SISTEM KRIPTOGRAFI MANAJEMEN FILE DATA PENUTUPAN ASURANSI MENGGUNAKAN ALGORITMA AES-128 STUDI KASUS : PT. ASURANSI BRINGIN SEJAHTERA ARTAMAKMUR (BRINS)

Sejati Waluyo[1], Ika Susanti[2], Anjar Imam Prasetyo[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur Jakarta
e-mail: [1]sejati.waluyo@budiluhur.ac.id, [2]ika.susanti@budiluhur.ac.id, [3]anjarimamp@gmail.com

Abstrak

Data konsumen ataupun customer didalam perusahaan asuransi adalah sesuatu yang penting, dimana data tersebut bersifat personal yang bukan merupakan konsumsi public. Sehingga perlu adanya kerahasian data yang perlu di jaga oleh perusahaan asuransi dalam hal ini adalah PT. Asuransi Bringin Sejahtera Artamakmus(BRINS). Informasi data yang terjaga dengan baik dapat meningkatkan kepercayaan konsumen terhadap perusahaan asuransi. Salah satu data penting tersebut adalah data penutupan asuransi. Data-data tersebut dalam bentuk berkas/file yang disimpan dalam komputer. Salah satu teknik pengamanan data file yang dapat digunakan dalam pengamanan data adalah teknik kriptografi atau enkripsi data. Dalam penelitian ini, di kembangkan sistem kriptografi enkripsi data menggunakan algoritma AES-128. Algoritma ini sangat aman untuk mengamankan file-file dokumen yang ada. Sehingga dengan adanya sistem ini keamanan data penutupan asuransi dapat terjaga dengan baik.

Kata Kunci*: data penutupan asuransi, sistem kriptografi, algoritmas AES-128*

1. PENDAHULUAN

Perkembangan teknologi informasi telah memberikan banyak manfaat dalam menyelesaikan berbagai permasalahan yang ada. Salah satu yang paling penting dalam sistem teknologi informasi adalah bagaimana data tersebut dapat tersimpan dengan baik, mudah di akses serta faktor yang tidak kalah penting dalam teknologi informasi adalah keamanan data itu sendiri. Berkembangannya teknologi keamanan data memberikan solusi dalam hal keamanan data. Salah satu yang dapat digunakan dalam keamanan data adalah teknologi enkripsi data. Dimana data diubah dalam bentuk lain yang tidak tidak dapat dibaca. Akan tetapi data tersebut dapat dikembalikan seperti semula sehingga informasi data tersebut tidak hilang.

PT. Asuransi Bringin Sejahtera Artamakmur yang lebih dikenal dengan nama BRINS merupakan salah satu perusahaan asuransi umum besar di Indonesia. Dengan misinya yaitu untuk menjadi perusahaan terkemuka, yang mampu memberikan rasa aman dan manfaat optimal kepada semua pihak yang berkepentingan. Untuk mendukung hal tersebut maka dibutuhkan keamanan informasi yang baik agar kredibilitas dan citra perusahaan terjaga dimata publik dan klien. Seperti yang kita ketahui pada umumnya, perusahaan asuransi banyak menyimpan data informasi mengenai nasabah tertanggung baik perorangan maupun perusahaan seperti alamat, nomor telepon, sampai nilai jual objek yang diasuransikan. Asuransi BRINS juga banyak bekerjasama dengan bank-bank besar seperti Bank BRI dan Bank Mandiri yang mengasuransikan objek harta yang dijaminkan ke bank tersebut. Setiap tahunnya pada akhir kontrak, bank-bank tersebut akan meminta data penutupan asuransi dimana data tersebut berisi informasi tentang tertanggung. Selama ini data tersebut disimpan tanpa ada pengamanan khusus untuk menjaga kerahasiaan data dan hanya diberikan password satu persatu saat data tersebut akan dikirim. Selain itu pengiriman data ke masing-masing bank dikirimkan langsung oleh staf yang bertanggung jawab, agar data tersebut sampai kepada pihak yang berhak, prosedur tersebut dinilai masih manual dan kurang efektif. Kemungkinan terjadinya pencurian dan penyalahgunaan data masih cukup tinggi, karena masih banyak faktor yang bisa dijadikan celah dalam hal keamanan data. Oleh karena itu, untuk menjamin keamanan data baik saat penyimpanan maupun pengiriman informasi, maka diperlukan aplikasi keamanan data untuk mengenkripsi agar data tersebut tidak bisa dengan mudah diakses orang lain yang tidak mempunyai otoritas, dan data yang terenkripsi juga tidak dapat didekripsi dengan aplikasi lain. Dengan adanya aplikasi enkripsi, diharapkan dapat memberi keefektifan dalam prosedur pengamanan data pada divisi terkait. Sehingga diharapkan aplikasi sistem enkripsi data ini mampu menyelesaikan masalah keamanan data yang dihadapi oleh PT. Asuransi Bringin Sejahtera Artamakmur.

2. METODE PENELITIAN

Metode penelitian ini digunakan sebagai pedoman penelitian dalam pelaksanaan penelitian agar hasil yang dicapai tidak menyimpang dari tujuan yang sudah ditetapkan.

2.1 Pengumpulan Data

Digunakan untuk mengumpulkan data-data yang diperlukan selama proses penyusunan Penelitian ini, yang diawali dengan tahap perancangan sampai implementasi pengujian. Beberapa metode pengumpulan data yang dilakukan, yaitu:

a. Studi Literatur, teknik ini diawali dengan pengumpulan data-data dengan cara mempelajari bahan-bahan, konsep, dan teori yang deperlukan dari beberapa sumber tertulis (Buku, Jurnal, Prosiding, Tutorial, dll), dan pemahaman yang diperlukan akan digunakan sebagai referensi penyusunan.
b. Observasi Langsung, dalam teknik ini akan diadakan pengamatan secara langsung terhadap gejala-gejala pokok dari apa yang sedang diteliti, pengamatan yang dilakukan dalam situasi yang sebenarnya diperlukan untuk keperluan khusus.

2.2 Perancangan Perangkat Lunak

Perancangan perangkat lunak yang digunakan dalam metode ini terdapat empat bagian yaitu :

a. Tahap Analisis (Analysis), pada tahapan ini intinya merupakan tahap dimana inisialisasi pendefinisian masalah untuk menyelesaikan teknik pengembangan prangkat lunak mulai dilakukan.
b. Tahap Perancangan (Design), pada tahap ini merupakan tempat perancangan yang meliputi proses penetapan rancangan masukan dari keluaran yang diperlukan, struktur dan rancangan tampilan.
c. Tahap Pengkodean (Code), fase dimana dilakukan konversi dari hasil rancangan (spesifikasi program) menjadi program jadi. Juga dilakukan pemeriksaan eksekusi bagian program yang dibuat.
d. Tahap Pengujian (Test), pada tahapan ini akan dilakukan pengujian untuk mencari kesalahan-kesalahan yang muncul pada saat pengkodean untuk selanjutnya dilakukan perbaikan untuk mengatasi masalah yang muncul tersebut.

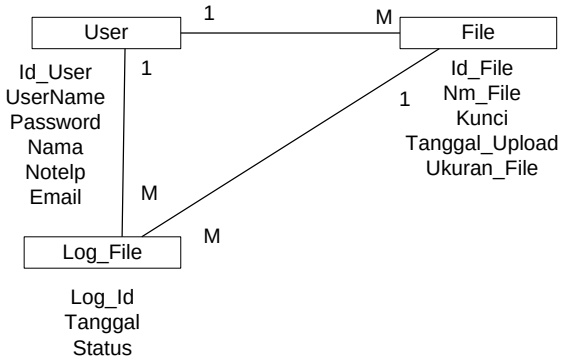
3. HASIL DAN PEMBAHASAN

Keamanan data adalah hal yang sangat penting bagi PT. Asuransi Bringin Sejahtera Artamakmur (BRINS). Karena sesuai dengan misinya tentang rasa aman, ini tidak hanya ditunjukkan untuk manfaat asuransi tetapi juga rasa aman akan data yang dirahasiakan oleh nasabah.

Data penutupan asuransi, dimana data tersebut menyimpan banyak informasi tentang tertanggung. Setiap masa perpanjangan kontrak dengan bank-bank yang bekerjasama, data tersebut akan dikirimkan ke masing-masing bank untuk ditinjau kembali. Biasanya data tersebut dikirimkan langsung oleh staf BRINS yang bertanggung jawab atas data tersebut untuk menjaga kerahasiaannya. Hal tersebut dinilai kurang efektif bila dilihat dari segi waktu dan biaya, tetapi bila data tersebut dikirimkan lewat email, dikhawatirkan data tersebut sampai kepada pihak yang tidak berwenang dan data tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab.

Dikarenakan kerahasian suatu data sangat penting, namun disisi lain data tetap harus dapat dibaca dikemudian hari apabila dibutuhkan. Maka untuk mengatasi hal tersebut diperlukan sebuah sistem berbasis Kriptografi yang dapat mengamankan data dan kerahasian informasi data penutupan asuransi. Sistem ini akan mengamankan data-data penting di PT. Asuransi Bringin Sejahter Artamakmur(BRINS) dalam bentuk enkripsi file sehingga apabila data tersebut diambil oleh orang lain maka isi dari data tersebut tetap aman, karena dibutuhkan kunci tertentu untuk membuka file maupun mendeskripsikan isi file. Sehingga sistem ini dapat melindungi data dari orang yang tidak memiliki hak terhadap data tersebut.

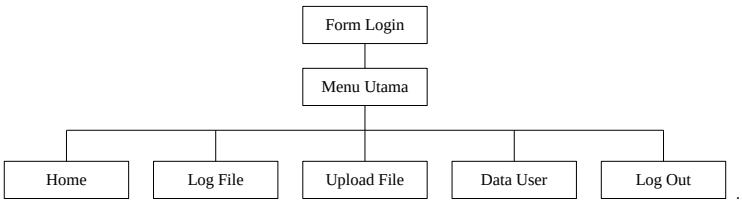
3.1 Design Database



Gambar 1. ERD Sistem Kriptografi Pengamanan File

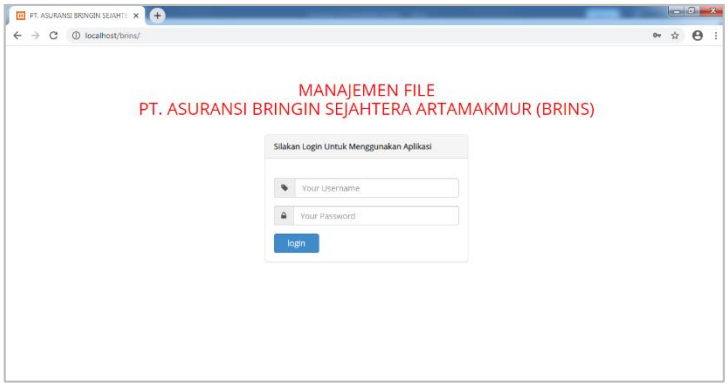
Database diperlukan untuk menyimpan data enkripsi maupun deskripsi file. Data ini juga menyimpan semua histori enkripsi file. Pengunaan database diperlukan karena enkripsi file ini melibatkan banyak dokumen yang setiap proses enkripsi bisa berbeda kunci enkripsinya. Sehingga memungkinkan lupa password enkripsi, dan tampa password file dokumen tidak dapat dibuka kembali. Sehingga perlu semua data enkripsi disimpan dan dapat digunakan dikemudan hari apabila dibutuhkan.

3.2. Struktur Menu Utama



Gambar 2. Strukur Menu Utama

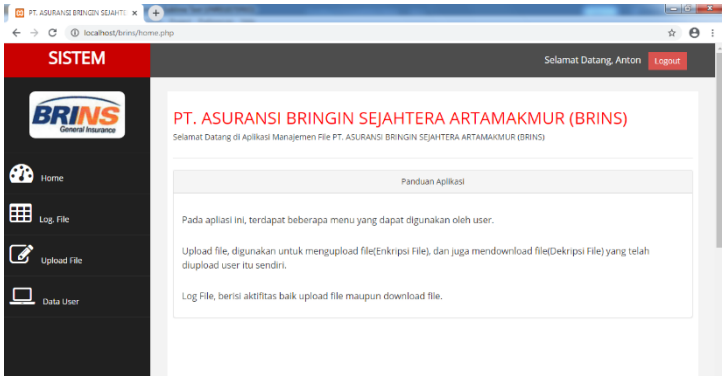
3.3 Form Login



Gambar 3. Halaman Login Sistem

Menu login, digunakan untuk mengakses sistem yang ada. User pengguna harus login ke dalam sistem sebelum menggunakan fitur yang ada didalam sistem.

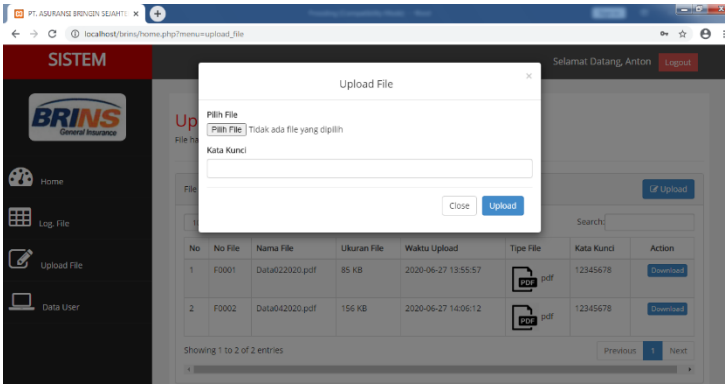
3.4 Menu Utama



Gambar 4. Halaman Menu Utama

Menu utama, merupakan halaman awal atau dashboard. Akan tampil pertama kali ketika user sudah melakukan authentifikasi melalui menu login. Menu utama juga berisi fitur apa saya yang ada pada sistem keamanan manajemn file.

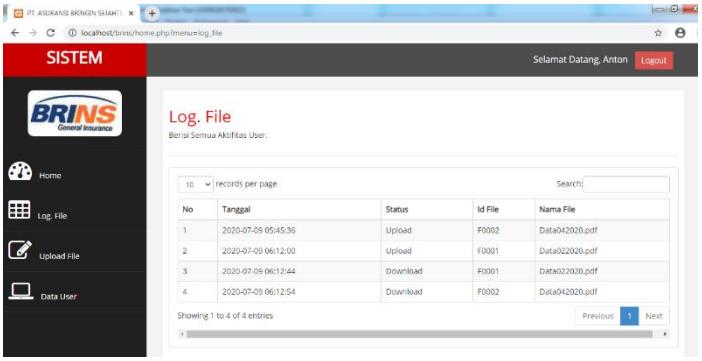
3.5 Form Upload File



Gambar 5. Halaman Upload File

Halaman upload file, menampilkan semua file yang telah diupload beserta kunci enkripsi file. Semua file yang dienkrip kunci enkripsinya akan selalu di simpan. Karena bukan hanya satu file yang dapat diupload. Sehingga berpotensi lupa kunci enkripsinya. Tampa kunci enkripsi file, file dokumen tidak mungkin dapat dibuka. Karena enkripsi file ini menggunakan algoritma AES-128, tampa kunci file maka data file yang telah diupload menjadi tidak dapat dibaca maupun dibuka kembali. Kata kunci ini hanya ditampilkan kepada user pemilik file dan user admin. Untuk tetap menjaga kerahasian data file yang telah di enkripsi. Di menu ini juga terdapat fitur untuk mendownload file yang telah di upload sebelumnya.

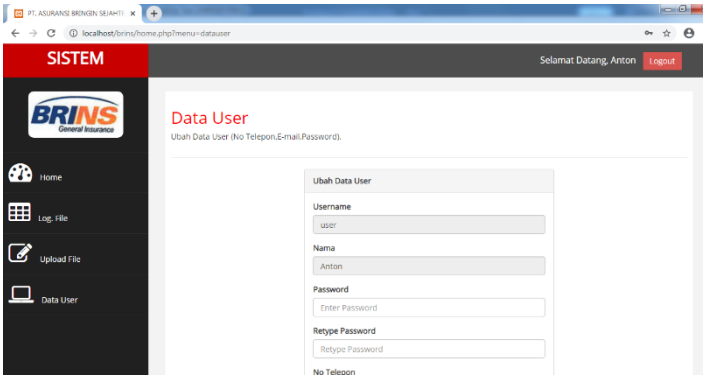
3.5. Log File



Gambar 5. Halaman Log File

Halaman log file, semua aktifitas user. Baik saat mengupload dokumen file enkripsi maupun mendownload file yang pernah di upload sebelumnya.

3.5. Data user



Gambar 6. Halaman Data User

Data user, berisi informasi data user. Dengan mengunakan menu ini user dapat melakukan update password secara.

4. KESIMPULAN

Berdasarkan analisa dan implementasi sistem keamanan manajemen file menggunakan algoritma AES-128 ini, dapat ditarik suatu kesimpulan bahwa Sistem keamanan file dapat berjalan dengan baik, dan mampu mengekripsi dan mendekripsi file yang telah dienkrip. Sistem keamanan file dapat melakukan manajemen file atau pengarsipan data. Sistem ini dapat memudahkan dalam pencarian file dengan mudah melalui fungsi searching. Sistem keamanan juga memanfaatkan fungsi database, dimana semua proses enkripsi selalu di simpan kunci enkripsinya. Hal ini memudahkan ketika user lupa kunci untuk membuka file yang telah dienkripsi.

DAFTAR PUSTAKA

[1] Komputer, Wahana. 2010 .The Best Encryption Tools. Jakarta : PT Elex Media Komputindo
[2] Schneier, Bruce. 1996 .”Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C’. Wiley Computer Publishing, Jhon Wiley & Sons, inc.
[3] M. Sihombing, J. N. Sitompul, and T. A. Putri, “Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio,” MEANS (Media Inf. Anal. dan Sist., vol. IV, no. 1, pp. 37–45, 2019.
[4] R. V. H. Chandra, A. Kusyanti, and M. Data, “Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File,” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. III, no. 1, pp. 481–486, 2019.