

PENERAPAN METODE ONE-TIME PAD CHIPER UNTUK MENGAMANKAN DATA KARYAWAN PADA PT. TRANSIMA CITRA INDO CONSULTANT

Salsa Carissa Sinaga[✉], Fithry Tahel

Program Studi Informatika, Universitas Potensi Utama, Medan, Indonesia

Email: salsasinaga87@gmail.com

ABSTRACT

PT. Transima Citra Indo Consultant, a company engaged in the field of tax consulting, requires a reliable data security system to maintain the confidentiality of sensitive information. One of the cryptographic methods that can be used is the One-Time Pad (OTP) method. One-Time Pad is an encryption algorithm with a very high level of security because it uses a unique key throughout the original message, thus ensuring that the encrypted message cannot be cracked as long as the key remains confidential. Therefore, this study will discuss the application of One-Time Pad in protecting employee data at PT. Transima Citra Indo Consultant as an effort to improve company data security. The results of this study are expected to provide significant benefits to PT. Transima Citra Indo Consultant in securing employee data, and also ensuring that only authorized parties can access it.

Keywords: OTP, Security, PT. Transima Citra Indo Consultant.

ABSTRAK

PT. Transima Citra Indo Consultant, merupakan sebuah perusahaan yang bergerak di bidang konsultan pajak, membutuhkan sistem keamanan data yang handal untuk menjaga kerahasiaan informasi yang bersifat sensitif. Salah satu metode kriptografi yang dapat digunakan adalah metode One-Time Pad (OTP). One-Time Pad merupakan algoritma enkripsi dengan tingkat keamanan yang sangat tinggi karena menggunakan kunci unik sepanjang pesan asli, sehingga memastikan pesan yang dienkripsi tidak dapat dipecahkan selama kunci tetap dirahasiakan. Oleh karena itu, penelitian ini akan membahas mengenai penerapan One-Time Pad dalam melindungi data karyawan di PT. Transima Citra Indo Consultant sebagai upaya meningkatkan keamanan data perusahaan. Hasil dari penelitian ini diharapkan dapat memberikan manfaat yang signifikan pada PT. Transima Citra Indo Consultant dalam mengamankan data karyawan, dan juga memastikan bahwa hanya pihak berwenang saja yang dapat mengaksesnya.

Kata Kunci: OTP, Keamanan, PT. Transima Citra Indo Consultant.

PENDAHULUAN

PT. Transima Citra Indo Consultant, merupakan sebuah perusahaan yang bergerak di bidang konsultan pajak, yang dimana sangat membutuhkan sebuah sistem keamanan data untuk menjaga kerahasiaan informasi mengenai data pribadi karyawan yang bersifat sensitif. Keamanan data karyawan mencerminkan bagus atau tidaknya sebuah perusahaan, karena ketika karyawan merasa data mereka dilindungi, mereka akan lebih percaya kepada perusahaan dan termotivasi untuk bekerja dengan optimal.

Keamanan menjadi isu krusial dalam sistem jaringan global, terutama terkait proses transmisi informasi antara sumber dan penerima. Di era digital saat ini, akses terhadap internet semakin mudah, sehingga meningkatkan potensi penyalahgunaan oleh pihak-pihak tidak bertanggung jawab yang berupaya mencuri informasi maupun data pribadi milik individu dan perusahaan. Umumnya, sasaran utama dalam tindakan pencurian data tersebut adalah berkas atau

dokumen digital yang memiliki nilai strategis dan ekonomi tinggi (Ziyad & Widodo, 2024).

Salah satu metode kriptografi yang dapat digunakan adalah One-Time Pad (OTP). One-Time Pad merupakan algoritma enkripsi dengan tingkat keamanan yang sangat tinggi karena menggunakan kunci unik sepanjang pesan asli, sehingga memastikan pesan yang dienkripsi tidak dapat dipecahkan selama kunci tetap dirahasiakan.

Berdasarkan penelitian yang dilakukan oleh Huda dkk. (2022) berjudul "Implementasi Algoritma One Time Menggunakan Algoritma Cipher Transposition Sebagai Pengamanan Rahasia Pesan", disimpulkan bahwa keamanan data merupakan aspek yang sangat krusial dalam proses pengiriman pesan, terutama untuk pesan yang bersifat rahasia. Hal ini dapat diamati dalam berbagai aktivitas sehari-hari, seperti penggunaan internet untuk mengirim e-mail, berkomunikasi melalui media sosial, melakukan transaksi jual beli daring, dan sebagainya. Oleh karena itu, diperlukan penerapan kode atau algoritma

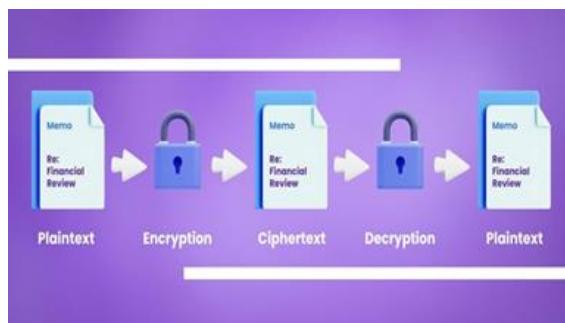
criptografi agar pesan tetap terjaga kerahasiaannya, mengingat data dan informasi yang dikirim melalui jaringan publik sangat rentan terhadap berbagai bentuk serangan.

Oleh karena itu, penelitian ini berfokus untuk mengamankan data karyawan pada PT. Transima Citra Indo Consultant, dan penelitian ini diharapkan dapat memberikan kontribusi nyata dalam membantu perusahaan menjaga kerahasiaan serta integritas data karyawan.

TINJAUAN PUSTAKA

Kriptografi

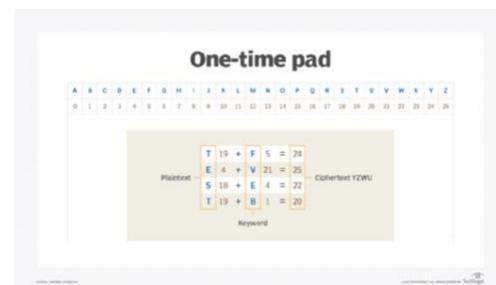
Keamanan merupakan aspek fundamental dalam jaringan global, khususnya dalam proses pertukaran informasi antara pengirim dan penerima. Pada era digital yang ditandai dengan kemudahan akses terhadap internet, muncul berbagai potensi ancaman dari pihak-pihak yang tidak bertanggung jawab yang berupaya memperoleh data pribadi maupun informasi sensitif milik individu dan organisasi. Secara umum, objek utama dalam tindak pencurian data tersebut adalah dokumen atau berkas digital yang memiliki nilai strategis serta signifikan secara ekonomi (Azahri, dkk, 2022).



Gambar 1. Kriptografi

One-Time Pad Chiper

One Time Pad (OTP) merupakan salah satu algoritma kriptografi simetris (konvensional) yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi pesan. Algoritma ini dianggap sebagai salah satu metode paling aman dalam menjaga kerahasiaan informasi. Ciri khas dari One Time Pad adalah panjang kuncinya yang harus sama dengan panjang plainteks atau teks asli, sehingga menimbulkan tantangan tersendiri dalam pembuatan dan pengelolaan kunci, terutama ketika plainteks memiliki jumlah karakter yang besar. (Sulaiman, 2020).



Gambar 2. OneTime Pad Chiper

Website

Website merupakan salah satu media penyedia informasi yang beroperasi di jaringan internet. Fungsinya tidak hanya terbatas pada penyebaran informasi, tetapi juga dapat dimanfaatkan sebagai sarana komersial, seperti pembuatan toko daring (*online shop*). Secara umum, website terdiri atas sekumpulan halaman web yang terhimpun dalam suatu domain atau subdomain dan diakses melalui jaringan *World Wide Web* (WWW). Setiap halaman web merupakan dokumen yang ditulis menggunakan format *Hyper Text Markup Language* (HTML), dan umumnya dapat diakses melalui protokol *Hypertext Transfer Protocol* (HTTP), yang berfungsi mengirimkan data dari server ke pengguna untuk ditampilkan melalui peramban (*web browser*). (Ma'rif, Faisol and Vendyansyah, 2020).



Gambar 3. Website

PHP (*Hypertext Preprocessor*)

PHP merupakan bahasa pemrograman berbasis *server-side scripting* yang dirancang khusus untuk pengembangan aplikasi web. Selain digunakan dalam konteks web, PHP juga dapat berfungsi sebagai bahasa pemrograman umum. Bahasa ini pertama kali dikembangkan oleh Rasmus Lerdorf pada tahun 1994. Saat ini, PHP dikenal sebagai singkatan rekursif dari *Hypertext Preprocessor*, yang menunjukkan bahwa kepanjangan istilah tersebut berasal dari akronimnya sendiri. PHP bersifat gratis (free) dan open source, serta didistribusikan di bawah PHP License, yang memiliki beberapa perbedaan dengan GNU General Public License (GPL) yang umumnya digunakan dalam

proyek perangkat lunak *open source* lainnya. (Rina Noviana, 2022).



Gambar 4. PHP

MySQL (*My Structure Query Language*)

MySQL (*My Structured Query Language*) merupakan salah satu perangkat lunak basis data (*database*) yang paling populer dan banyak digunakan di seluruh dunia. Sintaks MySQL menjadi pilihan utama bagi banyak pengembang aplikasi karena kemudahannya dalam dipahami dan diterapkan. Keunggulan lainnya adalah kemampuan MySQL untuk berintegrasi dengan berbagai bahasa pemrograman umum seperti C++, Java, PHP, dan Python, sehingga menjadikannya solusi yang fleksibel dan efisien dalam pengelolaan serta pengolahan data pada berbagai jenis aplikasi. (Bayu, 2023).



Gambar 5. MySql

Xampp

XAMPP merupakan perangkat lunak yang berfungsi sebagai *web server Apache* dan di dalamnya telah terintegrasi dengan server MySQL serta didukung oleh bahasa pemrograman PHP untuk membangun website yang bersifat dinamis. XAMPP mendukung dua sistem operasi utama, yaitu Windows dan Linux. Pada sistem operasi Linux, proses instalasi XAMPP dilakukan melalui command line, sedangkan pada sistem operasi Windows, instalasi dapat dilakukan melalui antarmuka grafis (*graphical interface*), sehingga penggunaannya di Windows cenderung lebih mudah dibandingkan di Linux. Secara umum, XAMPP memiliki tiga komponen utama, yaitu Apache sebagai web server, PHP sebagai bahasa pemrograman server-

side, dan MySQL sebagai sistem manajemen basis data. (Saputra, dkk, 2024).



Gambar 6. XAMPP

UML (*Unified Modelling Language*)

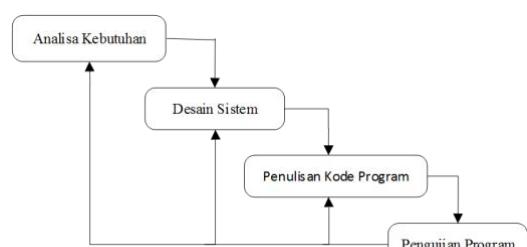
UML (*Unified Modeling Language*) merupakan bahasa pemodelan visual yang digunakan untuk mendeskripsikan berbagai aspek dalam pengembangan sistem berorientasi objek. UML berfungsi untuk memvisualisasikan, menspesifikasi, membangun, serta mendokumentasikan kebutuhan (requirement), analisis, desain, dan arsitektur perangkat lunak. Dalam penerapannya, UML menggunakan simbol-simbol grafis yang didukung oleh teks deskriptif guna memberikan pemahaman yang lebih jelas terhadap struktur dan perilaku sistem yang dirancang. (Andraini dan Bella, 2022).



Gambar 7. UML

METODE PENELITIAN

Penelitian ini membahas tahapan-tahapan yang dilakukan untuk mencapai tujuan penelitian dengan menerapkan suatu metode yang menjelaskan secara sistematis proses penyelesaian permasalahan yang dikaji. Adapun langkah penyelesaian penelitian yang dibuat dapat dilihat pada gambar dibawah ini:



Gambar 8. Waterfall Diagram Penelitian

Keterangan:

1. Analisa kebutuhan

Untuk mewujudkan sebuah aplikasi yang berfungsi dalam menjaga keamanan data karyawan, terdapat beberapa kebutuhan yang harus dipenuhi. Kebutuhan tersebut mencakup berbagai komponen penting yang diperlukan dalam proses perancangan dan pengembangan aplikasi tersebut, di antaranya adalah:

- a. Pada tahap ini dilakukan proses pengumpulan informasi melalui kegiatan observasi langsung di PT. Transima Citra Indo Consultant. Tujuannya adalah untuk memperoleh data yang relevan dan akurat sebagai dasar dalam perancangan serta pengembangan aplikasi keamanan data karyawan.
- b. Tahap ini meliputi penyediaan berbagai perangkat yang dibutuhkan dalam proses penelitian, seperti perangkat lunak (software), perangkat keras komputer, serta perangkat pendukung lainnya yang berfungsi untuk menunjang kelancaran kegiatan perancangan dan pengujian aplikasi.

2. Desain Sistem

Pada tahap ini, dilakukan perancangan program secara logis dengan memanfaatkan berbagai diagram UML (*Unified Modeling Language*), seperti use case diagram, class diagram, sequence diagram, dan activity diagram, yang berfungsi untuk menggambarkan alur sistem, hubungan antar komponen, serta interaksi antara pengguna dan sistem secara terstruktur. Penulisan Kode Program Pada tahap ini, program ditulis dalam bahasa pemrograman *PHP* dengan menggunakan software *Notepad++*, dan *MySQL*, sebagai DBMS-nya.

3. Penulisan Kode Program

Pada tahap ini, proses pengkodean program dilakukan dengan menggunakan bahasa pemrograman *PHP*. Penulisan kode dilakukan melalui perangkat lunak *Notepad++*, sedangkan pengelolaan basis data dilakukan menggunakan *MySQL* sebagai Database Management System (DBMS).

4. Pengujian Program

Pada tahap ini, program yang telah dikembangkan menggunakan bahasa pemrograman *PHP* dan basis data *MySQL* dinyatakan telah berhasil dibuat. Selanjutnya, dilakukan tahap pengujian (testing) untuk memastikan bahwa program berjalan sesuai dengan fungsionalitas yang dirancang serta mampu menghasilkan keluaran yang tepat dan sesuai dengan kebutuhan pengguna.

HASIL DAN PEMBAHASAN

Pembahasan

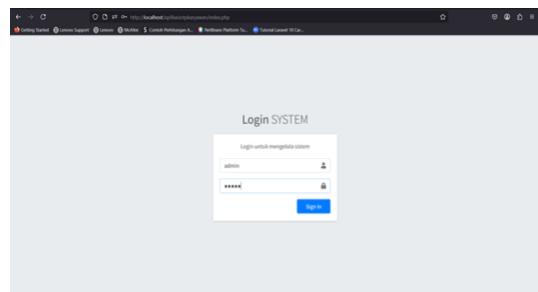
PT. Transima Citra Indo Consultant merupakan sebuah perusahaan yang bergerak di bidang konsultan pajak, sehingga membutuhkan sebuah sistem yang baik untuk bisa mengamankan data karyawan agar menghindari terjadinya lagi kebocoran data. Yang dimana jika data mengalami kebocoran maka para karyawan akan merasa tidak nyaman dan aman dalam bekerja, maka dari itu perusahaan mencari jalan untuk menangani permasalahan ini. Solusi yang peneliti berikan untuk memecahkan permasalahan ini adalah dibangunnya sebuah aplikasi yang dapat mengamankan data karyawan pada PT. Transima Citra Indo Consultant. Aplikasi yang akan dibangun adalah suatu aplikasi yang akan digunakan oleh admin untuk menjaga data karyawan agar tetap aman.

Hasil

Hasil yang diperoleh dari penelitian yang dilakukan ialah, sebuah aplikasi yang dapat mengamankan data karyawan dengan menggunakan metode *One-Time Pad* agar tidak lagi mengalami kebocoran data pada PT. Transima Citra Indo Consultant sebagai berikut:

Halaman Login

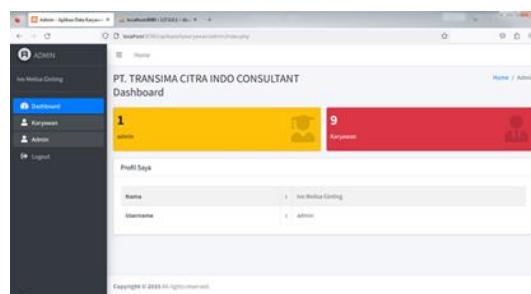
Halaman login berfungsi sebagai gerbang utama bagi admin untuk mengakses sistem dan melakukan pengolahan data karyawan. Melalui halaman ini, admin harus memasukkan identitas pengguna seperti username dan password sebagai bentuk autentikasi sebelum memperoleh hak akses ke dalam sistem. Tampilan halaman login dapat dilihat pada Gambar 9:



Gambar 9. Tampilan Halaman Login

Halaman Menu Utama

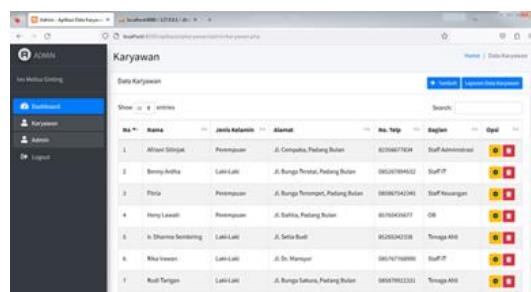
Halaman ini merupakan halaman utama (dashboard) yang muncul setelah proses login berhasil dilakukan. Pada halaman ini, admin dapat mengakses berbagai menu dan fitur yang tersedia untuk mengelola data karyawan serta melakukan pengaturan sistem. Tampilan halaman utama dapat dilihat pada Gambar 10:



Gambar 10. Tampilan Halaman Menu Utama

Halaman Data Karyawan

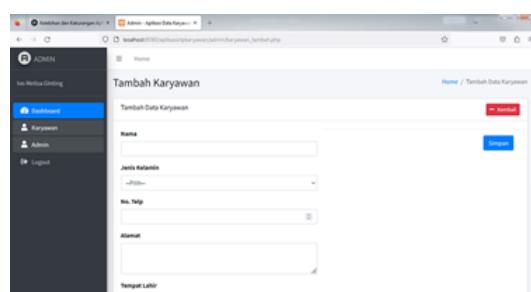
Halaman ini digunakan oleh admin untuk melakukan pengelolaan data karyawan, yang meliputi proses input, perubahan (edit), serta penghapusan data. Seluruh data yang diolah pada halaman ini terhubung langsung dengan database dan mendukung proses enkripsi serta dekripsi guna menjaga keamanan informasi. Tampilan halaman pengelolaan data karyawan dapat dilihat pada Gambar 11:



Gambar 11. Tampilan Halaman Data Karyawan

Halaman Tambah Data Karyawan

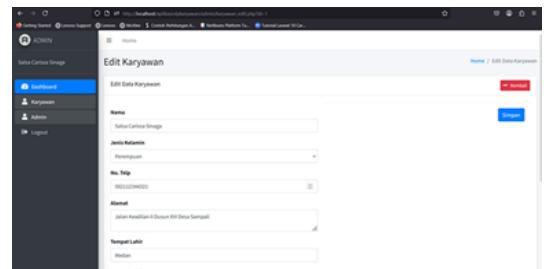
Halaman ini digunakan oleh admin untuk melakukan penambahan data karyawan yang terintegrasi langsung dengan database. Setiap data yang diinput melalui halaman ini akan diproses menggunakan metode enkripsi dan dekripsi sebagai upaya untuk menjaga kerahasiaan dan keamanan informasi karyawan. Tampilan halaman penambahan data karyawan dapat dilihat pada Gambar 12:



Gambar 12. Tampilan Halaman Tambah Data Karyawan

Halaman Edit Data Karyawan

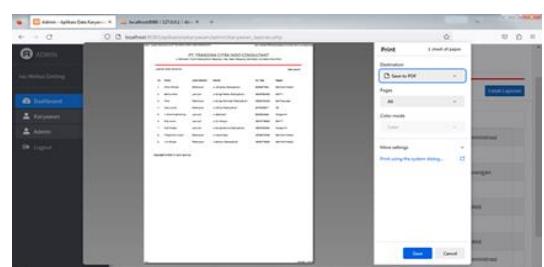
Halaman ini digunakan oleh admin untuk melakukan pengeditan atau pembaruan data karyawan yang tersimpan di dalam database. Setiap data yang diubah melalui halaman ini akan diproses dengan menerapkan mekanisme enkripsi dan dekripsi guna menjaga keamanan serta kerahasiaan informasi karyawan. Tampilan halaman pengubahan data karyawan dapat dilihat pada Gambar 13:



Gambar 13. Tampilan Halaman Edit Data Karyawan

Halaman Laporan Data Karyawan

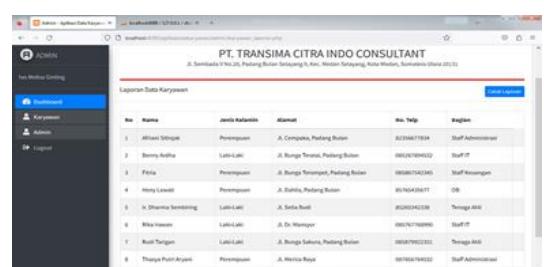
Halaman ini menampilkan laporan data karyawan yang disusun untuk disampaikan kepada pimpinan sebagai bentuk dokumentasi dan evaluasi data kepegawaian. Melalui halaman ini, admin dapat melihat dan mencetak laporan sesuai kebutuhan. Tampilan halaman laporan data karyawan dapat dilihat pada Gambar 14:



Gambar 14. Tampilan Halaman Laporan Data Karyawan

Halaman Cetak Laporan Data Karyawan

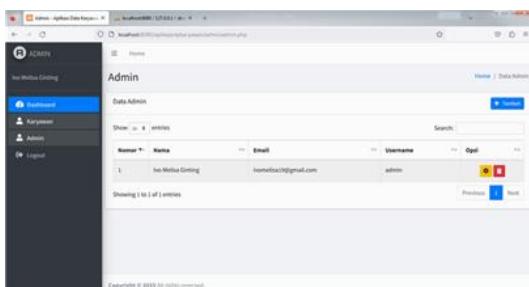
Halaman ini berisi laporan data karyawan yang akan di cetak, dan dilaporkan kepada pimpinan. Gambar tampilan dapat dilihat pada gambar 15:



Gambar 15. Tampilan Halaman Cetak Laporan Data Karyawan

Halaman Data Admin

Halaman ini digunakan oleh admin, untuk menginput data admin, mengubah data admin, dan menghapus data admin yang terhubung dengan database untuk proses enkripsi dan dekripsi. Adapun tampilan halaman ini dapat dilihat pada gambar 16:



Gambar 16. Tampilan Halaman Data Admin

Halaman Tambah Data Admin

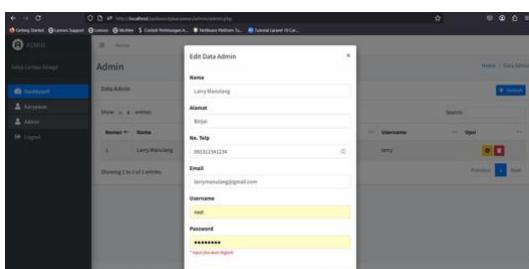
Halaman ini digunakan oleh admin, untuk menambahkan data admin yang menggunakan sistem, dan terhubung dengan database untuk proses enkripsi dan dekripsi. Adapun tampilan halaman ini dapat dilihat pada gambar 17:



Gambar 17. Halaman Tambah Data Admin

Halaman Edit Data Admin

Halaman ini digunakan oleh admin, untuk mengubah data admin, dan terhubung dengan database untuk proses enkripsi dan dekripsi. Adapun tampilan halaman ini dapat dilihat pada gambar 18:



Gambar 18. Halaman Edit Data Admin

KESIMPULAN

Kesimpulan yang diperoleh dari penelitian ini adalah sebagai berikut:

1. Penelitian ini menunjukkan bahwa One- Time Pad (OTP) dapat menjadi solusi yang efektif untuk memperkuat sistem keamanan data pada perusahaan, meskipun masih perlu perhatian pada aspek teknis seperti distribusi kunci.
2. Keamanan data karyawan sangat penting bagi PT. Transima Citra Indo Consultant karen menyangkut informasi pribadi yang bersifat sensitif.
3. One-Time Pad (OTP) merupakan metode enkripsi yang sangat aman karena menggunakan kunci unik untuk setiap pesan dan sulit untuk diretas.

DAFTAR PUSTAKA

Andraini, L. (2022). Pengelolaan Surat Menyurat Dengan Sistem Informasi (Studi Kasus: Kelurahan Gunung Terang). *Jurnal Portal Data*, 2(1).

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, 2(1), 2809-476.

Dakhi, O., Masril, M., Novalinda, R., Jufrialdi, J., & Ambiyar, A. (2020). Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Chiper. *Jurnal Inovasi Vokasional Dan Teknologi*, 20(1), 27-36.

Huda, C., Mulyana, D. I., Prasetyo, A. D., & Zulkarnain, A. Y. (2022). Implementasi Algoritma One Time Menggunakan Algoritma Chiper Transposition Sebagai Pengamanan Rahasia Pesan. *Jurnal J-COM (Jurnal Informatika Dan Teknologi Komputer) Vol*, 3(01), 40-48.

Mafrif, I., Faisol, A., & Vendyansyah, N. (2020). Pemetaan Daerah Perkebunan Berdasarkan Luas Dan Jumlah Produksi Di Kalimantan Tengah Berbasis Web. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 4(2), 170-175.

Saputra, L. N., Wulandari, K., Hasibuan, M., & Heryana, N. (2024). Implementasi Owncloud Sebagai Sistem Penyimpanan File Pribadi Berbasis Cloud Computing. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 8(1), 994-999.

Sulaiman, O. K. (2020). Generate Pseudo-Random Numbers Linear-Feedback Shift Register (LSFR) Pada Kunci Algoritma One Time Pad (OTP). *Semin. Nas. Teknol. Komput. Sains*, 171-175.

Ziyad, M. M., & Widodo, S. (2024). Analisis keamanan jaringan dan perlindungan data terhadap serangan siber di perusahaan luar sekolah. *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*, 5(2), 623-628.