IMPLEMENTASI ALGORITMA AES DAN RC4 UNTUK MENGAMANKAN FILE DATA CUSTOMER INSTALASI BARU

Andi Kurniawan[1*], Rizky Pradana[2]

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

Email : [1*]1511520197@student.budiluhur.ac.id, [2]rizky.pradana@budiluhur.ac.id
(* : corresponding author)

Abstrak-PT. Supra Primatama Nusantara atau lebih dikenal dengan Biznet Networks merupakan perusahaan infrastruktur digital terintegrasi di Indonesia yang menyediakan layanan Internet, Data Center, Cloud Computing dan IPTV. Berdasarkan analisa masalah yang akan dilakukan oleh peneliti pada Biznet Networks itu sendiri adalah terkait data-data customer baru pada yang akan dilakukan pemasangan atau instalasi layanan Internet baik untuk keperluan di rumah tempat tinggal, bisnis atau perkantoran. Untuk meningkatkan keamanan terhadap data atau file yaitu dengan menggunakan metode kriptografi. Terlebih dengan isi dari file tersebut bersifat penting dan rahasia seperti yang digunakan oleh Biznet adalah untuk data-data terkait data customer baru yang menggunakan jasa layanan Internet. Hasil dari penelitian sistem kriptografi file ini menggunakan bahasa pendukung pemrograman PHP dan database MySQL yang telah dirancang dan diimplementasikan ini dapat mengenkripsi dan mendekripsi file dokumen customer baru yang memiliki ekstensi .docx dan .pdf. Hasil dari implementasi aplikasi kriptografi yang dibuat menggunakan algoritma Advanced Encryption Standart (AES) dan RC4 (Rivest Code4) saat proses enkripsi dan dekripsi data file yang diterapkan pada internal program berhasil mengkonversi isi file atau dokumen asli menjadi acak dan ekstensi berubah menjadi .vic . Aplikasi ini di buat agar dapat memberikan keamanan lebih terhadap isi data customer baru yang bersifat rahasia tanpa takut adanya pihak lain yang tidak bertanggung jawab.

Kata Kunci: kriptografi, data, AES, RC4

IMPLEMENTATION OF AES AND RC4 ALGORITHM FOR SECURING NEW INSTALLATION CUSTOMER DATA FILES

Abstract- *PT. Supra Primatama Nusantara or better known as Biznet Networks is an integrated digital infrastructure company in Indonesia that provides Internet, Data Center, Cloud Computing and IPTV services. Based on the problem analysis that will be carried out by researchers at Biznet Networks itself is related to new customer data for those who will be installing or installing Internet services for both residential, business or office purposes. To increase the security of data or files by using cryptographic methods. Even more, the contents of the file are important and confidential as used by Biznet is for data related to new customer data using Internet services. The results of the research on this file cryptography system using the PHP programming language and MySQL database that have been designed and implemented can encrypt and decrypt new customer document files that have .docx and .pdf extensions. The results of the implementation of cryptographic applications made using the Advanced Encryption Standard (AES) and RC4 (Rivest Code4) algorithms when the data file encryption and decryption process applied to the internal program managed to change the contents of the original file or document to be random and the extension changed to .vic. This application was created in order to provide more security for the contents of new customer data that are confidential without fear of other parties who are not responsible.*

Keywords*: cryptography, data, AES, RC4*

1. PENDAHULUAN

Keamanan data merupakan hal yang sangat penting dalam bidang bisnis komersial (perusahaan) dan tradisional saat ini [1]. Data berisi informasi tersebut sangat mudah untuk dapat di akses oleh orang lain yang menggunakan komputer yang sama dikarenakan tidak adanya keamanan yang diterapkan.

Berdasarkan analisa masalah yang akan dilakukan oleh peneliti pada PT. Supra Primatama Nusantara atau lebih dikenal dengan Biznet Networks itu sendiri adalah terkait data-data customer (pelanggan) baru yang menggunakan jasa layanan Internet baik untuk keperluan di rumah tempat

tinggal, bisnis atau perkantoran. Salah satu cara untuk meningkatkan keamanan terhadap data atau file yaitu dengan menggunakan metode kriptografi. Terlebih lagi isi dari file tersebut bersifat penting dan rahasia seperti

yang digunakan oleh Biznet adalah untuk data-data terkait customer (pelanggan) baru yang menggunakan jasa layanan Internet.

Penelitian ini akan dilakukan pengamanan atau teknik *security key* berupa data-data yang digunakan oleh Biznet Networks dalam menangani data-data terkait *customer* (pelanggan) baru yang menggunakan jasa layanan Internet dalam format dan ekstensi .docx dan .pdf dengan mengimplementasikan *Encryption Decryption Algorithm*. *Encryption Decryption Algorithm* adalah algoritma yang digunakan untuk proses enkripsi dan dekripsi[2] .Algoritma yang digunakan yaitu algoritma *Advanced Encryption Standart* (AES) dan *Rivest Code4* (RC4) menggunakan bahasa pendukung pemrograman PHP dan database MySQL.

2. METODE PENELITIAN

2.1 Penerapan Metode

Tahapan tahapan pada penelitian yang akan dilakukan menggunakan Model Penelitian Waterfall yaitu :

a) Pengumpulan Data. Pengumpulan data terdapat 4 (empat) tahap, yaitu: Observasi (Pengamatan), tahap ini dimana penulis melakukan observasi (pengamatan) terkait tinjauan sumber data-data pelanggan yang ingin melakukan pemasangan instalasi internet, Dokumentasi, dimana penulis melakukan pengumpulan data berupa dokumentasi file yang terdapat pada CRM, Tinjauan Studi, tahap ini, dimana penulis melakukan pencarian beberapa sumber penelitian yang telah dilakukan terdahulu atau sebelumnya terhadap tema penelitian yang penulis lakukan saat ini dan Referensi Pustaka, Tahap ini, dimana penulis melakukan pengumpulan data-data berupa buku-buku, jurnal publikasi ISSN ataupun prosiding konferensi (seminar karya tulis terpublikasi ISBN).
b) Analisa Data. Tahap ini melakukan analisa secara berurutan, mulai dari analisis data masukan, analisis penerapan algoritma dan analisis terhadap sistem keluaran yang akan dibangun.
c) Perancangan (*Design*). Tahap ini menggambarkan desain dari perangkat lunak yang akan dibangun berupa *web*. Untuk itu, perlu menggambarkan beberapa perancangan, seperti: rancangan UML dan rancangan UI (*User Interface*).
d) Perancangan metode. Tahapan enkripsi file dilakukan menggunakan metode AES 128 dan RC4, enkripsi pertama dilakukan dengan metode AES 128 terlebih dahulu lalu dilanjut dengan RC4. Tahapan dekripsi file pertama dilakukan menggunakan metode RC4 terlebih dahulu lalu dilanjut dengan AES 128.
e) Pembuatan program. Tahap serangkaian instruksi yang ditulis untuk melakukan suatu fungsi spesifik pada aplikasi yang akan dibuat. Program yang akan digunakan saat membangun sistem menggunakan bahasa pemrograman PHP dan database MySQL.
f) Pengujian. Tahap ini penulis melakukan pengujian terhadap sistem secara bertahap. Tahap ini diharapkan agar sistem yang telah dibuat tidak ada masalah (*error*) dan dapat dijalankan sebagaimana mestinya.
g) Kesimpulan penelitian. Tahap ini adalah tahap paling terakhir dalam sebuah penelitian, dimana penulis akan melakukan *review* berupa hasil kesimpulan penelitian serta memberikan hasil analisa dari rumusan masalah yang telah diuraikan pada bab awal.

2.2 Rancangan Basis Data

Database adalah tempat tempat untuk menyimpan sebuah data data yang dapat saling terhubung. Dalam dunia komputer database bisa dikategorikan sangat spesial karena selalu menjadi hal utama dalam perancang sistem computer [3].

Berikut ini adalah susunan tabel yang digunakan dalam pembuatan aplikasi enkripsi dan dekripsi.

a. Tabel *Users*

Nama Tabel : users
Primary Key : username
Media Penyimpanan : *hard disk*
Tabel ini untuk menyimpan *user login*

Tabel 1. Tabel *Users*

No	Field	Type	Length	Keterangan
1	Username	Varchar	15	Primary Key
2	Password	Varchar	100	-
3	Fullname	Varchar	50	-
4	Job_title	Varchar	50	-

5	Join_date	Timestamp		-
6	Last_activity	Timestamp		-
7	status	Enum	(‘1’,’2’)	-

b. Tabel File

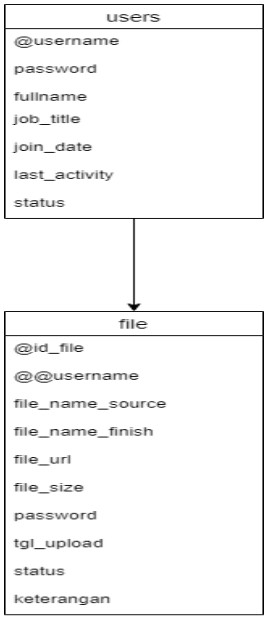
Nama Tabel : file
Primary Key : id_file
Media Penyimpanan: *Hard Disk*
Tabel ini untuk menyimpan data file

Tabel 2. Tabel *File*

No	Field	Type	Length	Keterangan
1	Id_file	Int	11	Primary Key
2	Username	Varchar	15	-
3	File_name_source	Varchar	255	-
4	File_name_finish	Varchar	255	-
5	File_url	Varchar	255	-
6	File_size	Float		-
7	Password	Varchar	16	-
8	Tgl_upload	Timestamp		-
9	Status	Enum	(‘1’,’2’)	-
10	Keterangan	Varchar	255	-

c. *Logical Record Structure* (LRS)

Simbol ‘@’ yang ada pada salah satu atribut sebagai tanda bahwa atribut tersebut adalah primary key.



Gambar 1. LRS

2.3 Algoritma

Menurut Goodman Hedet Niemi [4] mendefinisikan bahwa “*Algoritma adalah adalah urutan terbatas dari operasi-operasi terdefinisi dengan baik, yang masing-masing membutuhkan memori dan waktu yang terbatas untuk menyelesaikan suatu masalah*. Proses dekripsi [8] dilakukan pada blok-blok bilangan yang diperoleh dari proses enkripsi sehingga menghasilkan bilangan baru yang apabila diubah kembali kedalam pengkodean ASCII akan menghasilkan karakter yang sama dengan plainteks sebelum dilakukan proses enkripsi. Keamanan enkripsi hanya tergantung pada kunci, dan tidak bergantung apakah algoritmanya dilihat orang lain atau tidak [5]. Berikut algoritma yang digunakan:

a. Algoritma AES

Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Algoritma AES adalah merupakan cara enkripsi yang di terbitkan pada tahun 2001 oleh NIST (National Institute of Standard and Technology) [6],algoritma AES dijadikan standard untuk mengamankan data untuk menggantikan algoritma DES. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan mendekrip data.

b. Algoritma Rivest Code 4

RC 4 atau Rivest Code4 merupakan algoritma kriptografi yang berjenis stream cipher, yang dimaksud stream cipher adalah cara kerja algoritma ini yaitu persatuan data, seperti bit,byte,nible. Setiap memproses pengenkripsian satu satuan data digunakan kunci hasil dari pembangkitan sebelumnya.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Data

a. Analisis Data Masukan (Input)
Tahap ini, dimana penulis melakukan analisis data masukan terkait file-file bukti pemesanan pelanggan (customer order) yang dikirim oleh kedua belah pihak lewat E-mail, yang dimana data tersebut akan diolah sebagai data masukan (input) pada sistem yang akan dibuat dan diimplementasikan.

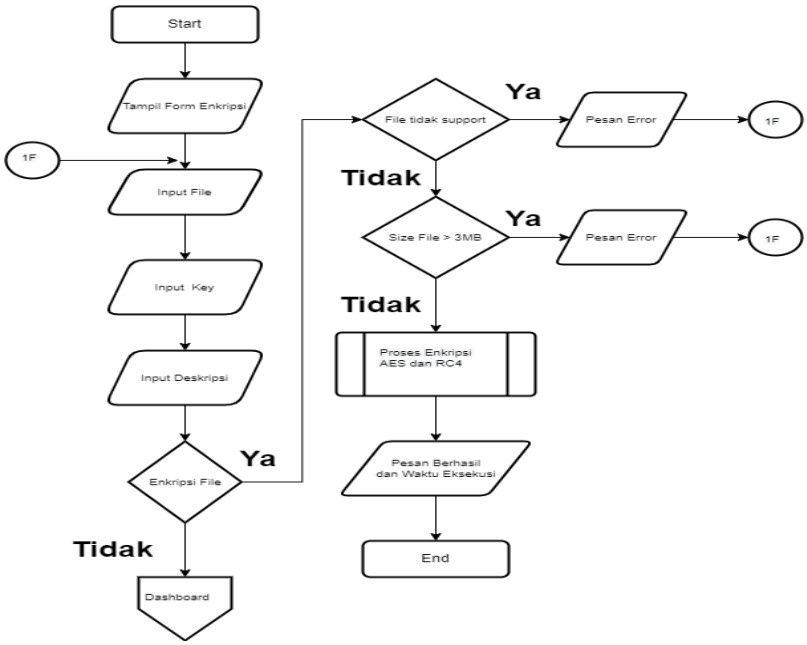
b. Analisis Penerapan Algoritma
Tahap ini, dimana penulis melakukan penerapan algoritma AES dan RC4 saat proses enkripsi algoritma AES melakukan enkripsi pertama lalu algoritma RC4 dan pada dekripsi RC4 melakukan proses dekripsi pertama lalu dilanjut dengan dekripsi AES data yang dilakukan pada saat proses sistem berjalan (running).

c. Analisis Data Keluaran (Output)
Tahap ini merupakan tahap untuk melakukan pengamanan pada data yang dienkripsi sebelum dimasukkan ke dalam sebuah basis data. Beberapa rancangan akan dibangun sesuai dengan proses kriptografi pada program, seperti proses enkripsi dan proses dekripsi sehingga dapat dilihat hasil keluaran (output) pada sistem telah sesuai atau tidak.

3.2 *Flowchart*

a. *Flowchart* Proses Upload File

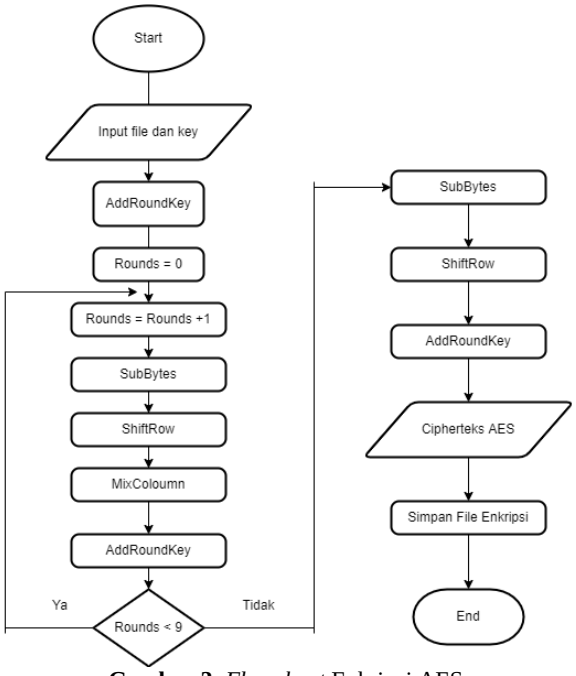
Pada gambar 2 proses pada saat upload file untuk melakukan enkripsi suatu file. Mulai dari tampilan form enkripsi sampai dengan file tersebut berhasil di enkripsi.



Gambar 2. *Flowchart Upload File*

b. *Flowchart* Proses Enkripsi AES

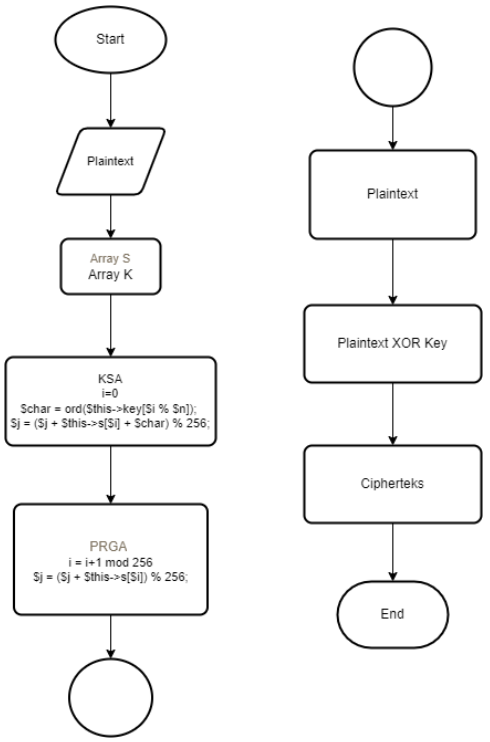
Flowchart pada gambar 3 dimulai dari input file atau file yang akan di enkripsi sebagai plaintext yang akan diubah menjadi chiperteks dan sebuah key. Kemudian putaran pertama SubByte, ShiftRows, MixColoumn, dan AddRoundKey. Proses berulang sampai dengan 1- Round, karena AES 128 memiliki 10 putaran. Jika >9 Round maka memasuki tahap final round SubByte, ShiftRows, MixColoumn. Setelah round terakhir maka hasilnya adalah chipertext AES yang menjadi sebuah file ekstensi. vic dan akan di simpan di folder file_encrypt.



Gambar 3. *Flowchart* Enkripsi AES

c. *Flowchart* Proses Enkripsi RC4

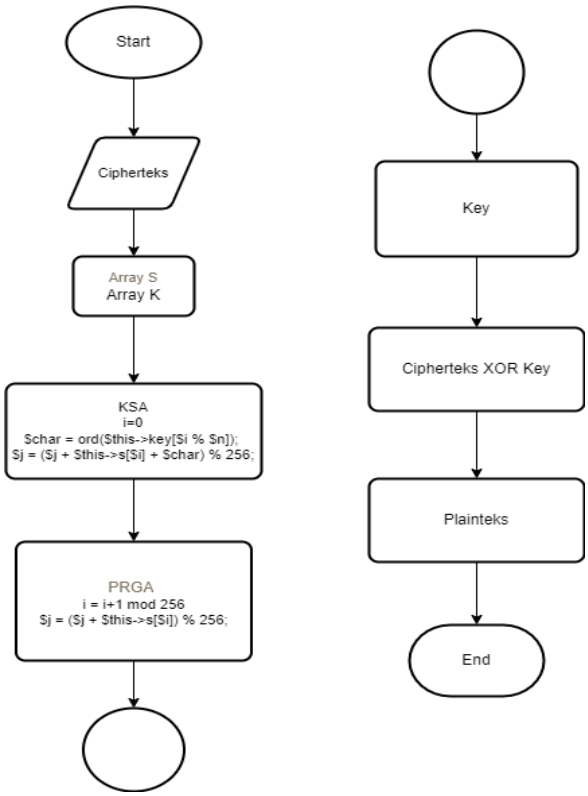
Flowchart pada gambar 4 dimulai inisialisasi inputan yang array S dan array K. Selanjutnya dilakukan proses KSA dan dilanjutkan dengan proses PRGA. Maka terbentuklah sebuah kunci. Tahap selanjutnya yaitu proses enkripsi dengan meng-XOR-kan plainteks dengan kunci yang telah terbentuk. Hasil akhirnya yaitu berupa cipherteks.



Gambar 4. *Flowchart* Enkripsi RC4

d. *Flowchart* Proses Dekripsi RC4

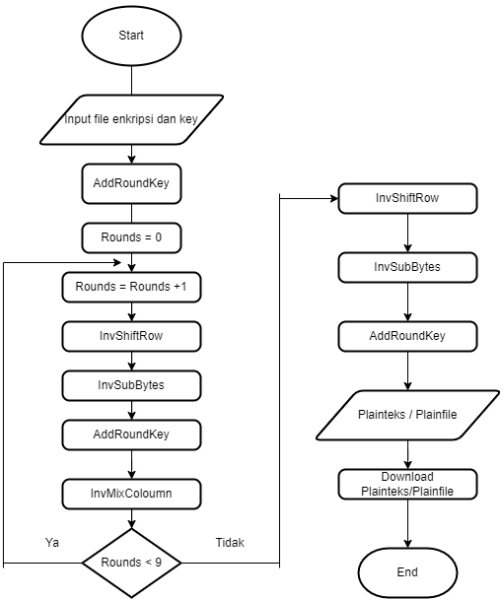
Flowchart pada gambar 5 sama halnya dengan flowchart enkripsi pada RC4, langkah dalam pembentukan kunci. Setelah kunci terbentuk, maka akan dilakukan proses dekripsi yaitu meng-XOR-kan cipherteks dengna kunci. Maka menghasilkan plainteks.



Gambar 5. *Flowchart* Dekripsi RC4

e. *Flowchart* Proses Dekripsi AES

Pada flowchart gambar 6 proses dekripsi AES 128 sistem akan memproses input-an dari pengguna berupa kunci atau key yang sama pada proses enkripsi. Pada tahap pertama proses AddRoundKey akan dilakukan transformasi Addroundkey pada tahap pertama proses enrkipsi adalah round = 0, tahap selanjutnya round +1. Kemudian melakukan putaran yang di dalamnya terjadi proses InverseShiftRows, InverseSubByte, AddRoundKey, dan InverseMixColumns. Jika >9 Round maka memasuki tahap final round yang dimana tahap proses InverseeShiftRows, InverseSubByte, dan AddRoundKey. Keluaran yang dihasilkan adalah Plainteks atau file asli dari input-an user.



Gambar 6. *Flowchart* Dekripsi AES

3.3 Tahap Pengujian

Pengujian ini menampilkan perbandingan antara proses enkripsi dan dekripsi file yang meliputi nama file, kata kunci, ukuran asli, ukuran file enkripsi, waktu enkripsi dan waktu dekripsi.

Table 3. Pengujian Perbandingan Enkripsi dan Dekripsi

No	Nama File	Kata Kunci	Ukuran File Asli	Ukuran File Enkripsi	Waktu Enkripsi	Waktu Dekripsi
1	WO Installation - ORD100632803.pdf	9f5eb3ee60132bed	464 KB	464 KB	45.18 detik	48.71 detik
2	WO Installation - ORD100635834.pdf	9f5eb3ee60132bed	464 KB	464 KB	45.22 detik	48.72 detik
3	WO Installation - ORD100645343.docx	9f5eb3ee60132bed	30 KB	30 KB	3.12 detik	3.76 detik
4	WO Installation - ORD100652470.docx	9f5eb3ee60132bed	30 KB	30 KB	2.83 detik	2.69 detik
5	WO Installation - ORD100655426.docx	9f5eb3ee60132bed	30 KB	30 KB	4.5 Detik	3.46 detik
6	Logo-budiluhur.png	9f5eb3ee60132bed	318 KB	318 KB	37.78 detik	31.26 detik
7	Budiluhur.png	9f5eb3ee60132bed	104 KB	104 KB	12.07 detik	10.84 detik

8	DataInstalasi (All).xlsx	9f5eb3ee60132bed	48 KB	48 KB	4.5 detik	4 detik
9	WO Installation - ORD100645311.pdf	9f5eb3ee60132bed	464 KB	464 KB	41.49 detik	42.13 detik
10	excel-contoh.xlsx	9f5eb3ee60132bed	184 KB	184 KB	17.52 detik	17.38 detik

4. KESIMPULAN

a. Sistem kriptografi file menggunakan bahasa pendukung pemrograman PHP yang telah dirancang dan diimplementasikan ini dapat mengenkripsi dan mendekripsi file-file dokumen yang memiliki ekstensi .docx,.pdf, .xlsx, pptx serta file-file gambar yang ber-ekstensi jpg dan png.

b. Hasil implementasi aplikasi kriptografi yang dibuat menggunakan algoritma Advanced Encryption Standart (AES) dan Rivest Code4 (RC4) saat proses enkripsi dan dekripsi data file yang diterapkan pada internal program berhasil mengkonversi file, dokumen maupun gambar foto menjadi matriks hexadecimal 4x4 yang disebut state sehingga keamanan file data dapat terjaga privasinya dan hanya pengguna Admin sistem sendiri yang dapat membuka kunci (key) pada data tersebut. Sedangkan Algoritma RC4 yang diterapkan lebih berperan sebagai salah satu jenis stream chiper, dimana unit dan input data dapat di proses pada satu saat.

c. Untuk pengujian waktu komputasi perlu dikembangkan kembali dengan analisa pengujian menggunakan *software* QoS (*Quality of Service*) untuk dapat melihat parameter kualitas jaringan yang digunakan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak pihak yang telah membantu menyelesaikan penelitian ini hingga terciptanya jurnal SENAFTI. Khususnya kepada Bpk. Rizky Pradana, S.Kom., M.Kom. selaku pembimbing yang telah membimbing saya dari awal penelitian hingga pembuatan jurnal SENAFTI.

DAFTAR PUSTAKA

[1] Rangkuti, A. Z. F., & Fahmi, H., "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, vol. 3, no. 2, pp. 170–175, 2020.

[2] Permana, A. A., & Nurnaningsih, D., "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES)," *Jurnal Teknik Informatika*, vol. 11, no. 2, pp. 177–186, 2018.

[3] Mandarani, P., & Gusman, R., "Rancang Bangun Sistem Pengelolaan Data Administrasi Perusahaan Menggunakan PHP Dan MYSQL (Studi Kasus: PT. Gapura Nirwana Agung Consultant)," *Jurnal TEKNOIF*, vol. *7*, no. 2, pp. 80–88, 2019.

[4] Suharya, Y., & Widia, H., "Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay," *Jurnal Informatika (Computing)*, vol. 07, no. 01, pp. 20–29, 2020.

[5] Suprianto, & Riswaya, A. R., "Sistem Pengkodean Data Pada File Teks Untuk Keamanan Informasi Dengan Menggunakan Metode Skipjack," *Jurnal Computech & Bisnis*, vol. 12, no. 1, pp 59–72, 2018.

[6] Widyawan, D., & Imelda. Pengamanan File Menggunakan Kriptografi Dengan Metode AES -128 Berbasis Web Di Komite. *SKANIKA*, Vol 4(1),Pp 15–22, 2021.

[7] Kirman, "Implementasi Algoritma RC4 Untuk Proteksi File MP3," *Pseudocode*, vol. *5*, no. 1, pp 80–86, 2018.

[8] S. Sutejo, "Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien," *INTECOMS: Journal of Information Technology and Computer Science*, vol. 4, no.1, pp. 104–114, 2021.

[9] Handayani, N., & Suprapto, D, "Rancang Bangun Sistem Informasi Kepegawaian Cuti Karyawan Di PT. Colorpark Indonesia Tbk Berbasis Web," *Jurnal Teknik Informatika (JIKA)*, vol. 1, no. 10, pp 33–44, 2018.

[10] Aziz, A, "Aplikasi Keamanan Data Multimedia Message Service (MMS) Pada Microsoft Office File Memanfaatkan Algoritma Rivest-Shamir Adleman (RSA) dan Blowfish Berbasis Android," *Jurnal Ilmu-Ilmu Informatika dan Manajemen STMIK*, vol. 14, no. 2, pp. 144–153, 2020.