JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

IMPLEMENTASI SISTEM KEAMANAN DOKUMEN KEPEGAWAIAN MENGGUNAKAN METODE AES-256 DAN VIGENERE CHIPER

Pandhu Adam[1], Moh. Ali Romli[2]

[1,2] Universitas Teknologi Yogyakarta, Sleman 55285
** Email Korespondensi: pandhua2000@gmail.com, ali.romli@uty.ac.id*

INFO ARTIKEL

Sejarah Artikel:
Diterima Tgl 7/10/23
Diperbaiki. Tgl 24/12/23
Disetujui. Tgl 28/12/23
Tersedia daring, Tgl 04/01/24

e-ISSN 2961-9009
p-ISSN 2963-1289

ABSTRAK

Dokumen kepegawaian merupakan data yang bersifat privat, sehingga harus ada pengamanan khusus pada data tersebut agar tidak disalahgunakan oleh orang yang tidak bertanggung jawab. BKPH Muria Patiayam Perhutani Kudus adalah Badan Usaha Milik Negara berbentuk Perusahaan Umum (Perum) yang memiliki tugas dan wewenang untuk mengelola sumber daya hutan negara di Kabupaten Kudus. Kriptografi merupakan salah satu metode pengamanan data yang dapat diterapkan untuk mengamankan data dokumen kepegawaian. Algoritma AES-256 dan Vigenere Cipher digunakan sebagai metode enkripsi dan dekripsi pada dokumen tersebut. Hasil pengujian yang dilakukan pada proses enkripsi dan dekripsi pada file pdf, docx, xlsx dan txt telah berhasil dilakukan pada sistem pengamanan data dokumen kepegawaian berbasis web. Hasil pengujian yang dilakukan menunjukan bahwa enkripsi yang dilakukan dapat berfungsi dengan benar dan orang-orang yang tidak memiliki kunci enkripsinya tidak dapat mengakses dokumen. Penerapan ilmu kriptografi metode AES-256 dan Vigenere Chiper berbasis web dapat meningkatkan keamanan dalam menyimpan data dokumen kepegawaian, serta melindungi data dari ancaman orang yang tidak bertanggung jawab.

DOI:
https://doi.org/10.58290/jukomtek.v2i2.166

Kata Kunci:
Kriptografi, Enkripsi, Dekripsi, AES-256, Vigenere Chiper.

PENDAHULUAN

Kebocoran data masih banyak terjadi pada lembaga pemerintahan di Indonesia. Seperti yang dilansir dari laman suara.com sebanyak 347GB dokumen penting milik 21.000 perusahaan Indonesia termasuk perusahaan asing yang memiliki cabang di Indonesia tersebar bebas di dark *web*. Informasi yang dipublikasikan oleh laman suara.com tersebut mengindikasikan bahwa keamanan data masih sangat rentan terjadi pada perusahaan di Indonesia.

Metode yang akan digunakan dalam penelitian ini adalah metode Algoritma kriptografi metode AES-256 dan Vigenere Chiper. Algoritma ini dipilih karena algoritma AES dengan panjang kunci 256-bit dapat menyandikan isi suatu *file* sehingga dapat mengamankan *file* tersebut. Dalam pengembangan sistem menyembunyikan folder yang digunakan untuk menyimpan *file* enkripsi maupun *file* dekripsi. Sedangkan Algoritma Vigenere Chiper setiap huruf pesan aslinya digeser sebanyak satu huruf pada kuncinya. Algoritma Vigenere Cipher ini menggunakan bujur sangkar vigenere untuk melakukan enkripsi.

Penelitian yang dilakukan diharapkan dapat menerapkan sistem keamanan data dokumen kepegawaian dengan menggunakan algoritma kriptografi AES-256 dan Vigenere Chiper. Mengenkripsi data dengan format dokumen yang ada diharapkan dapat untuk mengamankan dokumen kepegawaian.

LANDASAN TEORI

Menurut Saputro (2020) sistem merupakan aliran beberapa komponen yang dihubungkan bersama untuk mencapai tujuan tertentu. Sistem itu sendiri memiliki elemen penggerak yang membantu satu komponen mencapai tujuannya dalam kaitannya dengan komponen lainnya. Menurut Mulyawan (2022) keamanan data serangkaian standar dan teknik yang melindungi data dari kerusakan, perubahan, atau pengungkapan informasi yang disengaja atau tidak disengaja. Tujuanya mencakup semua aspek keamanan informasi, mulai dari keamanan fisik perangkat keras (hardware) dan perangkat penyimpanan, hingga manajemen dan kontrol akses, hingga keamanan logis perangkat lunak aplikasi (software). Sehingga dapat disimpulkan sistem keamanan merupakan sebuah serangkaian sistem yang melindungi data dari modifikasi, perubahan, dan pengungkapan informasi dari orang yang tidak berhak akan askes kepada data tersebut, bukan hanya sebatas dengan data digital, keamanan data juga mencakup hingga kemanan fisik pada perangkat keras maupun manajemen dan control akses dari data tersebut.

Menurut Rodin (2021) dalam bukunya yang berjudul "Teori dan Praktik Pengorganisasian Dokumen" menjelaskan bahwa dokumen adalah data sebuah kegiatan, surat, rekaman suara atau gambar yang dapat dipakai sebagai bukti keterangan agar lebih meyakinkan. Menurut Sanjaya (2020) menjelaskan bahwa kepegawaian berasal dari kata pegawai (berupa objek atau orang) dengan kata imbuhan ke-an yang menunjukkan suatu aktivitas atau kegiatan. Sehingga kepegawaian dapat diartikan sebagai suatu kegiatan yang dilakukan atau digunakan oleh suatu organisasi atau lembaga tertentu yang segala sesuatu kegiatanya adalah tanggung jawab dan milik perusahaan. Dapat disimpulkan bahwa Dokumen Kepegawaian adalah bukti atau keterangan atas jenis sumber apapaun mencakup segala aspek yang berkaitan dengan kedudukan, tugas, hak dan perkembangan pegawai.

Menurut Mukhtar (2019) dalam bukunya yang berjudul "Kriptografi Untuk Keamanan Data" menjelaskan bahwa kriptografi adalah ilmu yang mempelajari Teknik matematis yang berhubungan dengan aspek keamanan Informasi seperti tingkat keyakinan, integritas data, autentikasi dan autentikasi keaslian data. Kriptografi bisa pula diartikan sebagai suatu ilmu atau seni menjaga keamanan pesan. Dengan dua proses dasar kriptografi berupa enkripsi dan dekripsi. Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut: EK (P) = C (Proses Enkripsi) dan DK (C) = P (Proses Dekripsi).

AES (*Advanced Encryption Standard*) merupakan standar enkripsi dekripsi dengan kunci simetris yang menggantikan pendahulunya yaitu DES. Jenis AES terbagi 3, yaitu AES-128, AES-192 dan AES-256. Angka-angka yang berada di belakang kata AES merupakan panjang kunci yang digunakan pada tiap-tiap AES. Menurut Wiharto & Irawan (2018) Algoritma AES adalah blok *chipertext simetrik* yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. AES-256 Bit merupakan *blokchipertext simetrik* yang dapat mengenkripsi dan dekripsi data/informasi dengan ukuran kunci 256 bit. Sedangkan untuk konsep AES-256 diantaranya, setiap masukan 256-bit plaintext dimasukan kedalam state berbentuk matriks ordo 4x4. State ini kemudian dijumlahkan dengan key atau sandi menggunakan gerbang logika *XOR*. Kemudian dilakukan proses subbyte, shiftrows, mix column, roundkey dan sebanyak 14x karena

256-bit itu putarannya 14x. Dan pada perulangan ke 14 pada shift rows langsung turun ke hasil atau ciphertext.

Menurut Al Khowarizmi (2021) dalam bukunya yang berjudul "Pengantar Teknologi Informasi" Vigenere Chiper merupakan salah satu algoritma kriptografi klasik, diperkenalkan pada tahun 1986 pada abad ke-16. Algoritma kriptografi ini diterbitkan oleh diplomat dan kriptografer Prancis blaise de vigenere, namun sebenarnya algoritma tersebut sudah dijelaskan dalam buku La Cifra Del Sig (1553). Pada prosesnya, vigenere chiper mengenkripsi teks biasa dari sebuah pesan dengan menggeser karakter dalam pesan tersebut sejauh hingga nilai kunci alfabet. Vigenere Cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Algoritma ini mengganti satu alfabet di mana semua karakter dalam pesan dienkripsi dengan
kunci yang sama.

Menurut Rosaly (2019) *flowchart* atau diagram alur adalah jenis diagram yang mewakili suatu algoritma atau urutan langkah-langkah instruksi dalam suatu sistem. Analis sistem menggunakan diagram alur sebagai dokumentasi

untuk memberikan gambaran logis kepada pemrogram tentang sistem yang mereka buat.

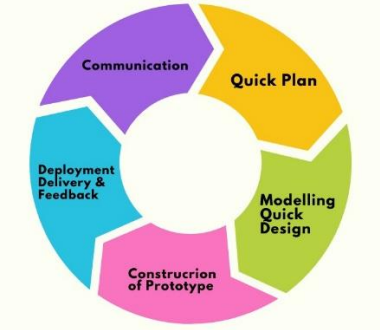
Menurut Rahmatuloh, dkk., (2022) *Use case diagram* adalah satu dari berbagai jenis diagram *Unified Modelling Language* (UML) yang menggambarkan hubungan interaksi antara aktor dan sistem.

Menurut Tanoto (2020) *Activity Diagram* atau Diagram aktivitas adalah bentuk visual dari alur kerja yang berisi aktivitas dan tindakan, yang juga dapat berisi pilihan, atau pengulangan.

METODE PENELITIAN

Penelitian ini mengimplementasikan metode prototipe. Metode pengembangan prototipe merupakan metode pengembangan

perangkat lunak yang sering digunakan oleh pengembang agar dapat saling berinteraksi dengan pengguna selama waktu pembuatan sistem (Pressman, 2015). Gambar 1 berikut merupakan metode prototipe.



Gambar 1. Metode *Prototype*
Sumber: Ardiyansah et al., 2021

Langkah-langkah dari metode *prototype* adalah sebagai berikut:

Communication, penggalian informasi yang dilakukan oleh pengembang terhadap pengguna tentang berbagai kebutuhan agar sistem yang direncanakan dapat berjalan sesuai tujuan.

Quick Plan, perencanaan pembuatan prototipe dilakukan secara cepat dengan analisis. Langkah awal dalam perencanaan adalah mengidentifikasi kebutuhan dalam perancangan aplikasi. Langkah tersebut akan menentukan *input*, *output*, dan proses pada sistem sehingga sistem dapat menghasilkan *output* sesuai ekspektasi.

*Modeling Quick Design***,** tahapan ini merancang model dengan *tools* UML yang menjelaskan tentang alur, aktor, dan proses sistem pada aplikasi berbasis *web*.

Construction of Prototipe, perancangan *prototype* dibuat berdasarkan aspek yang terlihat pada representasi perangkat lunak. Rancangan ini terlihat oleh *end user* yang ditunjukkan oleh desain antarmuka.

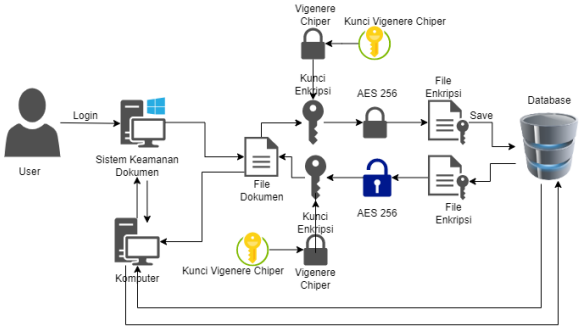
Deployment Delivery & Feedback, evaluasi dan pengujian prototipe dilakukan menggunakan metode *black box*. Pengujian fungsionalitas sistem menjadi parameter yang menunjukkan kelayakan.

ANALISIS DAN PERANCANGAN

A. Analisis Sistem

Sistem yang diusulkan adalah sistem keamanan dokumen kepegawaian dengan metode kriptografi AES-256 dan Vigenere Chiper, Ilustrasi analisis sistem yang diusulkan dapat dilihat pada Gambar 2**.**

e-ISSN 2961-9009
p-ISSN 2963-1289

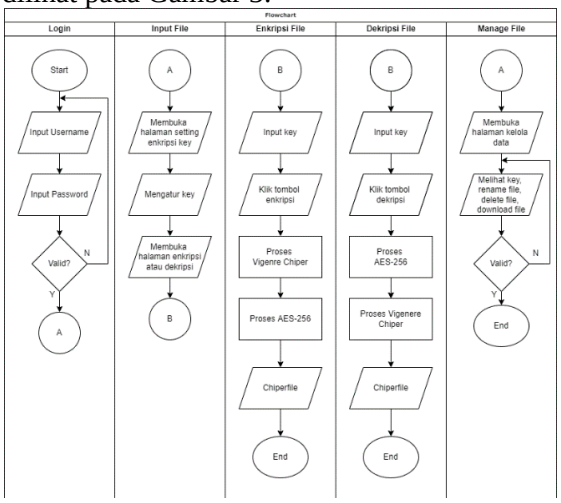


Gambar 2. Analisis Sistem

Model dari sistem terbagi dalam 2 tahap yaitu tahap enkripsi dan tahap dekripsi. Pada tahap enkripsi *user* memasukan sebuah dokumen kedalam sistem. Setelah itu sistem akan melakukan enkripsi yang melalui 2 metode yaitu pertama kunci akan dienkripsi dengan metode Vigenere Chiper dan kemudian dokumen akan dienkripsi dengan metode AES-256, setelah proses enkripsi selesai, *chiperfile* yang dihasilkan disimpan pada sistem oleh pengguna.

B. Desain Sistem

Penelitian ini menggunakan *flowchart* untuk menggambarkan alur dari sistem yang dibangun. *Flowchart* dapat menggambarkan bagaimana sistem berjalan saat proses enkripsi data maupun dekripsi data. *Flowchart* dapat dilihat pada Gambar 3.

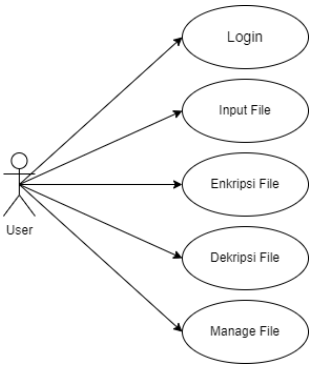


Gambar 3. *Flowchart*

Digambarkan terdapat 5 bagian pada *flowchart* diagram yaitu bagian *login*, input *file*, enkripsi data, dekripsi data, dan manage data. Pada bagian *login* dijelaskan tahap tahap apabila ada *user* akan *login* ke dalam sistem. Setelah itu pada bagian input data dijelaskan tahapan untuk menginput data yang akan diamankan.

Selanjutnya pada bagian enkripsi data digambarkan tahapan enkripsi dengan metode AES-245 dan Vigenere Chiper yang terjadi untuk proses pengamanan data. Sedangkan pada bagian dekripsi data digambarkan juga tahapan dekripsi dengan metode yang sama. Untuk bagian terakhir, digambarkan tentang tahapan bagaimana seorang *user* mengakses *tools* manage data dan apa saja yang dapat dilakukan pada tahap tersebut.

Use Case Diagram menggambarkan hubungan interaksi antara aktor dan sistem. Dengan kata lain, menggambarkan fungsional yang diharapkan dari sebuah sistem. *Use case* bertujuan untuk mempresentasikan interaksi antara aktor dengan sistem. *Use Case Diagram* dapat dilihat pada Gambar 4.

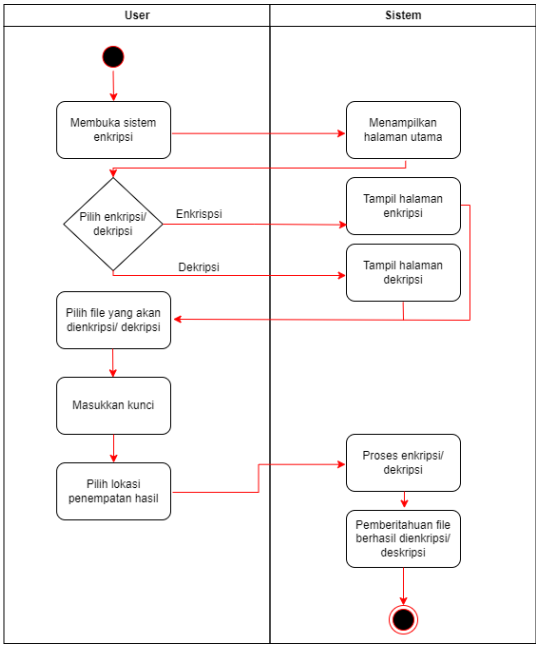


Gambar 4 *Use Case Diagram*

User pada sistem memiliki beberapa interaksi yang dapat dilakukan antaranya *login* dimana *user* dapat memakai sistem apabila sudah *login* terlebih dahulu. *User* juga dapat meninput *file* yang digunakan untuk proses enkripsi dan dekripsi. Lalu, *user* dapat melakukan manajemen *file* yang telah diolah dengan sistem.

Activity Diagram sistem enkripsi dapat dilihat pada Gambar 5.

e-ISSN 2961-9009
p-ISSN 2963-1289



Gambar 5. *Activity Diagram*

Pada bagian *activity diagram* proses enkripsi dan dekripsi, bagi *user* yang udah login yang bisa membuka halaman enkripsi dan dekripsi. Setelah tampil halaman enkripsi *user* dapat memilih file yang akan dienkripsi dan memasukkan kunci yang akan digunakan. Begitu juga dengan yang deskripsi. Setelah *user* memsaukkan file dan kunci enkripsi dan dekripsi dapat dilakukan, hasil akan keluar setelah prosesnya selesai

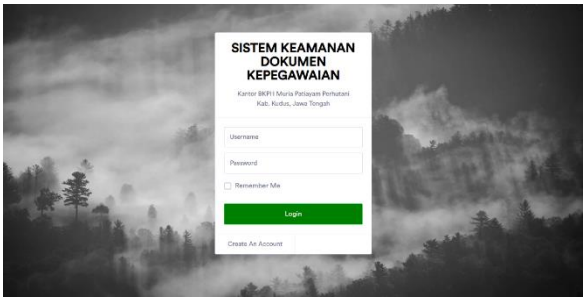
HASIL DAN PEMBAHASAN

A. Implementasi Sistem

Implementasi adalah penerapan fungsionalitas sistem yang terencana dengan baik, berdasarkan analisis dan perencanaan sistem yang sebelumnya dilakukan dalam bahasa pemrograman. Implementasi ini menjelaskan pembahasan hasil implementasi sistem. Implementasi sistem adalah tahap dimana implementasi sistem siap digunakan atau operasional.

1. Halaman *Login*

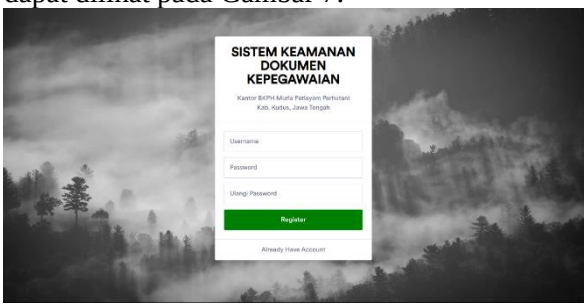
Halaman *login* merupakan halaman ketika program akan dijalanakan. Dalam halaman ini *user* harus menginputkan *user*name dan password untuk masuk kedalam sistem. Halaman *login* dapat dilihat pada Gambar 6.



Gambar 6. Halaman *Login*

2. Halaman *Register*

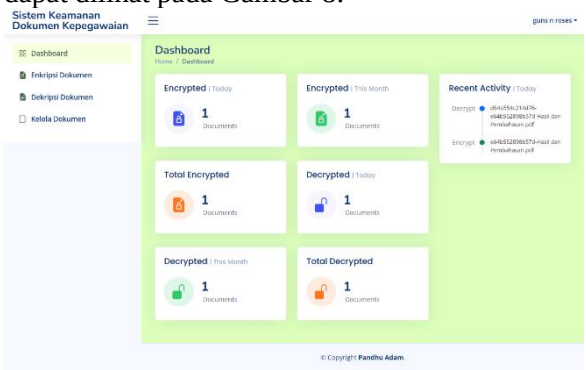
Daftar akun dilakukan oleh *user* yang belum memiliki akun untuk menggunakan sistem. Akun yang didaftar adalah akun yang belum pernah terdaftar pada sistem. Halaman daftar dapat dilihat pada Gambar 7.



Gambar 7. Halaman *Register*

3. Halaman *Dashboard*

Halaman *dashboard* merupakan halaman awal
saat dimana pengguna berhasil masuk kedalam sistem. Dalam halaman ini menampilkan menu-menu yang disediakan. Halaman *dashboard* dapat dilihat pada Gambar 8.

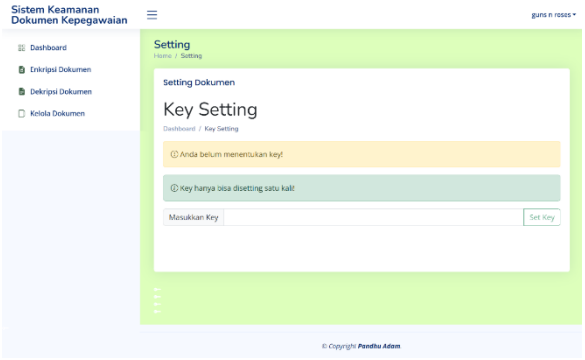


Gambar 8. Halaman *Dashboard*

4. Halaman *Setting*

Halaman *setting* merupakan halaman dimana pengguna melakukan *setting* pada *key user*. Sebelum melakukan enkripsi dokumen, pengguna diharuskan menentukan *key* terlebih dahulu. Halaman *setting* dapat dilihat pada Gambar 9.

e-ISSN 2961-9009
p-ISSN 2963-1289



Gambar 9. Halaman *Setting*

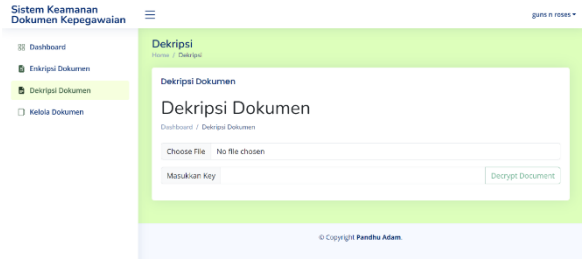
5. Halaman Enkripsi

Halaman enkripsi merupakan halaman dimana pengguna dapat mengunggah data yang akan di enkripsi menggunakan sistem ini. Halaman Enkripsi Data dapat dilihat pada Gambar 10.

Gambar 10. Halaman Enkripsi

6. Halaman Dekripsi

Halaman dekripsi data merupakan halaman dimana pengguna dapat mengunggah data yang akan di dekripsi menggunakan sistem ini. Halaman dekripsi dapat dilihat pada Gambar 11.



Gambar 11. Halaman Dekripsi

7. Halaman Kelola Data

Halaman kelola data merupakan halaman yang digunakan untuk mengelola data hasil enkripsi maupun dekripsi dokumen kepegawaian. Halaman Kelola Data dapat dilihat pada Gambar 12.

Gambar 12. Halaman Kelola Data

KESIMPULAN

Dari penelitian ini dapat disimpulkan bahwa sistem keamanan dokumen menggunakan metode kriptografi AES-256 dan Vigenere Chiper dapat membantu pengamanan dokumen kepegawaian.

Adanya sistem ini terbukti bahwa orang yang tidak memiliki kepentingan dan tidak mengetahui *key* enkripsi yang digunakan tidak dapat mengakses dokumen kepegawaian yang dienkripsi.

ACKNOWLEDGEMENTS

Paper ini adalah hasil penelitian tugas akhir mahasiswa.

DAFTAR PUSTAKA

Al-Khowarizmi. (2021). Pengantar Teknologi Informasi. Diambil dari https://www.google.co.id/books/edition/Pengantar_Teknologi_Informasi_Dalam_Perk/pkNDEAAAQBAJ?hl=id&gbpv=1&dq=buku+vigenere+cipher&pg=PT79&printsec=frontcover

Ardiyansah, D., Pahlevi, O., & Santoso, T. (2021). Implementasi Metode Prototyping pada Sistem Informasi Pengadaan Barang Cetakan Berbasis Web. Hexagon Jurnal Teknik Dan Sains, 2(2), 17–22.

Budi, dkk., (2019). Pengamanan File Dokumen Menggunakan Kombinasi Metode Subtitusi Dan Vigenere Cipher. ILKOM Jurnal Ilmiah, 11(3), 222–230.

Mulyawan, R. (2022). Memahami Pengertian Data Security: Apa itu Keamanan Data? Tujuan, Fungsi, Manfaat, Jenis, Macam, Contoh serta Kenapa itu Penting!

Rifqimulyawan.Com/.

Pressman, R. S. (2015). Rekayasa Perangkat Lunak: Pendekatan Praktisi Buku I. Yogyakarta. *Indonesia: Penerbit Andi*.

Rahmatuloh dkk. (2022). Rancang Bangun Sistem Informasi Jasa Pengiriman Barang Pada PT. Haluan Indah Transporindo Berbasis Web. 14

Rodin. R. (2021). Teori dan Praktik Pengorganisasian Dokumen. Diambil dari https://www.google.co.id/books/edition/Dasar_Dasar_Organisasi_Informasi_Teori_d/MJxxEAAAQBAJ?hl=id&gbpv=1&dq=buku+dokumen&pg=PA3&printsec=frontcover

Sanjaya, R. D. (2020). Sistem Informasi Kepegawaian Berbasis Web Pada PT. Tiga Berkah Syariah. Elibrary.Unikom.Ac.Id/.

Saputro, A. C. (2020). Perancangan Aplikasi Penyewaan Mobil Berbasis Android Pada CV GAP Ttansport Tugas Akhir.

Wiharto, Y., & Irawan, A. (2018). Enkripsi Data Menggunakan AES 256. 7(2).