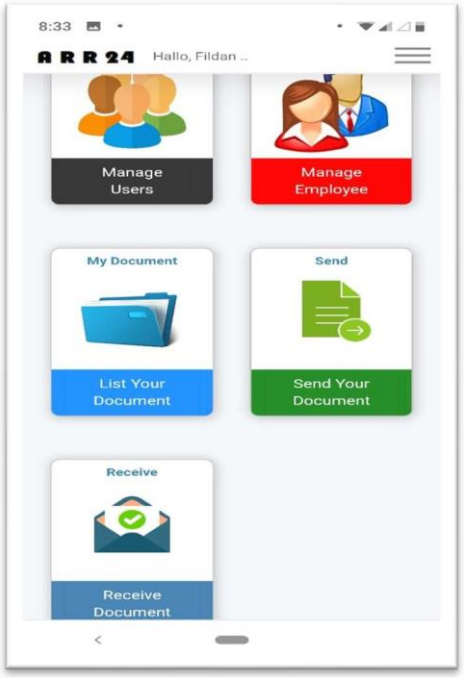
Gambar 8. Rancangan Layar Tampilan Beranda

Hasil Akhir

Implementasi Sistem



Gambar 9. Implementasi Sistem Login



Gambar 10. Implementasi Sistem Beranda

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian, pembahasan, pengujian dan analisis yang dilakukan maka, dapat ditarik kesimpulan sebagai berikut

1. Dalam penelitian ini menunjukkan hasil kecenderungan kenaikan waktu yang dibutuhkan untuk melakukan proses enkripsi dan 20 dekripsi, semakin besar ukuran suatu file maka akan semakin lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi
2. Jenis format file tidak berpengaruh terhadap lamanya proses enkripsi dan dekripsi
3. Besar ukuran file sesudah proses enkripsi tidak mengalami perubahan.
4. Besar ukuran file merupakan faktor yang sangat mempengaruhi lamanya waktu yang dibutuhkan dalam proses enkripsi dan dekripsi

Saran

Demi terciptanya suatu fungsi yang dapat bermanfaat dikemudian hari, maka saran untuk pengembangan sistem selanjutnya yaitu:

1. Ukuran file yang diunggah tidak terbatas hanya 1GB saja.
2. Agar dapat menggunakan kunci asimetris. Dengan begitu, setiap dokumen memiliki dua password, yaitu *password private* dan public.

DAFTAR PUSTAKA

[1] Janner, S., Sriadhi, dan Robbi, R.*KRIPTOGRAFI (Teknik Keamanan Data & Informasi)*.Yogyakarta: CV. Andi Offset, 2019.
[2] Sugiarti, Yuni. *Analisis & Perancangan UML (Unified Modeling Language) Generated VB.6*. Yogyakarta: Graha Ilmu, 2013.
[3] Indrajani. *Database Design (Case Study All in One)*. Jakarta: PT Elex Media Komputindo, 2015.
[4] Kadir, Abdul. *Buku Pintar Programmer Pemula PHP*. Yogyakarta: Penerbit Mediakom, 2013.
[5] Kadir, Abdul. *Pengenalan Sistem Informasi Edisi Revisi*. Yogyakarta: Penerbit Andi, 2014.
[6] Komputer Wahana. *Microsoft Visio untuk desain diagram dan flowchart*. Jakarta: PT Elex Media Komputindo, 2013.
[7] S., Rosa A. dan M. Shalahuddin. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika, 2013.
[8] Yudi, Priyadi. *Kolaborasi SQL dan ERD dalam implementasi database*. Yogyakarta: Andi, 2014