Jurnal Sistem Informasi dan Sistem Komputer, Vol. 8, No. 2, Juli 2023
ISSN: 2715-906X (Online)
10.51717/simkom.v8i2.135

PENGAMANAN BASIS DATA DENGAN ALGORITMA TRANSPOSISI RAIL FENCE

Muhammad Fadlan[1], Evi Dianti Bintari[2], Ajeng Tasya[3]
[1]fadlan@ppkia.ac.id, [2]evidianti@ppkia.ac.id, [3]2050009@student.ppkia.ac.id
[1,3]Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
[2]Manajemen Informatika, STMIK PPKIA Tarakanita Rahmawati

Abstrak

Keamanan data pemasok merupakan aspek penting dalam era digitalisasi yang semakin maju, khususnya dalam lingkungan ekonomi dan bisnis. Salah satu solusi yang dapat digunakan untuk mengamankan data pemasok adalah melalui kriptografi. Penelitian ini bertujuan untuk menginvestigasi penggunaan salah satu algoritma dalam kriptografi, yaitu transposisi *Rail Fence* dalam mengamankan data pemasok. Penelitian ini menggunakan pendekatan eksperimental dengan menggunakan data pemasok untuk melakukan simulasi penerapan transposisi *Rail Fence*. Penelitian ini berkontribusi dalam penerapan enkripsi untuk melindungi basis data pemasok. Secara garis besar, hasil penelitian menunjukkan bahwa penggunaan metode *Rail Fence* dapat diterapkan untuk meningkatkan keamanan data pemasok dalam sebuah perusahaan. Semakin tinggi jumlah baris yang digunakan sebagai kunci dalam *Rail Fence*, maka semakin sulit bagi pihak yang tidak berwenang untuk mendekripsi data.

Kata kunci: Keamanan Data, Kriptografi, Pemasok, Rail Fence, Transposisi

Abstract

Maintaining supplier data security is an important aspect in the increasingly advanced digitalization era, especially in the business and economics environment. One solution that can be used to secure supplier data is through cryptography. This study aims to investigate the use of one of the algorithms in cryptography, namely rail fence transposition in securing supplier data. This study uses an experimental approach using random supplier data to simulate the application of a Rail Fence transposition. This research contributes to the application of encryption to protect supplier data. The results of the study indicate that the use of the Rail Fence method can be applied to improve supplier data security within a company. The higher the number of lines used as keys in Rail Fence, the more difficult it is for unauthorized parties to decrypt data.

Keywords: *Data Security, Cryptography, Supplier, Rail Fence, Transposition*

1. Pendahuluan

Data pemasok merupakan salah satu jenis data yang sangat penting untuk diamankan oleh sebuah perusahaan. Perusahaan terkadang memiliki ketergantungan pada beberapa pemasok utama untuk pasokan bahan baku atau barang yang dibutuhkan [1]. Data pemasok berisi informasi sensitif seperti nama pemasok, alamat, harga, hingga persyaratan kontrak dengan pemasok. Jika data ini jatuh ke tangan yang salah, dapat menyebabkan masalah seperti persaingan yang tidak sehat atau kehilangan keuntungan [2]. Oleh karena itu, penting bagi perusahaan untuk menjaga kerahasiaan maupun keamanan data pemasok agar dapat menghindari risiko yang merugikan perusahaan.

Data pemasok adalah informasi penting yang harus dijaga kerahasiaannya agar tidak disalahgunakan oleh pihak-pihak yang tidak berwenang. Data pemasok yang tidak dijaga keamanannya dapat menjadi sasaran serangan siber dan dapat menyebabkan kerugian yang signifikan, baik bagi organisasi maupun pelanggan [3]. Oleh karena itu, perlindungan keamanan data pemasok menjadi prioritas bagi organisasi yang memproses data pemasok. Saat ini, banyak perusahaan masih menggunakan sistem keamanan tradisional seperti penggunaan password atau enkripsi sederhana dalam mengamankan data pemasok. Namun, sistem keamanan ini rentan terhadap serangan dari pihak yang tidak bertanggung jawab.

Salah satu metode yang sering digunakan dalam meningkatkan keamanan data pemasok adalah dengan menggunakan Kriptografi. Kriptografi merupakan ilmu dan seni dalam menjaga keamanan

Jurnal Sistem Informasi dan Sistem Komputer, Vol. 8, No. 2, Juli 2023
ISSN: 2715-906X (Online)
10.51717/simkom.v8i2.135

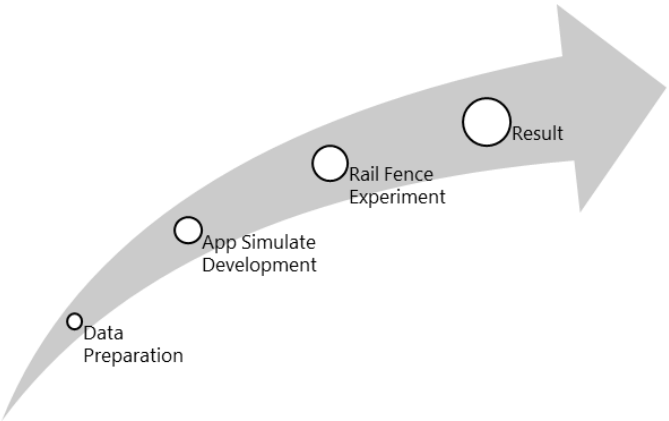
informasi melalui teknik-teknik pengkodean dan penyandian data [4]. Dalam era digital yang terus berkembang, keamanan informasi menjadi semakin penting. Kriptografi memiliki peran sentral dalam menjaga keamanan informasi di era digital yang terus berkembang dan dapat memberikan kontribusi yang signifikan dalam menghadapi tantangan keamanan yang semakin kompleks [5]–[7]. Penelitian ini bertujuan untuk menerapkan konsep kriptografi untuk melindungi data pemasok. Dengan memperkuat keamanan data pemasok, diharapkan perusahaan dapat menjaga reputasi dan memperkuat kepercayaan pelanggan terhadap setiap layanan perusahaan.

Terdapat beragam jenis algoritma dalam kriptografi, salah satunya adalah algoritma transposisi *Rail Fence* yang termasuk dalam jenis algoritma yang menerapkan prinsip dasar teknik transposisi atau mengubah susunan karakter dalam sebuah kata. *Rail Fence* merupakan salah satu teknik enkripsi yang relatif sederhana namun cukup efektif dalam mengamankan data [8], [9]. Beberapa penelitian telah dilakukan dengan menerapkan transposisi *Rail Fence*, diantaranya penelitian yang dilakukan oleh Purba & Puspasari (2020) yang membahas tentang penerapan algoritma *Rail Fence* dalam menghasilkan pesan rahasia di platform Android [10]. Penelitian yang dilakukan oleh Simamora, dkk (2022) memberikan wawasan tentang implementasi algoritma *Rail Fence* dan XOR dalam keamanan file PDF di platform Android. Aplikasi ini dapat digunakan sebagai solusi praktis untuk melindungi kerahasiaan dan integritas file PDF di perangkat Android [11]. Penelitian yang dilakukan oleh Dinata (2021) memberikan pemahaman tentang penerapan algoritma transposisi *Rail Fence* pada data rekam medis dan menjelaskan manfaatnya dalam meningkatkan keamanan data [12].

Dalam penelitian ini, *Rail Fence Cipher* digunakan sebagai solusi keamanan untuk mengamankan data pemasok pada perusahaan. Dalam penelitian ini, *Rail Fence Cipher* diimplementasikan pada data pemasok perusahaan dengan tujuan untuk memastikan keamanan data tersebut dan mencegah akses tidak sah dari pihak-pihak yang tidak berwenang. Penelitian ini diharapkan dapat memberikan kontribusi positif dalam pengembangan sistem keamanan data pada perusahaan. Dengan mengimplementasikan algoritma *Rail Fence*, perusahaan dapat memastikan bahwa data pemasok aman dari akses yang tidak sah dan kerahasiaannya dapat terjaga dengan baik.

2. Metode

Untuk menunjang proses penelitian dalam rangka mencapai tujuan dari penelitian ini, maka dibutuhkan sebuah urutan atau tahapan penelitian yang disusun dengan sistematis mulai dari tahap awal hingga tahap akhir. Namun, sebelum masuk kedalam tahapan penelitian yang utama terlebih dahulu juga telah dilakukan studi literatur terdapat berbagai referensi terkait dengan penelitian yang dilakukan yaitu mengenai penerapan *Rail Fence* dalam mengamankan basis data. Tahapan penelitian utama lebih lanjut dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Pada Gambar 1 dapat dilihat bahwa terdapat empat tahapan pertama dari penelitian ini, yaitu *Data Preparation, App Simulate Development, Rail Fence Experiment*, dan *Result.* Tahap pertama adalah *Data Preparation,* dalam tahap ini akan disiapkan data yang akan digunakan untuk melakukan eksperimen

Jurnal Sistem Informasi dan Sistem Komputer, Vol. 8, No. 2, Juli 2023
ISSN: 2715-906X (Online)
10.51717/simkom.v8i2.135

dalam penelitian ini (tahap ketiga). Adapun data yang disiapkan adalah basis data pemasok yang dalam penelitian ini hanya dibatasi pada kode pemasok, nama pemasok dan alamat pemasok.

Berikutnya adalah tahapan pengembangan aplikasi *(App Simulate Development)* untuk melakukan simulasi penerapan *Rail Fence* dalam mengamankan basis data pemasok. Dalam penelitian ini aplikasi sederhana berbasis visual akan dirancang menggunakan *Visual Studio 2012*. Tahapan ketiga yaitu melakukan eksperimen untuk mengamankan data pemasok dengan menerapkan algoritma transposisi *Rail Fence*.

Algoritma transposisi *Rail Fence* yang termasuk dalam jenis algoritma yang menerapkan prinsip dasar teknik transposisi atau mengubah susunan karakter dalam sebuah kata. Algoritma ini melibatkan pengaturan ulang karakter-karakter data dalam pola *zigzag*. Metode ini digunakan untuk mengacak dan menyusun kembali karakter-karakter data rekam medis sehingga sulit untuk dibaca oleh pihak yang tidak berwenang [9], [12]. Secara sederhana terdapat dua urutan proses dalam algoritma ini, yaitu:

a. Teks asli *(plaintext)* disusun ke bawah secara diagonal pada rel yang berurutan hingga rel bawah dan kemudian disusun bergerak ke atas dengan pola yang sama hingga rel paling atas, pola ini diulang hingga setiap karakter teks asli ditulis pada rel.
b. Setelah mengatur karakter dengan cara ini, karakter dibaca dari kiri ke kanan dari setiap rel satu per satu, dimulai dari rel paling atas.

Tahap terakhir dari Gambar 1 adalah mendapatkan hasil analisis dan melakukan penarikan kesimpulan terhadap penelitian yang telah dilakukan.

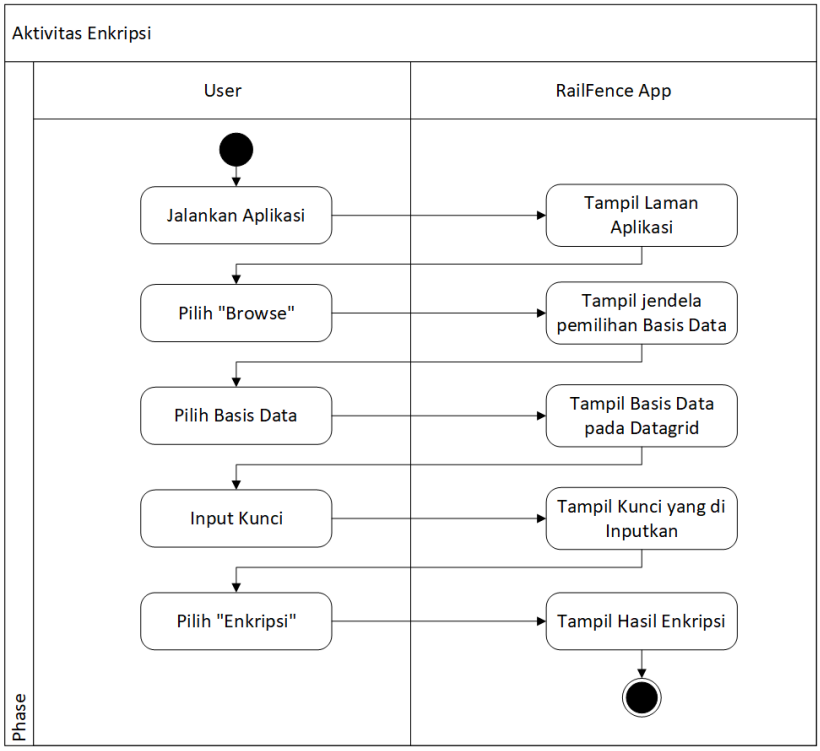
3. Hasil dan Pembahasan

Hasil penelitian ini berfokus pada penerapan algoritma *Rail Fence* dalam mengamankan basis data pemasok. Untuk mempermudah proses eksperimen dikembangkan sebuah aplikasi untuk melakukan simulasi pengamanan basis data pemasok tersebut. Dalam penelitian ini perancangan aplikasi simulasi pengamanan data hanya untuk satu pengguna saja dan dikembangkan menggunakan *Microsoft Visual Studio 2012*. Adapun spesifikasi kebutuhan dari aplikasi tersebut antara lain:

a. Pengguna dapat melakukan pemanggilan / *load* basis data dalam aplikasi.
b. Pengguna dapat memasukkan kunci untuk melakukan pengamanan basis data.
c. Pengguna dapat melakukan proses enkripsi data.
d. Pengguna dapat melakukan proses dekripsi data.

Berikutnya agar alur kerja atau aktivitas dibutuhkan agar pemanfaatan aplikasi simulasi menjadi lebih terarah, adapun penggambaran alur kerja dan urutan aktivitas dari suatu proses dalam aplikasi yang dirancang dapat dilihat pada Gambar 2.

Jurnal Sistem Informasi dan Sistem Komputer, Vol. 8, No. 2, Juli 2023
ISSN: 2715-906X (Online)
10.51717/simkom.v8i2.135



Gambar 2. Alur Aktivitas

Alur aktitivas yang terdapat pada Gambar 2 menunjukan tahapan kerja aktivitas proses enkripsi yang dapat dilakukan dalam aplikasi simulasi yang dirancang, mulai dari tahap awal menjalankan aplikasi, pemilihan basis data, memasukkan kunci, hingga melakukan proses enkripsi. Selanjutnya, untuk proses dekripsi memiliki kesamaan aktivitas dengan proses enkripsi namun yang beda hanyalah pada aktivitas terakhir dari *user* dimana yang dipilih adalah "Pilih Dekripsi" bukan "Pilih Enkripsi".

Dalam penelitian ini algoritma *Rail Fence* akan diterapkan dalam mengamankan basis data pemasok. Adapun basis data pemasok dalam penelitian ini hanya terbatas pada kode pemasok, nama dan alamat pemasok. Tiap-tiap *field* tersebut akan dienkripsi menggunakan algoritma *Rail Fence* menjadi bentuk tersandi / teracak. Dalam algoritma *Rail Fence* yang terpenting adalah tahapan-tahapan dalam pengerjaannya bukan terletak pada sulitnya persamaan / rumus yang digunakan. Berikut adalah beberapa tahapan utama dalam algoritma *Rail Fence* yang digunakan penelitian ini:

a. Siapkan teks asli *(plaintext)* dan kunci *(key).*
b. Teks asli *(plaintext)* disusun ke bawah secara diagonal pada rel / baris yang berurutan hingga rel bawah dan kemudian disusun bergerak ke atas dengan pola yang sama hingga rel paling atas, pola ini diulang hingga setiap karakter teks asli ditulis pada rel.
c. Setelah mengatur karakter dengan cara ini, karakter dibaca dari kiri ke kanan dari setiap rel / baris satu per satu, dimulai dari rel / baris paling atas.

Sebagai contoh sebuah plaintext "Jurnal SISKOM" dan kunci = 4, maka akan terbentuk pola pagar imajiner seperti yang dapat terlihat pada Gambar 3.

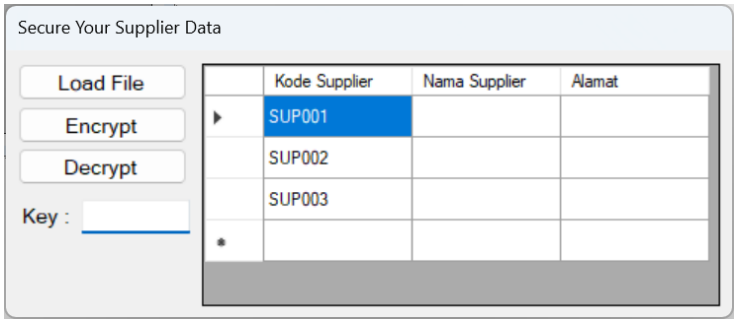
Baris Kunci	**Karakter Plaintext**												
1	J						_						M
2		u				l		S				O	
3			r		a				I		K		
4				n						S			

Gambar 3. Pola Zigzag – Pagar Imajiner

Jurnal Sistem Informasi dan Sistem Komputer, Vol. 8, No. 2, Juli 2023
ISSN: 2715-906X (Online)
10.51717/simkom.v8i2.135

Berdasarkan Gambar 3 bagian baris kunci menunjukkan jumlah baris kunci yang telah ditentukan yaitu 4, sehingga pola zigzag turun naik dalam pagar *imajiner* akan dibuat sebanyak 4 baris ke bawah kemudian balik kembali naik ke baris pertama. Cara seperti ini terus dilakukan hingga semua karakter *plaintext* telah masuk dalam pola tersebut. Berikutnya, *ciphertext* didapatkan dengan mengambil tiap-tiap karakter yang ada didalam pola dengan dimulai dari baris kunci pertama = *J M*, baris kunci kedua = *ulSO*, baris kunci ketiga = *raIK*, hingga baris kunci keempat = *nS*. Adapun hasil *ciphertext* akhir yang terbentuk adalah penggabungan karakter dari tiap-tiap baris tersebut = "*J MulSOraIKnS"*.

Selanjutnya, hasil pengembangan aplikasi sederhana simulasi untuk pemanfaatan algoritma *Rail Fence* dalam mengamankan basis data pemasok dapat dilihat pada Gambar 4.



Gambar 4. Form Simulasi

Pada Gambar 4 memberikan gambaran terkait dengan hasil aplikasi yang telah dikembangkan untuk melakukan simulasi proses pengamanan basis data dengan menerapkan algoritma *Rail Fence*. Pada Gambar 4 tersebut terdapat beberapa komponen yang digunakan, antara lain *button*, *textbox* dan *datagridview*. Lebih lanjut terkait dengan penjelasan dari komponen-komponen tersebut dapat dilihat pada Tabel 1.

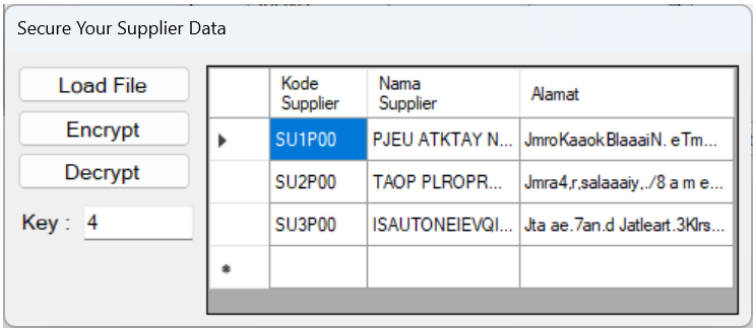
Tabel 1. Komponen Aplikasi

Jenis Komponen	**Nama Komponen**	**Fungsi**
Button	LoadFile	Memanggil basis data dan memasukkannya ke dalam datagridview
	Encypt	Melakukan proses enkripsi data
	Decrypt	Melakukan proses dekripsi data
Textbox	tkey	Inputan kunci yang digunakan
Datagridview	dgv1	Menampilkan data dari basis data

Berdasarkan Gambar 4 dan Tabel 1, maka terdapat beberapa alur atau tahapan kerja dari aplikasi simulasi yang telah dikembangkan, antara lain:

a. Memanggil / load basis data yang akan dienkripsi maupun didekripsi menggunakan *Button Load File*.
b. Memasukkan kunci yang akan digunakan untuk proses enkripsi maupun dekripsi.
c. Melakukan proses enkripsi maupun dekripsi menggunakan button *Encrypt* atau *Decrypt.*
d. Hasil enkripsi maupun dekripsi akan terlihat pada Datagridview, seperti yang dapat dilihat pada Gambar 5 dan Gambar 6.

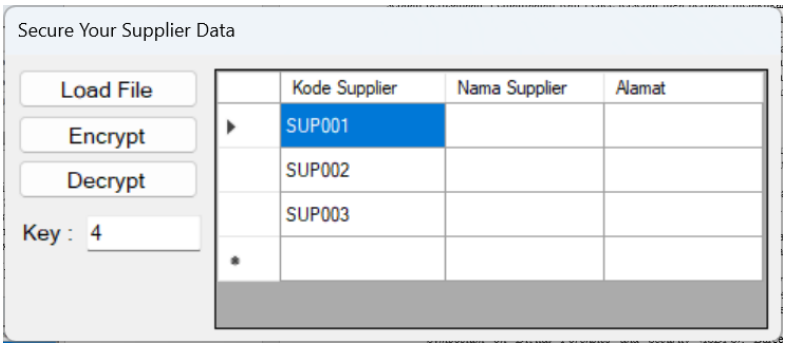
Jurnal Sistem Informasi dan Sistem Komputer, Vol. 8, No. 2, Juli 2023
ISSN: 2715-906X (Online)
10.51717/simkom.v8i2.135



Gambar 5. Ilustrasi Hasil Enkripsi

Pada Gambar 5 dapat dilihat hasil dari proses enkripsi menghasilkan data yang teracak pada datagridview, misalnya pada Kode Supplier plaintext awalnya adalah "SUP001" setelah di enkripsi menjadi ciphertext "SU1P00", begitu juga untuk data lainnya seperti nama supplier dan alamat.

Untuk Gambar 6 dapat dilihat hasil dari proses dekripsi yang menghasilkan kembali data yang telah teracak ke dalam bentuk semula, misalnya Kode Supplier ciphertext awalnya adalah "SU1P00" setelah di dekripsi akan kembali menjadi "SUP001", hal yang sama juga berlaku pada data nama dan alamat supplier (dalam ilustrasi gambar sengaja dihilangkan untuk menjaga kerahasiaan).



Gambar 6. Ilustrasi Hasil Dekripsi

Eksperimen lebih lanjut dilakukan terhadap beberapa basis data lainnya. Ringkasan hasil eksperimen tersebut dapat dilihat pada Tabel 2.

Tabel 2. Eksperimen

Kode	Enkripsi	Dekripsi	Kesimpulan
Exp001	√	√	Sesuai
Exp002	√	√	Sesuai
Exp003	√	√	Sesuai
Exp004	√	√	Sesuai
Exp005	√	√	Sesuai

Pada Tabel 2 dapat dilihat bahwa terdapat lima eksperimen yang telah dilakukan dengan perbedaan pada ukuran (*size*) basis data yang digunakan sebagai sampel. Dari lima sampel eksperimen tersebut proses enkripsi dari *DBPlain* (basis data asli) menjadi *DBCipher* (basis data tersandi) berhasil dilakukan untuk semua kode eksperimen (100%), hal ini juga berlaku pada saat proses dekripsi dari *DBCipher* (basis data tersandi) *DBPlain* (basis data asli). Berdasarkan hasil eksperimen ini disimpulkan bahwa algoritma *Rail Fence* dapat dimanfaatkan dalam melakukan pengamanan terhadap basis data pemasok dalam sebuah perusahaan. Adapun implikasi dari penelitian ini adalah pemanfaatan algoritma *Rail Fence Cipher* memungkinkan untuk diterapkan terhadap basis data lainnya yang sejenis dengan basis data pemasok.

4. Kesimpulan dan Saran

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa pemanfaatan ilmu kriptografi melalui transposisi *Rail Fence* dapat dilakukan untuk mengamankan basis data pemasok dalam sebuah perusahaan. Pemanfaatan *Rail Fence* tersebut juga berhasil melakukan proses enkripsi basis data pemasok menjadi teks teracak dan mengembalikannya dalam bentuk semula melalui proses dekripsi. Implikasi dari penelitian ini adalah bahwa perusahaan dapat mempertimbangkan penggunaan metode *Rail Fence* sebagai salah satu langkah untuk meningkatkan keamanan data pemasok. Meskipun *Rail Fence* dapat memperkuat keamanan data pemasok, tidak menutup kemungkinan tetap ada celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengembangkan teknik enkripsi yang lebih kuat dan lebih aman dalam melindungi data pemasok.

Daftar Pustaka

[1] N. Putra, D. R. Habibie, and I. F. Ika Fitri Handayani, "Sistem Pendukung Keputusan Pemilihan Supplier Pada TB.Nameene Dengan Metode Simple Additive Weighting (SAW)," *Jurnal Sistem Informasi dan Manajemen*, vol. 8, no. 1, pp. 45–51, 2020.

[2] R. R. Saputra, E. Setiawan, A. Ambarwati, and J. S. Informasi, "Manajemen Risiko Teknologi Informasi Menggunakan Metode OCTAVE Allegro pada PT. Hakiki Donarta Surabaya," *Jurnal Sains, Teknologi dan Industri*, vol. 17, no. 1, pp. 1–10, 2019.

[3] E. Monica Setiawan, "Implikasi Perkembangan Teknologi Informasi Siklus Transaksi Bisnis Pada Keamanan Data Dan Sistem Pengendalian Internal Pada Perusahaan Dagang," *Jurnal Ilmu Ekonomi, Sosial dan Pendidikan*, vol. 1, no. 3, pp. 25–37, 2021.

[4] F. Maqsood, M. Ahmed, M. Mumtaz Ali, and M. Ali Shah, "Cryptography: A Comparative Analysis for Modern Techniques," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 442–448, 2017, [Online]. Available: www.ijacsa.thesai.org

[5] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, 2019. doi: 10.1109/ISDFS.2019.8757514.

[6] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, Jun. 2019. doi: 10.1088/1757-899X/518/5/052003.

[7] D. Kumar Sharma, N. Chidananda Singh, D. A. Noola, A. Nirmal Doss, and J. Sivakumar, "A review on various cryptographic techniques & algorithms," in *Materials Today: Proceedings*, Elsevier Ltd, 2021, pp. 104–109. doi: 10.1016/j.matpr.2021.04.583.

[8] K. Nahar* and P. Chakraborty*, "Improved Approach of Rail Fence for Enhancing Security," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 9, pp. 583–585, Jul. 2020, doi: 10.35940/ijitee.I7637.079920.

[9] S. Godara, S. Kundu, and R. Kaler, "An Improved Algorithmic Implementation of Rail Fence Cipher," *International Journal of Future Generation Communication and Networking*, vol. 11, no. 2, pp. 23–32, Mar. 2018, doi: 10.14257/ijfgcn.2018.11.2.03.

[10] D. Febriani Purba and R. Puspasari, "Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android Application of Rail Fence Algorithm for Producing Secret Messages Based on Android," *Jurnal FTIK*, vol. 1, no. 1, pp. 745–756, 2020.

[11] A. Putra Simamora *et al.*, "Perancangan Aplikasi Keamanan File PDF Dengan Algoritma Rail Fence + Xor Berbasis Android Designing PDF File Security Application with Android Based Rail Fence + Xor Algorithm," *Jurnal VOI (Voice Of Informatics)*, vol. 11, no. 1, pp. 57–69, 2022.

[12] S. J. Dinata, "Implementasi Algoritma Penyandian Transposisi Rail Fence Pada Data Rekam Medis," 2020.