P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 7 No. 1, Maret, 2026, Hal. 30-36

PENERAPAN KRIPTOGRAFI AES 256 CBC UNTUK KEAMANAN DATA DI SEKRETARIAT DAERAH LAMPUNG TENGAH

Muhammad Fadly Afsi[1], Dedi Irawan[2], Mujito[3]
[1,2,3]Program Studi Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro

[1,2,3]Jalan Gatot Subroto, Yosodadi, kec. Batanghari, kota Metro, Lampung 34381, Indonesia
[1]fadlyafsi10@gmail.com, [2]dedi.mti@gmail.com, [3]mujito@ummetro.ac.id

ABSTRAK: Keamanan data menjadi aspek penting dalam lingkungan pemerintahan yang mengelola dokumen sensitif. Penelitian ini dilakukan di Kantor Pembangunan Sekretariat Daerah Lampung Tengah guna merancang sistem perlindungan dokumen dengan menggunakan teknik kriptografi AES-256-CBC. Sistem ini dikembangkan menggunakan pendekatan kualitatif deskriptif, metode pengembangan SDLC, serta diuji dengan Black-Box dan Beta Testing. Sistem dibangun berbasis PHP dan HTML dan dijalankan melalui PHP Desktop. Hasil dari penelitian ini menunjukkan bahwa dokumen dapat dienkripsi dan disimpan dengan aman di Google Drive, hanya dapat diakses oleh pengguna yang memiliki hak dan kunci akses. Dengan penerapan sistem ini, keamanan informasi meningkat dan proses kerja menjadi lebih efisien.

Kata kunci: Kriptografi, Keamanan Data, AES-256-CBC, Enkripsi Dokumen, Google Drive

ABSTRACT**:** *Data security is essential in government institutions managing confidential documents. This study was conducted at the Development Office of the Regional Secretariat of Central Lampung to design a secure document protection system using AES-256-CBC cryptographic techniques. The system was developed using a descriptive qualitative approach, SDLC development method, and tested with Black-Box and Beta Testing. It was built using PHP and HTML and run via PHP Desktop. The results showed that documents can be securely encrypted and stored on Google Drive, accessible only to authorized users with proper decryption keys. This implementation enhances information security and supports work efficiency.*

Keywords*: Cryptography*, Data *Security*, AES-256-CBC, Document *Encryption*, Google Drive

PENDAHULUAN

Di era digital saat ini, keamanan informasi menjadi hal yang sangat penting, terutama dalam lingkungan instansi pemerintahan yang mengelola berbagai dokumen penting dan bersifat rahasia. Salah satu lembaga yang memiliki tantangan dalam menjaga keamanan data adalah Kantor Pembangunan Sekretariat Daerah Lampung Tengah. Dalam praktiknya, kantor ini banyak mengelola dokumen strategis seperti rencana pembangunan, anggaran, dan laporan evaluasi proyek. Namun, pada tahun 2020 pernah terjadi insiden kebocoran data akibat pengiriman dokumen melalui email yang tidak terenkripsi. Hal ini menunjukkan bahwa

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 7 No. 1, Agustus, 2025, Hal. 1-6

perlindungan data yang memadai belum diterapkan secara optimal dan menimbulkan risiko serius terhadap kelancaran program pembangunan daerah.Untuk mengatasi permasalahan tersebut, dibutuhkan sistem keamanan dokumen yang andal dan terotomatisasi. Salah satu pendekatan yang dapat digunakan adalah penerapan teknik kriptografi, khususnya algoritma AES (*Advanced Encryption Standard*) dengan mode CBC (*Cipher Block Chaining*). AES-256-CBC merupakan algoritma enkripsi simetris yang telah terbukti kuat dan efisien dalam mengamankan informasi digital. Selain itu, integrasi sistem dengan penyimpanan cloud seperti Google Drive juga diperlukan agar dokumen dapat diakses secara fleksibel dari berbagai lokasi oleh pengguna yang berwenang.

Berdasarkan permasalahan tersebut, penelitian ini dilakukan dengan tujuan untuk menerapkan teknik kriptografi AES-256-CBC dalam pengamanan dokumen pada Kantor Pembangunan Sekretariat Daerah Lampung Tengah serta mengintegrasikan sistem penyimpanan cloud guna mendukung efisiensi kerja staf. Penelitian ini menggunakan pendekatan kualitatif deskriptif, dengan metode pengembangan perangkat lunak SDLC (*System Development Life Cycle*) dan pengujian menggunakan *Black-Box Testing* serta *Beta Testing.*

Beberapa teori yang mendasari penelitian ini antara lain konsep keamanan data, kriptografi, AES-256-CBC, serta teknologi penyimpanan cloud. Kajian dari Santoso (2023) menekankan pentingnya pengamanan data terhadap akses tidak sah menggunakan enkripsi, sedangkan penelitian Wicaksono (2023) menunjukkan bahwa AES-256 mampu memberikan perlindungan yang kuat untuk dokumen digital. Studi serupa juga dilakukan oleh Dandhi Aldianto (2023) yang membandingkan tingkat keamanan dari berbagai panjang kunci AES dan merekomendasikan penggunaan AES-256 untuk data sangat sensitif.Dengan landasan teori dan hasil kajian sebelumnya tersebut, sistem yang dibangun dalam penelitian ini diharapkan mampu memberikan solusi praktis dan aman dalam pengelolaan dokumen digital, khususnya di lingkungan pemerintahan. Pendekatan ini tidak hanya menjawab permasalahan teknis terkait keamanan, tetapi juga mendukung pengembangan ilmu komputer dalam penerapan teknologi informasi yang berdampak langsung pada efisiensi layanan publik.

KAJIAN PUSTAKA DAN LANDASAN TEORI

Keamanan Data

Menurut Cindy Vania (2023: 656) menarik kesimpulan sebagai berikut: Keamanan data atau data security merupakan prosedur untuk melakukan perlindungan terhadap data dari kerusakan data baik secara disengaja ataupun tidak disengaja, modifikasi data yang tidak dilakukan oleh pihak yang memiliki wewenang dan kepentingan serta penyebaran data tanpa persetujuan pemilikdata dalam kondisi apapun, baik sengaja ataupun tidak disengaja, dengan mempertimbangkan peraturan dan regulasi yang berlaku.

Enkripsi

Menurut Schneier (2020: 45-67) menarik kesimpulan sebagai berikut: enkripsi memainkan peran kunci dalam menjaga integritas dan kerahasiaan data, memungkinkan individu dan organisasi untuk melindungi informasi sensitif dari pengintaian dan akses yang tidak sah. Dengan semakin meningkatnya jumlah data yang disimpan dan ditransmisikan

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 7 No. 1, Agustus, 2025, Hal. 1-6

secara online, risiko terhadap keamanan informasi juga meningkat. Hal ini menjadikan enkripsi sebagai metode yang esensial untuk melindungi data dari berbagai ancaman, termasuk serangan siber, pencurian identitas, dan kebocoran informasi.

Dekripsi

Menurut Schneier (2020:45-67) menarik kesimpulan sebagai berikut: Dekripsi adalah langkah kunci dalam sistem kriptografi, di mana data yang aman dapat dipulihkan untuk digunakan setelah melalui proses enkripsi. Dalam situasi di mana data perlu dibagikan antara pihak-pihak yang memiliki otoritas tertentu, dekripsi memainkan peran vital untuk memastikan bahwa informasi yang sensitif dapat diakses dengan cara yang aman dan terkendali.

***Advanced Encryption Standard* (AES)**

Menurut Wicaksono (2023: 15-40) menarik kesimpulan sebagai berikut: AES menjadi standar enkripsi yang diadopsi secara luas karena kecepatan, fleksibilitas, dan kemampuannya dalam menangani data dengan volume besar tanpa mengurangi tingkat keamanan. Dengan AES, data dapat terlindungi dari akses tidak sah, baik saat ditransmisikan maupun disimpan.

***Cipher Block Chaining* (CBC)**

Menurut Melani Afsari (2022: 75) menarik kesimpulan sebagai berikut: Proses enkripsi dan dekripsi Cipher Block Chaining memerlukan waktu yang singkat karna metode Cipher Block Chaining (CBC) memiliki kecepatan dan efisiensi yang lebih tinggi dan dinilai lebih mudah di implementasikan. Operasi Cipher Block Chaining (CBC) merupakan algoritma moderen yang beroperasi pada level bit (0 atau 1) maupun sekelompok atau blok bit dan bukan karakter.

Penyimpanan Cloud (Google Drive)

Menurut Pratama (2023: 90-110) menarik kesimpulan sebagai berikut: Google Drive menawarkan kemudahan bagi pengguna dalam menyimpan dan mengakses data di mana saja dan kapan saja. Penyimpanan (*cloud*) ini mendukung kolaborasi *real-time* dan memungkinkan berbagai file diakses dan diedit bersama secara simultan, yang sangat bermanfaat bagi lingkungan kerja berbasis tim dan Google Drive juga memilki kelebihan dan kekurangan mulai dari akses dan penyimpanan.

PHP (*Hypertext Preprocessor*)

Menurut Pratama (2023: 88-110) menarik kesimpulan sebagai berikut: PHP menawarkan fleksibilitas dalam pengembangan aplikasi web, dengan dukungan komunitas yang luas dan dokumentasi yang tersedia secara gratis Hal ini menjadikan PHP pilihan utama dalam membangun sistem manajemen konten, situs *e-commerce*, dan aplikasi berbasis web lainnya.

HTML (*HyperText Markup Language*)

Menurut Pratama (2023: 32-50) menarik kesimpulan sebagai berikut: HTML memberikan fondasi penting dalam pembuatan web karena memungkinkan pengembang untuk menampilkan konten yang terstruktur secara rapi di berbagai perangkat. Elemen-elemen HTML, seperti <*header*>, <*nav*>, <*main*>, dan <*footer*>, membantu memisahkan. bagian-bagian halaman, yang meningkatkan keterbacaan dan aksesibilitas situs web.

Base64

Menurut Pratama (2023: 111-120) menarik kesimpulan sebagai berikut: Base64 sangat membantu dalam mengamankan dan menyamarkan data mentah, karena hasil *encoding*-nya tidak langsung terbaca oleh manusia. Meskipun

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 7 No. 1, Agustus, 2025, Hal. 1-6

bukan metode enkripsi, Base64 mampu menyederhanakan pengiriman file atau data melalui jaringan dengan mengubah karakter biner menjadi teks standar. *Base*64 juga memiliki kelebihan dari segi kompatibilitas lintas sistem dan platform, namun memiliki kekurangan seperti ukuran data hasil encoding yang lebih besar dibandingkan ukuran aslinya, sehingga kurang efisien untuk file berukuran besar.

Notepad ++

Menurut Lee (2021: 18-30) menarik kesimpulan sebagai berikut: Kemampuan *Notepad*++ untuk mendukung berbagai *plugin* membuatnya sangat fleksibel untuk kebutuhan yang berbeda, dari analisis teks sederhana hingga pengembangan web kompleks. Fleksibilitas ini menjadikannya alat yang disukai baik oleh profesional maupun pemula dalam bidang pemrograman.

PHP Desktop Chrome 57.0 RC versi PHP 7.1.3 Menurut Pratama (2023: 88-105) menarik kesimpulan sebagai berikut:

PHP *Desktop* menawarkan fleksibilitas bagi pengembang yang ingin membangun aplikasi desktop dengan teknologi *web*. Dengan memanfaatkan *Chrome* sebagai peramban bawaan, PHP Desktop memungkinkan aplikasi untuk memiliki antarmuka yang modern dan mendukung fitur HTML5 dan *CSS*3. Penggunaan PHP 7.1.3 juga memberikan peningkatan performa dan keamanan dalam eksekusi kode PHP.

***Software Development Life Cycle* (SDLC)**

Menurut Pratama (2023: 45-65) menarik kesimpulan sebagai berikut: SDLC memberikan struktur yang jelas dan terorganisir dalam pengembangan perangkat lunak. Dengan mengikuti tahapan SDLC, pengembang dapat memastikan bahwa setiap aspek dari proyek diperhatikan, mulai dari perencanaan hingga pemeliharaan. Hal ini tidak hanya meningkatkan kualitas perangkat lunak, tetapi juga mengurangi risiko kesalahan.

Black-Box Testing

Menurut Pratama (2023: 60-80) menarik kesimpulan sebagai berikut : *Black-Box Testing* sangat efektif untuk memastikan bahwa perangkat lunak berfungsi sesuai dengan kebutuhan pengguna, terutama dalam hal validasi *input* dan *output*. Melalui pengujian ini, penguji dapat menemukan berbagai *bug* atau *error* yang mungkin terjadi pada antarmuka pengguna, validasi *input*, atau perhitungan *output* tanpa memeriksa kode sumber.

Beta Testing

Menurut Pressman (2020: 180-220) menarik kesimpulan sebagai berikut: *Beta testing* adalah proses pengujian yang melibatkan pengguna eksternal untuk memberikan umpan balik tentang aplikasi atau perangkat lunak yang hampir selesai. Pengujian ini memungkinkan pengembang mengetahui bagaimana perangkat lunak berfungsi.

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk menggambarkan secara sistematis dan faktual mengenai kondisi di lapangan terkait kebutuhan keamanan dokumen di Kantor Pembangunan Sekretariat Daerah Lampung Tengah. Rancangan penelitian mengacu pada model System Development Life Cycle (SDLC) yang terdiri dari tahapan perencanaan, analisis, desain, implementasi, pengujian, dan pemeliharaan.

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 7 No. 1, Agustus, 2025, Hal. 1-6

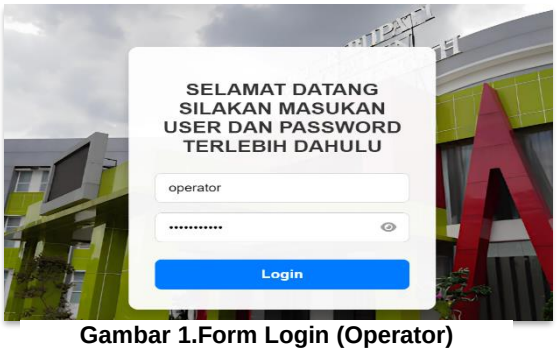
a. Pengumpulan Data
Dilakukan dengan beberapa teknik yaitu observasi langsung terhadap aktivitas pengelolaan dokumen, wawancara dengan pegawai terkait, serta studi dokumentasi terhadap data dan arsip digital. Selain itu, dilakukan kajian pustaka untuk memperoleh teori yang relevan terkait kriptografi, keamanan data, algoritmaAES-256-CBC,dancloud.
b. Penelitian
Dilaksanakan di Kantor Pembangunan Sekretariat Daerah Kabupaten Lampung Tengah selama tiga bulan, yaitu dari bulan Januari hingga Maret 2025. Dalam proses pengembangan sistem, digunakan bahasa pemrograman PHP dan HTML, serta tools seperti Notepad++ dan PHPDesktop.
c. Data Yang Diperoleh
Dianalisis secara deskriptif melalui tahapan identifikasi kebutuhan, perancangan sistem, implementasi algoritma enkripsi AES-256-CBC, hingga proses pengujian menggunakan metode *Black-Box Testing* dan Beta Testing. Analisis ini digunakan untuk menilai keandalan sistem dalam mengamankan dokumen, kemudahan penggunaan sistem oleh staf, serta efektivitas penyimpanan dan pengaksesan data melalui Google Drive.

HASIL DAN PEMBAHASAN

Setelah perancangan sistem dilakukan, berikut ini adalah hasil implementasi sistem keamanan dokumen berbasis aplikasi web yang dibangun menggunakan bahasa pemrograman PHP dan HTML, serta dijalankan melalui PHP Desktop. Sistem ini menggunakan algoritma kriptografi AES-256-CBC untuk proses enkripsi dan dekripsi file. Di bawah ini merupakan tampilan hasil implementasi antarmuka (interface) sistem setelah proses desain dan pengembangan dilakukan:

Tampilan Login Operator

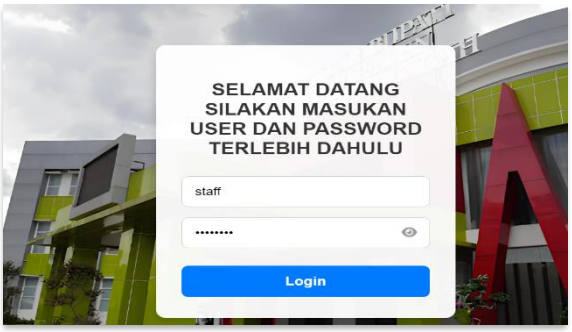
Pada bagian form login operator, operator login menggunakan *user* dan *password.*



Gambar 1.Form Login (Operator)
(Sumber, Penulis 2025)

Tampilan Login Staf

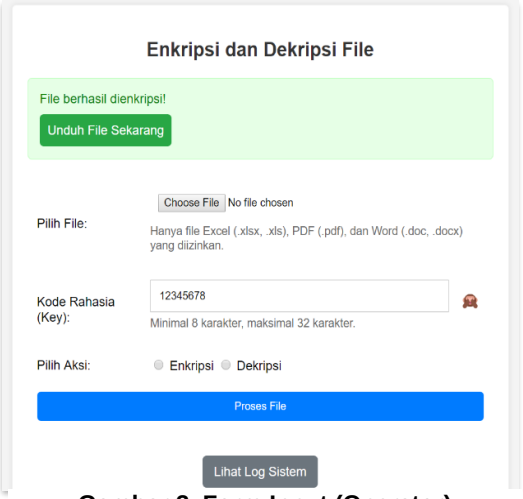
Pada bagian form login staf, staf login menggunakan *user* dan *password*.



Gambar 2.Form Login (Staf)
(Sumber, Penulis 2025)

Form input (Operator)

pada bagian form input operator, operator dapat melakukan enkripsi dan dekripsi.

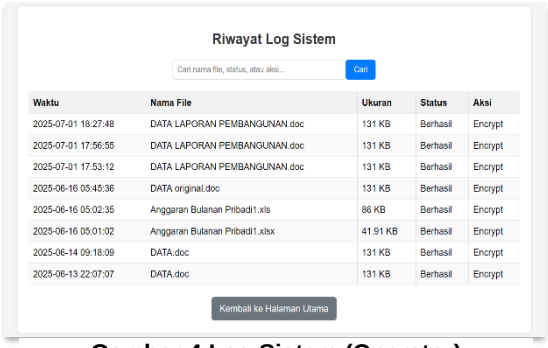


Gambar 3. Form Input (Operator)
(Sumber, Penulis 2025)

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 7 No. 1, Agustus, 2025, Hal. 1-6

Log Sistem (Operator)

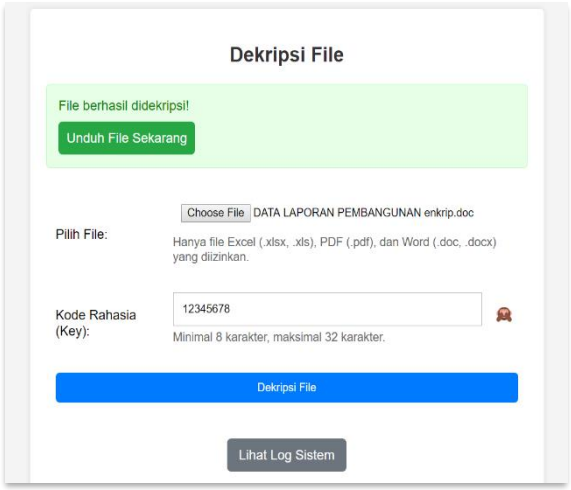
Pada bagian log sistem operator, merupakan riwayat atau hasil setelah enkripsi akan di rekam dalam log sistem terdiri dari nama file,waktu, tanggal, ukuran, status dan aksi (enkripsi).



Gambar 4.Log Sistem (Operator)
(Sumber, Penulis 2025)

Form Input (Staf)

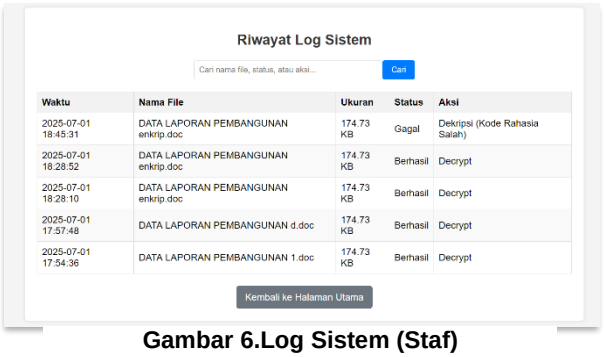
Pada bagian form input staf, operator dapat melakukan dekripsi



Gambar 5.Form Input (Staf)
(Sumber, Penulis 2025)

Log Sistem (Staf)

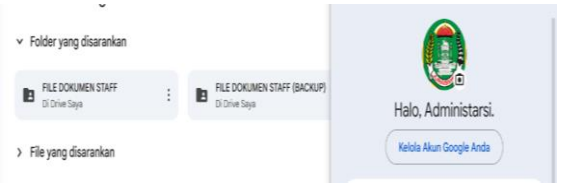
Pada bagian log sistem staf, merupakan riwayat atau hasil setelah dekripsi akan di rekam dalam log sistem terdiri dari nama file,waktu, tanggal, ukuran, status dan aksi (dekripsi).



Gambar 6.Log Sistem (Staf)
(Sumber, Penulis 2025)

Penyimpanan Google Drive

pada bagian penyimpanan Google Drive, merupakan tempat hasil enkripsi oleh operator dan dibuat 2 folder yaitu “file dokumen staf dan “file dokumen staf (*backup*).



Gambar 7.Penyimpanan Dokumen
(Sumber, Penulis 2025)

KESIMPULAN

Setelah melakukan kajian penelitian di Kantor Sekretariat Daerah Lampung Tengah, khususnya pada bagian pembangunan, penulis berhasil membangun sebuah sistem keamanan dokumen berbasis aplikasi web dengan menerapkan algoritma kriptografi AES-256-CBC. Penelitian menggunakan metode SDLC (*System Development Life Cycle*) sebagai pendekatan perancangan sistem serta diuji menggunakan metode pengujian *Black-Box* dan *Beta Testing* agar sistem berfungsi dengan baik dan optimal. Penulis menyimpulkan bahwa tujuan penelitian, yaitu menciptakan sistem keamanan dokumen menggunakan teknik kriptografi AES-256-CBC untuk melindungi data penting, telah tercapai. Sistem ini memberikan solusi praktis bagi pegawai

dalam menjaga kerahasiaan dan integritas dokumen penting yang berkaitan dengan pembangunan di daerah.

Berdasarkan penelitian tersebut, kesimpulan yang dapat diambil adalah sebagai berikut:

1. Dengan diterapkannya sistem keamanan, maka proses perlindungan terhadap dokumen penting di bagian kantor pembangunan menjadi lebih terjamin dan terlindungi dari akses tidak sah.
2. Sistem yang berbasis aplikasi web memudahkan pegawai dalam melakukan proses enkripsi dan dekripsi dokumen di berbagai perangkat tanpa memerlukan instalasi khusus.
3. Algoritma yang digunakan, yaitu AES-256-CBC, merupakan standar enkripsi tingkat tinggi yang banyak digunakan secara global dan telah terbukti kuat dalam menjaga keamanan data digital.

REFRENSI

[1.] Afsari, M., Mulyana, D. I., Damaiyanti, A., & Sa'adah, N. (2022). Implementasi mode operasi kombinasi cipher block chaining dan metode LSB-1 pada pengamanan data text. *Jurnal Pendidikan Sains dan Komputer, 2*(1), 75.

[2.] Lee, J. (2021). Notepad++: Fleksibilitas dan penggunaannya dalam pemrograman. *Jurnal Programming Tools, 9*(2), 18–30.

[3.] Pratama, A. (2023). PHP desktop: Pengembangan aplikasi desktop dengan teknologi web. *Jurnal Web Development, 14*(1), 88–105.

[4.] Pratama, A. (2023). SDLC dalam pengembangan perangkat lunak: Struktur dan manfaat. *Jurnal Software Engineering, 11*(2), 45–65.

[5.] Pratama, A. (2023). Pengujian perangkat lunak: Black-box testing dan keefektifannya. *Jurnal Software Testing, 14*(4), 60–80.

[6.] Pratama, A. R. (2023). Implementasi encoding Base64 untuk keamanan data. *Jurnal Keamanan Informasi, 12*(1), 111–120.

[7.] Pratama, F. (2023). Manajemen data digital di era cloud. *Jurnal Cloud Data Management, 14*(2), 90–110.

[8.] Pratama, R. (2023). Pemrograman web dengan PHP. *Jurnal Web Applications, 15*(3), 88–110.

[9.] Pratama, R. (2023). Pengembangan web dengan HTML: Struktur dan aksesibilitas dalam desain web. *Jurnal Web Design, 15*(4), 32–50.

[10.] Pressman, R. S. (2020). Software engineering: A practitioner's approach. *Jurnal Software Development Practices, 13*(2), 180–220.

[11.] Schneier, B. (2020). Cryptography engineering: Design principles and practical applications. *Jurnal Cryptography, 8*(2), 45–67.

[12.] Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia, 2*(3), 656.

[13.] Wicaksono, A. (2023). Keamanan data dengan enkripsi AES. *Journal of AES Standards, 16*(3), 15–40.