SISTEM KEAMANAN *MANAGEMENT FILE* MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-128) STUDI KASUS: TABITHA INDONESIA

Sejati Waluyo[1], Ferdiansyah[2], Firman[3]
[1]Jurusan Teknik informatika, Fakultas Teknik Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara Jakarta Selatan Telp 021 585 3753
Email: sejati.waluyo@budiluhur.ac.id
[2]Jurusan Teknik informatika, Fakultas Teknik Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara Jakarta Selatan Telp 021 585 3753
Email: ferdiansyah@budiluhur.ac.id
[3]Jurusan Teknik informatika, Fakultas Teknik Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara Jakarta Selatan Telp 021 585 3753
Email: firmanbrawi@gmail.com

ABSTRAK

Perkembangan teknologi informasi yang pesat saat ini, mampu memberikan solusi bagi perusahaan dalam menyelesaikan permasalahan yang dihadapi, pemanfaatan teknologi informasi juga dapat meningkatkan daya saing dari perusahaan tersebut. Di mana dengan adanya penggunaan sistem informasi yang baik dan sesuai dengan kebutuhan, dapat meningkatkan efisiensi dari proses bisnis yang ada di perusahaan tersebut. Tabitha Indonesia adalah perusahaan yang bergerak di bidang logistik, jasa pengiriman barang baik dalam negeri maupun luar negeri. Dalam kegiatan proses bisnisnya banyak sekali berhubungan dengan dokumen yang berkaitan dengan data logistik dan data-data perusahaan yang sifatnya adalah rahasia. Mengingat pentingnya dokumen tersebut dan menjaga kerahasiaan data dari orang yang tidak memiliki wewenang atas data tersebut, penulis mengembangkan sistem management file *yang menggunakan teknologi kriptografi untuk mengamankan dokumen perusahaan dan memberikan kemudahan dalam hal pengarsipan dokumen sehingga apabila dibutuhkan dapat diakses dengan mudah namun kerahasiaan dokumen perusahaan tetap terjaga. Di harapkan dengan sistem* managamen file *ini, mampu memberikan kemudahan dalam pengarsipan dokumen perusahaan dan memberikan keamanan terhadap informasi dokumen perusahaan tersebut.*

Kata kunci*: Management File*; Pengamanan Dokumen; Pengarsipan Dokumen Penting

PENDAHULUAN

Dewasa ini perkembangan teknologi informasi dan komunikasi semakin merambah pada penerapan yang mendukung untuk kemudahan kebutuhan manusia. Dapat terlihat bahwa beberapa aspek kehidupan menerapkan sistem yang telah terkomputerisasi. Sistem yang telah terkomputerisasi tentunya memiliki data atau informasi yang perlu perhatian khusus dalam faktor kerahasiaan, keutuhan, dan ketersediaan. PT. Tabitha Express merupakan perusahaan yang bergerak dibidang jasa distribusi barang ekspedisi dalam negeri maupun luar negeri, memiliki beberapa dokumen penting yang melibatkan pihak jasa ekspedisi, agen, dan *customer*. Dokumen tersebut terdiri dari data tagihan dan data logistik *customer* yang mencantumkan kuantitas serta nominal finansial cukup besar dan ini perlu pengamanan lebih lanjut. Sehingga tidak ada pihak yang mampu memanipulasi data tersebut pada saat dilakukannya penyampaian data ke *customer*, audit atau keperluan lainnya.

Terkait dengan masalah yang ada dengan pentingnya pengamanan informasi, maka penulis mencoba mengimplementasikan konsep penyandian pesan informasi. Ilmu yang mempelajari konsep penyandian pesan informasi ini disebut dengan istilah kriptografi. Dalam kriptografi terdapat metode yang cukup penting dalam kasus pengamanan data. Pada dasarnya data yang akan diamankan akan dilakukan penyandian atau pengacakan kode. Sehingga data tidak mudah bisa dibaca karena telah tersandi. Apabila data dapat terbaca, maka harus melakukan pengembalian data yang telah tersandi tersebut ke data aslinya. Banyak metode algoritma kriptografi yang ada hingga digunakan saat ini. Penulis memilih dan menggunakan algoritma AES (*Advanced Encryption Standard*) dikarenakan telah menjadi standarisasi yang memiliki tingkat keamanan

tinggi. Kerahasiaan pesan informasi dilakukan dengan melalui proses enkripsi dan dekripsi. Proses enkripsi yaitu mengubah pesan asli (*plaintext*) menjadi pesan dalam bentuk tersandi (cipher*text*). Sementara proses enkripsi dari *plaintext* memerlukan kunci (*key*) untuk menghasilkan cipher*text*, begitu juga sebaliknya pada proses dekripsi dari cipher*text* memerlukan kunci (key) yang sama untuk menghasilkan kembali *plaintext*.

Landasan Teori

Keamanan Data

Bagi sebuah institusi atau pengguna lainnya, sarana komunikasi data elektronik memunculkan masalah baru, yaitu keamanan. Di mana pada zaman yang serba canggih ini, sistem *autentifikasi* konvensional dengan KTP, SIM, dan yang lainnya yang berstandar pada keunikan tanda tangan, tidak berlaku untuk komunikasi elektronis. Komunikasi data eletronik memerlukan perangkat keamanan yang benar-benar berbeda dengan komunikasi konvensional.

secara mayoritas, pihak-pihak yang bertukar informasi menggunakan beberapa macam metode untuk menjaga kerahasiaan pesan yang ingin disampaikan, di antaranya menggunakan sebuah metode penyandian pesan yang bernama kriptografi (*Cryptography*) untuk merahasiakan pesan yang mereka kirimkan. keamanan merupakan komponen yang vital dalam komunikasi data elektronis. masih banyak yang belum menyadari bahwa keamanan (*security*) merupakan sebuah komponen penting yang tidak murah. teknologi kriptografi sangat berperan juga dalam proses komunikasi, yang digunakan untuk melakukan enkripsi (pengacakan) data yang ditransaksikan selama perjalanan dari sumber ke tujuan dan juga melakukan dekripsi (menyusun kembali) data yang telah teracak tersebut.

AES (*Advanced Encryption Standard*)

Advanced Encryption Standard merupakan algoritma kriptografi simetris yang dapat digunakan untuk mengamankan data. Algoritma ini merupakan standar enkripsi dengan kunci simetris. Jenis algoritma ini terbagi menjadi tiga, yaitu AES-128, AES-192 dan AES-256. Masing-masing jenis algoritma AES tersebut dapat mengenkripsi dan dekripsi data pada blok 128 bit, di mana blok 128 bit itu adalah ukuran tetap blok cipher yang digunakan pada algoritma AES.

Algoritma Rijndael(dibaca : Rhine-doll) kemudian dikenal dengan *Advanced Encryption Standard*(AES). Algoritma Rijndael yang disosialisasikan oleh National Institute of Standards and Technology(NIST) pada November 2001 lahir sebagai standar baru enkripsi yang dikembangkan dari algoritma DES (*Data Encryption Standard*) melalui seleksi yang ketat dengan algoritma yang lainnya. AES yang dicetuskan oleh dua orang yang kedua namanya merupakan bagian dari gabungan nama algoritma ini adalah Vincent Rijmendan Joan Daemen menjadi pemenang pada saat seleksi algoritma baru untuk menggantikan DES. Alasan utama terpilihnya algoritma Rijndael ini bukan karena algoritmanya yang paling aman dari MARS, RC6, Serpent, Twofish, dan yang lainnya, tetapi algoritma Rijndael memiliki keseimbangan antara keamanan serta fleksibilitas dalam berbagai platform perangkat keras dan perangkat lunak.

Sejarah AES (*Advanced Encryption Standard*)

Pada tahun 1972 dan 1974 National Bureau of Standards (sekarang dikenal dengan nama National Institute of Standards and Technology, NIST) menerbitkan permintaan kepada public untuk membuat standar enkripsi. Hasil dari permintaan pada saat itu adalah DES (Data Encryption Standard), yang banyak digunakan di dunia. DES adalah algoritma kriptografi simetris dengan panjang kunci 56 bit dan blok data 64 bit. Dengan semakin majunya teknologi, para kriptografer merasa bahwa panjang kunci untuk DES terlalu pendek, sehingga keamanan algortima ini dianggap kurang memenuhi syarat. Untuk mengatasi hal itu, akhirnya muncul triple DES (3DES).

Triple DES pada waktu itu dianggap sudah memenuhi syarat dalam standar enkripsi, namun teknologi yang tidak pernah berhenti berkembang akhirnya juga menyebabkan standar ini dianggap kurang memenuhi syarat dalam standar kriptografi. Akhirnya NIST mengadakan kompetisi untuk standar kriptografi yang terbaru, yang dinamakan AES (Advanced Encryption Standard). Dari hasil seleksi yang dilakukan oleh NIST, akhirnya NIST lima finalis AES, yaitu : MARS, RC6, Rijndael, Serpent, dan Twofish. Kompetisi ini selanjutnya dimenangkan oleh Rijndael dan secara resmi diumumkan oleh NIST pada tahun 2001. Rijndael ditulis oleh Vincent Rijmen dan Joan Daemen.

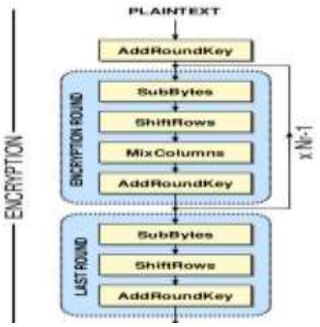
AES diumumkan oleh National Institute of Standards and Technology (NIST) sebagai standar pemrosesan informasi Federal (Federal Information Processing Standars, FIPS) publikasi 197 (FIPS 197) pada tanggal 26 November 2001 setelah proses standarisasi selama lima tahun, dimana ada 15 desain enkripsi yang disajikan dan dievaluasi, sebelum Rijndael terpilih sebagai yang paling cocok. AES efektif menjadi standar pemerintah Federal pada tanggal 26 Mei 2002 setelah persetujuan dari Menteri Perdagangan. AES

tersedia dalam berbagai paket enkripsi yang berbeda. AES merupakan standar yang pertama dapat diakses publik dan sandi-terbuka yang disetujui oleh NSA untuk informasi rahasia. Salah satu alasan mengapa AES bekerja dengan baik adalah metode enkripsi ini bekerja pada beberapa *network* layer pada saat yang sama. Walaupun AES dan Rijndael digunakan secara bergantian, terdapat beberapa perbedaan yang dapat dengan mudah diketahui. Sementara AES menggunakan blok *cipher* 128-bit, Rijndael dapat menggunakan blok *cipher* apa saja dan kunci 32-bit. Ukuran kunci dan blok *cipher* yang digunakan memiliki berkisar antara 128-bit sampai 256-bit. AES ini merupakan algoritma blok *cipher* dengan menggunakan sistem permutasi dan substitusi (P-box dan S-box) bukan dengan jaringan Feistel sebagaimana blok *cipher* pada umumnya. Tidak seperti DES yang berorientasi bit, Rijndael beroperasi dalam orientasi *byte*.

Algoritma Enkripsi AES-128

Garis besar Algoritma Rijndael yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (di luar proses pembangkitan *round key*) :

1. AddRoundKey: melakukan XOR antara stateawal (*plaintext*) dengan *cipher key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak Nr –1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes* : substitusi *byte* dengan menggunakan tabel substitusi (S-box).
   b. *ShiftRows*: pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumns* : mengacak data di masing-masing kolom *array state*.
   d. *AddRoundKey* : melakukan XOR antara *state* sekarang dengan *round key.*
3. Final round: proses untuk putaran terakhir :
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

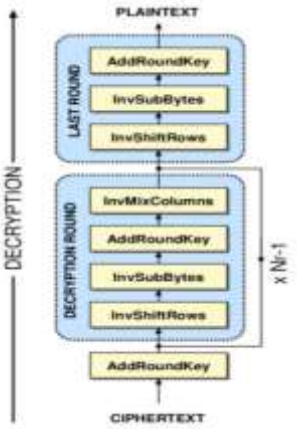


Gambar 1. Proses Enkripsi AES

Algoritma Dekripsi AES-128

Tahapan dekripsi adalah kebalikan dari tahapan enkripsi yang sebagian tahapan metode dan perhitungannya sama. Berikut adalah tahapan-tahapannya :

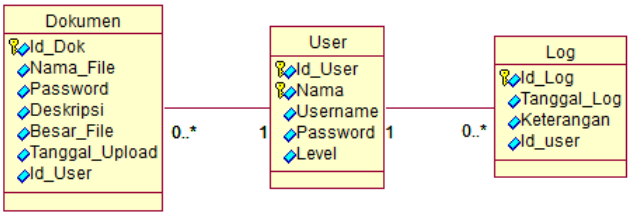
1. *AddRoundKey*: melakukan XOR antara *state* awal (*ciphertext*) dengan *cipher key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak Nr –1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *InverseShiftRows* : pergeseran baris-baris array statesecara wrapping kebalikan dari ShiftRows.
   b. *InverseSubBytes* : substitusi *byte* dengan menggunakan tabel *invers* substitusi (*invers* S-box).
   c. *AddRoundKey*: melakukan XOR antara *state* sekarang dengan *round key*.
   d. *InverseMixColumns*: membalikkan operasi *MixColumns*.
3. Final round: proses untuk putaran terakhir :
   a. InverseShiftRows
   b. InverseSubBytes
   c. AddRoundKey



Gambar 2. Proses Dekripsi AES

HASIL DAN PEMBAHASAN

Design *Database*



Gambar 3. Class Diagram

Database diperlukan untuk melakukan *management file*, di mana setiap *file* yang dienkripsi akan di catat oleh sistem dan pemilik *file* tersebut juga dicatat. Selain pengarsipan *file* mengingat untuk keamanan data menggunakan algoritma AES-128 yang tergolong keamanannya tinggi maka hampir tidak mungkin apabila *file* yang dienkripsi lupa *password* untuk di kembalikan seperti semula. Sehingga perlu untuk menyimpan

password masing-masing dokumen, dinama fitur ini hanya bisa di akses oleh administrator. Sehingga apabila lupa *password file* dapat dikembalikan seperti semula dan dokumen dapat dibaca kembali.

Form Login

Gambar 4. Form Login

Form Login digunakan untuk autentifikasi *user*, apakah dapat menggunakan sistem atau tidak. *User* yang ada di dalam sistem ada dua level, level *user* pengguna dan level administrator. *User* pengguna pada dasarnya adalah pemilik *file* maupun dokumen yang di upload dan di enkrip. Sedangkan user admin digunakan untuk manajemen sistem dan dapat mengakses semua *file* yang telah di *upload*.

Menu Utama

Gambar 5. Menu Utama

Menu ini berisi fitur apa saja yang ada di dalam sistem keamanan *management file*, yang meliputi Enkripsi *file*, Dekripsi *File*, Dokumen, Pengguna, Daftar *User* Baru, Ubah *Password* dan Log Kegiatan yang dilakukan oleh *User*.

Form* Enkripsi *File

Gambar 6. Enkripsi *File*

Form ini digunakan untuk meng-*upload file* dokumen, dan mengenkripsi *file* yang telah di-*upload*, dalam proses ini setiap dokumen yang di-*upload* akan diberikan kata kunci yang digunakan untuk mengenkripsi *file*

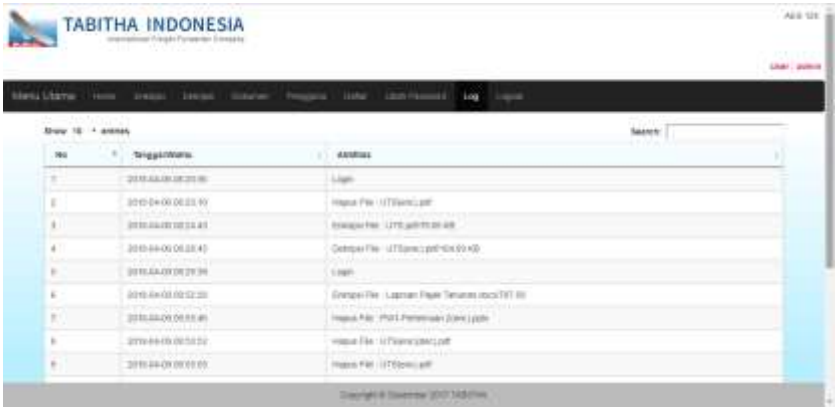
dokumen dan juga digunakan untuk mendekripsi *file* itu kembali. Setiap *file* yang di-*upload* akan ditandai siapa pemilik dokumen tersebut.

Menu Dokumentasi

Gambar 7. Menu Dokumentasi

Menu Dokumentasi, digunakan untuk menampilkan semua dokumen yang telah di upload. Data yang ditampilkan sesuai dengan kepemilikan *file* pada saat meng-*upload* dan mengenkripsi *file* dokumen. Sehingga keamanan data tetap terjaga di samping *file* dalam keadaan terenkripsi yang juga apabila dapat di-*download* tidak dapat dibaca. Menu dokumentasi juga sudah dilengkapi dengan *DataTable*, yang di lengkapi fungsi *search* sehingga memudahkan pada saat pencarian *file* dokumen. Menu dokumentasi akan menampilkan *password file* yang dienkrip apabila *user* yang digunakan administrator, untuk mengatasi apabila *user* pemilik *file* lupa *password* untuk mendeskripsi *file* dokumen mereka.

Menu *Log File*



Gambar 8. Data Log User

Menu Log *File*, Berisi semua aktivitas *user*. Menu ini menampilkan semua kegiatan *user* terhadap akses sistem, mulai dari *login*, enkripsi *file*, deskripsi *file*, menghapus *file*. Menu ini juga merupakan bagian dari keamanan data *file* dokumen. Sehingga dapat di lihat histori aktivitas *user* terhadap *file* dokumen.

KESIMPULAN

1. Dengan adanya sistem keamanan manajemen *file*, semua data dokumen penting perusahaan tersentralisasi pada server, sehingga memudahkan dalam hal *management file*. Pencarian *file* dokumen penting menjadi lebih mudah karena terkumpul dalam satu lokasi. Sistem ini juga mencatat kepemilikan *file* dokumen jadi walaupun semua data terkumpul menjadi satu, identitas *file* tetap terjaga.
2. *File* dokumen penting dienkripsi menggunakan AES 128, yang merupakan algoritma yang kuat dan teruji sehingga setiap *file* yang dienkripsi dapat didekripsi kembali. *File* yang telah di-*upload* juga tidak dapat dibaca informasi yang ada di dalamnya apabila tidak memiliki kunci pembuka *file*.
3. Pembuatan kunci enkripsi *file*, sepenuhnya diserahkan kepada *user* pemilik *file*, sehingga kerahasiaan *file* dokumen sangat aman. Akan tetapi ada kemungkinan *user* lupa *key/password file* dokumen, sehingga sistem keamanan manajemen *file* selalu menyimpan *key* setiap dokumen yang hanya dapat diakses oleh *user* administrator.

DAFTAR PUSTAKA

Ariyus, Dony, 2008. "Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi."ANDI, PENERBIT. Yogyakarta: STMIK AMIKOM.

Daemen, Joan, dan Rijmen Vincent, 2001. "Announcing the ADVANCEDENCRYPTION STANDARD (AES)." FIPS 197, Federal Information Standards Publications.

Wijayanto, B., dan Wardoyo, R., 2011. "An Implementation of Catmap-Rijndael (AES) Algorithm For Image Security(Study Case Making Students Card At Universitas Jenderal Soedirman)." Indonesian Journal of Computing and Cybernetics Systems, Universitas Gajah Mada. Vol.5 No.1.

Stewart, J.M., Chapple, M., dan Gibson, D., 2012. "Certified Information System Security Professional, Study Guide Sixth Edition." Indianapolis: John Wiley & Sons.Inc.

Komputer, W., (2010). "The Best Encryption Tools",Elex Media Komputindo.