JURNAL INTITALAFA **ISSN (Cetak): 2085-0573**
Vol.16, No.1, Januari-Juni 2024, pp.54-60 **ISSN (Online): 2829-1506**

APLIKASI PENGAMANAN DATA METODE RIVEST SHAMIR ADLEMEN DAN ADVANCE ENCRYPTION STANDARD (STUDI KASUS PT. BESS FINANCE CABANG TALAGA KAB. MAJALENGKA)

M. Habbi Fikki[1], Maksudi[2], Harry Gunawan[3]
[123]*Program Studi Teknik Informatika, Fakultas Teknik,Universitas Muhammadiyah Cirebon jl. Fatahillah, Watubelah, Kec. Sumber, Cirebon, Jawa Barat, Indonesia, 45611*
[1]*mhafikki@gmail.com,* [2]*mxbocah@gmail.com,* [3]*harygunawan@umc.ac.id*

Abstrak

Pesatnya perkembangan teknologi informasi sudah menjadikan berita menjadi kebutuhan pokok bagi setiap orang. info juga ialah hal yang penting bagi sebuah perusahaan. karena informasi dapat membantu suatu perusahaan untuk terus berkembang dalam persaingan dunia. Masalah yang terjadi pada proses pengamanan data pada perusahaan apabila terjadi kerusakan dan kehilangan data pada komputer atau laptop maka data perusahaan akan terancam jika tidak adanya backup data pada data-data perusahaan dan akan menyebabkan kerugian besar bagi perusahaan. Salah satu cara mengamankan data atau informasi dari kerusakan dan kehilangan pada komputer maupun laptop adalah menggunakan konsep kriptografi. Setelah dilakukan pengujian apabila terjadi kerusakan pada komputer administrator dapat memudahkan mengamankan data penting perusahaan dan sistem berhasil melakukan enkripsi dan dekripsi serta menbackup file penting dengan menggunakan Metode Rivest Shamir Adlemen Dan Advance Encryption Standard dan hasil sesuai dengan yang dibutuhkan sistem dapat mengelola data file yang ingin di amankan dengan baik.

Kata kunci*: keamanan, data, enkripsi, RSA*

Abstract

The rapid development of information technology has made news a basic need for everyone. Information is also important for a company. because information can help a company to continue to grow in world competition. Problems that occur in the data security process at the company if there is damage and loss of data on a computer or laptop, the company's data will be threatened if there is no data backup on company data and will cause big losses for the company. One way to secure data or information from damage and loss on computers and laptops is to use the concept of cryptography. After testing, if there is damage to the computer, the administrator can make it easier to secure important company data and the system can successfully encrypt and decrypt and back up important files using the Rivest Shamir Adleman Method and Advance Encryption Standard and the results are in accordance with what is needed, the system can manage the data files you want to save. secure it well.

Keywords: *security, data, encryption, RSA*

1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi sudah menjadikan berita menjadi kebutuhan pokok bagi setiap orang. info juga ialah hal yang penting bagi sebuah perusahaan. karena informasi dapat membantu suatu perusahaan untuk terus berkembang dalam persaingan dunia.
Masalah yang terjadi pada proses pengiriman ataupun mendapatkan informasi adalah apabila informasi itu bersifat rahasia. Bila informasi tersebut tersebar luas karena adanya penyandapan, pencurian, dan pemalsuan informasi, akan menyebabkan kerugian besar bagi pemilik informasi. Salah satu cara mengamankan data atau informasi dari tindak kejahatan tersebut adalah menggunakan konsep kriptografi.
PT. Bess Finance Cabang Talaga adalah perusahaan yang bergerak di bidang pembiayaan konsumen yang beralamat di Jalan Talaga Bantarujeg, Campaga, Kec. Talaga, Kabupaten Majalengka, Jawa Barat. Setelah dilakukan penelitian dibagian Administrasi Support, beberapa *file* penting haya disimpan begitu saja di dalam *folder* komputer di salah satu pegawai PT. BESS Finance Cabang Talaga.
Oleh karena itu dibuatlah sistem keamanan yang berguna untuk mengamankan data *file* nasabah dan sebagainya agar pegawai perusahaan bisa menjaga file tersebut dengan aman dan tidak merugikan perusahaan tersebut.

2. METODE PENELITIAN

Berdasarkan permasalahan yang ada dilihat dari latar belakang diatas maka dibuatlah sistem keamanan data *file* dengan menggunakan metode *Rivest Shamir Adlemen Method and Advance Encryption Standard*. *Advanced Encryption Standard (AES).* [1]. Metode *AES* merupakan *algoritma cryptographic* yang dapat digunkan untuk mengamakan data. *Algoritma AES* adalah blok chipertext simetrik yang dapat mengenkripsi (*encipher*) dan *dekripsi* (*decipher*) informasi.
Secara umum metode yang digunakan dalam pemrosesan terbagi dua, yaitu :
1. *Enkripsi*
2. *Dekripsi*
[2]. Metode *RSA* merupakan lgoritma kriptografi kunci publik (asimetris). Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, *RSA* mempunyai dua kunci, yaitu kunci publik dan kunci rahasia.

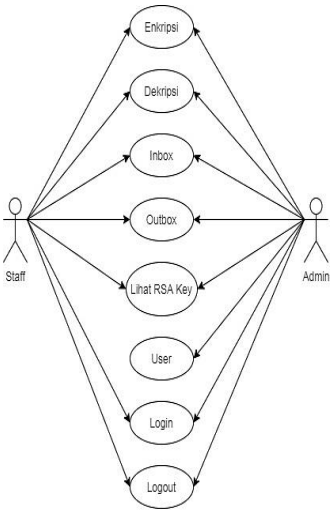
2.1. Perancangan

2.1.1 Sistem Usulan

Analisis prosedur sistem yang diusulkan adalah gambaran alur sistem pengamanan data dengan metode *Rivest Shamir Adlemen Dan Advance Encryption Standard* yang diusulkan untuk mengetahui alur berjalannya suatu sistem program.

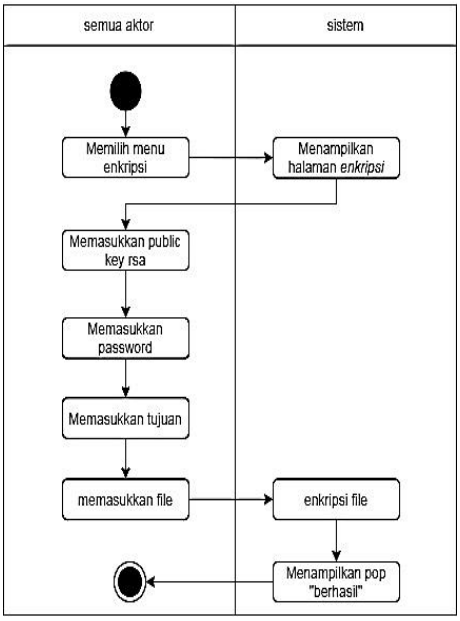
a. *Admin* dan *user* memasuki sistem *login* dengan memasukan *user*name dan *password* untuk hak akses ke dalam sistem.
b. *User* melakukan registrasi untuk mendapatkan hak akses ke dalam sistem.
c. *User* dapat mengelola *file* jika ingin mengamankan *file* maka *user* meng*enkripsi*, *dekripsi*, dan mengirim *file* ke *user* lainnya.
d. *User* bisa meng*enkripsi* dan *dekripsi* dengan format *Jpg*, *Docx*, *txt*.

2.1.2 *Use Case* Diagram



Gambar 1 use case diagram

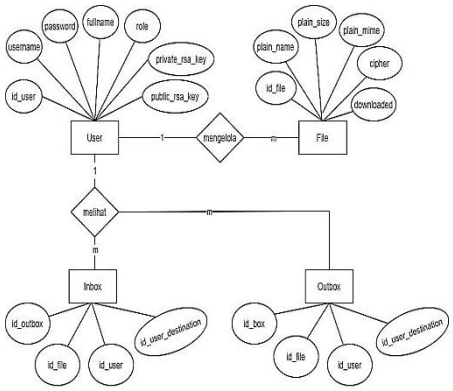
2.1.3 *Activity* Diagram



Gambar 2 Activity Diagram

2.1.4 *Entity Relationship* (ERD)

Kumpulan bagian dari keseluruhan **s**uatu yang berwujud serta kumpulan penghubung antar pihak seluruh data yang ada. Seperti pada gambar 3 adalah gambar rancangan ERD :



Gambar 3 Entity Relationship (ERD)

2.2. Implementasi

```
<tfoot>
<tr>
<td colspan="2" align="right">
<button class="btn btn-primary
btn-sm" type="button" id="add-
item">
<i class="mdi mdi-plus"></i>
Tambah
</button>
</td>
</tr>
</tfoot>
</table>
```

Gambar 4 menambahkan file enkripsi

```
<button class="btn btn-success"
type="submit">
<i class="mdi mdi-lock-
open"></i> Deskripsi</button>
</div>
```

Gambar 5 mendekripsikan file

```
</div>
<div class="col-lg-6">
<div class="form-group">
<label> Private Key RSA
(Untuk Deskripsi) </label>
<textarea class="form-control"
placeholder="Masukkan
Private Key RSA" rows="6"
readonly><?= $private_key;
?></textarea>
</div>
```

Gambar 6 mendekripsikan file

ISSN (Cetak): 2085-0573
ISSN (Online): 2829-1506

2.3. Rencana Pengujian

Tabel 1 Rencana Pengujian

No	Kelas Uji	Kode Butir Uji	Butir Uji	Level pengguna
1	*Login*	1	*Login* dengan *user* dan *password* yang benar	Semua Aktor
		2	*Login* dengan *username* yang salah	
		3	*Login* dengan *password* yang salah	
		4	Menambahkan *User* Baru (*Sign Up*)	
2	*Enkripsi*	5	Mengisi *form input* dan memilih *enkripsi*	Semua Aktor
		6	Mengosongkan semua *form input enkripsi*	
		7	Menghapus data *file* pada *form*	
		8	Menambahkan data *file* pada *form input* pilih *file*	
3	*Dekripsi*	9	Melihat *File Dekripsi*	Semua Aktor
		10	Mengisi *form input* dan memilih *dekripsi* lalu *download* hasil *dekripsi*	
		11	Mengosongkan *form input*	
4	*Inbox*	12	Melihat pesan masuk data *file*	Semua Aktor
		13	Mengisi *form input inbox* dan memilih *dekripsi* lalu *download* hasil *dekripsi*	
		14	Mengosongkan *form input*	
5	*Outbox*	15	Melihat pesan keluar data *file*	Semua Aktor
		16	Mengisi *form input outbox* dan memilih *dekripsi* lalu *download* hasil *dekripsi*	
		17	Mengosongkan *form input*	
6	*Lihat RSA Key*	18	Menampilkan kunci *public key RSA* (untuk *enkripsi*), dan *private key RSA* (untuk *dekripsi*)	Semua Aktor
7	*User*	19	Menampilkan data *user* yang terdaftar pada sistem	Admin
		20	Menghapus salah satu *user*	

3. HASIL DAN PEMBAHASAN

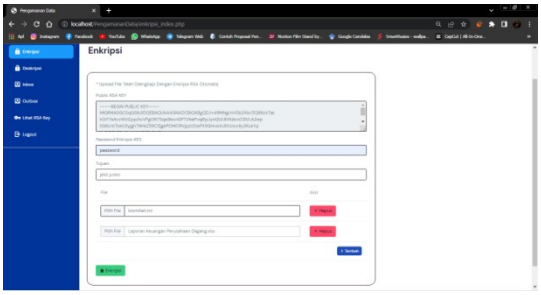
3. HASIL DAN PEMBAHASAN

3.1.1 Hasil Pengujian

Tabel 2 Pengujian Kode Butir

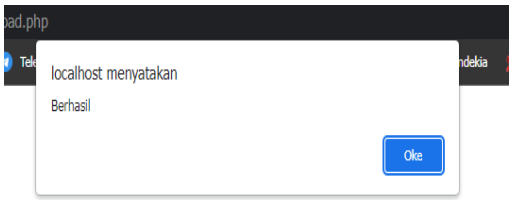
Kode uji butir	5		
Nama uji	Mengisi *form input* dan memilih *enkripsi*		
Kelas uji	*Enkripsi*		
Tujuan	Berhasil melakukan *enkripsi*		
Kondisi awal	Halaman *Enkripsi*		
Skenario			
1. Masuk kehalaman *enkripsi* 2. Isi *form input enkripsi* 3. Klik tombol *enkripsi*			
Hasil			
Data yang diberikan	Yang diharapkan	Pengamatan	Kesimpulan
Mengisi data *form enkripsi*	*File* Berhasil ter*enkirpsi* tampil pesan "Berhasil"	• Mengisi semua *form enkripsi* • klik *enkripsi* • Sistem menampilkan pesan "Berhasil" (Gambar 6.13)	Berhasil

Berdasarkan Tabel 2 Pengujian Kode Uji Butir 6 sistem berhasil meng*enkripsi* data *file*.



Gambar 7 Halaman Enkripsi

ISSN (Cetak): 2085-0573
ISSN (Online): 2829-1506

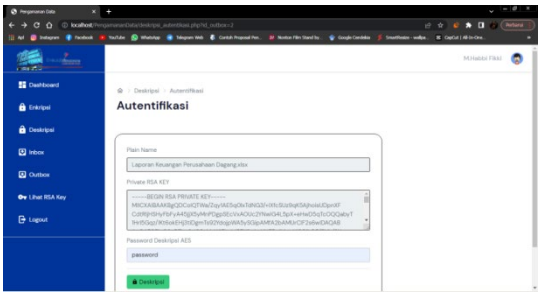


Gambar 8 Notifikasi Dari Enkripsi

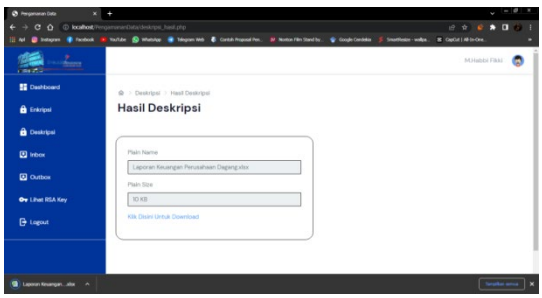
Tabel 3 Pengujian kode Butir

Kode uji butir	10		
Nama uji	Mengisi *form input dekripsi* dan memilih *dekripsi* lalu *download* hasil *dekripsi*		
Kelas uji	*Dekripsi*		
Tujuan	Berhasil melakukan *dekripsi*		
Kondisi awal	Halaman *Dekripsi*		
Skenario			
1. Masuk kehalaman *dekripsi* 2. Pilih *file* yang ingin *dekripsi* 3. Memasukkan *password* 4. Klik tombol *dekripsi* 5. *Klik link download*			
Hasil			
Data yang diberikan	Yang diharapkan	Pengamatan	Kesimpulan
Mengisi data *password* dengan benar dan men*download* hasil *dekripsi*	*File* berhasil ter*dekripsi* dan menampilkan hasil *dekripsi*	• Mengisi *password* pada dengan benar *form dekripsi* • Klik *dekripsi* • Sistem menampilkan hasil *dekripsi* dan *link download* (Gambar 6.18)	Berhasil

Berdasarkan Tabel 3 Pengujian Kode Uji Butir 13 sistem berhasil meng*dekripsikan* data *file*.



Gambar 9 Halaman Dekripsi



Gambar 10 Halaman Hasil Dekripsi

3.1.2 Rangkuman Hasil Pengujian

Berdasarkan pengujian yang dilakukan pada aplikasi sebagai dapat menghasilkan kesimpulan, yaitu:

1. Pendaftaran *user* baru pada halaman *login* dengan masuk ke *sign up*
2. Sistem dapat mengidentifikasi *level* pengguna dan mengalihkannya ke halaman lain sesuai dengan *level* pengguna.
3. Sistem pada *level enkripsi* dapat melakukan pengamanan data dengan mengisi semua data-data yang tersedia.
4. Sistem pada *level dekripsi* dapat melakukan membaca isi data yang ter*enkripsi* dengan data-data yang tersedia.
5. Sistem pada *level inbox* melihat pesan masuk *file* data yang terkirim dari pengguna lain.
6. Sistem pada *level outbox* dapat melihat pesan *file* data keluar yang mengirim dari pengguna.
7. Sistem pada *level* lihat *RSA key* dapat melihat kunci untuk memasukkan ke halaman *enkripsi* dan *dekripsi.*

Sistem pada *level user* dapat melihat pengguna *user* yang terdaftar pada *aplikasi* oleh *admin.*

4. KESIMPULAN

Berdasarkan hasil yang dibuat sistem dapat melakukan *enkripsi* data *file* dan *dekripsi* data *file*. Sistem dapat mengelola data-data yang ingin diamankan dengan keamanan yang baik.

Adapun saran dari peneliti yaitu semoga sistem ini dapat di kembangkan menjadi berbasis *android* dan *dekstop*.

DAFTAR PUSTAKA

[1] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[2] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2015, doi: 10.14710/jtsiskom.3.2.2015.253-258.