Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2024, VII (3): 1320 – 1326 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATABASE DENGAN MENGGUNAKAN ALGORITMA TWOFISH PADA PUSKESMAS ILIR TALO

Edy Rahmat[1],Juju Jumadi[2], Deri Lianda[3]
Universitas Dehasen, Bengkulu
e-mail: [1]edyrahmatramadhan@gmail.com

Abstract: *Security and confidentiality of data or information is one of the important aspects of data or information. The issue of security and confidentiality of computer data is something that is important in this information era, especially for Ilir Talo Health Center. Various ways are done to protect the data or information. One of them is by using cryptography with Twofish algorithm. Cryptography with a block cipher symmetric key with the length of each block is fixed at 128 bits. System implementation using PHP programming language with MySql database. The method used in this research is waterfall, this application is designed using UML (Unified Modeling Language). From the analysis and discussion, it is obtained that the encryption results produced by Twofish utilize bit manipulation techniques, permutation/ whitening boxes. The result of this research is a software application that is useful for maintaining the security of medical record databases using Twofish method. With this application, it can be one of the solutions in securing the database.*

Keywords: *security, cryptography, twofish, medical records.*

Abstrak: Keamanan dan kerahasiaan data atau informasi merupakan salah satu aspek yang penting dari suatu data atau informasi. Masalah keamanan dan kerahasiaan data komputer merupakan sesuatu yang penting dalam era informasi ini terutama bagi Puskesmas Ilir Talo. Berbagai cara pun dilakukan untuk melindungi data atau informasi tersebut. Salah satunya dengan menggunakan kriptografi dengan algoritma Twofish. kriptografi dengan kunci simetrik cipher blok dengan panjang setiap blok adalah tetap 128 bit. Implementasi sistem menggunakan bahasa pemrograman PHP dengan database MySql. Metode yang digunakan dalam penelitian ini adalah waterfall, aplikasi ini dirancang menggunakan UML (Unified Modelling Language). Dari analisa dan pembahasan diperoleh bahwa hasil enkripsi yang dihasilkan oleh Twofish memanfaatkan teknik pemanipulasian bit, kotak permutasi/pemutihan. Hasil dari penelitian ini adalah sebuah aplikasi perangkat lunak yang berguna untuk menjaga keamanan database rekam medik dengan metode Twofish. Dengan adanya aplikasi ini dapat menjadi salah satu solusi dalam pengamanan database.

Kata kunci: keamanan, kriptografi, twofish, rekam medik

PENDAHULUAN

Database digunakan untuk menyimpan data, membuka data, mengelola data-data dan mengelola informasi. Basis Data adalah suatu susunan atau kumpulan data operasional lengkap dari suatu organisasi/perusahaan yang dikelola dan simpan secara terintregasi dengan menggunakan metode tertentu menggunakan komputer sehingga mampu menyediakan informasi optimal yang diperlukan pemakainya. Kebanya kan pengelola database tidak memper dulikan masalah keamanan. Padahal keamanan dalam sebuah database sangatlah penting, sebab para pencuri informasi dapat mencuri data-data di

dalam database yang tidak memiliki keamanan. Oleh karena itu perlunya diterapkan teknik yang dapat menciptakan keamanan pada sebuah isi database.

Kriptografi salah satu dari sekian banyak cara yang bisa diterapkan pada data untu memberikan keamanan tambahan akan sangat membantu dalam mengamankan data-data pada Puskesmas Ilir Talo. Salah satu metode kriptografi yang bisa dimanfaatkan adalah metode Twofish. Algoritma Twofish adalah algoritma kriptografi simetris yang menggunakan block cipher dengan panjang 128 bit yang dibuat oleh Bruce Scheiner. Algoritma Twofish memiliki 16 ronde jaringan Feistel. Di dalam jaringan Feistel terdapat tabel substitusi, transformasi Pseudo Hadamard, rotasi terhadap nilai-nilai bit. Algoritma Twofish dapat menerima 3 panjang kunci yaitu 128, 192 atau 256 bit. Teks yang akan dienkripsi pertama akan diubah dulu menjadi nilai integer yang diambil dari tabel American Standard Code for Information Interchange (ASCII) sebelum dienkripsi. Dan hasil dari enkripsi akan diubah menjadi nilai heksadesimal. Implementasi berasal dari Bahasa Inggris yaitu to implement yang berarti mengimplementasikan merupakan penye di aan sarana untuk melaksanakan sesuatu yang menimbulkan dampak atau akibat itu dapat berupa Undang-Undang (UU), peraturan pemerintah, keputusan peradilan dan kebijakan yang dibuat oleh lembaga-lembaga pemerintah dalam kehidupan kenegaraan (Dewi, 2018).

Tujuan dari implementasi sebuah sistem ialah untuk menyelesaikan desain sistem yang telah disetujui, menguji serta mendokumentasikan program-program dan prosedur sistem yang diperlukan, memastikan bahwa personil yang terlibat dapat mengoperasikan sistem yang baru dan memastikan bahwa konversi sistem lama ke sistem baru dapat berjalan dengan baik dan benar (Gunawan & Kirman, 2019).

Untuk menghindari kesalahpaha man, istilah keamanan mengacu ke seluruh masalah keamanan dan istilah mekanisme proteksi mengacu ke mekanisme sistem yang digunakan untuk memproteksi atau melindungi informasi pada sistem komputer (Silalah & Sindar, 2020).

Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Kriptografi sendiri berasal dari kata "Crypto" yang berarti rahasia dan "graphy" yang berarti tulisan. Jadi, dapat dikatakan kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang yang tidak mengetahui bagaimana tulisan tersebut disembunyikan tidak akan mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut (Puspita & Wayahdi, 2018) Criptography berasal dari bahasa Yunani. Menurut bahasanya, istilah tersebut terdiri dari kata kripto dan graphia. Kripto berarti secret (rahasia) dan graphia berarti writing (tulisan) (Fauzah & Iqbal, 2021). Plaintext atau teks biasa adalah informasi atau pesan yang dikirim dalam format yang mudah dibaca atau asli (Ziliwu & Maslan, 2022).

Kegiatan perubahan isi pesan dari plaintext ke ciphertext disebut enkripsi, dan prosedur mengembalikan teks dari ciphertext ke plaintext disebut dekripsi (Ziliwu & Maslan, 2022)

Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi ciphertext, sedangkan dekripsi adalah proses yang dilakukan untuk mengubah pesan tersandi menjadi pesan yang dapat dibaca dan dimengerti (Ridho et al., 2022).

Kriptografi bertujuan untuk layanan keamanan yang memiliki beberapa aspek keamanan yang memiliki yaitu sebagai berikut (Azlin et al., 2018) :

Authentication

Layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/infor masi. Fasilitas yang berkaitan untuk

melakukan identifikasi terlebih dahulu antara pengirim dan penerima pesan.

Integrity

Keuntungan yang didapatkan dalam menggunakan teknik kriptografi yaitu menjamin bahwa pesan akan diterima dalam keadaan masih utuh dan belom mengalamai perubahan selama proses pengiriman. Layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

Kriptografi ini hanya melakukan pengacakan pada huruf A-Z, dan sangatlah tidak disarankan untuk menga mankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern (Pardede, Manurung, & Filina, 2017).

Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern (Manaor & Pardede, 2019).

Algoritma Twofish merupakan algoritma yang diciptakan oleh Bruce Scheiner, sebelumnya beliau menciptakan Algoritma Blowfish. Algoritma Twofish merupakan salah satu kandidat AES disebabkan Twofish memenuhi semua kriteria NIST, yaitu 128-bit block, 192 bit dan 256 bit key atau kata kunci (Awal, Nurkifli, & Padilah, 2022). Perancangan Twofish dilakukan dengan memperhati kan kriteria-kriteria yang diajukan National Institute of tandards and Technology (NIST) untuk kompetisi Advanced Encryption Standard (AES) dan menjadi salah satu finalis. Twofish adalah block cipher yang berukuran 128 bit yang dapat menerima kunci dengan panjang mencapai 256 bit. Twofish merupakan algoritma yang beroperasi dalam mode blok (Imelda & Prawira, 2018)

Website adalah suatu kumpulan-kumpulan halaman yang menampilkan berbagai macam informasi teks, data, gambar, video maupun gabungan dari semuanya bersifat statis dan dinamis (Nursyanti, Alamsyah, & Perdana, 2019)
Website awalnya merupakan suatu layan an sajian informasi yang menggunakan konsep hiperlink yang memudahkan surfer (sebutan bagi pemakai komputer yang melakukan penyelusuran informasi di internet) untuk mendapatkan informasi dengan cukup mengklik suatu link berupa teks atau gambar maka informasi dari teks atau gambar akan ditampilkan secara lebih terperinci (Nurmalasari, Anna, & Arissusand, 2019). Sedangkan web browser menggambarkan bahwa web browser digunakan untuk menampilkan hasil website yang telah dibuat. Web browser yang paling sering digunakan, di antaranya Mozilla Firefox, Google Chrome, Internet Explorer, Opera, dan Safari (Handayani, Wijianto, & Anggoro, 2018).

Untuk menjalankan kode-kode program PHP, file harus di upload kedalam server. Upload adalah proses mentransfer data atau file dari komputer client ke dalam web server (Mubarak, 2019). Cara kerja PHP adalah dengan menyelipkannya diantara kode HTML (Hypertext Markup Language) (Wahyuni & Irawan, 2020). Sedangkan pengertian sistem basis data adalah sebagai koleksi dari data-data yang terorganisasi sedemikian rupa sehingga data mudah disimpan dan dimanipulasi (diperbarui, dicari, diolah dengan perhitungan-perhitungan tertentu, serta dihapus (Novendri, Saputra, & Firman , 2019)
Basis data adalah sekumpulan data yang terhubung satu sama lain secara logika dan suatu deskripsi data yang dirancang untuk memenuhi kebutuhan informasi suatu organisasi atau perusahaan. Jadi Database merupakan suatu sistem atau perangkat lunak yang dibuat untuk mengelola basis data dan menjalankan

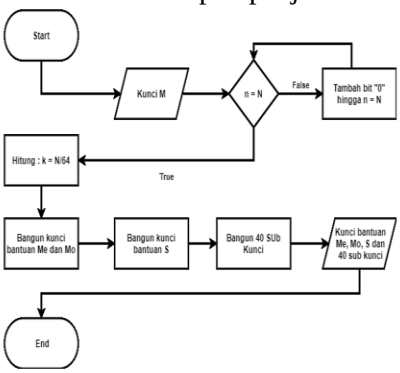
operasi terhadap data yang dibutuhkan banyak pengguna (Rizki & OP, 2021).
MySQL merupakan database server yang bersifat multiuser dan multi-threaded. SQL adalah bahasa database standar yang memudahkan penyimpanan, pengubahan dan akses informasi. Pada MySQL dikenal istilah database dan tabel. Tabel adalah sebuah struktur data dua dimensi yang terdiri dari baris-baris record dan kolom (Nurmalasari, Anna, & Arissu sand, 2019)

Flowchart adalah bagan yang menunjukkan alur atau alur dalam suatu program atau prosedur sistem secara logis. Flowchart (bagan alir) adalah sebuah ilustrasi berupa diagram alir dari algoritma-algoritma dalam suatu program, yang menyatakan arah aliran dari program tersebut (Yulianeu & Oktamala, 2022)

METODE

Dalam melakukan penelitian ini, penulis menggunakan metode terapan (*applied research*). Penelitian terapan atau *applied research* dilakukan berkenaan dengan kenyataan-kenyataan praktis, penerapan, dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Tujuan utama penelitian terapan adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok maupun untuk keperluan industri atau politik dan bukan untuk wawasan keilmuan semata.

Algoritma twofish memiliki panjang kunci 128 bit (16 karakter). Oleh karena aplikasi ini berlangsung real time maka agar proses keamanan teks berlangsung singkat. Kunci ditanamkan pada program dengan panjang 128 bit Tahap penjadwalan kunci bertujuan membangun 40 sub kunci, dari kunci yang diperluas K0,…,K39, yang akan digunakan pada proses enkripsi dan dekripsi. Dan 4 buah S-Box key-dependent yang digunakan di dalam fungsi g. Twofish didefinisikan untuk kunci-kunci dengan panjang N= 128, N= 192, dan N= 256. Beberapa kunci yang lebih pendek dari 256 bit dapat digunakan oleh lapisannya dari nol hingga yang lebih besar yang didefinisikan sebagai panjang kunci. Kemudian di defenisikan *k=N/64*. Tahapan penjadwalan kunci terdiri dari 5 bagian, yakni penambahan panjang kunci, *key-dependent S-Boxes*, fungsi *h*, dan permutasi *q* dan ekspansi kunci. Pada saat kunci dimasukkan di algoritma twofish didefenisikan sebagai kunci M. Kunci M terdiri dari 8k *byte*, yakni m0,…,m8k-1. *Byte-byte* adalah yang pertama diubah ke dalam kata-kata berukuran 2k dari setiap 2 bit.
Berikut adalah tahapan penjadwalan kunci



Bangun kunci bantuan Me dan Mo. Kunci M terdiri dari *8k mi* , bentuk kunci menjadi *byte-byte* m0, m1…, m*k-1*. Kelompokkan *byte-byte* hasil dari langkah 4a dalam 2k *word* sepanjang 32 bit dengan aturan pada persamaan berikut:

$$M_i = \sum_{j=0}^{3} m_{(4i+j)} \cdot 2^{8j} \qquad i = 0, \ldots, 2k-1$$

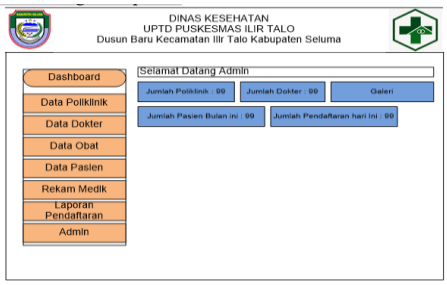
Berikut adalah tahapan proses enkripsi algoritma Twofish aplikasi keamanan data

Plainteks = Welcome TwoFish
Plainteks dikonversi ke heksadesimal sehingga menjadi :
Plainteks = 57 65 6C 63 6F 6D 65 20 54 77 6F 46 69 73 68
Karena plainteks belum mencapai panjang minimum plainteks maka dilakukan *padding* sehingga menjadi :

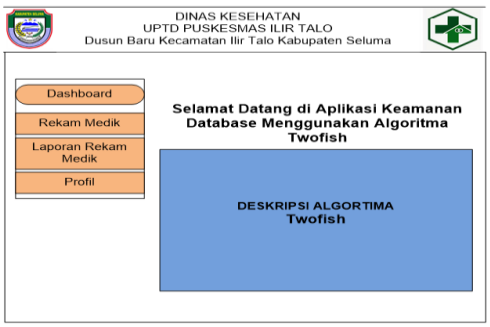
Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2024, VII (3): 1320 – 1326 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Plainteks = 57 65 6C 63 6F 6D 65 20 54 77 6F 46 69 73 68 00

Rancangan menu utama merupakan halaman menu yang muncul ketika berhasil masuk pada menu login. Menu utama menyediakan fasilitas/modul yang dapat digunakan untuk mengelola aplikasi.



Rancangan Halaman Home Pasien

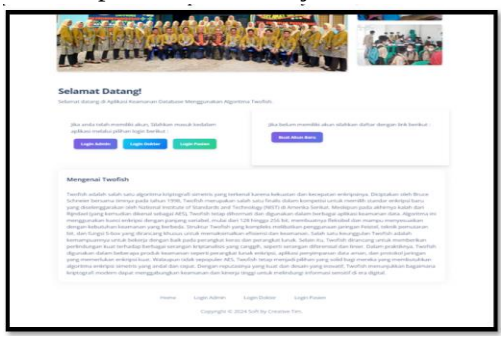


Pengujian sistem merupakan proses eksekusi sistem dengan tujuan mencari kesalahan atau kelemahan dari program tersebut. Proses tersebut dilakukan dengan mengevaluasi kemampuan program. Suatu program yang diuji akan dievaluasi apakah keluaran atau output yang dihasilkan telah sesuai dengan yang diinginkan atau tidak

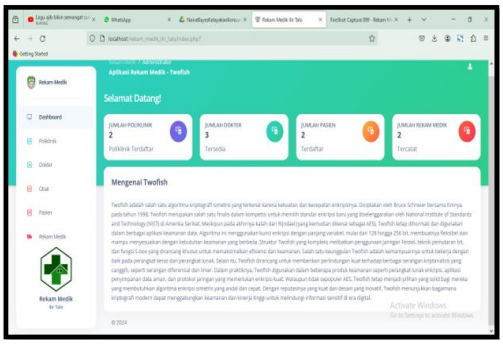
HASIL DAN PEMBAHASAN

Aplikasi keamanan database menggunakan *Twofish* berbasis *webiste* ini dibangun dengan tujuan untuk menjaga keamanan database sistem informasi data pada Puskesmas Ilir Talo. Secara garis besar sistem memiliki dua fungsi utama, yaitu fungsi Enkripsi dan Dekripsi bagi database. Pada sistem yang dibuat oleh penulis, masing-masing proses dibuat atau disajikan dalam windows yang berbeda untuk menghindari kesalahan penggunaan sistem, dan juga untuk mempermudah pengguna dalam pemakaian sistem secara optimal.

Pada aplikasi implementasi keamanan database menggunakan algoritma *Twofish* berbasis *webiste* ini terdapat beberapa *interface* atau antarmuka yang di desain untuk mempermudah *user* atau pemakai dalam menggunakan atau menjalankan aplikasi ini. Untuk mengoperasikan atau menjalankan aplikasi dilakukan dengan cara mengetikan *localhost*/rekam _medik_ilir_talo. Halaman *beranca* merupakan halaman pertama kali muncul ketika aplikasi berhasil dijalankan.

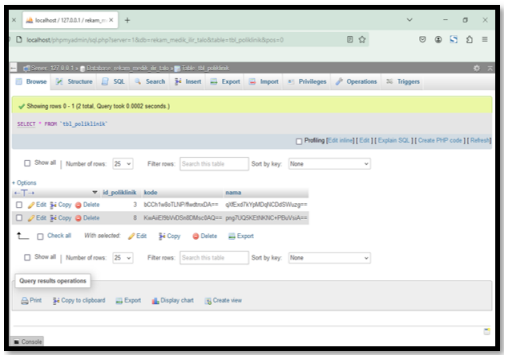


Pada halaman utama beranda aplikasi terdapat beberapa pilihan *login* yaitu : *login* admin, *login* dokter dan *login* serta buat akun baru untuk pasien yang belum terdaftar atau belum pernah berobat pada puskesmas ilir talo.

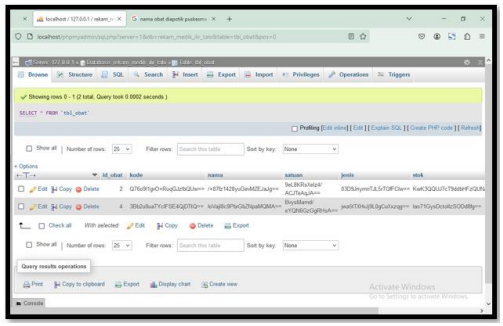


Merupakan *form* yang digunakan untuk mengolah data poliklinik.

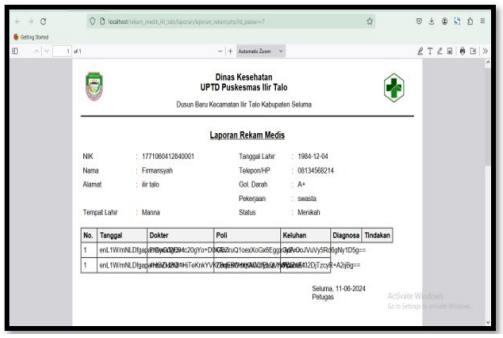
Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2024, VII (3): 1320 – 1326 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



untuk melakukan koreksi data poliklinik yang telah di input sebelumnya.



Untuk menampilkan laporan rekam medik pasien dapat dilakukan dengan meng-klik tombo "Cetak Rekam Medik" maka laporan rekam medik pasien akan terlihat sebagi berikut:



SIMPULAN

Aplikasi keamanan database rekam medik dibuat menggunakan Bahasa Pemrograman PHP dan Database MySql. Pada aplikasi ini telah diterapkan salah satu algoritma kriptografi Twofish untuk mengamankan isi record database, sehingga yang tersimpan di dalam database record yang telah diacak oleh algoritma tersebut.

Aplikasi yang dibangun dapat memberikan keamanan data yang sangat rahasia bagi user yang membutuhkan, terutama pada proses enkripsi dan dekripsi file dengan algoritma twofish, dimana proses enkripsi, dapat mengenkripsi teks dimana berubah teks enkripsi dan dekripsi sehinggga teks yang dibuat menjadi teks rahasia.

DAFTAR PUSTAKA

Afiifah, K., Azzahra, Z. F., & Anggoro, A. D. (2022). Analisis Teknik Entity-Relationship Diagram dalam Perancangan Database : Sebuah Literature Review. JURNAL INTECH (INFORMATIKA DAN TEKNOLOGI), 8-11.

Awal, E. E., Nurkifli, E., & Padilah, T. N. (2022). ANALISIS PERBANDINGAN HASIL ENKRIPSI DAN DEKRIPSI ALGORITMA KRIPTOGRAFI RIJNDAEL DAN TWOFISH UNTUK PENYANDIAN DATA. Jurnal Mahasiswa Ilmu Komputer, 260-265.

Dewi, E. (2018). IMPLEMENTASI KEBIJAKAN TENTANG PENGELOLAAN PERPUSTAKAAN OLEH PEGAWAI PERPUSTAKAAN DALAM UPAYA MENINGKATKAN MINAT BACA MASYARAKAT (Studi Analisis di Kecamatan Cijulang Kabupaten Pangandaran). Jurnal MODERAT, 60-68.

Ekta , N., Christian, A., & Wijaya, K. (2021). Implementasi Metode (User Centered Design) PadaRancang Bangun Sistem Informasi Perpustakaan : Studi Kasus : SMK Negeri 1 Gelumbang. Jurnal Pengembangan Sistem Informasi dan Informatika, 69-77.

Firman, A. (2019). Analisis dan Perancangan Sistem Informasi. Surabaya: Penerbit Qiara Media.

Gunawan, & Kirman. (2019). Implementasi Algoritma Turbo Boyer Moore Untuk Pencarian Data Pada Transaksi Keuangan Duta Phonecell Sawah Lebar. Jurnal Media Infotama, 9-15.

Handayani, V. R., Wijianto, R., & Anggoro, A. (2018). SISTEM INFORMASI PENDAFTARAN SELEKSI KERJA BERBASIS WEB PADA BKK (BURSA KERJA KHUSUS) TUNAS INSAN KARYA SMK NEGERI 2 BANYUMAS. Jurnal Evolusi, 76-84.

Imelda , I., & Prawira, E. (2018). Pengamanan Disposisi Dokumen secara online menggunakan Kriptografi Twofish dan Kompresi Huffman pada CV. TMU. Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri , 363-369.

Junaidi, A., & Wadisman, C. (2022). Sistem Informasi Antrian Online Berbasis Web di Klinik Sahabat Padang. Journal of Computer Science and Information Systems (JCoInS), 136-148.

Mubarak, A. (2019). RANCANG BANGUN APLIKASI WEB SEKOLAH MENGGUNAKAN UML (UNIFIED MODELING LANGUAGE) DAN BAHASA PEMROGRAMAN PHP (PHP HYPERTEXT PREPROCESSOR) BERORIENTASI OBJEK. JIKO (Jurnal Informatika dan Komputer), 19-25.

Novendri, M. S., Saputra, A., & Firman , C. E. (2019). APLIKASI INVENTARIS BARANG PADA MTS NURUL ISLAM DUMAI MENGGUNAKAN PHP DAN MYSQL. Lentera Dumai, 46-57.

Nurmalasari, Anna, & Arissusand, R. (2019). RANCANG BANGUN SISTEM INFORMASI AKUNTANSI LAPORAN LABA RUGI BERBASIS WEB PADA PT. UNITED TRACTORS PONTIANAK. Evolusi: Jurnal Sains dan Manajemen, 6-14.

Nursyanti, R., Alamsyah, R. R., & Perdana, S. (2019). PERANCANGAN APLIKASI BERBASIS WEB UNTUK MEMBANTU PENGUJIAN KUALITAS KAIN TEKSTIL OTOMOTIF (STUDI KASUS PADA PT. ATEJA MULTI INDUSTRI). Explore – Jurnal Sistem Informasi dan Telematika, 153-159.

Pardede, A., Manurung, H., & Filina, D. (2017). ALGORITMA VIGENERE CIPHER DAN HILL CIPHER DALAM APLIKASI KEAMANAN DATA PADA FILE DOKUMEN. Jurnal Teknik Informatika Kaputama (JTIK), 26-33.

Rizki, M. A., & OP, A. (2021). RANCANG BANGUN APLIKASI E-CUTI PEGAWAI BERBASIS WEBSITE (STUDI KASUS : PENGADILAN TATA USAHA NEGARA). Jurnal Teknologi dan Sistem Informasi (JTSI), 1-13.

Silalah, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. Jurnal Nasional Komputasi dan Teknologi Informasi, 182-186.

Wahyuni, R., & Irawan, Y. (2020). APLIKASI E-BOOK UNTUKATURAN KERJA BERBASIS WEB DI PENGADILAN NEGERI MUARA BULIAN KELAS II JAMBI . Jurnal Ilmu Komputer, 20-26.

Yulianeu, A., & Oktamala, R. (2022). SISTEM INFORMASI GEOGRAFIS TRAYEK ANGKUTAN UMUM DI KOTA TASIKMALAYA BERBASIS WEB. JUTEKIN (JURNAL TEKNIK INFORMATIKA), 125-134.