

Vol. 4 No. 2 September 2025

E-ISSN : 2962-8628

PROSIDING

SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI (SENAFTI)

"Agentic AI: Dampak Pada Interaksi Manusia dan Mesin"

- **Cyber Security**
- **Programming**
- **Artificial Intelligence**
- **Information System**

STEERING COMMITTEE

Pelindung

Prof. Dr. Agus Setyo Budi, M.Sc

Penanggung Jawab

Dr. Ir. Achmad Solichin, S.Kom., M.T.I

Ketua Pelaksana

Dr. Moh. Syafrullah, M.Kom., M.Sc

Wakil Ketua Pelaksana

Bima Cahya Putra, S.Kom, M.Kom

Sekretaris

Retno Wulandari, S.Kom., M.Kom.

Bendahara

1. Widodo MS, S.Kom
2. Noni Juliasari, S.Kom., M.Kom.

Humas, Publikasi, Dokumentasi dan Desain

1. Reva Ragam Santika, S.Kom., M.M., M.Kom
2. Rizka Tiaharyadini, S.Kom., M.M., M.Kom
3. Fahmi AkhtarRakaiz

Acara

1. Dr. Indra, S.Kom., M.T.I
2. Windarto, S.Kom., M.Kom
3. Agnes Aryasanti, S.Kom., M.Kom

Pengelola Makalah dan Mitra Bestari

1. Wahyu Pramusinto, S.Kom., M.Kom
2. Kukuh Harsanto, S.Kom., M.Kom
3. Dian Anubhakti, S.Kom., M.Kom

Pengelola Editor dan Jurnal

1. Rizky Pradana, S.Kom., M.Kom
2. Indah Puspasari Handayani, S.Kom., M.Kom
3. Yesi Puspita Dewi, S.Kom., M.Kom
4. Hadidtyo Wisnu Wardani, S.Kom., M.Kom
5. Sri Wahyuningsih, S.Kom., M.Kom
6. Ikhsan Rahdiana, S.Kom., M.Kom
7. Jeremy Jonathan, S.Kom., M.Kom
8. Anwar Rifai, M.Kom
9. Iman Permana, S.Kom, M.Kom

Pengelola Teknologi Informasi

1. Sovan Dianarto, S.Kom.
2. Dolly Virgian Shaka Yudha Shakti, S.Kom., M.Kom.

REDAKSI

Pelindung : Prof. Dr. Agus Setyo Budi, M.Sc
Penanggung Jawab : Dr. Ir. Achmad Solichin, S.Kom., M.T.I
Ketua Pelaksana : Dr. Moh. Syafrullah, M.Kom., M.Sc
Wakil Ketua Pelaksana : Bima Cahya Putra, S.Kom, M.Kom

Wakil Ketua Redaksi :

1. Wahyu Pramusinto, S.Kom., M.Kom
2. Kukuh Harsanto, S.Kom., M.Kom
3. Dian Anubhakti, S.Kom., M.Kom

Redaksi Pelaksana :

1. Rizky Pradana, S.Kom, M.Kom
2. Indah Puspasari Handayani, S.Kom., M.Kom.
3. Devit Setiono, S.Kom., M.Kom.
4. Jeremy Jonathan, S.Kom., M.Kom.
5. Yesi Puspita Dewi, S.Kom., M.Kom.
6. Hadidtyo Wisnu Wardani, S.Kom., M.Kom.
7. Sri Wahyuningsih, S.Kom, M.Kom.
8. Anwar Rifai, M.Kom
9. Iman Permana, S.Kom, M.Kom

MITRA BESTARI

1. Prof. Dr. Edy Winarno, S.T., M.Eng. (Universitas Muhammadiyah Semarang)
2. Dr. Suwanto raharjo, S.Si., M.Kom (IST AKPRIND Yogyakarta)
3. Dr. EH. Riyadi, MTL. (Badan Pengawas Tenaga Nuklir)
4. Dr. Budi Rahmani, S.Pd., M.Kom. (STMIK Banjarbaru)
5. Dr. Hamdani (Universitas Mulawarman)
6. Dr. Ir. Didit Suprihanto, S.T., M.Kom., IPM (Univ. Mulawarman)
7. Dr. Nanang Triagung Edi Hermawan, M.T. (BAPETEN)
8. Dr. Khoerul Anwar, ST, MT (STMIK PPKIA PRADNYA PARAMITA)
9. Dr. Ir. Ridowati Gunawan, S.Kom., M.T. (Universitas Sanata Dharma)
10. Dr. Ir. Mardi Hardjianto, M.Kom. (Universitas Budi Luhur)
11. Dr. Ir. Goenawan Brotosaputro, S.Kom., M.Sc. (Institut Sains dan Bisnis Atma Luhur)
12. Dr. Achmad Solichin, S.Kom., M.T.I (Universitas Budi Luhur)
13. Dr. Ir. Deni Mahdiana, S.Kom, M.M, M.Kom (Universitas Budi Luhur)
14. Dr. Darwan, M.Kom. (IAIN Syekh Nurjati Cirebon)
15. Dr. Ir. Gandung Triyono, S.Kom., M.Kom (Universitas Budi Luhur)
16. Dr. Aji Supriyanto, S.T., M.Kom (Universitas Stikubank)
17. Dr. Jumi, S.Kom, M.Kom. (Politeknik Negeri Semarang)
18. Dr. Aris Sugiharto, S.Si, M.Kom (Universitas Diponegoro)
19. Dr. Anindita Septiarini, S.T., M.Cs. (Universitas Mulawarman)
20. Dr. Imelda, M.Kom (Universitas Budi Luhur)
21. Dr. Ir. Utomo Budiyanto, M.Kom., M.Sc (Universitas Budi Luhur)
22. Dr. Ir. Jan Everhard R MT (Universitas Budi Luhur)
23. Dr. Ir. Hari Soetanto, S.Kom, M.Sc (Universitas Budi Luhur)
24. Dr. Abdiansah, S.Kom., M.CS. (Universitas Sriwijaya)
25. Dr. Indra, M.T.I (Universitas Budi Luhur)
26. Dr. Heriyanto, A.Md, S.Kom, M.Cs (UPN Veteran Yogyakarta)
27. Dr. Lilis Susanti Setianingsih, S.T., M.S. (Badan Pengawas Tenaga Nuklir)
28. Dr. Linda Nur Afifa, S.T., M.T (Universitas Darma Persada)
29. Dr. Helna Wardhana, M.Kom. (Universitas Bumigora)
30. Dr. Khasnur Hidjah, S.Kom., M.Cs. (Universitas Bumigora Mataram)
31. Dr. Hendra Cipta, M.Si (Universitas Islam Negeri Sumatera Utara Medan)
32. Dr. Yulianto Triwahyuadi Polly, S.Kom., M.Cs (Universitas Nusa Cendana)
33. Dr. Mohammad Syafrullah, M.Kom, M.Sc (Universitas Budi Luhur)
34. Dr. Ir. Aslan Alwi, S.Si., M.Cs (Universitas Muhammadiyah Ponorogo)
35. Dr. Gamma Kosala, S.Si (Telkom University)
36. Dr. Ir. Lasmedi Afuan, ST.,M.Cs (Universits Jenderal Soedirman)
37. Dr. Rahmad Hidayat S.Kom., M.Cs (Politeknik Negeri Lhokseumawe)
38. Dr. Indra Riyanto, S.T., M.T (Universitas Budi Luhur)
39. Dr. Ir. Nurul Hidayat, SPt., M.Kom (Universitas Jenderal Soedirman)
40. Dr. Muhammad Syaukani, ST, SH, M.Cs,M.Kom (Institut Teknologi Bisnis dan Bahasa Dian Cipta Cendikia)
41. Ts. Setyawan Widyarto, MSc., PhD. (Universiti Selangor, Universitas Budi Luhur)
42. Dr.Eng. Akhmad Unggul Priantoro (Universitas Budi Luhur)
43. Dr. Dedi Trisnawarman, S.Si., M.Kom (Universitas Tarumanagara)
44. Windarto, S.Kom, M.Kom (Universitas Budi Luhur)
45. Agus Umar Hamdani, M.Kom (Universitas Budi Luhur)
46. Irawan, S.Kom., M.Kom. (Universitas Budi Luhur)

47. Hendri Irawan, S.Kom., M.T.I. (Universitas Budi Luhur)
48. Yuliazmi S.Kom, M.Kom (Universitas Budi Luhur)
49. Grace Gata, S.Kom., M.kom (Universitas Budi Luhur)
50. Dolly Virgian Shaka Yudha Sakti, M.Kom (Universitas Budi Luhur)
51. Kelik Sussolaikah, S.Kom., M.Kom (Universitas PGRI Madiun)
52. Anita Ratnasari, S.Kom, M.Kom (Universitas Dian Nusantara)
53. Dwi Pebrianti, S.T., M. Eng., Ph.D, Eng. Tech., SMIEEE, IPU (Universitas Budi Luhur)
54. Arita Witanti S.T.,M.T (Universitas Mercu Buana Yogyakarta)
55. Wiwien Hadikurniawati, S.T., M.Kom. (Universitas Stikubank)
56. Reva Ragam Santika, M.Kom (Universitas Budi Luhur)
57. Agnes Aryasanti, M.Kom (Universitas Budi Luhur)
58. Atik Ariesta, S.Kom., M.Kom. (Universitas Budi Luhur)

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT dan hanya karena rahmat dan karunia-Nya, Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Ke-6 pada Tahun 2025 dapat terlaksana dengan baik. Prosiding seminar ini merupakan kumpulan makalah hasil penelitian para akademisi dan peneliti yang sebelumnya telah dipresentasikan pada SENAFI ke-4 secara daring (*online*) pada tanggal 20 September 2025 dengan tema “Agentic AI: Dampak Pada Interaksi Manusia dan Mesin”. SENAFI ke-6 telah menerima dan menerbitkan artikel ilmiah dari beberapa perguruan tinggi yang berasal dari 3 provinsi di Indonesia, yaitu DKI Jakarta, UPN Veteran Yogyakarta (Yogyakarta), Universitas Stikubank (Jawa Tengah) dan Univ. Muhammadiyah Metro (Lampung).

Penyusunan prosiding ini bertujuan untuk penyebarluasan hasil-hasil penelitian dan kajian dalam bidang teknologi informasi. Selain itu, penyusunan prosiding ini juga dimaksudkan agar masyarakat luas dapat mengetahui berbagai informasi terkait dengan penyelenggaraan SENAFI ke-6. Buku prosiding ini berisi 4 (empat) topik yaitu: Cyber Security, Artificial Intelligence, Programming, Information System.

Pada kesempatan ini kami menyampaikan terima kasih yang sebesar-besarnya kepada para akademisi dan peneliti atas hasil karya dan sumbangan pemikiran yang dipresentasikan dalam bentuk makalah dan presentasi ilmiah. Juga kami sampaikan terima kasih kepada para mitra bestari yang telah mereview semua makalah sehingga kualitas isi dari makalah dapat terjaga dan dipertanggungjawabkan. Tak lupa kepada semua pihak yang telah memberikan dukungan bagi terselenggaranya SENAFI dan atas tersusunnya prosiding ini. Harapan kita bersama, semoga prosiding ini dapat menambah khasanah pengembangan ilmu pengetahuan dan teknologi informasi di Indonesia.

Jakarta, September 2025

Tim Penyusun

DAFTAR ISI

STEERING COMMITTEE	i
REDAKSI.....	3
MITRA BESTARI.....	4
KATA PENGANTAR.....	6
DAFTAR ISI.....	7

CYBER SECURITY

IMPLEMENTASI AES-256 UNTUK MENGAMANKAN DOKUMEN KREDENSIAL KLIEN (STUDI KASUS: PT STUDIO INOVASI TEKNOLOGI) Iqbal Syafiudin, Titin Fatimah	1-10
PERBANDINGAN ALGORITMA KRIPTOGRAFI AES-128 DAN DES UNTUK KEAMANAN DOKUMEN PADA PT JASA RAHARJA PUTERA Sultan Nabil, Hari Soetanto.....	11-20
IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN DATA PENJUALAN DI TOKO DIAH KEMASAN KOSMETIK Danang Pandya Pangestu; Dolly Virgian Shaka Yudha Sakti	21-28
IMPLEMENTASI ENKRIPSI DATA SISWA DAN TRANSAKSI PAUD AI-HANIF MENGGUNAKAN ALGORITMA RC4 BERBASIS WEB Muhamad Salamun, Reva Ragam Santika	29-38
IMPLEMENTASI KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN RC4 MODIFIKASI UNTUK MENGAMANKAN DATA Galih Sadewo, Dolly Virgian Shaka Yudha Sakti.....	39-48
IMPLEMENTASI AES-128 EFISIEN PADA APLIKASI WEB UNTUK PENGAMANAN DOKUMEN BANTUAN SOSIAL DI TINGKAT KELURAHAN Rizki Apriansyah Wijaya, Sri Mulyati.....	49-58
PENERAPAN ALGORITMA NAIVE BAYES UNTUK ANALISIS SENTIMEN APLIKASI SPOTIFY PADA GOOGLE PLAY STORE Novrian Novrian, Hari Soetanto	59-68
PENERAPAN KRIPTOGRAFI AES-128 UNTUK KEAMANAN DATA PEGAWAI PADA PERUSAHAAN LOGISTIK DI JAKARTA Prasetyo Ari Nugroho, Rizky Pradana	69-76

PENERAPAN ALGORITMA AES-CBC DAN AES-GCM UNTUK PENGAMANAN DOKUMEN	GEREJA
Leonard Reinhard Roscott, Subandi	77-84
IMPLEMENTASI ALGORITMA AES-192 UNTUK MENGAMANKAN FILE DATA DI POJOK	UMKM KOTA CILEDUG
Ahmad Dhani Yazid Saputro, imelda	85-94
IMPLEMENTASI AES-256 BERBASIS WEB PADA DATA PENJUALAN HARIAN DI TOKO	KOPI TUKU JOGLO
Hanifah, Dewi Kusumaningsih	95-103
IMPLEMENTASI HYBRID ENCRYPTION ECC-AES UNTUK PENGAMANAN KOMUNIKASI DAN BERBAGI FILE BERBASIS WEB	
Risqi Rahman Pratama, Dolly Virgian Shaka Yudha Sakti	104-113
OPTIMALISASI KEAMANAN DATA DENGAN PENERAPAN ALGORITME KRIPTOGRAFI	AES-128 BERBASIS WEB
Rafli Adhies Attha, Titin Fatimah	114-121
PROTOTIPE SISTEM MONITORING SUHU DAN KELEMBABAN RUANG SERVER BERBASIS	IOT ESP32 DAN DHT22
Fahrul Kusuma, Sejati Waluyo	122-129
OTOMASI PENGATURAN JARINGAN LAN BERBASIS MIKROTIK DENGAN BAHASA	PEMROGRAMAN PYTHON
Hadi Prasetyo, Gunawan Pria Utama	130-137
IMPLEMENTASI KEAMANAN FILE BERBASIS WEB DENGAN METODE ADVANCED ENCRYPTION	STANDARD (AES)-256 COUNTER MODE
Ahmad Najib Syafi'I, Noni Juliasari	138-145
MANAJEMEN JARINGAN BEBASIS WEB MENGGUNAKAN SNMP UNTUK FAKULTAS	EKONOMI DAN BISNIS UNIVERSITAS TRISAKTI
Aris Wiyono; Reva Ragam Santika	146-154
IMPLEMENTASI AES-128 UNTUK PENGAMANAN FILE TRANSAKSI PENJUALAN PADA	CV. DNN BERBASIS WEB
Fransiskus Aldi Jebadu, Sejati Waluyo	155-163
PENERAPAN AUTENTIKASI DUA FAKTOR MENGGUNAKAN TIME-BASED ONE TIME PASSWORD (TOTP) BERBASIS EMAIL DAN GOOGLE AUTHENTICATOR	PADA APLIKASI MANAJEMEN PERANGKAT MIKROTIK
Izhar Nurkholis Sukma, Achmad Solichin	164-173

OPTIMALISASI KEAMANAN DATA DENGAN PENERAPAN ALGORITME KRIPTOGRAFI *AES-128* BERBASIS *WEB*

Rafli Adhies Attha^{1*}, Titin Fatimah²

^{1,2} Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: ^{1*}2111501363@student.budiluhur.ac.id, ²titin.fatimah@budiluhur.ac.id

(* : corresponding author)

Abstrak- Kerahasiaan data merupakan aspek penting dalam menjaga keamanan informasi, terutama bagi perusahaan yang menyimpan *file* sensitif. PT Laz Coal Mandiri menghadapi risiko kebocoran data karena minimnya perlindungan terhadap *file* internal seperti slip gaji, laporan keuangan, dan dokumen proyek. *File* selama ini disimpan pada komputer maupun media eksternal tanpa sistem keamanan yang memadai, sehingga rawan diakses pihak tidak berwenang. Untuk mengatasi permasalahan tersebut, penelitian ini mengembangkan aplikasi berbasis *web* yang menerapkan algoritma kriptografi *Advanced Encryption Standard (AES-128)*. Aplikasi mendukung beberapa format *file* dengan ukuran hingga 8MB, serta dilengkapi fitur log aktivitas agar pengguna dapat memantau riwayat penggunaan sistem. Hasil pengujian menunjukkan bahwa proses enkripsi berjalan dengan baik tanpa error, dengan ukuran *file* hasil enkripsi hanya bertambah sekitar 0,01 KB. Waktu enkripsi meningkat seiring bertambahnya ukuran *file* dan juga dipengaruhi oleh spesifikasi perangkat. Proses dekripsi berhasil mengembalikan *file* ke bentuk aslinya tanpa kerusakan data, dengan ukuran identik dengan *file* awal. Tahapan enkripsi menghasilkan data terenkripsi yang tidak terbaca, sedangkan dekripsi mampu mengembalikannya ke bentuk semula, membuktikan sistem bekerja dengan baik dalam menjaga integritas serta kerahasiaan data. Dari penelitian ini dapat disimpulkan bahwa penerapan *AES-128* pada aplikasi berbasis *web* mampu meminimalkan risiko kebocoran informasi dan meningkatkan keamanan data internal perusahaan. Sistem ini menjadi solusi praktis

Kata Kunci: Data, Kriptografi, *AES-128*, Enkripsi, Dekripsi

OPTIMIZATION DATA SECURITY WITH THE APPLICATION OF WEB-BASED *AES-128* CRYPTOGRAPHY ALGORITHM

Abstract- Data confidentiality is an important aspect of maintaining information security, especially for companies that store sensitive files. PT Laz Coal Mandiri faces the risk of data leaks due to the lack of protection for internal files such as pay slips, financial reports, and project documents. These files have been stored on computers and external media without adequate security systems, making them vulnerable to unauthorized access. To address this issue, this study developed a web-based application that implements the *Advanced Encryption Standard (AES-128)* cryptography algorithm. The application supports multiple file formats with sizes up to 8MB and includes an activity log feature to allow users to monitor system usage history. Testing results indicate that the encryption process runs smoothly without errors, with the encrypted file size increasing by only approximately 0.01 KB. Encryption time increases with file size and is also influenced by device specifications. The decryption process successfully restores the file to its original form without data corruption, with the same size as the original file. The encryption process produces unreadable encrypted data, while decryption is able to restore it to its original form, proving that the system works well in maintaining data integrity and confidentiality. From this study, it can be concluded that the implementation of *AES-128* in web-based applications can minimize the risk of information leaks and enhance the security of internal company data. This system is a practical solution in supporting digital data protection at PT Laz Coal Mandiri and other companies with similar needs.

Keywords: Data, Cryptography, *AES-128*, Encryption, Decryption

1. PENDAHULUAN

Kerahasiaan sebuah data atau informasi merupakan hal yang sangat penting dan harus dijaga agar tidak diketahui oleh pihak yang tidak berkepentingan. Data atau informasi adalah salah satu aset yang sangat berharga untuk dilindungi keamanannya. Sejak zaman dahulu, perlindungan informasi sudah menjadi perhatian besar, misalnya pada masa perang di mana digunakan sandi morse untuk mengirimkan pesan-pesan rahasia agar tidak dapat dimengerti oleh pihak yang tidak berkepentingan.

Pada era digital seperti sekarang ini, di mana data semakin memainkan peran penting dalam operasional perusahaan, perlindungan data menjadi sangat vital. Meningkatnya kebutuhan ini juga terjadi peningkatan permintaan untuk mengembangkan sistem keamanan data yang lebih efisien dalam mengelola informasi[1]. Data

bisa berupa informasi pribadi, laporan keuangan, transaksi bisnis, hingga dokumen-dokumen penting lainnya. Banyak dokumen penting khususnya yang berkaitan dengan sebuah perusahaan berisi data rahasia yang hanya dapat dilihat oleh individu tertentu [2] .

PT Laz Coal Mandiri, sebuah perusahaan yang bergerak di bidang jasa kontraktor di Kalimantan Selatan, menyimpan berbagai data penting terkait proyek pertambangan, seperti laporan keuangan dan slip gaji karyawan, dalam berbagai format *file* seperti *.doc*, *.xlsx*, *.pdf*, dan lainnya. Namun, data tersebut disimpan tanpa adanya sistem keamanan yang memadai, membuat *file-file* tersebut sangat rentan terhadap akses yang tidak sah atau bahkan kemungkinan kehilangan data. Khususnya jika data disimpan dalam perangkat penyimpanan seperti flash disk, HDD (*Hard Disk Drive*), atau SSD (*Solid State Drive*), yang tidak menjamin kerahasiaan data tersebut.

Kriptografi adalah gabungan antara ilmu dan seni dalam menjaga keamanan data digital, termasuk *file*[3]. Salah satu metode yang terbukti efektif dan banyak digunakan untuk mengamankan data digital adalah *Advanced Encryption Standard* (AES) dengan panjang kunci 128-bit[4]. AES-128 terkenal karena kecepatannya dalam proses enkripsi dan dekripsi, serta tingkat keamanannya yang tinggi. Oleh karena itu, penerapan algoritma AES-128 pada sistem yang digunakan oleh PT Laz Coal Mandiri diharapkan dapat melindungi data perusahaan dari ancaman dunia maya serta penyalahgunaan informasi.

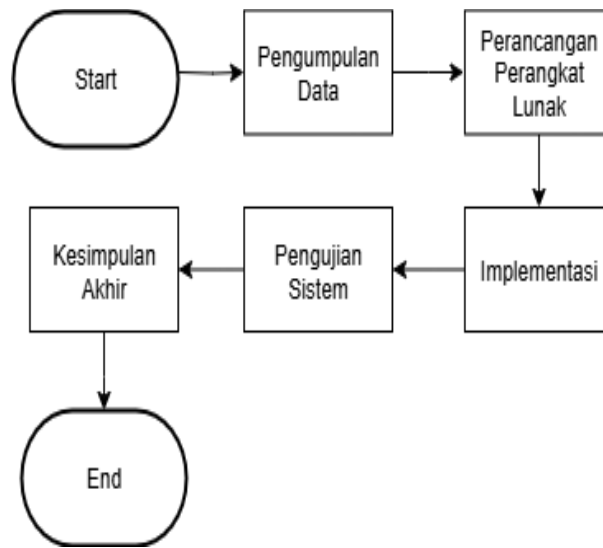
Pada penelitian sebelumnya yang dilakukan oleh Widyawan dan Imelda (2021), telah berhasil diterapkan algoritma AES-128 untuk mengamankan *file* investigasi di Komite Nasional Keselamatan Transportasi. Penelitian tersebut menunjukkan bahwa algoritma ini hanya dapat mengenkripsi *file* seperti *Excel*, *PowerPoint*, *Word*, *PDF*, dan *file* teks, dengan batasan ukuran *file* maksimal 5MB. Dalam penelitian tersebut, waktu enkripsi untuk *file* dengan ukuran 1.800KB memakan waktu sekitar 80 detik, sedangkan waktu dekripsi sekitar 79 detik.

Penelitian ini bertujuan untuk melakukan penerapan serupa, namun dengan menambahkan beberapa fitur baru. Selain menggunakan algoritma AES-128 untuk kriptografi, peneliti juga akan menambahkan fitur log aktivitas yang memungkinkan pengguna untuk melacak aktivitas sistem. Selain itu, penelitian ini juga akan menambahkan beberapa jenis *file* yang dapat dienkripsi hingga ukuran maksimal 8MB.

2. METODE PENELITIAN

2.1 Tahapan Metode

Dalam pelaksanaan penelitian, metode ini digunakan sebagai acuan untuk mendukung tercapainya tujuan yang telah direncanakan. Tahap awal penelitian dilakukan dengan pengumpulan data melalui wawancara daring dengan staf PT Laz Coal Mandiri serta observasi tidak langsung terhadap lingkungan kerja. Metode ini dipilih untuk menggali informasi terkait penerapan sistem keamanan dan memahami proses kerja perusahaan. Setelah data terkumpul, penelitian dilanjutkan dengan perancangan perangkat lunak yang berfokus pada pengembangan modul enkripsi-dekripsi dan antarmuka pengguna dengan penerapan algoritme AES-128. Pada tahap ini, *file* dienkripsi menggunakan kunci identik sehingga *plaintext* berubah menjadi *ciphertext*, lalu didekripsi kembali dengan kunci yang sama agar data dapat dibaca kembali dalam bentuk aslinya [5]. Tahap pengujian dilakukan guna mengonfirmasi bahwa sistem yang dikembangkan telah sesuai dengan hasil analisis dan berfungsi sebagaimana mestinya [6]. Untuk memastikan sistem berjalan sesuai dengan rancangan, dilakukan pengujian sistem dengan metode *blackbox testing* yang menilai kesesuaian input dan output tanpa melihat proses internal. Tujuan dari pengujian ini adalah untuk menemukan kesalahan serta memastikan bahwa sistem telah berfungsi sesuai ketentuan. Tahap akhir berupa kesimpulan, yang diperoleh dari hasil pengujian untuk menilai efektivitas penerapan algoritme AES-128 dalam menjaga keamanan data pada PT Laz Coal Mandiri. Setiap tahapan penelitian dijalankan secara sistematis sesuai dengan alur yang ditunjukkan pada Gambar 1.



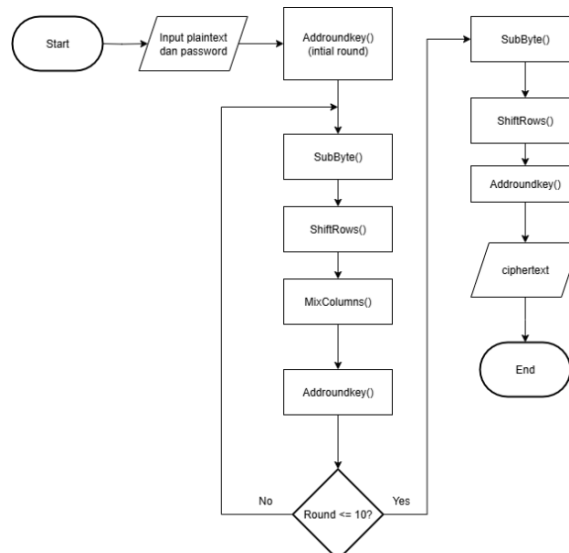
Gambar 1 Tahapan Metode

2.2 Advanced Encryption Standard (AES)

AES digolongkan sebagai algoritma blok *non-Feistel* karena menggunakan struktur blok dengan panjang tetap sebesar 128 bit yang dapat dibalik. Proses enkripsinya melibatkan sejumlah putaran (*round*) yang dilakukan secara berulang menggunakan kunci tertentu [7]. AES memiliki tiga variasi yang dibedakan berdasarkan panjang kunci yang digunakan, yaitu *AES-128*, *AES-192*, dan *AES-256* [8]. Masing-masing varian memiliki jumlah *round* enkripsi yang berbeda, di mana semakin panjang kunci yang digunakan, semakin kompleks dan aman proses enkripsinya.

2.3 Proses Enkripsi AES-128

AES-128 melakukan proses enkripsi dilakukan sebanyak 10 putaran (*round*) dengan menggunakan kunci sepanjang 128 bit, yang pada setiap putaran akan berbeda melalui proses ekspansi kunci (*key expansion*). Proses ekspansi ini menghasilkan rangkaian *round key* yang digunakan dalam setiap putaran enkripsi untuk memperkuat keamanan.



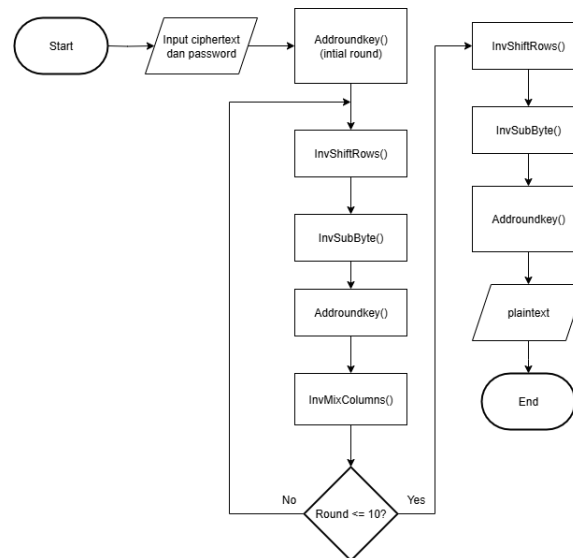
Gambar 2 Proses Enkripsi AES-128

- Initial Round-AddRoundkey*: Tahap awal enkripsi melakukan XOR antara blok data dan *round key* pertama untuk mencampurkan data dengan kunci.
- Putaran Utama (*Round 1-9*): Setiap putaran terdiri dari empat transformasi.

1. *SubBytes* : proses transformasi pada tingkat *byte*, di mana setiap elemen dalam *State* diganti menggunakan tabel substitusi yang dikenal sebagai *S-Box* [9].
 2. *ShiftRows* : Pada langkah ini, masing-masing baris dalam matriks *state* mengalami pergeseran posisi *byte*. Baris pertama tetap, baris kedua digeser satu *byte* ke kiri, baris ketiga digeser dua *byte*, dan baris keempat digeser sebanyak tiga *byte* ke arah yang sama [10].
 3. *MixColumns* : Setiap elemen blok *cipher* dikalikan dengan matriks tetap, lalu hasilnya membentuk blok *cipher* baru.
 4. *AddRoundkey* : Tahap ini melakukan XOR hasil *MixColumns* dengan *round key*, di mana perbedaan kunci tiap putaran menjadi inti keamanan AES.
- c. Putaran Akhir (*Round 10*) : Putaran akhir AES hanya mencakup *SubBytes*, *ShiftRows*, dan *AddRoundKey* tanpa *MixColumns* untuk menjaga struktur *cipher* tetap sesuai.

2.4 Proses Dekripsi AES-128

Dekripsi AES-128 membalik proses enkripsi dengan kunci yang sama melalui tahapan *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* untuk mengembalikan *ciphertext* menjadi *plaintext*.



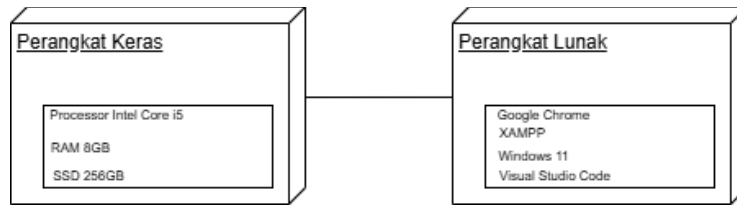
Gambar 3 Proses Dekripsi AES-128

- a. *Inverse ShiftRows* : Menggeser baris matriks *State* ke kanan secara melingkar untuk membalik proses *ShiftRows*.
- b. *Inverse SubBytes* : Memulihkan setiap *byte* pada *State* menggunakan tabel *Inverse S-Box* untuk membalik proses *SubBytes*.
- c. *Inverse MixColumns* : Setiap kolom dalam *State* dikalikan dengan matrik perkalian dalam AES.
- d. *Inverse AddRoundkey* : Dalam dekripsi, *round key* digunakan untuk XOR dengan *State*, sama seperti enkripsi karena sifat XOR yang dibalik.

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Implementasi aplikasi didukung oleh perangkat keras dan perangkat lunak yang digunakan dalam perancangan serta pengujian sistem.



Gambar 4 Deployment Diagram

3.2 Tabel Pengujian

Bagian ini menyajikan sebuah tabel yang merangkum hasil pelaksanaan proses enkripsi dan dekripsi *file* oleh sistem melalui aplikasi. Tabel tersebut memperlihatkan hasil pengujian yang dilakukan terhadap sejumlah *file* yang telah diuji.

a. Tabel hasil pengujian enkripsi

Tabel 1 Pengujian Enkripsi

No	Nama Asli File	Ukuran Awal File	Nama File Enkripsi	Ukuran Enkripsi	File	Durasi Enkripsi
1.	19. Raiky Adhies N.A_SPV HCMGA.pdf	205.15KB	1752640214_68772ad66ab42_19_Raiky_Adhies_N.A_SPV_HCMGA.pdf.enc	205.16KB		4.29 detik
2.	58. Muhammad Noor_Foreman GA.pdf	202.23KB	1752641546_6877300a8ca5f_58_Muhammad_Noor_Foreman_GA.pdf.enc	202.23KB		3.85 detik
3.	191. Juna B_Admin HRGA.pdf	180.29KB	1752641616_68773050bf138_191_Juna_B_Admin_HRGA.pdf.enc	180.30KB		3.64 detik
4.	RAPORT PK Desember 2024.xlsx	2030.52 KB	1752641734_687730c67a99f_RAPORT_PK_Desember_2024.xlsx.enc	2030.53 KB		38.36 detik
5.	0. Master Surat Pengalaman KerjaCertificat.docx	151.18 KB	1752641935_6877318fcd58c_0_Master_Surat_Pengalaman_KerjaCertificat.docx.enc	151.19 KB		2.91 detik
6.	logo.jpg	43.84 KB	1753348633_6881fa1966779_logo.jpg.enc	43.84 KB		0.64 Detik
7.	Catatan.txt	0.22 KB	1753348663_6881fa37a5e27_Catatan.txt.enc	0.23 KB		0.01 Detik
8.	0. Surat Keputusan Pengangkatan Karyawan Tetap.docx	151.16 KB	1753349196_6881fc4c84e55_0_Surat_Keputusan_Pengangkatan_Karyawan_Tetap.docx.enc	151.17 KB		2.22 Detik
9.	File Data NIK Karyawan.txt	0.16 KB	1754556209_68946731dee9b_File_Data_NIK_Karyawan.txt.enc	0.17 KB		0.01 Detik
10.	0. Presentasi Pekerjaan HRGA.pptx	1915.18 KB	1754556248_68946758a1102_0_Presentasi_Pekerjaan_HRGA.pptx.enc	1915.19 KB		8.46 Detik
11.	safety.png	678.20 KB	1754556768_689469604bb13_safety.png.enc	678.22 KB		3.1 Detik

Berdasarkan tabel hasil pengujian terhadap beberapa *file* dengan ukuran dan format berbeda, dapat disimpulkan bahwa proses enkripsi berjalan dengan baik tanpa ditemukan error, ukuran *file* hasil enkripsi hanya mengalami sedikit peningkatan sekitar 0,01 KB dan durasi enkripsi cenderung meningkat seiring bertambahnya ukuran *file* serta dapat dipengaruhi oleh spesifikasi perangkat yang digunakan, meskipun hal ini masih perlu dikaji lebih lanjut untuk memastikan konsistensi pada skenario yang lebih luas.

b. Tabel hasil pengujian dekripsi

Tabel 2 Pengujian Dekripsi

No	Nama Asli File	Ukuran Awal File	Nama File Dekripsi	Ukuran File Dekripsi	Durasi Dekripsi
1.	19. Raiky Adhies N.A_SPV HCMGA.pdf	205.15KB	1752640238_68772aed8621_19. Raiky Adhies N.A_SPV HCMGA.pdf	205.15 KB	10.9 detik
2.	58. Muhammad Noor_Foreman GA.pdf	202.23KB	1752641584_68773030989b1_58. Muhammad Noor_Foreman GA.pdf	202.23 KB	10.76 detik
3.	191. Juna B_Admin HRGA.pdf	180.29KB	1752641641_68773069e125f_191. Juna B_Admin HRGA.pdf	180.29 KB	9.72 detik
4.	RAPORT PK Desember 2024.xlsx	2030.52 KB	1752641863_6877314751eee_RAPORT PK Desember 2024.xlsx	2030.52 KB	102.13 detik
5.	0. Master Surat Pengalaman KerjaCertificat.docx	151.18 KB	1752641960_687731a89b15c_0. Master Surat Pengalaman KerjaCertificat.docx	151.18 KB	7.65 detik
6.	logo.jpg	43.84 KB	1753348648_6881fa28a44be_logo.jpg	43.84 KB	1.44 Detik
7.	Catatan.txt	0.22 KB	1753348678_6881fa467bd93_Catatan.txt	0.22 KB	0.01 Detik
8.	0. Surat Keputusan Pengangkatan Karyawan Tetap.docx	151.16 KB	1753349227_6881fc6b8f2a9_0. Surat Keputusan Pengangkatan Karyawan Tetap.docx	151.16 KB	4.96 Detik
9.	File Data NIK Karyawan.txt	0.16 KB	1754556226_689467421611f_File Data NIK Karyawan.txt	0.16 KB	0.01 Detik
10.	0. Presentasi Pekerjaan HRGA.pptx	1915.18 KB	1754556282_6894677a22196_0. Presentasi Pekerjaan HRGA.pptx	1915.18 KB	18.99 Detik
11.	safety.png	678.20 KB	1754556782_6894696e086f9_safety.png	678.20 KB	6.71 Detik

Berdasarkan tabel hasil pengujian dekripsi terhadap beberapa *file* dengan ukuran dan format berbeda, dapat disimpulkan bahwa proses dekripsi berjalan dengan baik tanpa terjadi kerusakan data, ukuran *file* hasil dekripsi sama dengan *file* aslinya dan durasi dekripsi umumnya meningkat seiring bertambahnya ukuran *file* serta dapat dipengaruhi oleh spesifikasi perangkat yang digunakan, meskipun hal ini masih perlu dikaji lebih lanjut untuk memastikan keandalan pada kondisi yang lebih beragam.

3.3 Hasil Proses Enkripsi dan Dekripsi

Dalam proses enkripsi dan dekripsi pada sistem, terdapat tiga yang ditampilkan. Pertama adalah data asli yang dimasukkan sebelum dilakukan enkripsi, yang menunjukkan isi informasi dalam bentuk awal. Setelah dilakukan enkripsi, sistem menghasilkan data dalam bentuk terenkripsi yang tidak dapat dibaca secara langsung, menandakan bahwa proses penyandian telah berhasil. Selanjutnya, pada tahap dekripsi, data terenkripsi diubah kembali ke bentuk semula, yang menunjukkan bahwa sistem mampu mengembalikan informasi dengan benar. Tahapan ini membuktikan bahwa enkripsi dan dekripsi bekerja sebagaimana mestinya dalam menjaga dan mengembalikan integritas data, dapat dilihat pada Gambar 5, Gambar 6, dan Gambar 7 berikut.

PT. LAZ COAL MANDIRI SLIP GAJI KARYAWAN PERSEOR: BULAN APRIL 2025			
NIR	92-2098	Level Gol	Staff
Nama	Rafly Adhies Hopen Attha	Grade	S-C
Jabatan	Supervisor HCBGA	Project	KINTAP
Tanggal Masuk	13-Mey-21	gol/Peker	B
Departemen	HCBGA	PTNP	K1
A. Penghasilan :			
Gaji Pokok	Rp	9.988.000	
Tunjangan Jabatan	Rp	3.190.000	
Tunjangan Lain-Lain	Rp	383.400	
BPJS Kesehatan Perusahaan (4%)	Rp	394.640	
Jaminan Hari Tua (3.7%)	Rp	354.845	
Jaminan Pensiun (2%)	Rp	191.700	
Jaminan Kesehatan Kerja (0.24%)	Rp	166.779	
Jaminan Kematian (0.2%)	Rp	28.755	
GAJI KOTOR	Rp	13.905.279	
B. Potongan Tanggungan Perusahaan :			
BPJS Kesehatan Perusahaan (4%)	Rp	394.640	
Jaminan Hari Tua (3.7%)	Rp	354.845	
Jaminan Pensiun (2%)	Rp	191.700	
Jaminan Kesehatan Kerja (0.24%)	Rp	166.779	
Jaminan Kematian (0.2%)	Rp	28.755	
Total Tanggungan Perusahaan :	Rp	1.126.279	
C. Potongan Karyawan :			
BPJS Kesehatan Karyawan (1%)	Rp	99.880	
Jaminan Hari Tua Karyawan (2%)	Rp	191.700	
Jaminan Pensiun (1%)	Rp	95.850	
PPH-21	Rp	143.775	
Akumulasi Tak Dibayar	Rp	-	
Potongan Lain-lain	Rp	-	
Total Potongan Karyawan :	Rp	527.175	
D. Tambahan Lain-lain :			
Ajutan Biaya Istimewa	Rp	-	
Kompensasi PKWT	Rp	-	
Sumbangan Buluh Duka	Rp	-	
GAJI BERSIH (A-B-C+D)	Rp	12.262.825	
BANK TRANSFER : BRI			
Nama Rekening :			
Nomor Rekening :			
Kintap, 01 Mei 2025			
SLIP GAJI INI DICETAK SECARA KOMPUTERISASI SEHINGGA TIDAK MEMERLUKAN TANDATANG			

Rekapitulasi Absensi		
NAME	TANGGAL	ABSENSI
Attha	1-Apr-25	D
Attha	2-Apr-25	D
Attha	3-Apr-25	D
Attha	4-Apr-25	D
Attha	5-Apr-25	D
Attha	6-Apr-25	D
Attha	7-Apr-25	D
Attha	8-Apr-25	D
Attha	9-Apr-25	D
Attha	10-Apr-25	D
Attha	11-Apr-25	D
Attha	12-Apr-25	D
Attha	13-Apr-25	D
Attha	14-Apr-25	D
Attha	15-Apr-25	D
Attha	16-Apr-25	D
Attha	17-Apr-25	D
Attha	18-Apr-25	D
Attha	19-Apr-25	D
Attha	20-Apr-25	D
Attha	21-Apr-25	D
Attha	22-Apr-25	D
Attha	23-Apr-25	D
Attha	24-Apr-25	D
Attha	25-Apr-25	D
Attha	26-Apr-25	D
Attha	27-Apr-25	D
Attha	28-Apr-25	D
Attha	29-Apr-25	D
Attha	30-Apr-25	D
Attha	1-May-25	D

Gambar 5 Data Asli



Gambar 6 Ciphertext

PT. LAZ COAL MANDIRI SLIP GAJI KARYAWAN PERSEOR: BULAN APRIL 2025			
NIR	92-2098	Level Gol	Staff
Nama	Rafly Adhies Hopen Attha	Grade	S-C
Jabatan	Supervisor HCBGA	Project	KINTAP
Tanggal Masuk	13-Mey-21	gol/Peker	B
Departemen	HCBGA	PTNP	K1
A. Penghasilan :			
Gaji Pokok	Rp	9.988.000	
Tunjangan Jabatan	Rp	3.190.000	
Tunjangan Lain-Lain	Rp	383.400	
BPJS Kesehatan Perusahaan (4%)	Rp	394.640	
Jaminan Hari Tua (3.7%)	Rp	354.845	
Jaminan Pensiun (2%)	Rp	191.700	
Jaminan Kesehatan Kerja (0.24%)	Rp	166.779	
Jaminan Kematian (0.2%)	Rp	28.755	
GAJI KOTOR	Rp	13.905.279	
B. Potongan Tanggungan Perusahaan :			
BPJS Kesehatan Perusahaan (4%)	Rp	394.640	
Jaminan Hari Tua (3.7%)	Rp	354.845	
Jaminan Pensiun (2%)	Rp	191.700	
Jaminan Kesehatan Kerja (0.24%)	Rp	166.779	
Jaminan Kematian (0.2%)	Rp	28.755	
Total Tanggungan Perusahaan :	Rp	1.126.279	
C. Potongan Karyawan :			
BPJS Kesehatan Karyawan (1%)	Rp	99.880	
Jaminan Hari Tua Karyawan (2%)	Rp	191.700	
Jaminan Pensiun (1%)	Rp	95.850	
PPH-21	Rp	143.775	
Akumulasi Tak Dibayar	Rp	-	
Potongan Lain-lain	Rp	-	
Total Potongan Karyawan :	Rp	527.175	
D. Tambahan Lain-lain :			
Ajutan Biaya Istimewa	Rp	-	
Kompensasi PKWT	Rp	-	
Sumbangan Buluh Duka	Rp	-	
GAJI BERSIH (A-B-C+D)	Rp	12.262.825	
BANK TRANSFER : BRI			
Nama Rekening :			
Nomor Rekening :			
Kintap, 01 Mei 2025			
SLIP GAJI INI DICETAK SECARA KOMPUTERISASI SEHINGGA TIDAK MEMERLUKAN TANDATANG			

Rekapitulasi Absensi		
NAME	TANGGAL	ABSENSI
Attha	1-Apr-25	D
Attha	2-Apr-25	D
Attha	3-Apr-25	D
Attha	4-Apr-25	D
Attha	5-Apr-25	D
Attha	6-Apr-25	D
Attha	7-Apr-25	D
Attha	8-Apr-25	D
Attha	9-Apr-25	D
Attha	10-Apr-25	D
Attha	11-Apr-25	D
Attha	12-Apr-25	D
Attha	13-Apr-25	D
Attha	14-Apr-25	D
Attha	15-Apr-25	D
Attha	16-Apr-25	D
Attha	17-Apr-25	D
Attha	18-Apr-25	D
Attha	19-Apr-25	D
Attha	20-Apr-25	D
Attha	21-Apr-25	D
Attha	22-Apr-25	D
Attha	23-Apr-25	D
Attha	24-Apr-25	D
Attha	25-Apr-25	D
Attha	26-Apr-25	D
Attha	27-Apr-25	D
Attha	28-Apr-25	D
Attha	29-Apr-25	D
Attha	30-Apr-25	D
Attha	1-May-25	D

Gambar 7 Hasil Dekripsi

3.4 Analisa Pengujian

Analisis hasil pengujian dilakukan untuk menilai performa serta tingkat keandalan dari suatu program. Proses ini juga berperan penting dalam meninjau keluaran pengujian guna mendukung peningkatan kualitas perangkat lunak. Setelah dilakukan serangkaian pengujian, diperoleh sejumlah temuan sebagai berikut :

- a. Durasi waktu dekripsi lebih lama disbanding enkripsi bergantung dengan ukuran *file*.
- b. Perbedaan ukuran *file* asli dengan *file* terenkripsi maupun dekripsi tidak begitu jauh, yaitu 0,01KB.

4. KESIMPULAN

Penelitian ini telah berhasil mengimplementasikan algoritma kriptografi Advanced Encryption Standard (AES-128) dalam pengembangan aplikasi pengamanan data pada PT Laz Coal Mandiri. Aplikasi yang dibangun mampu melaksanakan proses enkripsi maupun dekripsi *file* secara efektif, sehingga dapat mendukung peningkatan kerahasiaan serta integritas data perusahaan. Hasil pengujian menunjukkan bahwa kinerja enkripsi dipengaruhi oleh ukuran *file*, di mana semakin besar ukuran *file*, semakin lama pula waktu pemrosesan yang dibutuhkan. Kendati demikian, sistem yang dihasilkan terbukti mampu memberikan solusi dalam optimalisasi keamanan data perusahaan. Sebagai tindak lanjut, penelitian selanjutnya direkomendasikan untuk mengembangkan sistem dengan pendekatan multi-algoritma kriptografi. Penggabungan beberapa metode diharapkan dapat meningkatkan tingkat keamanan secara signifikan dan memberikan perlindungan lebih kuat terhadap potensi ancaman pencurian data oleh pihak yang tidak berwenang. Ucapan terima kasih disampaikan kepada PT Laz Coal Mandiri atas dukungan dan kerja samanya dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

- [1] P. A. Rizky, S. Soim, And Sholihin, "Implementasi Algoritma Kriptografi Aes Cbc Untuk Keamanan Komunikasi Data Pada Hardware," *Jurnal Resistor*, Vol. 3, No. 1, Pp. 71–78, Apr. 2024, Doi: <https://doi.org/10.31598/jurnalresistor.V7i2.1650>.
- [2] D. A. Fauzan, A. Fathurrozi, And Sugiyatno, "Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma Rsa (Rivest Shamir Adleman) Dan Aes (Advanced Encryption Standard) Berbasis Web," *Journal Of Information And Information Security (Jiforty)*, Vol. 4, No. 1, Pp. 91–104, Jun. 2023, [Online]. Available: <http://ejournal.ubharajaya.ac.id/index.php/jiforty>
- [3] D. Widyawan And Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Sknika: Sistem Komputer Dan Teknik Informatika*, Vol. 4, No. 1, Pp. 15–22, Jan. 2021.
- [4] A. P. R. Tarigan, P. S. Ramadhan, And K. Ibnutama, "Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode Aes (Advanced Encryption Standard)," *Jurnal Cyber Tech*, Vol. 5, No. 1, Pp. 26–35, Apr. 2023, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jct/index>
- [5] R. Febrianto And S. Waluyo, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (Aes-256) Untuk Mengamankan Database Penilaian Karyawan Pada Kjpp Ndr," *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, Vol. 20, No. 1, Pp. 44–49, Apr. 2023.
- [6] M. Rizki And P. F. Ariyani, "Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal," *Sknika: Sistem Komputer Dan Teknik Informatika*, Vol. 4, No. 2, Pp. 77–82, Jul. 2021.
- [7] A. T. Pandya And J. C. Chandra, "Aplikasi Keamanan File Menggunakan Algoritme Kriptografi Aes 128 Berbasis Web Pada Pilar Medical Center," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (Senafiti)*, Vol. 2, No. 2, Pp. 36–45, 2023.
- [8] T. M. Aziz And S. Dwiasnati, "Aplikasi Penomoran Surat Dengan Metode Aes Dan Rsa Untuk Penyimpanan Surat Berbasis Web," *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, Vol. 9, No. 1, Pp. 1–7, 2023.
- [9] N. Cristy And F. Riandari, "Implementasi Metode Advanced Encryption Standard (Aes 128 Bit) Untuk Mengamankan Data Keuangan," *Jikomsi [Jurnal Ilmu Komputer Dan Sistem Informatika]*, Vol. 4, No. 2, Pp. 75–85, Sep. 2021.
- [10] K. Zalukhu, Y. Syahra, And T. Syahputra, "Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan," *Jurnal Teknologi Sistem Informasi Dan Sistem Komputer Tgd*, Vol. 3, No. 2, Pp. 138–150, Jul. 2020, Doi: <https://doi.org/10.53513/jsk.V3i2.2419>.



FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS BUDI LUHUR

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260

<https://senafti.budiluhur.ac.id/>