

PENERAPAN ALGORITMA RIVEST CODE 4 (RC4) UNTUK KEAMANAN FILE PADA SMPN 149 JAKARTA

Fachrul Fatahillah^{1*}, Hari Soetanto²

^{1,2}Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: ^{1*}fachrulfatahillah@gmail.com, ²hari.soetanto@budiluhur.ac.id

(* : corresponding author)

Abstrak-Penelitian ini membahas mengenai pengamanan data keuangan, soal ujian, dan nilai-nilai siswa-siswi di SMPN 149 Jakarta. Perkembangan teknologi informasi terbukti telah membantu manusia dalam berbagai aspek kehidupan terutama dalam masalah penyimpanan data. Memberikan keamanan dan kerahasiaan informasi sangat penting ketika bertukar informasi melalui jaringan komunikasi. Dengan adanya pencurian data dokumen maka aspek keamanan data dalam pertukaran informasi serta penyimpanan data dianggap sangat penting. Sebagai instansi yang bergerak di bidang pendidikan, SMPN 149 Jakarta mempunyai masalah lokal terkait data atau informasi keuangan, soal ujian dan nilai-nilai siswa-siswi yang dapat merugikan SMPN tersebut. Terkait dengan permasalahan yang ada dengan pentingnya pengamanan data atau informasi, maka untuk melindungi data atau informasi tersebut, perlu diterapkan teknologi terkini untuk mengamankan data. Teknik mengamankan data yang bisa digunakan untuk mengenkripsi serta mendekripsi data adalah kriptografi. Metode yang digunakan adalah algoritma rivest code 4 (RC4) yang diimplementasikan untuk pengamanan data keuangan, soal ujian, dan nilai-nilai siswa-siswi SMPN 149 Jakarta. Dengan adanya aplikasi pengamanan file pada SMPN 149 Jakarta ini, dapat mengurangi kemungkinan terjadinya kebocoran data. Aplikasi ini dibuat berbasis web menggunakan bahasa pemrograman PHP dan database server MySQL. Dari hasil percobaan menyimpulkan bahwa aplikasi ini dapat berhasil mengamankan file sehingga tidak bisa dibaca. Aplikasi ini juga dapat memulihkan atau mengembalikan file terenkripsi seperti semula.

Kata Kunci: kriptografi, algoritma rivest code 4, SMPN 149 jakarta

THE APPLICATION OF RIVEST CODE (RC4) ALGORITHM FOR SECURING FILES ON SMPN 149 JAKARTA

Abstract-This study discusses the security of financial data, exam questions, and the values of students at SMPN 149 Jakarta. The development of information technology has been proven to have helped humans in various aspects of life, especially in the problem of data storage. Providing security and confidentiality of information is very important when exchanging information through the communication network. With the theft of document data, data security aspects in the exchange of information and data storage are considered very important. As an agency engaged in education, SMPN 149 Jakarta has local problems related to financial data or information, exam questions and the values of students who can harm the junior high school. Related to existing problems with the importance of securing data or information, then to? Protect the data or information, it is necessary to apply the latest technology to secure data. The technique of securing data that can be used to encrypt and decrypted data is cryptography. The method used is the Rivest Code 4 (RC4) algorithm which is implemented to secure financial data, exam questions, and the values of students of SMPN 149 Jakarta. With the file security application at SMPN 149 Jakarta, it can reduce the possibility of data leakage. This application is made web-based using the PHP programming language and MySQL database server. From the experimental results concluded that this application can successfully secure files so that it cannot be read. This application can also restore or restore the encrypted file as before.

Keywords: cryptography, rivest code 4 algorithm, SMPN 149 jakarta

1. PENDAHULUAN

Pada era teknologi informasi saat ini, keamanan saat menyimpan dan mengirimkan data dan informasi sangatlah penting dan tidak bisa diabaikan [1]. Berbagi data dan informasi menjadi lebih mudah, baik melalui media fisik maupun tidak. Dengan berkembangnya teknologi informasi, seringkali data menjadi sangat berharga dan tidak semua orang boleh mengetahuinya [2]. Oleh karena itu, keamanan data yang tersimpan sangat penting untuk melindungi dari berbagai ancaman berupa akses, modifikasi, dan penghapusan data oleh pihak ketiga yang tidak bertanggung jawab. [3].

Banyak teknik yang bisa digunakan untuk melindungi data-data tersebut diantaranya adalah kriptografi [4], [5] teknik kriptografi yang dibutuhkan masa kini tetap harus mengikuti dirinya terhadap menyebarnya penggunaan komputer digital pada masa kini. Kriptografi merupakan ilmu dalam menjaga keamanan data dengan

mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data saat proses pengiriman data dokumen dengan menggunakan suatu metode algoritma untuk proses enkripsi dan dekripsinya [6], [7] dalam kriptografi RC4 Proses enkripsi dan dekripsi mempunyai proses yang sama sehingga hanya ada satu kunci untuk menjalankan kedua proses tersebut. RC4 mempunyai sebuah S – Box dan key dalam bentuk array 256 byte yaitu : dari S0, sampai S255 yang berisi bilangan 0 - 255, dari K0, sampai K255 [8].

Dalam Kriptografi meliputi penyandian (*encryption*), proses penyamaran data dari *plaintext* (data asli) menjadi *ciphertext* (data terenkripsi), dan dekripsi (*decryption*), proses mengubah *ciphertext* kembali menjadi *plaintext* disebut Enkripsi diandalkan untuk mengatasi masalah keamanan data atau informasi untuk transmisi, penyimpanan, dan tujuan lain untuk menjaga kerahasiaan data atau informasi. [9].

Berdasarkan uraian permasalahan yang dihadapi SMPN 149 Jakarta, penelitian ini akan membuat aplikasi web yang melindungi isi data dokumen dan meminimalisir penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Dengan menggunakan prosedur algoritma RC4, tingkat keamanan yang cukup tinggi diharapkan dapat menjaga keamanan dan kerahasiaan data atau informasi penting tersebut.

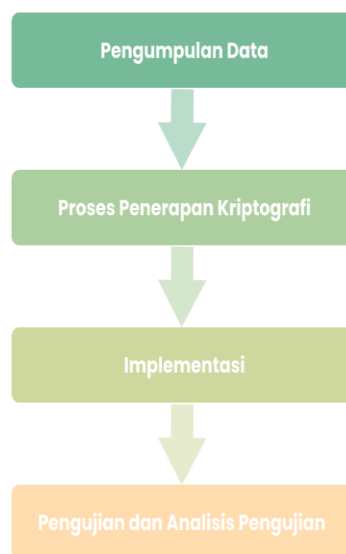
2. METODE PENELITIAN

2.1 Data Penelitian

Data yang akan digunakan dalam penelitian ini adalah soal ujian dan latihan soal siswa/siswi yang dimana data berupa dokumen SMPN 149 Jakarta. Sumber data diambil secara langsung oleh peneliti kepada sumbernya tanpa ada perantara dengan cara menggali sumber asli secara langsung melalui responden. Data yang didapatkan sebagai proses uji coba pengamanan file menggunakan metode Rivest Code 4 (RC4).

2.2 Penerapan Metode

Metode penelitian digunakan sebagai pedoman dalam pelaksanaan penelitian agar hasil yang dicapai tidak menyimpang dari tujuan yang telah dilakukan sebelumnya. Tahapan penelitian pada penelitian ini dapat dilihat pada gambar 1. berikut :



Gambar 1. Penerapan Metode

a. Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data yang diperoleh dari hasil wawancara dan observasi yang dilakukan dengan pihak sekolah. Hal ini dilakukan untuk mendapatkan informasi yang dibutuhkan dalam pembuatan aplikasi.

b. Proses Penerapan Kriptografi

Setelah melakukan pengumpulan data, maka dilakukan proses penerapan proses kriptografi menjelaskan tahap menerapkan metode RC4 pada proses pengamanan *file*. Pada tahapan ini dilakukan :

- 1) Menentukan *file* yang akan digunakan untuk proses enkripsi dan dekripsi.
- 2) Proses enkripsi *file*, yaitu proses mengubah *file plaintext* ke bentuk *file ciphertext*.
- 3) Proses dekripsi menggunakan kunci dekripsi yang sama dengan kunci enkripsi, yaitu proses mengubah menjadi *file* yang dapat terbaca kembali (*plaintext*).

c. Implementasi

Setelah melakukan proses penerapan kriptografi maka dilakukan Implementasi sistem. Pada proses implementasi ini dilakukan pembuatan modul-modul yang telah dirancang dalam tahap perancangan ke dalam bahasa pemrograman tertentu. Perangkat lunak yang dilakukan untuk pengamanan dokumen menggunakan bahasa pemrograman PHP dan menggunakan MySQL [10].

d. Pengujian dan Analisis Pengujian

Pada tahap terakhir pada pengujian dan analisis hasil pengujian yaitu dilakukan dengan black box testing, yaitu dengan menguji satu persatu fitur yang sudah dibuat.

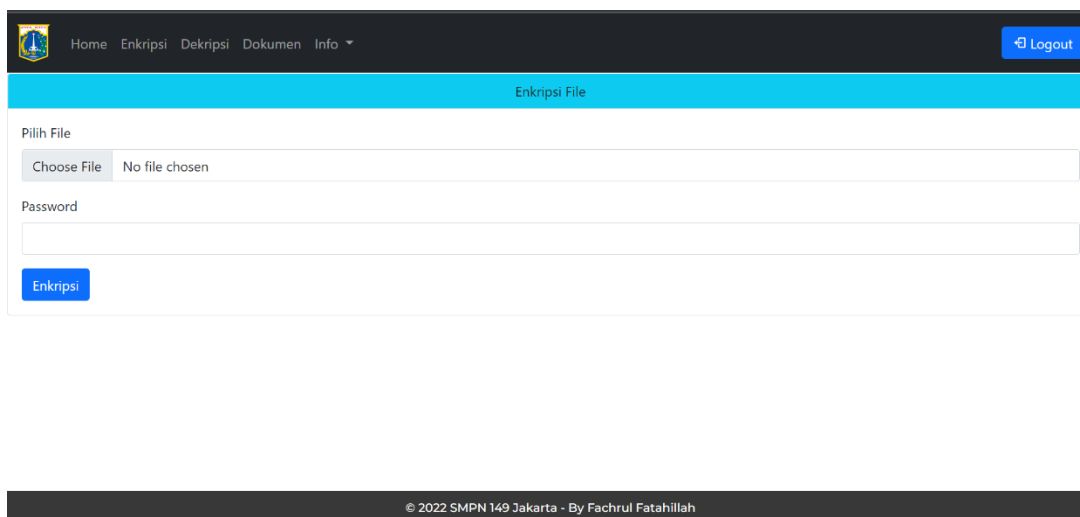
3. HASIL DAN PEMBAHASAN

3.1 Implementasi

Berdasarkan metode yang diusulkan pada bab sebelumnya yaitu menggunakan algoritma kriptografi Rivest Code (RC4) untuk mengamankan *file*. Implementasi metode tersebut akan dijelaskan pada tahapan berdasarkan inputan atau contoh menggunakan enkripsi dan dekripsi di aplikasi tersebut.

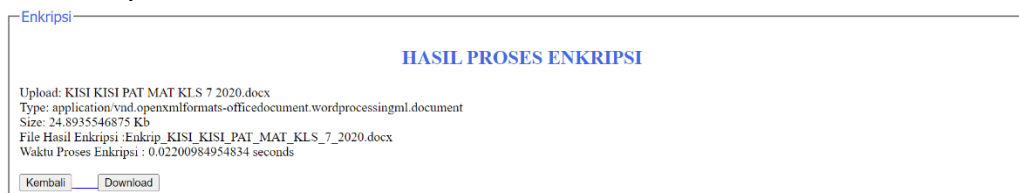
a. Enkripsi *File*

Enkripsi *file* dengan cara mengisi form yang sudah disediakan dan memilih *file* yang akan dienkrpsi dan memasukan password minimal 8 karakter. Dapat dilihat pada Gambar 2 dibawah ini :



Gambar 2. Menu Form Enkripsi

Kemudian setelah admin atau pegawai berhasil mengenkripsi, maka data yang di input akan masuk ke dalam database, *file* yang di pilih saat inputan form akan masuk ke folder *upload* dan *file* akan mengganti nama depan *file* secara otomatis yaitu Enkrip_namafilename. Berikut dibawah ini Gambar 3 tampilan layar jika *file* sudah berhasil terenkripsi :



Gambar 3. Hasil Proses Enkripsi

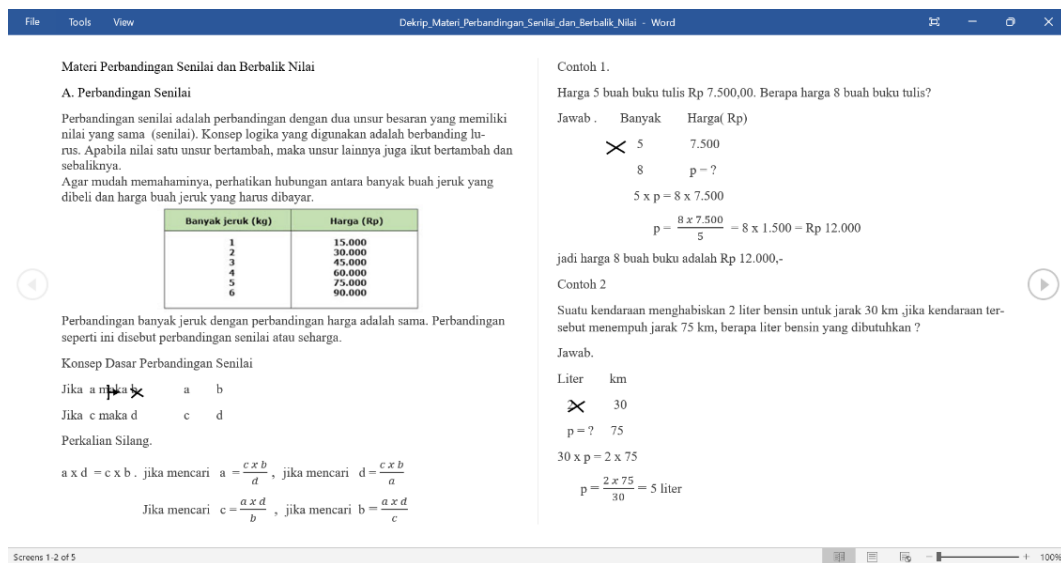
File sebelum Dienkrpsi dan sesudah di enkripsi dapat dilihat pada Gambar 4 dan Gambar 5 di bawah ini :

Kemudian setelah admin atau pegawai berhasil mendekripsi, maka akan muncul hasil *file* yang telah di dekripsi. Berikut Gambar 7 hasil proses dekripsi *file* :



Gambar 7. Hasil Proses Dekripsi

Hasil dekripsi bisa dilihat pada Gambar 8 dibawah ini :



Gambar 8. Hasil File yang Sudah Didekripsi

3.2 Pengujian

Pengujian pada aplikasi ini menggunakan pengujian blackbox dan yang akan diuji adalah data yang diberikan oleh SMPN 149 Jakarta. Pengujian dilakukan dengan 2 cara yaitu dengan pengujian Enkripsi, dekripsi dan pengujian Aplikasi.

a. Pengujian Proses Enkripsi dan Dekripsi

Pada pengujian enkripsi dan dekripsi penulis menggunakan pengujian pada waktu proses melakukan enkripsi dan dekripsi menggunakan waktu Milidetik pada suatu file yang diberikan pada tempat riset dan diinput pada aplikasi. Dapat dilihat pada Tabel 1 dan Tabel 2 di bawah ini :

Tabel 1. Pengujian Enkripsi File

No	Nama File Asli	Ukuran File Asli (kb)	Nama File Setelah dienkrpsi	Ukuran File Setelah dienkrpsi (kb)	Waktu Enkripsi (detik)
1.	KISI KISI PAT MAT KLS 7 2020.docx	24	Enkrip_KISI_KISI PAT_MAT_KLS_7_2020.docx	24	0.025
2.	Latihan Soal Jajar Genjang.docx	84	Enkrip_Latihan_Soal_Jajar_Genjang.docx	84	0.127
3.	Latihan soal Membandingkan, Penjumlahan dan	175	Enkrip_Latihan_soal_Membandingkan, Penjumlahan dan Pengurangan_Bilangan_Pecahaan.pdf	175	0.501

No	Nama File Asli	Ukuran File Asli (kb)	Nama File Setelah dienkripsi	Ukuran File Setelah dienkripsi (kb)	Waktu Enkripsi (detik)
4.	Pengurangan Bilangan Pecahaan.pdf Latihan Soal PG Diagram Venn.docx	50	Enkrip_Latihan_Soal_PG_Diagram_Venn.docx	50	0.057
5.	MATERI BENTUK ALJABAR, JUMLAH, PENGURANGAN.docx	22	Enkrip_MATERI_BENTUK_ALJABAR,_JUMLAH,_PENGURANGAN.docx	22	0.016
6.	Materi Perbandingan Senilai dan Berbalik Nilai.docx	62	Enkrip_Materi_Perbandingan_Senilai_dan_Berbalik_Nilai.docx	62	0.079
7.	RPP ONLINE MATEMATIKA SESI 10.docx	17	Enkrip_RPP_ONLINE_MATEMATIKA_SESI_10.docx	17	0.011
8.	LATIHAN SOAL HIMPUNAN.docx	17	Enkrip_LATIHAN_SOAL_HIMPUNAN.docx	17	0.013

Tabel 2. Pengujian Dekripsi File

No	Nama File Asli	Ukuran File Asli (kb)	Nama File Setelah didekripsi	Ukuran File Setelah didekripsi (kb)	Waktu Dekripsi (detik)
1.	Enkrip_KISI_KISI PAT_MAT_KLS_7_2020.docx	24	Dekrip_KISI_KISI_PAT_MAT_KLS_7_2020.docx	24	0.051
2.	Enkrip_Latihan_Soal_Jajar_Genjang.docx	84	Dekrip_Latihan_Soal_Jajar_Genjang.docx	84	0.379
3.	Enkrip_Latihan_soal_Membandingkan, Penjumlahan dan Pengurangan Bilangan Pecahaan.pdf	175	Dekrip_Latihan_soal_Membandingkan, Penjumlahan dan Pengurangan Bilangan Pecahaan.pdf	175	1.352
4.	Enkrip_Latihan_Soal_PG_Diagram_Venn.docx	50	Dekrip_Latihan_Soal_PG_Diagram_Venn.docx	50	0.149
5.	Enkrip_MATERI_BENTUK_ALJABAR, JUMLAH, PENGURANGAN.docx	22	Dekrip_MATERI_BENTUK_ALJABAR, JUMLAH, PENGURANGAN.docx	22	0.053
6.	Enkrip_Materi_Perbandingan_Senilai dan Berbalik_Nilai.docx	62	Dekrip_Materi_Perbandingan_Senilai dan Berbalik_Nilai.docx	62	0.215
7.	Enkrip_RPP_ONLINE_MATEMATIKA_SESI_10.docx	17	Dekrip_RPP_ONLINE_MATEMATIKA_SESI_10.docx	17	0.031

No	Nama File Asli	Ukuran File Asli (kb)	Nama File Setelah didekripsi	Ukuran File Setelah didekripsi (kb)	Waktu Dekripsi (detik)
8.	Enkrip_LATIHAN_SOAL_HI MPUNAN.docx	17	Dekrip_LATIHAN_S OAL_HIMPUNAN.d ocx	17	0.028

Dari pengujian diatas dapat disimpulkan bahwa pengujian pada aplikasi kriptografi yang dibuat penulis menggunakan file yang diberikan pada tempat riset dengan hasil pengujian waktu lama proses enkripsi lebih lama dari pada waktu proses dekripsi dan makin besar ukuran file maka lebih lama juga waktu enkripsi dan dekripsi.

b. Pengujian Aplikasi

Pengujian pada aplikasi ini peneliti menggunakan metode black box untuk menguji aplikasi kriptografi yang sudah dibuat. Dapat dilihat pada tabel di bawah ini :

Tabel 3. Pengujian Aplikasi

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian
1.	Admin atau pegawai mengisi form login sesuai dengan role	Tampil halaman menu home	Sesuai Harapan
2.	Admin atau pegawai memilih menu Enkripsi atau Dekripsi	Tampil halaman menu enkripsi atau dekripsi	Sesuai Harapan
3.	Pilih file kemudian masukkan password dan klik tombol enkripsi atau dekripsi untuk file yang akan dienkripsi atau didekripsi	Tampil halaman hasil proses enkripsi atau dekripsi	Sesuai Harapan
4.	Mendownload file yang sudah terenkripsi dan terdekripsi	Berhasil mendownload file	Sesuai Harapan
5.	Admin memilih menu user	Tampil halaman menu user	Sesuai Harapan
6.	Admin menambahkan user	Berhasil menambah user	Sesuai Harapan
7.	Admin menghapus pada user yang terdaftar	Berhasil menghapus user	Sesuai Harapan
8.	Admin atau pegawai memilih menu help	Tampil halaman menu help	Sesuai Harapan
9.	Admin atau pegawai memilih menu about	Tampil halaman menu about	Sesuai Harapan
10.	Admin atau pegawai menekan tombol logout	Kembali kehalaman login	Sesuai Harapan

4. KESIMPULAN

Pada aplikasi ini dapat menerapkan metode *Rivest Code 4 (RC4)* dengan baik dan dikhususkan untuk mengamankan file dalam bentuk format *.xls, *.xlsx, *.doc, *.docx, *.pdf, *.txt, dan Aplikasi yang telah dibuat terjamin keutuhan file pada saat enkripsi dan dekripsi maupun didekripsikan tanpa mengalami kerusakan atau perubahan data.

Pengembangan yang bisa dilakukan pada penelitian berikutnya diantaranya pengembangan sistem pengamanan file dengan mengenkripsi database serta menambahkan fitur-fitur lain sesuai kebutuhan dan dapat diharapkan aplikasi ini dapat dikembangkan dalam bentuk mobile dan juga dapat menggunakan 2 algoritma untuk melakukan proses enkripsi dan dekripsi agar dapat lebih aman seperti menggunakan algoritma kombinasi seperti algoritma kunci simetris dan kunci asimetris.

DAFTAR PUSTAKA

- [1] R. T. Jurnal, “Penerapan Algoritma Rivest Code 4 (Rc 4) Pada Aplikasi Kriptografi Dokumen,” *Petir*, vol. 11, no. 1, pp. 38–47, 2018.
- [2] K. Kirman, “Implementasi Algoritma Rc4 Untuk Proteksi File Mp3,” *Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018.
- [3] M. D. Wulandari *et al.*, “Aplikasi Pengamanan Database Berbasis Desktop dengan Algoritma AES-128 dan Rivest Code (RC4),” *Skatika*, vol. 1, no. 1, pp. 373–379, 2018.
- [4] A. Setiawan and T. Fatimah, “Implementasi Algoritma Kriptografi Rc4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada Pt. Trans Intra Asia,” *Skatika*, vol. 4, no. 1, pp. 66–71, 2021.
- [5] M. Diana and T. Zebua, “Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS,” *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, pp. 12–22, 2018.
- [6] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, and I. Gunawan, “Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4,” *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 114, 2020.
- [7] Andrico and M. Syafrullah, “Aplikasi enkripsi database menggunakan algoritma rc4 berbasis desktop 1,” vol. 1, no. 3, pp. 1011–1017, 2018.
- [8] L. Risnanda and N. Juliasari, “Rc4 (Rivest Code 4) Pada Database Berbasis Java,” *Skatika*, vol. 1, no. 3, pp. 1100–1107, 2018.
- [9] R. Rivaldi and S. Subandi, “Implementasi Keamanan Data Arsitektur Menggunakan Algoritma Kriptografi Dengan Metode Rivest Code (4 Rc4) Pada Pt. Naviri Indah Cemerlang,” *Skatika*, vol. 4, no. 2, pp. 63–67, 2021.
- [10] M. Sitinjak Daniel Dido Jantce TJ and J. Suwita, “Analisa Dan Perancangan Sistem Informasi Administrasi Kursus Bahasa Inggris Pada Intensive English Course Di Ciledug Tangerang,” *Ipsikom*, vol. 8, no. 1, pp. 1–19, 2020.