INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v21i1.8720

VOL. 21. NO. 1 AGUSTUS 2026
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

PENGAMANAN DATA PELANGGAN SISTEM INFORMASI PROVIDER WIFI MENGGUNAKAN ALGORITMA AES-128 MODE CIPHER BLOCK CHAINING

Muhammad Andara Ghazy Ar Ramadhan[1*]; Ismail Abdurrozzaq Zulkarnain[2]; Adi Fajaryanto Cobantoro[3]

Program Studi Teknik Informatika[1,2,3]
Fakultas Teknik Universitas Muhammadiyah Ponorogo, Ponorogo, Indonesia[123]
https://teknik.umpo.ac.id/[1,2,3]
andaraghazy@gmail.com[1*], ismail@umpo.ac.id[2], adifajaryanto@umpo.ac.id[3]

(*) Corresponding Author

Abstract— *The increasing use of web-based information systems by Internet Service Providers (ISPs) has increased the need to protect customers' personal data from unauthorized access and misuse. This study aims to implement the Advanced Encryption Standard (AES-128) algorithm in Cipher Block Chaining (CBC) mode to improve customer data security in a web-based WiFi provider information system. The system was developed using the Waterfall method, including requirement analysis, system design, implementation, testing, and maintenance. Customer data were encrypted before being stored in the database and decrypted when users with access rights can view it. System validation was conducted using White Box Testing with the Path Testing technique. Based on the test results, the plaintext "ANDARA1234567890" can be processed into the ciphertext "539E82687FC3424ADA78E95A877AE37E7DE45E3AEA0B76E97D26D3C15152E74B" using the AES-128 algorithm in CBC mode. Through the decryption process, the ciphertext can be restored to its original plaintext form without altering the data, while all independent paths can be executed according to the logic flow designed for the program. Therefore, the implementation of AES-128 in CBC mode supports the confidentiality of customer data in a web-based WiFi provider information system through the applied encryption mechanism.*

Keywords*: AES-128, Cipher Block Chaining, Cryptography, Customer Data Security, Web-Based Information System.*

Abstrak— Pemanfaatan sistem informasi berbasis web pada penyedia layanan internet semakin meningkatkan kebutuhan akan perlindungan data pelanggan dari akses tidak sah dan penyalahgunaan informasi. Penelitian ini bertujuan mengimplementasikan algoritma *Advanced Encryption Standard* (AES-128) menggunakan *mode Cipher Block Chaining* (CBC) untuk meningkatkan keamanan data pelanggan pada sistem informasi provider layanan WiFi berbasis web. Pengembangan sistem dilakukan menggunakan metode *Waterfall* yang meliputi analisis kebutuhan, perancangan sistem, implementasi, pengujian, pemeliharaan. Data pelanggan dienkripsi sebelum disimpan di basis data dan didekripsi saat pengguna yang memiliki hak akses dapat melihatnya. Pengujian sistem dilakukan menggunakan *White Box Testing* dengan teknik *Path Testing*. Berdasarkan hasil pengujian, *plaintext* "*ANDARA1234567890"* diproses menjadi *ciphertext* "539E82687FC3424ADA78E95A877AE37E7DE45E3AEA0B76E97D26D3C15152E74B" menggunakan algoritma AES-128 mode CBC. Melalui proses dekripsi, *ciphertext* dapat dipulihkan ke bentuk *plaintext* semula tanpa perubahan data, sementara seluruh *independent path* dapat dijalankan sesuai dengan alur logika program yang telah dirancang. Dengan demikian, penerapan AES-128 mode CBC mendukung perlindungan kerahasiaan data pelanggan pada sistem informasi provider layanan WiFi berbasis web melalui mekanisme enkripsi yang diterapkan.

Kata kunci: AES-128, *Cipher Block Chaining, Keamanan Data, Kriptografi, Sistem Informasi Berbasis Web.*

PENDAHULUAN

Pemanfaatan teknologi informasi telah menjadi bagian penting dalam mendukung aktivitas operasional berbagai sektor, termasuk penyedia layanan internet (*Internet Service Provider*). Digitalisasi proses administrasi memungkinkan pengelolaan data pelanggan dilakukan secara lebih cepat, akurat, dan terintegrasi. Namun, peningkatan penggunaan sistem informasi juga diikuti oleh bertambahnya jumlah data pribadi yang tersimpan dalam basis data. Kondisi tersebut menjadikan keamanan informasi sebagai aspek yang perlu mendapat perhatian karena data pelanggan berpotensi mengalami kebocoran maupun penyalahgunaan apabila tidak dilengkapi dengan mekanisme perlindungan yang memadai (Arif & Nurokhman, 2023); (Ramalinda et al., 2024).

Data pelanggan yang dikelola oleh penyedia layanan internet umumnya mencakup informasi identitas, seperti nama, Nomor Induk Kependudukan (NIK), nomor telepon, serta alamat pemasangan layanan. Informasi tersebut termasuk data pribadi yang harus dijaga kerahasiaannya karena dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab apabila berhasil memperoleh akses terhadap basis data. Selain berpotensi merugikan pelanggan, insiden kebocoran data juga dapat menurunkan tingkat kepercayaan masyarakat terhadap penyedia layanan. Oleh sebab itu, diperlukan mekanisme keamanan yang mampu memberikan perlindungan terhadap data sensitif tanpa mengurangi kemudahan dalam proses pengelolaannya (Assidiq et al., 2024).

Salah satu metode yang banyak diterapkan untuk menjaga kerahasiaan informasi adalah kriptografi. Teknik ini bekerja dengan mengubah data asli (*plaintext*) menjadi bentuk tersandi (*ciphertext*) sehingga informasi hanya dapat dipahami oleh pihak yang memiliki kunci dekripsi. Di antara berbagai algoritma kriptografi simetris, *Advanced Encryption Standard* (AES-128) dikenal memiliki tingkat keamanan yang tinggi serta efisiensi yang baik dalam proses enkripsi maupun dekripsi data.

Penggunaan mode *Cipher Block Chaining* (CBC) semakin memperkuat mekanisme keamanan karena setiap blok data diproses menggunakan *initialization vector*, sehingga menghasilkan *ciphertext* yang berbeda meskipun terdapat kesamaan pada data masukan (Oktavani et al., 2023). Dalam penelitian ini, implementasi AES-128 mode CBC difokuskan untuk menjaga kerahasiaan (confidentiality) data pelanggan melalui mekanisme enkripsi. Penelitian ini tidak mencakup mekanisme autentikasi maupun perlindungan integritas data, sehingga pembahasan difokuskan pada aspek kerahasiaan informasi yang tersimpan dalam basis data. Efektivitas penerapan AES dalam melindungi data juga telah dibuktikan pada berbagai penelitian, seperti (Batau, 2024) yang menunjukkan bahwa implementasi AES mampu meningkatkan keamanan data pelanggan, serta (Gandhara et al., 2025) yang menyatakan bahwa pemilihan algoritma kriptografi perlu disesuaikan dengan karakteristik sistem agar mampu memberikan perlindungan data yang optimal.

Berbagai penelitian telah membuktikan bahwa algoritma AES mampu meningkatkan keamanan informasi pada berbagai jenis sistem. (Priambudi & Mufti, 2023) menerapkan AES-128 untuk melindungi data pada aplikasi berbasis web dan menunjukkan bahwa proses enkripsi mampu menjaga kerahasiaan informasi yang tersimpan. Penelitian lain oleh (Irawan et al., 2023) juga menunjukkan bahwa penerapan AES dapat mengurangi risiko akses tidak sah terhadap data yang berada pada sistem informasi. Selain itu, (Assidiq et al., 2024) mengembangkan mekanisme keamanan dengan mengombinasikan AES dan SHA-3 untuk meningkatkan perlindungan data pada aplikasi berbasis web. Hasil penelitian tersebut menunjukkan bahwa AES merupakan algoritma yang efektif dalam menjaga kerahasiaan informasi digital, meskipun implementasinya masih disesuaikan dengan kebutuhan masing-masing sistem.

Penelitian lain juga menunjukkan bahwa penerapan algoritma kriptografi dan penggunaan metode pengembangan sistem yang terstruktur dapat mendukung keamanan serta kualitas implementasi sistem informasi. (Cobantoro, Wicahyono, et al., 2025) mengimplementasikan algoritma RSA untuk melindungi data pasien pada sistem berbasis web dan menunjukkan bahwa proses enkripsi mampu meningkatkan kerahasiaan informasi dari akses yang tidak berwenang. Sementara itu, (Cobantoro, Islami, et al., 2025) menerapkan metode *Waterfall* pada pengembangan sistem pembayaran berbasis RFID dan memperoleh hasil bahwa tahapan pengembangan yang sistematis mampu menghasilkan sistem yang berjalan sesuai dengan kebutuhan pengguna. Temuan tersebut memperkuat bahwa penerapan algoritma kriptografi yang didukung metode pengembangan yang tepat dapat meningkatkan keamanan sekaligus kualitas implementasi sistem informasi.

Walaupun implementasi AES telah banyak diterapkan pada berbagai penelitian, sebagian besar masih berorientasi pada pengamanan dokumen digital, aplikasi web secara umum,

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v21i1.8720

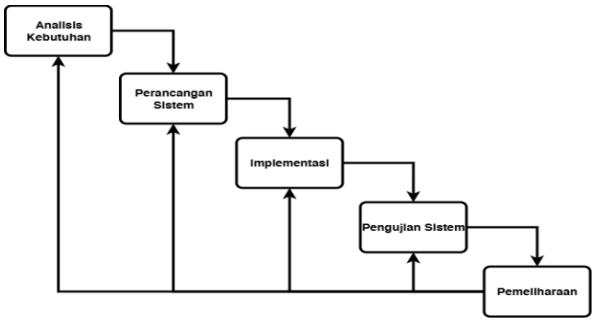
VOL. 21. NO. 1 AGUSTUS 2026
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

maupun sistem transaksi elektronik. Kajian mengenai penerapan AES-128 dengan mode CBC untuk mengamankan data pelanggan pada sistem informasi provider layanan WiFi masih relatif terbatas. Di samping itu, masih terbatas penelitian yang mengintegrasikan mekanisme enkripsi secara langsung pada proses penyimpanan data pelanggan ke dalam basis data sehingga informasi sensitif tetap terlindungi selama proses pengelolaan data. Kondisi tersebut menunjukkan adanya peluang untuk mengembangkan implementasi AES pada sistem informasi yang digunakan oleh penyedia layanan internet.

Atas dasar permasalahan yang telah diuraikan, penelitian ini diarahkan untuk menerapkan algoritma *Advanced Encryption Standard* (AES-128) menggunakan mode *Cipher Block Chaining* (CBC) sebagai mekanisme pengamanan data pelanggan pada sistem informasi provider layanan WiFi berbasis web. Algoritma diterapkan guna melakukan enkripsi data sebelum penyimpanan dalam basis data dan mendekripsinya ketika diakses oleh pengguna yang memiliki hak akses. Implementasi tersebut diharapkan mampu meningkatkan kerahasiaan data pelanggan sekaligus menjadi salah satu alternatif penerapan kriptografi pada sistem informasi penyedia layanan internet.

BAHAN DAN METODE

Metode *Waterfall* digunakan dalam penelitian ini untuk mengembangkan sistem informasi provider layanan WiFi yang berjalan pada platform web dengan menerapkan algoritma AES-128 menggunakan mode CBC sebagai mekanisme pengamanan data pelanggan. Metode *Waterfall* dipilih karena memiliki tahapan pengembangan yang sistematis sehingga prosesnya dapat dilakukan bertahap dari analisis kebutuhan sampai tahap pemeliharaan sistem (Duma & Pusvita, 2023). Penelitian ini dilakukan pada Provider WiFi Zix's Com yang berlokasi di Kabupaten Ponorogo, Jawa Timur, sebagai penyedia layanan internet berbasis WiFi. Sistem informasi pada provider tersebut digunakan untuk mengelola data pelanggan. Pada penelitian ini diterapkan algoritma AES-128 mode CBC untuk meningkatkan keamanan data pelanggan. Tahapan pengembangan sistem yang diterapkan dalam penelitian ditampilkan pada Gambar 1. Merujuk pada Gambar 1, proses pengembangan sistem dilakukan melalui lima tahapan, yaitu analisis kebutuhan, perancangan sistem, implementasi, pengujian sistem, dan pemeliharaan.



Sumber: (Hasil Penelitian, 2026)

Gambar 1: Tahapan Pengembangan Sistem Menggunakan Metode *Waterfall*

Setiap tahapan dilakukan secara berurutan sehingga hasil yang diperoleh pada suatu tahap digunakan sebagai acuan untuk tahap selanjutnya.

Data penelitian diperoleh melalui beberapa teknik berikut.

1. Observasi, dilakukan secara langsung pada provider layanan WiFi Zix's Com untuk memperoleh informasi mengenai proses pengelolaan data pelanggan, mekanisme penyimpanan data, serta alur kerja sistem yang sedang diterapkan. Hasil observasi digunakan untuk mengidentifikasi kebutuhan sistem serta menentukan bagian data yang memerlukan mekanisme pengamanan.
2. Wawancara, dilakukan dengan pemilik provider layanan WiFi Zix's Com untuk mendapatkan informasi terkait kebutuhan sistem, mekanisme pengelolaan data pelanggan, beserta kendala yang dihadapi dalam menjaga keamanan data. Hasil wawancara tersebut digunakan sebagai acuan dalam merancang kebutuhan sistem.
3. Studi Pustaka, dilakukan melalui penelaahan berbagai sumber berupa buku, artikel ilmiah, serta penelitian sebelumnya yang membahas algoritma AES-128, mode CBC, keamanan data, metode *Waterfall*, serta pengembangan sistem informasi berbasis web. Referensi tersebut digunakan sebagai dasar dalam proses perancangan dan implementasi sistem.

Tahapan pengembangan sistem menggunakan metode *Waterfall* dijelaskan sebagai berikut.

1. Analisis Kebutuhan

Tahap analisis kebutuhan ditujukan untuk menentukan kebutuhan fungsional dan nonfungsional sistem berdasarkan hasil observasi serta wawancara. Analisis difokuskan pada mekanisme pengelolaan informasi pelanggan, identifikasi data yang bersifat sensitif, serta kebutuhan penerapan algoritma AES-128 mode

CBC untuk meningkatkan keamanan penyimpanan data pada sistem.

Pada tahap analisis kebutuhan juga dilakukan analisis kerentanan terhadap data pelanggan yang dikelola oleh sistem. Analisis ini bertujuan mengidentifikasi potensi risiko kebocoran data selama proses penyimpanan sehingga ditetapkan kebutuhan penerapan mekanisme enkripsi menggunakan algoritma AES-128 mode CBC untuk menjaga kerahasiaan data pelanggan. Hasil analisis tersebut menjadi dasar pada tahap perancangan dan implementasi sistem.

2. Perancangan Sistem

Tahap perancangan dilaksanakan dengan menyusun rancangan antarmuka pengguna, struktur basis data, serta alur implementasi algoritma AES-128 mode CBC pada sistem informasi. Perancangan ini bertujuan memastikan proses enkripsi dan dekripsi dapat diintegrasikan dengan baik ke dalam sistem tanpa mengubah fungsi utama pengelolaan data pelanggan.

3. Implementasi

Tahap implementasi, sistem dikembangkan menggunakan PHP dan MySQL. Pada proses ini algoritma AES-128 mode CBC diterapkan guna mengenkripsi data pelanggan sebelum data disimpan pada basis data, sementara dekripsi dilakukan saat data diakses kembali oleh pengguna yang berwenang.

4. Pengujian Sistem

Pengujian sistem menerapkan *White Box Testing* melalui teknik *Path Testing* untuk mengevaluasi logika program pada modul autentikasi, proses enkripsi, dan proses dekripsi. Pengujian bertujuan memastikan seluruh jalur program dapat dieksekusi sesuai dengan rancangan sehingga setiap fungsi sistem berjalan dengan baik (Shiddiq, 2022).

5. Pemeliharaan

Tahap Pemeliharaan dilaksanakan setelah sistem berhasil diterapkan dan diuji. Kegiatan dalam tahap tersebut meliputi perbaikan atas kesalahan yang ditemukan selama pengujian serta penyesuaian sistem apabila diperlukan agar tetap dapat digunakan sesuai kebutuhan pengguna.

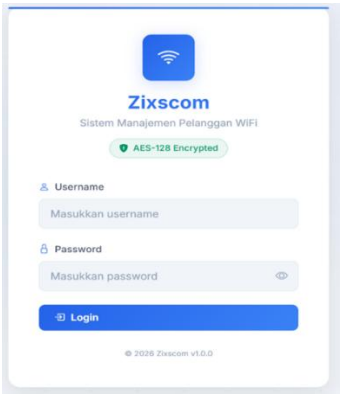
Data dianalisis berdasarkan hasil implementasi dan pengujian yang dilakukan. Hasil pengujian dibandingkan terhadap kebutuhan yang telah ditentukan sebelumnya untuk memastikan setiap fungsi dapat berjalan berdasarkan rancangan. Implementasi algoritma AES-128 mode CBC dinyatakan berhasil apabila data pelanggan dapat diamankan melalui enkripsi sebelum penyimpanan dalam basis data, menghasilkan bentuk *ciphertext* yang tidak dapat dipahami tanpa proses dekripsi, serta dapat dipulihkan menjadi bentuk *plaintext* melalui dekripsi menggunakan *secret key* yang sesuai.

Metode *Waterfall* dipilih karena sistem memiliki kebutuhan yang telah terdefinisi secara jelas sejak awal penelitian dan pengembangan sistem dilaksanakan melalui proses bertahap yang mencakup analisis kebutuhan hingga pengujian. Dalam penelitian ini, aspek keamanan telah dipertimbangkan sejak tahap analisis kebutuhan melalui identifikasi kerentanan dan penentuan kebutuhan mekanisme enkripsi sehingga metode *Waterfall* tetap sesuai dengan ruang lingkup penelitian yang berfokus pada implementasi algoritma AES-128 mode CBC.

HASIL DAN PEMBAHASAN

Implementasi Sistem

Sistem informasi provider layanan WiFi dikembangkan berbasis web dengan PHP sebagai bahasa pemrograman dan MySQL sebagai basis data. Sistem ini digunakan untuk mendukung pengelolaan data pelanggan sekaligus meningkatkan keamanan informasi melalui penerapan algoritma AES-128 dengan mode CBC. Pengguna sistem terdiri atas administrator yang memiliki hak untuk mengelola data pelanggan, paket layanan, pembayaran, serta melakukan proses penyimpanan data yang telah diamankan menggunakan mekanisme enkripsi. Tampilan login pada Gambar 2 digunakan untuk proses autentikasi sebelum pengguna memperoleh akses ke sistem. Sementara itu, Gambar 3 menampilkan halaman dashboard yang memuat rangkuman informasi dan menu utama yang tersedia:

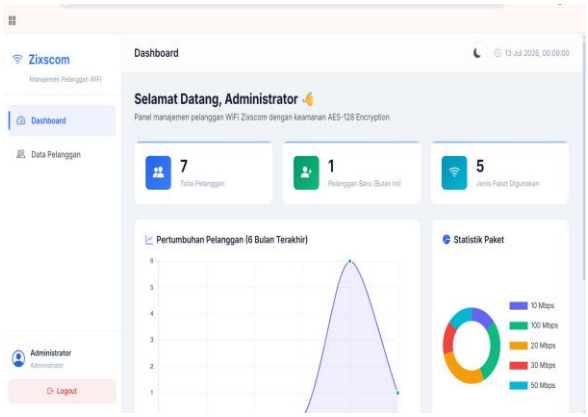


Sumber: (Hasil Penelitian, 2026)

Gambar 2: Tampilan Login Sistem

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v21i1.8720
VOL. 21. NO. 1 AGUSTUS 2026
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

Tampilan login berfungsi sebagai mekanisme autentikasi pengguna dengan memverifikasi username dan password sebelum sistem memberikan hak akses. Proses ini bertujuan membatasi akses sehingga hanya administrator yang terdaftar yang dapat mengelola data pelanggan dan menggunakan seluruh fitur yang tersedia pada sistem.



Sumber: (Hasil Penelitian, 2026)

Gambar 3: Tampilan Dashboard Sistem

Dashboard menampilkan informasi utama yang diperlukan administrator setelah berhasil masuk ke sistem. Halaman ini menyediakan menu navigasi menuju pengelolaan data pelanggan, data paket internet, transaksi pembayaran, data pengguna, serta fitur lainnya yang mendukung operasional provider layanan WiFi.

Selain menyediakan fitur autentikasi dan dashboard, sistem turut dilengkapi bagian menu Data Pelanggan untuk mengelola identitas pelanggan, bagian menu Paket Internet untuk mengatur informasi layanan yang tersedia, menu Pembayaran untuk mencatat transaksi pelanggan, serta menu Pengguna untuk mengelola akun administrator. Pada proses penyimpanan data pelanggan, sistem secara otomatis menerapkan algoritma AES-128 dengan mode CBC sehingga data sensitif tidak disimpan dalam bentuk *plaintext*, melainkan terlebih dahulu dienkripsi sebelum disimpan ke dalam basis data. Dengan mekanisme tersebut, informasi pelanggan tetap dapat dikelola melalui sistem, namun memiliki tingkat kerahasiaan yang lebih baik apabila basis data diakses oleh pihak yang tidak berwenang.

Implementasi Enkripsi Menggunakan AES-128 Mode CBC

Implementasi algoritma AES-128 dengan mode CBC diterapkan pada proses penyimpanan data pelanggan untuk menjaga kerahasiaan informasi yang tersimpan di dalam basis data. Implementasi AES-128 dilakukan melalui serangkaian transformasi berupa tahapan *SubBytes*, *ShiftRows*, *MixColumns*, serta *AddRoundKey* hingga menghasilkan *ciphertext* yang dapat dipulihkan ke bentuk *plaintext* dengan kunci yang tepat (Nugraha & Arifin, 2022). Pada mode CBC, setiap blok *plaintext* diproses secara berantai menggunakan *Initialization Vector* (IV) pada blok pertama dan *ciphertext* dari blok sebelumnya pada blok berikutnya. Mekanisme tersebut dapat menghasilkan *ciphertext* yang berbeda walaupun memiliki *plaintext* dengan nilai yang sama, sehingga mampu meningkatkan tingkat keamanan data dibandingkan mode *Electronic Codebook* (ECB).

Algoritma AES-128 pada penelitian ini diawali dengan proses *Initial AddRoundKey* yang mengombinasikan state awal dengan *round key* menggunakan operasi Exclusive OR (XOR). Selanjutnya proses enkripsi dilanjutkan melalui sembilan ronde utama yang masing-masing terdiri atas proses *SubBytes*, *ShiftRows*, *MixColumns*, serta *AddRoundKey*. Sementara pada ronde terakhir diterapkan proses *SubBytes*, *ShiftRows*, serta *AddRoundKey* tanpa melalui proses *MixColumns* sesuai dengan spesifikasi algoritma AES-128. Setelah seluruh tahapan selesai dilaksanakan, dihasilkan *ciphertext* sebagai keluaran proses enkripsi. Sebelum memasuki tahapan enkripsi AES-128, *plaintext* terlebih dahulu diproses menggunakan metode PKCS#7 *Padding* agar panjang data menjadi kelipatan 16 byte sesuai ukuran blok algoritma AES. Apabila panjang *plaintext* telah tepat 16 byte, metode PKCS#7 tetap menambahkan satu blok *padding* penuh sehingga proses dekripsi dapat mengidentifikasi dan menghapus *padding* secara benar sesuai standar implementasi AES-128 mode CBC.

Tahap awal proses enkripsi dilakukan dengan mengombinasikan blok *plaintext* pertama dengan *Initialization Vector* (IV) menggunakan operasi Exclusive OR (XOR). Proses ini bertujuan menghasilkan state awal yang berbeda sebelum memasuki tahapan inti algoritma AES-128. Operasi XOR pada mode CBC dinyatakan pada Persamaan (1).

$$C_0 = P_0 \otimes IV \quad (1)$$

Keterangan: C_0 merupakan state awal hasil operasi XOR, P_0 adalah blok *plaintext* pertama yang akan dienkripsi, sedangkan *Initialization Vector* (IV) merupakan nilai awal yang digunakan pada mode CBC untuk menghasilkan state yang berbeda pada setiap proses enkripsi.

Berdasarkan implementasi yang dilakukan, proses XOR menghasilkan state awal dalam bentuk heksadesimal yang selanjutnya digunakan sebagai masukan pada proses *SubBytes*. Hasil implementasi proses XOR ditunjukkan pada Tabel 1.

Tabel 1. Hasil Operasi XOR antara *Plaintext* dan *Initialization Vector* (IV)

F7	F8	06	21
8B	56	A2	43
7B	C2	4F	1C
E2	25	4F	55

Sumber: (Hasil Penelitian, 2026)

Tahap *SubBytes* merupakan proses substitusi nonlinier yang mengganti setiap byte pada state menggunakan tabel Substitution Box (S-Box) sehingga menghasilkan nilai baru yang lebih kompleks. Berdasarkan implementasi yang dilakukan, seluruh byte pada state berhasil ditransformasikan menggunakan S-Box, sehingga menghasilkan nilai baru yang akan diproses pada tahap *ShiftRows*. Hasil implementasi proses *SubBytes* ditunjukkan pada Tabel 2.

Tabel 2. Hasil Transformasi *SubBytes*

95	14	FB	6A
98	12	3E	40
7B	79	F2	31
81	43	E5	3C

Sumber: (Hasil Penelitian, 2026)

Tahap *ShiftRows* dilakukan dengan menggeser posisi byte pada setiap baris state. Baris pertama tidak mengalami pergeseran, sedangkan baris kedua, baris ketiga dan keempat secara berurutan digeser ke kiri sebesar satu, dua, dan tiga byte. Berdasarkan implementasi yang dilakukan, proses *ShiftRows* menghasilkan susunan state baru sehingga distribusi data menjadi lebih merata sebelum memasuki tahap *MixColumns*. Hasil implementasi proses *ShiftRows* ditunjukkan pada Tabel 3.

Tabel 3. Hasil Transformasi *ShiftRows*

95	14	FB	6A
12	3E	40	98
F2	31	7B	79
3C	81	43	E5

Sumber: (Hasil Penelitian, 2026)

Tahap *MixColumns* melakukan transformasi pada setiap kolom state menggunakan operasi perkalian polinomial pada medan hingga GF(2^8). Transformasi tersebut dinyatakan pada Persamaan (2).

$$S'(x) = a\,(x) \otimes s(x) \quad (2)$$

Keterangan: $S'(x)$ merupakan state setelah proses *MixColumns*, $a\,(x)$ adalah polinomial konstan yang digunakan dalam transformasi *MixColumns*, $s(x)$ merupakan state sebelum transformasi, sedangkan simbol $\otimes$ menyatakan operasi perkalian polinomial pada medan hingga GF(2^8).

Berdasarkan implementasi yang dilakukan, proses *MixColumns* menghasilkan perubahan nilai pada setiap kolom state sehingga data menjadi lebih kompleks sebelum dikombinasikan dengan *Round Key*. Hasil implementasi proses *MixColumns* ditunjukkan pada Tabel 4.

Tabel 4. Hasil Transformasi *MixColumns*

C9	DA	15	FB
80	BA	B5	2F
3C	D0	88	34
3C	2A	AB	8E

Sumber: (Hasil Penelitian, 2026)

Tahap *AddRoundKey* dilakukan dengan mengombinasikan state hasil transformasi sebelumnya dengan *Round Key* menggunakan operasi XOR sebagaimana ditunjukkan pada Persamaan (3).

$$State' = State \oplus RoundKey \quad (3)$$

Keterangan: State merupakan hasil transformasi sebelum proses *AddRoundKey*, sedangkan *Round Key* merupakan kunci yang dihasilkan melalui proses *key expansion* berdasarkan *secret key* AES-128. Operasi XOR menghasilkan state baru yang digunakan sebagai masukan pada ronde berikutnya. Berdasarkan implementasi yang dilakukan, proses *AddRoundKey* menghasilkan state baru yang selanjutnya diproses hingga seluruh ronde enkripsi selesai dan menghasilkan *ciphertext*. Hasil implementasi proses *AddRoundKey* ditunjukkan pada Tabel 5.

Tabel 5. Hasil Transformasi *AddRoundKey*

55	25	8F	18
CA	9F	E3	48
43	C2	D1	5F
F9	AE	4A	57

Sumber: (Hasil Penelitian, 2026)

Setelah seluruh tahapan enkripsi selesai dilakukan, diperoleh *ciphertext* sebagai hasil akhir penerapan AES-128 mode CBC. Pada implementasi sistem, *secret key* AES-128 digunakan sebagai kunci utama dalam proses enkripsi dan dekripsi, sedangkan *Initialization Vector* (IV) berukuran 16 byte dibangkitkan secara acak pada setiap proses enkripsi sehingga setiap transaksi menggunakan IV yang berbeda. Penggunaan IV yang berbeda bertujuan menghindari dihasilkannya *ciphertext* yang identik pada *plaintext* yang sama serta meningkatkan kerahasiaan data sesuai

VOL. 21. NO. 1 AGUSTUS 2026
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

karakteristik mode CBC. Nilai IV disimpan bersama hasil enkripsi agar dapat digunakan kembali pada proses dekripsi, sedangkan *secret key* digunakan oleh sistem sebagai kunci utama selama proses kriptografi. Nilai *ciphertext* yang diperoleh dapat dilihat pada Tabel 6.

Tabel 6. Hasil Akhir Enkripsi (*Ciphertext*)

Parameter	Nilai
Plaintext	ANDARA1234567890
Secret Key	ZixscomAesKey128
Initialization Vector	B6C53FA3AA17F31735967A79167B2565
Ciphertext	539E82687FC3424ADA78E95A877AE37E7DE45E3AEA0B76E97D26D3C15152E74B

Sumber: (Hasil Penelitian, 2026)

Berdasarkan Tabel 6, data pelanggan berhasil diubah menjadi *ciphertext* dalam format heksadesimal sehingga informasi tidak dapat langsung dibaca tanpa menggunakan *secret key* serta *Initialization Vector* (IV) yang sesuai. Meskipun *plaintext* pada contoh implementasi berukuran 16 byte, *ciphertext* yang dihasilkan berukuran 32 byte karena metode PKCS#7 *Padding* menambahkan satu blok *padding* penuh ketika panjang *plaintext* telah sama dengan ukuran blok AES, yaitu 16 byte. Penambahan *padding* tersebut memungkinkan proses dekripsi mengembalikan *plaintext* ke bentuk semula secara tepat. Pada tahap dekripsi, IV yang digunakan harus identik dengan IV yang digunakan pada tahap enkripsi sehingga *ciphertext* dapat dikembalikan ke bentuk *plaintext* secara tepat.

Proses dekripsi dilakukan menggunakan *secret key* dan *Initialization Vector* (IV) yang sama dengan proses enkripsi. Setelah seluruh tahapan dekripsi selesai dilakukan, *ciphertext* berhasil dikembalikan ke bentuk *plaintext* semula. Hasil pengujian dekripsi pada beberapa sampel data ditunjukkan pada Tabel 7.

Tabel 7. Hasil Akhir Dekripsi

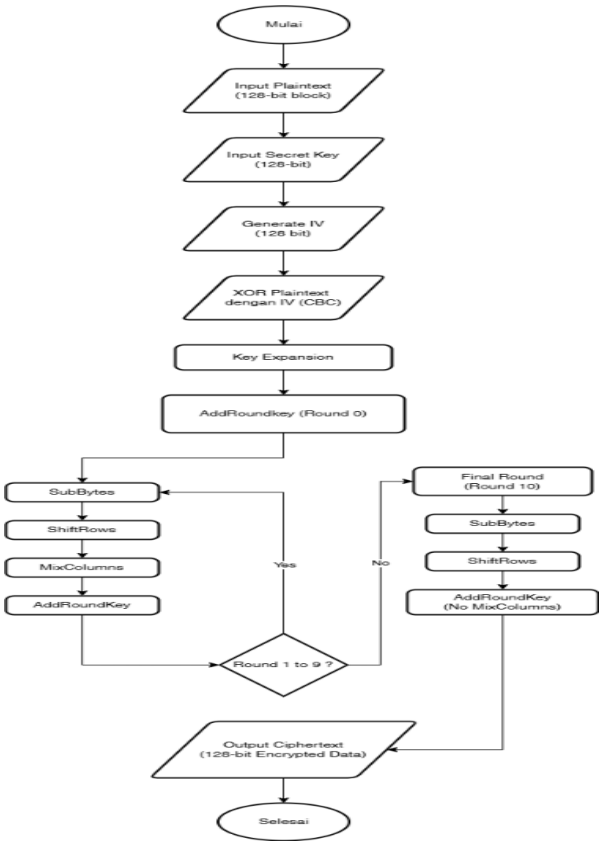
Ciphertext	Plaintext
539E82687FC3424ADA78E95A877AE37E7DE45E3AEA0B76E97D26D3C15152E74B	ANDARA1234567890
55151696186A1EDC79ECE2265EB43D477ABA62A6398873630060AE9201706EFA	Firman Ashr Rozaqulloh
5884319FD7FEFD55221A1F6109528CA5	Hapizh Trisna
4DD774805598AA560A6CA38F3A5A7C614B95C59B98BE4AEF24FDFC092A79770D	Ibnu Rosyida APIP
BA052AB2EAC6C6B348B7E919813006F0	Lalang Bach

Sumber: (Hasil Penelitian, 2026)

Merujuk pada Tabel 7, seluruh *plaintext* berhasil dienkripsi menjadi *ciphertext* menggunakan algoritma AES-128 mode CBC. Selanjutnya, seluruh *ciphertext* berhasil dikembalikan ke bentuk *plaintext* semula tanpa mengalami perubahan data pada proses dekripsi. Hasil tersebut menunjukkan bahwa implementasi algoritma AES-128 mode CBC mampu melakukan proses enkripsi dan dekripsi secara konsisten pada berbagai sampel data, sehingga kerahasiaan data selama proses penyimpanan tetap terjaga dan informasi dapat dipulihkan kembali secara utuh pada proses dekripsi.

Pengujian Sistem

Pengujian sistem menerapkan metode *White Box Testing* melalui teknik *Basis Path Testing* untuk mengevaluasi struktur logika program pada modul login dan modul enkripsi AES-128 mode CBC. Proses pengujian dilakukan dengan menganalisis *flowgraph* pada setiap modul guna menentukan nilai *Cyclomatic Complexity* dan menentukan *independent path* yang akan diuji. Diagram alir proses enkripsi AES-128 mode CBC yang digunakan sebagai acuan dalam penyusunan *flowgraph* ditunjukkan pada Gambar 4.



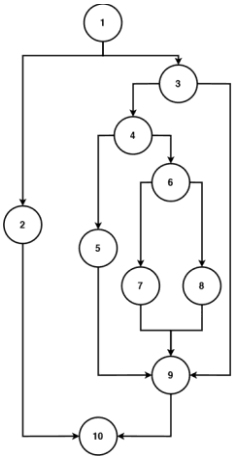
Sumber: (Hasil Penelitian, 2026)

Gambar 4. Diagram Alir Proses Enkripsi AES-128 Mode CBC

VOL. 21. NO. 1 AGUSTUS 2026
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v21i1.8720

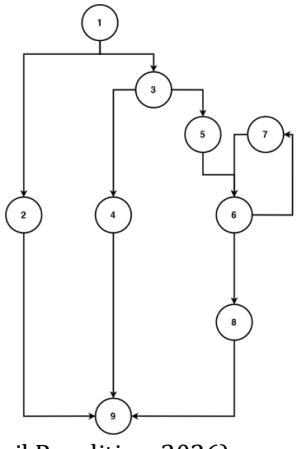
Berdasarkan diagram alir pada Gambar 4, dilakukan pembentukan *flowgraph* untuk mempermudah analisis struktur logika program menggunakan metode *White Box Testing*. *Flowgraph* merepresentasikan alur kontrol program dalam bentuk node dan edge sehingga dapat digunakan untuk memperoleh nilai *Cyclomatic Complexity* serta menetapkan *independent path* yang akan diuji. Pada penelitian ini, analisis *flowgraph* dilakukan terhadap modul login dan modul enkripsi AES-128 mode CBC.



Sumber: (Hasil Penelitian, 2026)

Gambar 5. *Flowgraph* Modul Login

Gambar 5 menunjukkan *flowgraph* modul login yang merepresentasikan alur kontrol proses autentikasi pengguna. Hasil analisis menunjukkan bahwa modul login memiliki 10 node, 13 edge, dan 4 predicate node. Nilai tersebut menjadi dasar dalam perhitungan *Cyclomatic Complexity* untuk menentukan jumlah *independent path* yang harus diuji.



Sumber: (Hasil Penelitian, 2026)

Gambar 6. *Flowgraph* Modul Enkripsi AES-128 Mode CBC

Gambar 6 menunjukkan *flowgraph* modul enkripsi AES-128 mode CBC yang merepresentasikan alur kontrol proses enkripsi data pelanggan sebelum proses penyimpanan pada basis data. Hasil analisis menunjukkan bahwa modul enkripsi memiliki 9 node, 11 edge, dan 3 predicate node. Nilai tersebut selanjutnya digunakan dalam perhitungan *Cyclomatic Complexity*. Berdasarkan *flowgraph* yang telah dibentuk pada modul login dan modul enkripsi AES-128 mode CBC, tahap berikutnya dilakukan perhitungan *Cyclomatic Complexity* guna mengukur kompleksitas alur program serta menetapkan jumlah *independent path*. Perhitungan tersebut menggunakan Persamaan (4).

$$V(G) = E - N + 2 \quad (4)$$

Keterangan: $V(G)$ merupakan hasil *Cyclomatic Complexity*, E menyatakan banyaknya edge, sedangkan N menunjukkan banyaknya node dalam *flowgraph*. Nilai *Cyclomatic Complexity* menunjukkan banyaknya jalur independen (*independent path*) yang perlu diuji pada setiap modul program. Berdasarkan hasil analisis *flowgraph*, modul login memiliki 10 node, 13 edge, dan 4 predicate node, sehingga diperoleh nilai *Cyclomatic Complexity* sebesar 5. Sementara itu, modul enkripsi AES-128 mode CBC memiliki 9 node, 11 edge, dan 3 predicate node, sehingga diperoleh nilai *Cyclomatic Complexity* sebesar 4. Nilai tersebut menunjukkan bahwa terdapat lima *independent path* pada modul login dan empat *independent path* pada modul enkripsi yang harus diuji. Ringkasan hasil perhitungan disajikan pada Tabel 8.

Tabel 8. Ringkasan Hasil Pengujian *White Box Testing*

Modul	Node	Edge	Predicate Node	V(G)	Independent Path	Hasil
Login	10	13	4	5	5	Berhasil
Enkripsi AES-128 Mode CBC	9	11	3	4	4	Berhasil

Sumber: (Hasil Penelitian, 2026)

Untuk memverifikasi seluruh jalur logika program yang telah diperoleh melalui perhitungan *Cyclomatic Complexity*, dilakukan identifikasi *independent path* pada masing-masing modul. Hasil identifikasi *independent path* untuk modul login dan modul enkripsi AES-128 mode CBC disajikan pada Tabel 9 dan Tabel 10.

Tabel 9. *Independent Path* Modul Login

Path	Jalur
P1	1 → 2 → 10
P2	1 → 3 → 9 → 10
P3	1 → 3 → 4 → 5 → 9 → 10
P4	1 → 3 → 4 → 6 → 7 → 9 → 10
P5	1 → 3 → 4 → 6 → 8 → 9 → 10

Sumber: (Hasil Penelitian, 2026)

Tabel 10. *Independent Path* Modul Enkripsi AES-128 Mode CBC

Path	Jalur
P1	1 → 2 → 9
P2	1 → 3 → 4 → 9
P3	1 → 3 → 5 → 6 → 8 → 9
P4	1 → 3 → 5 → 7 → 6 → 8 → 9

Sumber: (Hasil Penelitian, 2026)

Berdasarkan hasil perhitungan *Cyclomatic Complexity* pada Tabel 8 serta identifikasi *independent path* pada Tabel 9 dan Tabel 10, setiap jalur independen pada kedua modul dapat dijalankan sesuai alur logika program yang telah dirancang. Pada modul login, pengujian menunjukkan bahwa proses autentikasi dapat menangani kondisi kredensial yang valid maupun tidak valid sesuai dengan alur yang ditentukan. Sementara itu, pada modul enkripsi AES-128 mode CBC, setiap tahapan mulai dari pembentukan state, transformasi algoritma AES, hingga menghasilkan *ciphertext* berhasil dilaksanakan tanpa adanya kesalahan logika. Hasil pengujian menunjukkan bahwa implementasi algoritma AES-128 mode CBC telah terintegrasi dengan baik pada sistem informasi provider layanan WiFi dan mampu menjalankan fungsi enkripsi maupun dekripsi sesuai kebutuhan fungsional sistem.

Hasil penelitian menunjukkan bahwa implementasi algoritma AES-128 dengan mode CBC berhasil diterapkan pada sistem informasi provider layanan WiFi untuk mengamankan data pelanggan sebelum proses penyimpanan dalam basis data. Proses enkripsi menghasilkan *ciphertext* dalam format heksadesimal sehingga informasi tidak bisa dibaca langsung tanpa menggunakan *secret key* serta *Initialization Vector* (IV) yang sesuai. Selain itu, hasil *White Box Testing* menunjukkan bahwa seluruh jalur independen pada modul login maupun modul enkripsi berhasil dieksekusi sesuai dengan logika program yang telah dirancang.

Temuan tersebut membuktikan bahwa implementasi AES-128 mode CBC mampu meningkatkan kerahasiaan data sekaligus mempertahankan fungsionalitas sistem, sehingga proses penyimpanan dan pengelolaan data pelanggan tetap berjalan sesuai dengan kebutuhan pengguna. Jika dibandingkan dengan penelitian (Priambudi & Mufti, 2023) yang mengimplementasikan AES-128 untuk pengamanan file berbasis web serta penelitian (Linda et al., 2023) yang menerapkan AES-128 pada keamanan basis data aplikasi kepelangganan, dan penelitian (Assidiq et al., 2024) yang mengimplementasikan algoritma AES dan SHA-3 untuk melindungi informasi sensitif pengguna pada website transaksi, penelitian ini juga memiliki tujuan serupa dalam meningkatkan keamanan penyimpanan data menggunakan algoritma AES. Hasil penelitian (Assidiq et al., 2024) menunjukkan bahwa implementasi algoritma AES mampu menjaga kerahasiaan data sensitif pada sistem berbasis web melalui mekanisme enkripsi. Perbedaannya terletak pada penerapan mode *Cipher Block Chaining* (CBC) yang memanfaatkan *Initialization Vector* (IV) yang dapat menghasilkan *ciphertext* berbeda walaupun *plaintext* yang digunakan identik. Selain itu, penelitian ini menerapkan mekanisme enkripsi secara langsung ke dalam sistem informasi provider layanan WiFi dan memvalidasi implementasinya menggunakan *White Box Testing*. Dengan demikian, hasil penelitian ini mendukung penelitian terdahulu bahwa penerapan AES-128 mode CBC merupakan pendekatan yang efektif untuk meningkatkan perlindungan data dalam sistem informasi berbasis web.

KESIMPULAN

Penerapan algoritma *Advanced Encryption Standard* (AES-128) dengan mode CBC berhasil diimplementasikan sebagai mekanisme enkripsi untuk melindungi data pelanggan pada sistem informasi provider layanan WiFi. Data pelanggan yang tersimpan pada basis data berhasil diubah menjadi *ciphertext* sehingga informasi tidak bisa dipahami tanpa melalui tahap dekripsi menggunakan kunci yang sesuai, sementara proses dekripsi tetap dapat memulihkan informasi menjadi bentuk semula dengan akurat. Hasil pengujian juga memperlihatkan bahwa seluruh fungsi utama sistem, termasuk proses autentikasi dan enkripsi data, berjalan sesuai dengan logika program yang dirancang sehingga implementasi algoritma tidak memengaruhi fungsionalitas sistem. Dengan demikian, implementasi AES-128 mode CBC dapat mendukung perlindungan kerahasiaan data pelanggan pada sistem informasi berbasis web melalui mekanisme enkripsi yang diterapkan. Penelitian selanjutnya dapat mengembangkan mekanisme pengelolaan kunci yang lebih aman serta membandingkan performa AES dengan algoritma kriptografi lainnya untuk memperoleh pendekatan yang lebih optimal dalam pengamanan data.

REFERENSI

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *JTSI*, *4*(2), 394–405. https://doi.org/10.35957/jtsi.v4i2.6077

Assidiq, M. L., Mahardika, F., & Santika, D. (2024). Implementasi Algoritma Kriptografi AES dan SHA-3 Dalam Mengamankan Data Sensitif Pengguna Pada Website Transaksi. *Simpatik: Jurnal Sistem Informasi Dan Informatika*, *4*(1), 44–52. https://doi.org/10.31294/simpatik.v4i1.3386

Batau, R. (2024). Implementasi Algoritma Advanced Encryption Standard Untuk Keamanan Data Customer Pegadaian UPC Pacongkang. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *7*(1), 187–194. https://doi.org/10.57093/jisti.v7i1.221

Cobantoro, A. F., Islami, M. V. D. L., Munaji, Arifin, R., & Setyawan, M. B. (2025). Implementation of RFID Technology as an Innovative Solution for Payment Systems in Supermarkets. *International Journal of Information System and Technology*, (5). https://oneamd.com/JOL/index.php/IJOINT/article/view/71

Cobantoro, A. F., Wicahyono, F. Y., & Z, I. A. (2025). Implementasi Algoritma RSA Untuk Keamanan Data Pasien Menggunakan Teknologi QR CODE Implementation of RSA Algorithm For Securing Patient Data using QR Code Technology. *Jurnal Ilmiah NERO*, *10*(1), 2025. https://doi.org/10.21107/nero.v10i1.30052

Duma, A., & Pusvita, E. A. (2023). Pengembangan Sistem Informasi Data Siswa Berbasis Web Pada SMPN 09 Nabire Dengan Metode Waterfall. *Journal of Information System Management (JOISM)*, *5*(1), 2715–3088. https://doi.org/10.24076/joism.2023v5i1.1115

Gandhara, Z. S., Satria, T. P., Saragih, H., & Abror, M. N. N. (2025). Evaluasi Kinerja Algoritma Kriptografi dalam Pengamanan Video: Studi Perbandingan AES, DES dan Blowfish. *JURNAL ILMIAH RESEARCH STUDENT*, *2*(2), 917–923. https://doi.org/10.61722/jirs.v2i2.5908

Irawan, B. O. P. I., Tahir, M., Windrastuti, N. A., Cholili, D. Y., Mulaikah, D., & Wachid, A. B. M. S. (2023). Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma Advance Encryption Standard. *Jurnal SimanteC*, *11*(2), 167–174. https://doi.org/10.21107/simantec.v11i2.20034

Linda, H., Sitorus, S. H., & Ristian, U. (2023). Penerapan Algoritma Advanced Encryption Standard (AES)-128 Bit Pada Keamanan Database Aplikasi Kepelangganan (Studi Kasus: Perumda Air Minum Tirta Khatulistiwa). *Coding : Jurnal Komputer Dan Aplikasi*, *11*(01), 128–136. https://doi.org/10.62866/jurikti.v1i2.55

Nugraha, F., & Arifin, T. (2022). Enkripsi dan Dekripsi Suara Menggunakan Metode AES 128b dengan Secret Key. *SISTEMASI: Jurnal Sistem Informasi*, *11*(1), 97–07. https://doi.org/10.32520/stmsi.v11i1.1627

Oktavani, S., Rizky, F., & Gunawan, I. (2023). Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES). *JURNAL MEDIA INFORMATIKA [JUMIN]*, *4*(2), 97–101. https://doi.org/10.55338/jumin.v4i2.435

Priambudi, I., & Mufti. (2023). Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, *6*(1), 22–31. https://doi.org/10.36080/skanika.v6i1.2997

Ramalinda, D., Jayadi, & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, *2*(6), 665–671. https://doi.org/10.62504/jimr679

Shiddiq, M. I. (2022). Implementasi White Box Testing Berbasis Path Pada Form Login Aplikasi Berbasis Web. *Jurnal Siliwangi Seri Sains Dan Teknologi*, *8*(1), 2022. https://doi.org/10.37058/jssainstek.v8i1.4093

