Journal of Information and Information Security (JIFORTY)
Vol. 6, No. 2, Desember 2025, 81 – 94
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Penerapan Keamanan AES-256 Pada Sistem Kehadiran Karyawan Berbasis Kordinat

Dani Yusuf [1,*], Uus Rusmawan [2]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17142;
e-mail: dani.yusuf@dsn.ubharajaya.ac.id
[2] Teknik Informatika; Universitas Dian Nusantara; Jl. Tanjung Duren Barat ll No. 1 Grogol Jakarta Barat, 11470;
e-mail: uus.rusmawan@undira.ac.id

* Korespondensi: e-mail: dani.yusuf@dsn.ubharajaya.ac.id

Diterima: 29 Des 2025; Review: 1 Jan 2026; Disetujui: 1 Jan 2026; Diterbitkan: 2 Jan 2026

Abstract

The development of information technology has encouraged the implementation of coordinate-based employee attendance systems to improve accuracy and minimize fraud in attendance recording. However, this system poses security risks to sensitive data, such as employee identities, attendance timestamps, and location coordinates. Therefore, a reliable data security mechanism is required. This study aims to implement the Advanced Encryption Standard (AES) algorithm with a 256-bit key length in a coordinate-based employee attendance system to enhance data security. The research method used is an experimental method consisting of requirement analysis, system design, implementation of the AES-256 algorithm, and system testing stages. The results show that the implementation of AES-256 is able to encrypt attendance data effectively so that the data cannot be directly read without a decryption process. In addition, the encryption and decryption processes do not have a significant impact on system performance. Thus, the AES-256 algorithm can be effectively applied to improve security in coordinate-based employee attendance systems.
***Keywords**: Attendance System, Data Security, AES-256, Coordinates, Cryptography*

Abstrak

Perkembangan teknologi informasi mendorong penerapan sistem kehadiran karyawan berbasis koordinat untuk meningkatkan akurasi dan meminimalkan kecurangan dalam pencatatan kehadiran. Meskipun demikian, sistem ini memiliki risiko keamanan terhadap data sensitif, seperti identitas karyawan, waktu presensi, dan koordinat lokasi. Oleh karena itu, diperlukan mekanisme pengamanan data yang andal. Penelitian ini bertujuan untuk menerapkan algoritma Advanced Encryption Standard (AES) dengan panjang kunci 32-bit pada sistem kehadiran karyawan berbasis koordinat guna meningkatkan keamanan data. Metode penelitian yang digunakan adalah metode eksperimental dengan tahapan analisis kebutuhan, perancangan sistem, implementasi algoritma AES-256, serta pengujian sistem. Hasil penelitian menunjukkan bahwa penerapan AES-256 mampu mengenkripsi data kehadiran dengan baik sehingga data tidak dapat dibaca secara langsung tanpa proses dekripsi. Selain itu, proses enkripsi dan dekripsi tidak memberikan dampak signifikan terhadap kinerja sistem. Dengan demikian,

algoritma AES-256 dapat diterapkan secara efektif untuk meningkatkan keamanan pada sistem kehadiran karyawan berbasis koordinat.
Kata kunci: Sistem Kehadiran, Keamanan Data, AES-256, Koordinat, Kriptografi

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong berbagai instansi dan perusahaan untuk mengadopsi sistem digital dalam pengelolaan sumber daya manusia, salah satunya pada sistem kehadiran karyawan. Sistem kehadiran berbasis koordinat atau lokasi geografis (Global Positioning System/GPS) semakin banyak digunakan karena mampu meningkatkan akurasi pencatatan kehadiran serta meminimalkan praktik kecurangan seperti titip absen. Dengan memanfaatkan data koordinat lokasi, perusahaan dapat memastikan bahwa karyawan melakukan presensi dari lokasi yang telah ditentukan.

Namun demikian, penggunaan sistem kehadiran berbasis koordinat juga menimbulkan tantangan baru, khususnya terkait keamanan data. Data kehadiran karyawan yang meliputi identitas pengguna, waktu presensi, dan koordinat lokasi merupakan informasi sensitif yang berpotensi disalahgunakan apabila tidak dilindungi dengan mekanisme keamanan yang memadai. Ancaman seperti penyadapan data, manipulasi informasi kehadiran, dan akses tidak sah dapat merugikan perusahaan maupun karyawan.

Kriptografi adalah bidang ilmu yang mempelajari tentang cara untuk menjaga keamanan pesan dalam proses pengiriman dengan menggunakan metode penyandian tertentu, dengan tujuan agar informasi dalam pesan tersebut tidak disalahgunakan oleh orang yang bukan penerima aslinya. Kriptografi memiliki beragam metode untuk menyandikan pesan atau informasi yang ingin kita sembunyikan, seperti *Caesar Cipher*, *Affine*, *Monoalphabetic*, *Polyalphabetic*, *Vigenere*, Transposisi, dan banyak lagi metode-metode dalam kriptografi ini (Aditya Permana, 2018).

Untuk mengatasi permasalahan tersebut, diperlukan penerapan metode keamanan yang mampu melindungi kerahasiaan dan integritas data. Salah satu algoritma kriptografi yang banyak digunakan dan terbukti keamanannya adalah Advanced Encryption Standard (AES) (Huo & Wang, 2023).

Advanced Encryption Standard(AES) adalah salah satu algoritma kriptografi yang berfungsi untuk melakukan proses mengubah data asli menjadi data tersandi (encrypt) dan begitu juga sebaliknya (decrypt) dari sebuah informasi atau data (Y. Putra et al., 2021). Dibutuhkan sebuah kunci yang menjamin data tersebut terlindungi dalam kedua proses diatas. Kunci tersebut berfungsi untuk mengamankan tiap proses perubahan data. Algoritma AES menggunakan kunci simetrik yaitu kunci yang sama setiap melakukan proses enkripsi maupun deskripsi (Andriyanto & Sukmasetya, 2022).

Salah satu algoritma dalam kriptografi yaitu algoritma AES Advanced Encryption Standard (AES yang memanfaatkan teknik blok simetris dalam proses penyandian pesannya. Pengembang dari algoritma ini berasal dari Belgia yang bernama Dr. Vincent Rijmen dan Dr.

Joan Daemen pada tahun 1997. Sebagai kandidat AES, mereka berdua mengajukan algoritma ini dan berhasil menjadikannya proposal terpilih bagi AES oleh NIST (National Institute of Standard and Technology) pada tanggal 26 November 2001 (Indrayani & Suartana, 2019).

Algoritma *Advanced Encryption Standard (*AES) adalah suatu algoritma *block chiper* dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi (Nugrahantoro et al., 2020).

Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Penyandian AES menggunakan proses yang berulang yang disebut dengan *ronde*. Jumlah *ronde* yang digunakan oleh AES tergantung dengan panjang kunci yang digunakan. Setiap *ronde* membutuhkan kunci *ronde* dan masukan dari *ronde* berikutnya. Kunci *ronde* dibangkitkan berdasarkan kunci yang diberikan. Algoritma AES dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Panjang kunci mempengaruhi jumlah *round* (perputaran) (Widodo & Purnomo, 2020).

AES-256 merupakan varian AES dengan panjang kunci 32-bit yang menawarkan keseimbangan antara tingkat keamanan yang tinggi dan efisiensi kinerja, sehingga cocok diterapkan pada sistem aplikasi berbasis mobile maupun web. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menerapkan algoritma AES-256 pada sistem kehadiran karyawan berbasis koordinat guna meningkatkan keamanan data kehadiran (Indrayani & Suartana, 2019).

Diharapkan dengan penerapan enkripsi AES-256, data yang dikirim dan disimpan dalam sistem dapat terlindungi dari ancaman keamanan, sehingga sistem kehadiran menjadi lebih andal, aman, dan terpercaya dalam mendukung pengelolaan kehadiran karyawan secara digital (Nirwan et al., 2024).

Pengembangan pengamanan yang ketat terus dikembangkan untuk mencegah data pribadi bocor. Melindungi kerahasiaan file di komputer sangat penting untuk mencegah perusakan, pencurian, atau penyalahgunaan data oleh pihak yang tidak berwenang melalui jaringan computer (J. S. Putra et al., 2024).

2. Metode Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini adalah metode eksperimental, yaitu dengan merancang dan mengimplementasikan sistem kehadiran karyawan berbasis koordinat yang dilengkapi dengan mekanisme keamanan menggunakan algoritma AES-256. Tahapan penelitian dilakukan secara sistematis untuk memastikan tujuan penelitian dapat tercapai dengan baik.

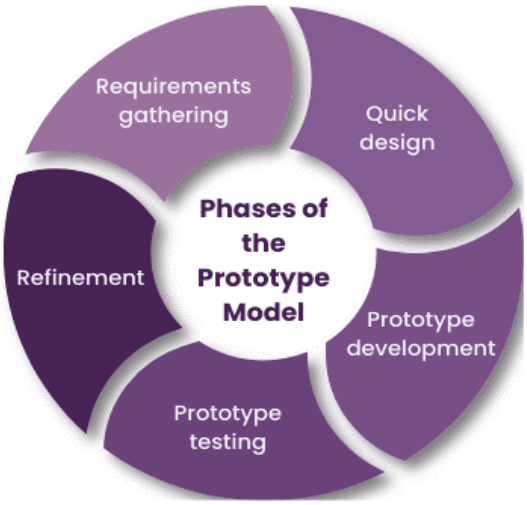
2.1. Analisis Kebutuhan

Pada tahap ini dilakukan identifikasi kebutuhan sistem, baik kebutuhan fungsional maupun non-fungsional. Kebutuhan fungsional meliputi proses login pengguna, pengambilan

koordinat lokasi karyawan, pencatatan waktu kehadiran, serta penyimpanan data kehadiran. Kebutuhan non-fungsional difokuskan pada aspek keamanan data, khususnya perlindungan terhadap data identitas karyawan dan koordinat lokasi.

2.2. Perancangan Sistem

Perancangan sistem dilakukan dengan membuat arsitektur sistem kehadiran berbasis koordinat. Sistem dirancang agar data kehadiran yang dikirim dari perangkat pengguna ke server terlebih dahulu dienkripsi menggunakan algoritma AES-256. Proses perancangan meliputi perancangan alur sistem, basis data, serta mekanisme enkripsi dan dekripsi data. Metode pengembangan sistem yang digunakan adalah metode pengembangan prototype dengan tahapan sebagai berikut.



Sumber: (Pressman, 2020)

Gambar 1. Model Pengembangan Sistem Prototype

Pada gambar 1 menunjukan model pengembangan sistem prototype yaitu:

1. **Pengumpulan Kebutuhan**

   Tahap awal dalam metode Prototype adalah pengumpulan kebutuhan sistem. Pada tahap ini dilakukan identifikasi kebutuhan fungsional dan non-fungsional sistem kehadiran karyawan berbasis koordinat. Kebutuhan fungsional meliputi proses autentikasi pengguna, pengambilan koordinat lokasi, pencatatan waktu kehadiran, serta pengelolaan data kehadiran. Kebutuhan non-fungsional difokuskan pada aspek keamanan data, khususnya perlindungan data identitas karyawan dan koordinat lokasi menggunakan algoritma AES-256.

2. **Desain Sistem**

   Tahap berikutnya adalah desain sistem Berdasarkan kebutuhan yang telah dikumpulkan, dilakukan perancangan sistem menggunakan UML. Pada tahap ini, perancangan database juga sudah dilakukan menggunakan tools MySQL Workbench.

3. **Pembuatan Prototype**

Berdasarkan kebutuhan yang telah dikumpulkan, dilakukan pembuatan prototype sistem kehadiran berbasis koordinat. Prototype ini dirancang untuk menampilkan fungsi utama sistem, seperti proses presensi berbasis lokasi dan alur pengiriman data ke server. Pada tahap ini, mekanisme enkripsi AES-256 mulai diterapkan pada data kehadiran sebelum data disimpan atau dikirimkan. Prototype yang telah dibuat kemudian dievaluasi oleh pengguna atau pihak terkait. Evaluasi dilakukan untuk menilai kesesuaian fungsi sistem dengan kebutuhan pengguna serta kemudahan penggunaan sistem. Masukan dan saran yang diperoleh pada tahap ini digunakan sebagai dasar untuk melakukan perbaikan dan pengembangan prototype pada tahap selanjutnya.

4. Pengujian Sistem

Setelah sistem dikembangkan, dilakukan pengujian untuk memastikan seluruh fungsi berjalan sesuai dengan perancangan. Pengujian meliputi pengujian fungsional sistem kehadiran, pengujian proses enkripsi dan dekripsi menggunakan AES-256, serta pengujian keamanan data kehadiran.

5. Penyempurnaan

Hasil pengujian dianalisis untuk mengetahui efektivitas metode Prototype dalam pengembangan sistem serta keberhasilan penerapan algoritma AES-256 dalam meningkatkan keamanan sistem kehadiran karyawan berbasis koordinat.

2.3. Teknik Pengumpulan Data

Dalam penelitian, terdapat berbagai teknik pengumpulan data yang umum digunakan, tergantung pada jenis penelitian, tujuan, dan sumber data yang diperlukan. Berikut adalah beberapa teknik pengumpulan data yang sering digunakan:

1. Kuesioner

   Kuesioner adalah seperangkat pertanyaan tertulis yang diberikan kepada responden untuk diisi. Kuesioner diberikan kepada pengguna aplikasi pengajuan bantuan sosial yang terdiri dari staff dinas sosial dan dari pihak kelurahan sebagai end users untuk mengetahui tingkat kepuasan pengguna.

2. Wawancara

   Wawancara adalah teknik pengumpulan data melalui percakapan langsung antara peneliti dan responden. Wawancara dilakukan kepada pejabat dinas sosial untuk mengetahui alur proses pengajuan bantuan sosial yang berjalan saat ini.

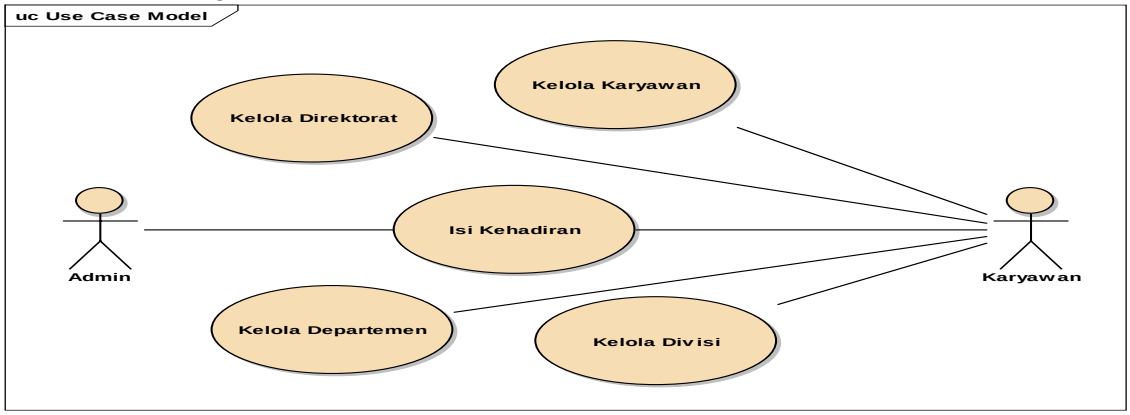
3. Observasi

   Observasi adalah teknik pengumpulan data dengan mengamati perilaku, kejadian, atau fenomena secara langsung. Observasi dilakukan di kantor Koperasi Karyawan Ubhara Jakarta Raya.

4. Studi Dokumen

Teknik ini melibatkan pengumpulan data dari dokumen, arsip, atau catatan yang sudah ada. Peneliti melakukan studi dokumen dengan mempelajari dokumen-dokumen yang terkait dengan sistem berjalan saat ini.

2.4. Use case diagram



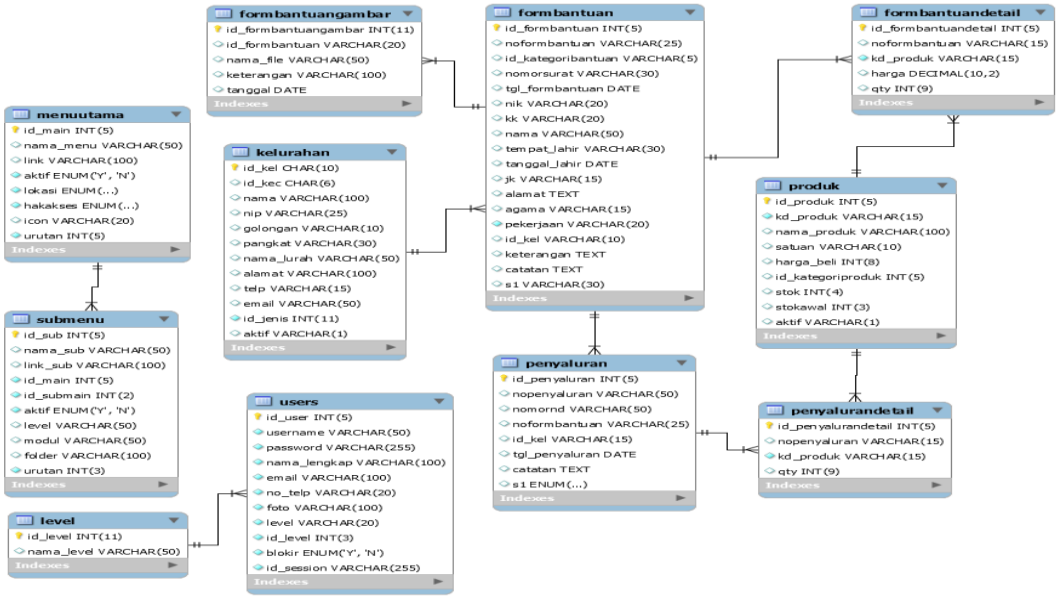
Sumber: Hasil Penelitian (2025)

Gambar 2. Use Case Diagram

Pada gambar 2 menunjukan use case diagram yang terdiri dari 2 aktor dan 5 entitas.

2.5. Enhance Entity Relationship Diagram

EERD (Enhanced Entity Relationship Diagram) digunakan untuk memodelkan struktur data secara lebih detail dan kompleks dibandingkan ERD biasa. Berikut kegunaan utamanya, dijelaskan singkat dan jelas:

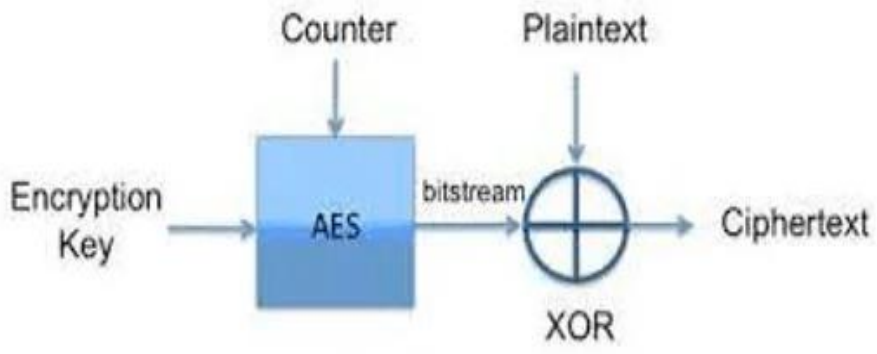


Sumber: Hasil Penelitian (2025)

Gambar 3. EERD

Pada gambar 3 menunjukan EERD dari sistem yang dibuat.

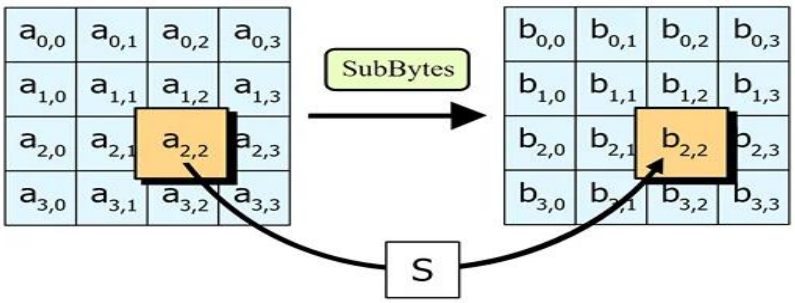
2.6. Implementasi Algoritma AES-256



Sumber: Hasil Penelitian (2025)

Gambar 4. Algoritma AES-256

Pada gambar 4 menunjukan Algoritma AES-256 digunakan untuk mengenkripsi data sensitif seperti nomor identitas, alamat, dan informasi keuangan. Proses enkripsi dan dekripsi dilakukan pada saat data dikirim dan diterima oleh sistem.



Sumber: Hasil Penelitian (2025)

Gambar 5. Metode Enkripsi AES-256

Pada gambar 5 menunjukan tahap implementasi, algoritma AES-256 diterapkan untuk mengenkripsi data kehadiran, termasuk data identitas karyawan, waktu presensi, dan koordinat lokasi. Kunci enkripsi digunakan sepanjang 32-bit sesuai dengan standar AES. Proses enkripsi dilakukan sebelum data dikirimkan ke server, sedangkan proses dekripsi dilakukan saat data akan ditampilkan atau diproses lebih lanjut oleh sistem.

AES menggunakan empat operasi dasar yang berulang secara berurutan selama proses enkripsi dan dekripsi. Operasi-operasi ini adalah SubBytes, ShiftRows, MixColumns dan AddRoundKey.

1. SubBytes

   Operasi SubBytes menggantikan setiap byte dalam blok data dengan byte yang sesuai dari S-Box (Substitution Box). S-Box adalah tabel substitusi non-linear yang menghasilkan substitusi byte yang acak, menjadikannya lebih sulit untuk melacak pola dan struktur data asli.
2. ShiftRows

Operasi ShiftRows menggeser baris dalam blok data. Hal ini memastikan bahwa data pada setiap baris tersebar secara merata di seluruh blok, sehingga meningkatkan difusi dan kesulitan analisis terhadap data.

3. MixColumns

   Operasi MixColumns melakukan transformasi kolom pada blok data. Setiap kolom dikalikan dengan matriks tetap tertentu untuk memperkenalkan difusi lebih lanjut dan membuat hubungan yang rumit antara setiap byte dalam blok.

4. AddRoundKey

   Operasi AddRoundKey memadukan blok data dengan kunci enkripsi yang sesuai. Ini melibatkan operasi XOR antara byte dalam blok data dan byte dalam kunci enkripsi yang bersesuaian.

2.7. Pengujian Sistem

Pengujian dilakukan untuk memastikan sistem berjalan sesuai dengan kebutuhan dan tujuan penelitian. Pengujian mencakup:

- Pengujian fungsional sistem kehadiran
- Pengujian keberhasilan proses enkripsi dan dekripsi data
- Pengujian keamanan dengan melihat perubahan data hasil enkripsi yang tidak dapat dibaca secara langsung

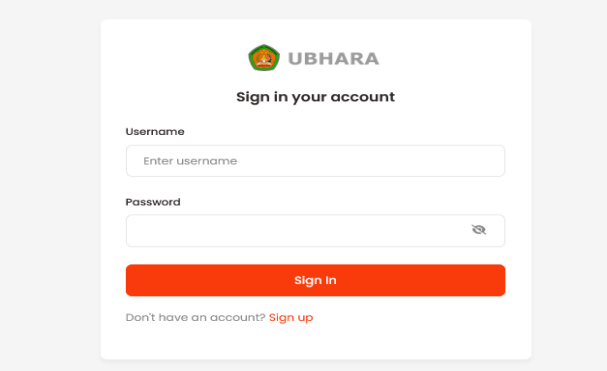
2.8. Analisis Hasil

Hasil pengujian dianalisis untuk menilai efektivitas penerapan AES-256 dalam meningkatkan keamanan sistem kehadiran berbasis koordinat.

3. Hasil dan Pembahasan

Pada bagian ini akan dijelaskan mengenai hasil penelitian dan pembahasan mengenai penelitian Penerapan Keamanan AES-256 pada Sistem Kehadiran Karyawan Berbasis Kordinat.

3.1 Login

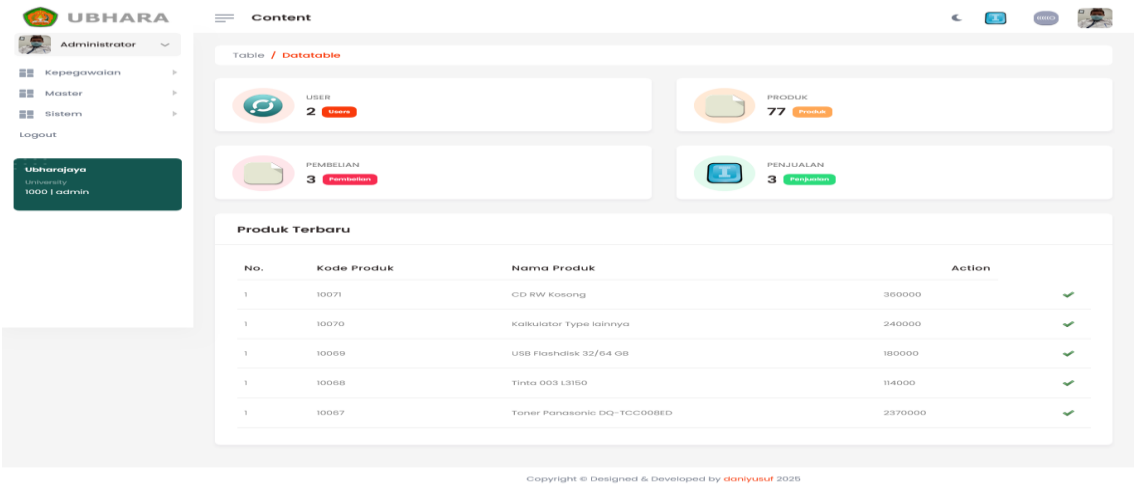


Sumber: Hasil Penelitian (2025)

Gambar 6. Halaman Login

Pada gambar 6 menunjukan mplementasi berupa prototype untuk mendapatkan masukan untuk masuk ke dalam sistem user harus memasukkan username dan password pada halaman login.

3.2 Halaman Utama



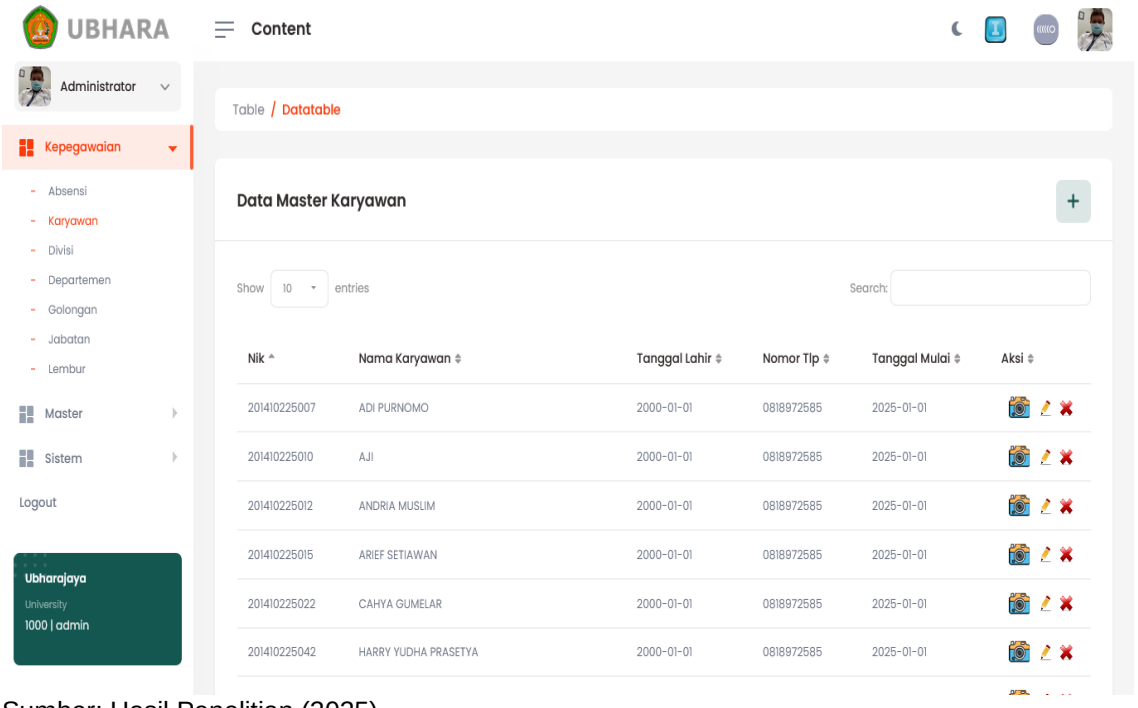
Sumber: Hasil Penelitian (2025)

Gambar 7. Halaman Utama

Pada gambar 7 menunjukan Halaman Utama yang berisi menu-menu yang dapat diakses oleh *user*.

3.3 Halaman Master Karyawan

.

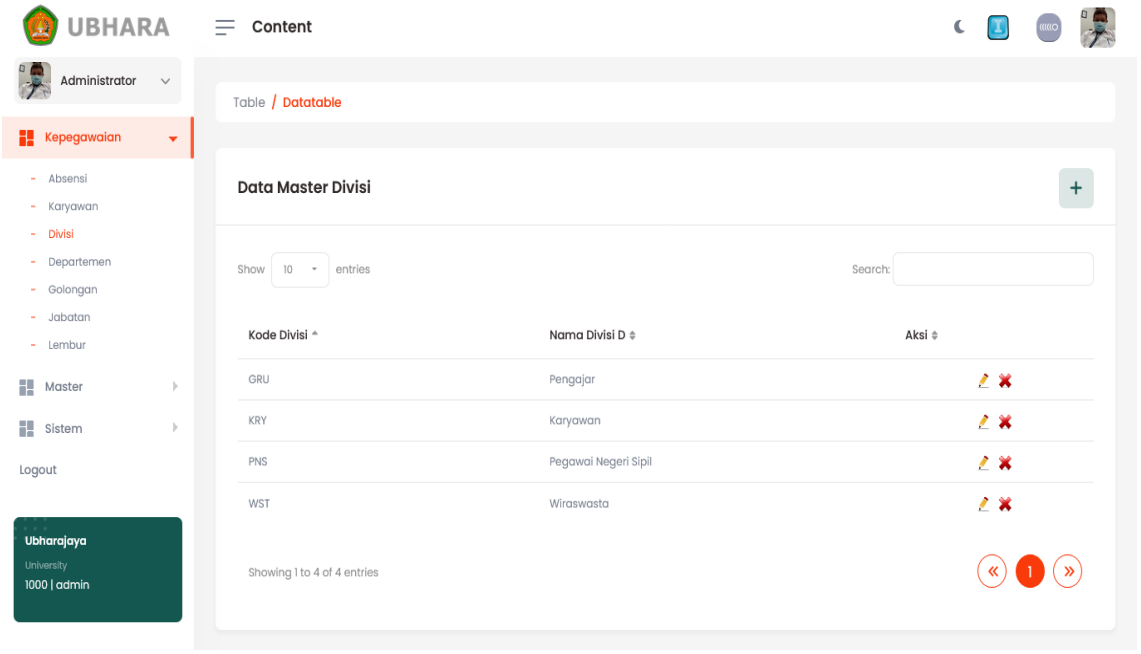


Sumber: Hasil Penelitian (2025)

Gambar 8. Halaman Master Karyawan

Pada gambar 8 menunjukan Halaman Master Karyawan yang digunakan oleh admin untuk mengelola data master karyawan.

3.4 Halaman Divisi

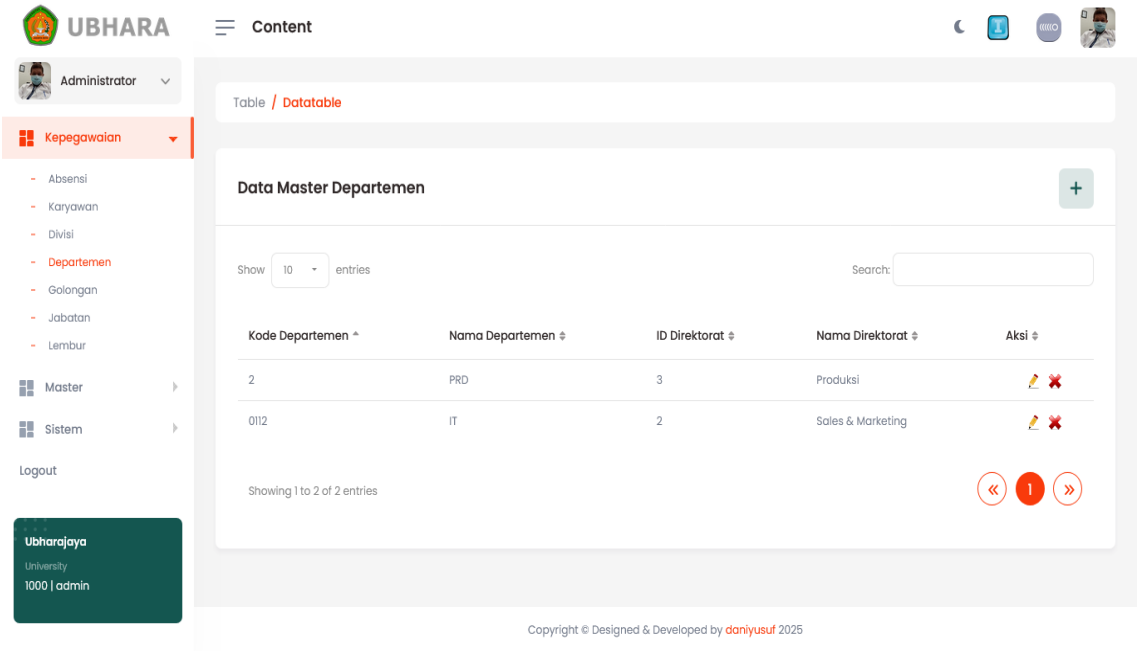


Sumber: Hasil Penelitian (2025)

Gambar 9. Halaman Master Divisi

Pada gambar 9 menunjukan Halaman Divisi digunakan oleh admin untuk mengelola data master divisi.

3.5 Halaman Departemen

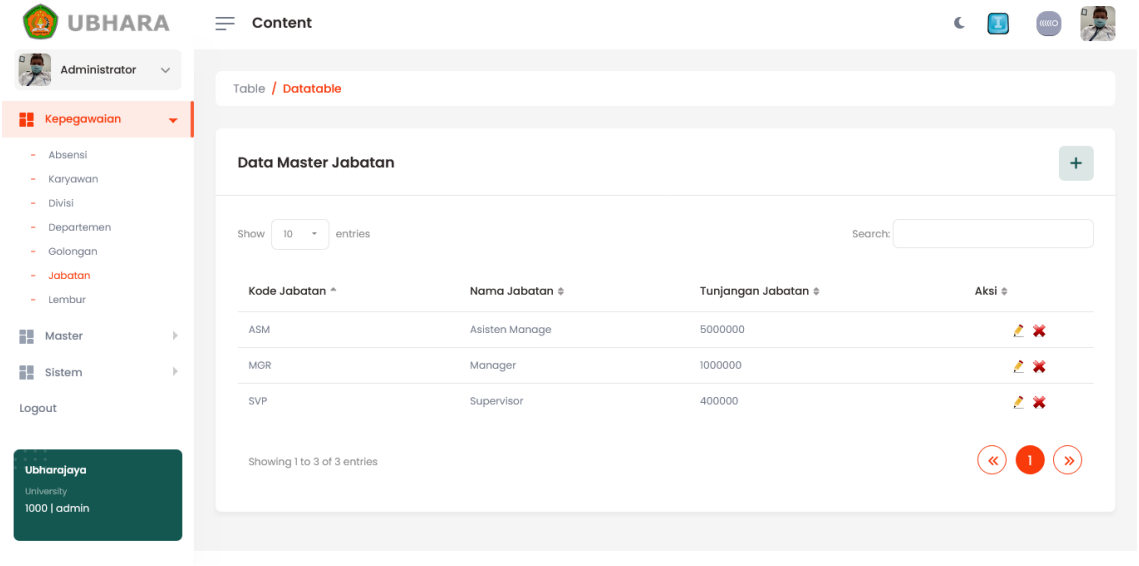


Sumber: Hasil Penelitian (2025)

Gambar 10. Halaman Master Departemen

Pada gambar 10 menunjukan Halaman Departemen yang digunakan oleh admin untuk mengelola data master departemen.

3.6 Halaman Jabatan

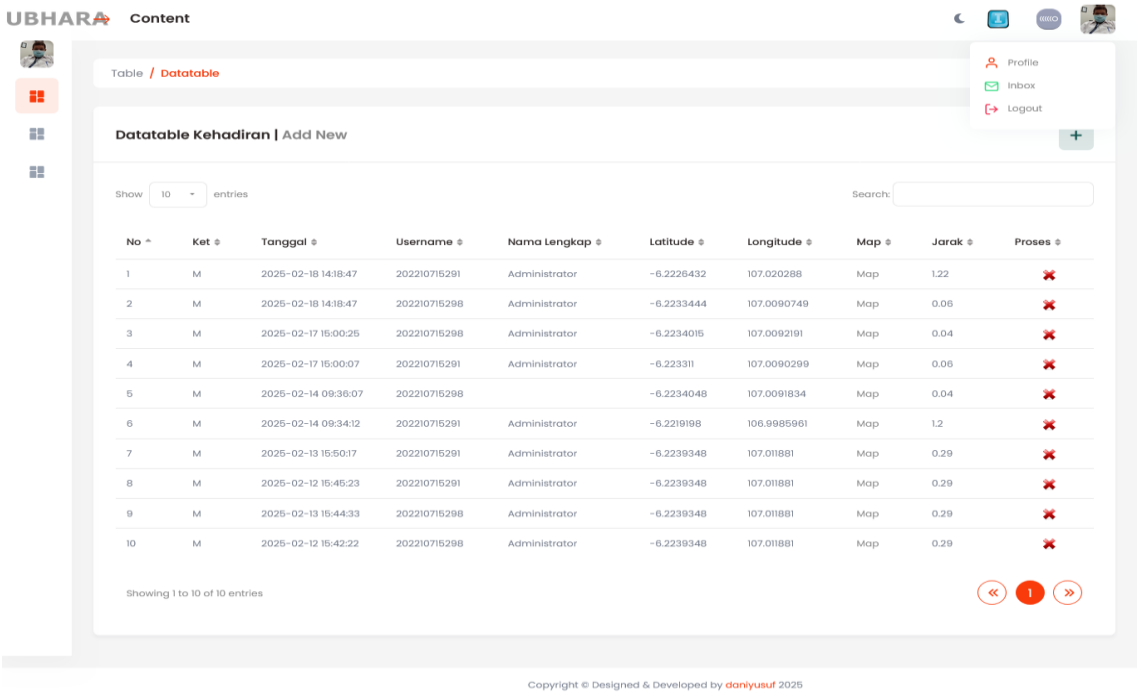


Sumber: Hasil Penelitian (2025)

Gambar 11. Halaman Master Jabatan

Pada gambar 11 menunjukan Halaman Jabatan yang digunakan oleh admin untuk mengelola data master jabatan.

3.7 Halaman Absensi

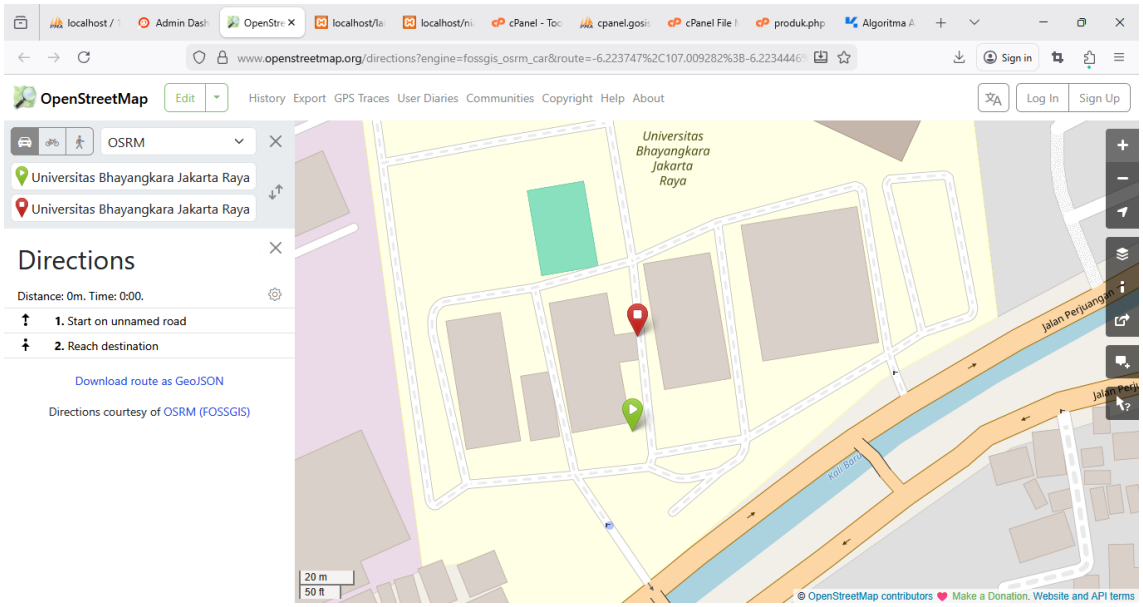


Sumber: Hasil Penelitian (2025)

Gambar 12. Halaman Kehadiran Karyawan

Pada gambar 12 menunjukan Halaman Kehadiran Karyawan yang digunakan oleh karyawan untuk absensi.

3.8 Lokasi Kehadiran Karyawan

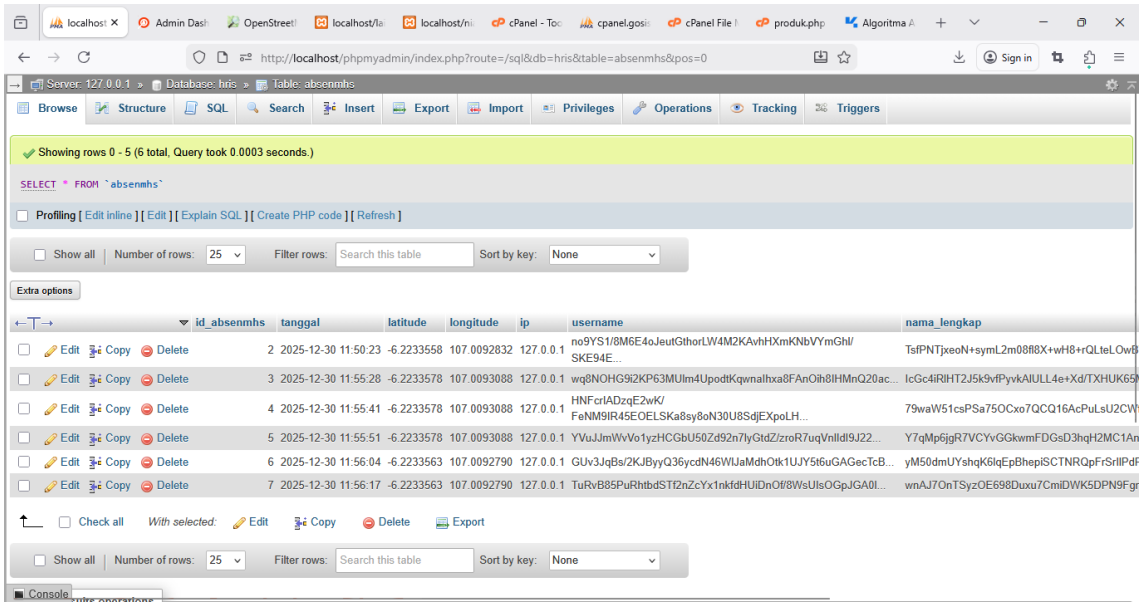


Sumber: Hasil Penelitian (2025)

Gambar 13. Lokasi Kehadiran Karyawan

Pada gambar 13 menunjukan lokasi kehadiran karyawan yang digunakan oleh admin untuk mengetahui lokasi absen karyawan.

3.9 Hasil Enkripsi Data



Sumber: Hasil Penelitian (2025)

Gambar 14. Hasil Enkripsi Data

Pada gambar 14 menunjukan Hasil Enkripsi Data yang digunakan oleh admin untuk mengelola Hasil Enkripsi Data.

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, sistem kehadiran karyawan berbasis koordinat berhasil berjalan sesuai dengan perancangan. Sistem mampu

merekam data kehadiran karyawan berdasarkan lokasi geografis dan waktu presensi secara otomatis. Penerapan algoritma AES-256 menunjukkan bahwa data kehadiran yang disimpan dan dikirimkan dalam sistem telah terenkripsi dengan baik. Data yang telah dienkripsi tidak dapat dibaca secara langsung tanpa melalui proses dekripsi menggunakan kunci yang sesuai. Hal ini membuktikan bahwa algoritma AES-256 mampu menjaga kerahasiaan data karyawan dari potensi penyadapan atau manipulasi data oleh pihak yang tidak berwenang. Selain itu, hasil pengujian menunjukkan bahwa proses enkripsi dan dekripsi menggunakan AES-256 tidak memberikan pengaruh signifikan terhadap kinerja sistem. Waktu proses masih berada dalam batas yang dapat diterima, sehingga sistem tetap responsif dan nyaman digunakan oleh pengguna. Dengan demikian, penerapan AES-256 dinilai efektif dan efisien untuk meningkatkan keamanan sistem kehadiran berbasis koordinat.

4. Kesimpulan

Berdasarkan pengujian yang dilakukan, sistem pengajuan bantuan sosial dengan algoritma AES-256 berhasil mengamankan data sensitif dengan baik. Data yang dienkripsi tidak dapat dibaca tanpa kunci dekripsi yang sesuai, sehingga mengurangi risiko kebocoran data. Selain itu, metode pengembangan prototype memungkinkan sistem untuk terus disempurnakan berdasarkan masukan dari pengguna

Penelitian ini menunjukkan bahwa penerapan algoritma AES-256 pada sistem pengajuan bantuan sosial dapat meningkatkan keamanan data sensitif. Metode pengembangan sistem prototype memungkinkan sistem untuk dikembangkan secara iteratif dan partisipatif, sehingga sesuai dengan kebutuhan pengguna. Sistem ini diharapkan dapat menjadi solusi untuk meningkatkan kepercayaan masyarakat terhadap proses pengajuan bantuan sosial. Untuk penelitian selanjutnya, dapat dilakukan pengembangan sistem dengan algoritma kriptografi yang lebih kompleks atau integrasi dengan teknologi blockchain untuk meningkatkan keamanan dan transparansi proses pengajuan bantuan sosial. Beberapa keunggulan sistem ini antara lain: Keamanan Data: Algoritma AES-256 memberikan tingkat keamanan yang tinggi untuk data sensitif. Fleksibilitas: Metode prototype memungkinkan penyesuaian sistem sesuai kebutuhan pengguna. Kemudahan Penggunaan: Antarmuka sistem dirancang sederhana sehingga mudah digunakan oleh masyarakat. Namun, terdapat beberapa tantangan dalam implementasi sistem ini, seperti kebutuhan sumber daya komputasi yang lebih tinggi untuk proses enkripsi dan dekripsi, serta pentingnya manajemen kunci yang aman.

Daftar Pustaka

Aditya Permana, A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, *4*(3), 110–115.

Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of*

Computer System and Informatics (JoSYC), *4*(1), 179–187. https://doi.org/10.47065/josyc.v4i1.2451

Huo, X., & Wang, X. (2023). Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system. *Results in Engineering*, *20*(November). https://doi.org/10.1016/j.rineng.2023.101589

Indrayani, L. A., & Suartana, I. M. (2019). Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document. *Journal of Informatics and Computer Science (JINACS)*, *1*(01), 42–47. https://doi.org/10.26740/jinacs.v1n01.p42-47

Nirwan, S., Hamidin, D., & Azzalea, S. E. (2024). Implementation of AES-256 Algorithm for Encryption on Chatting Platforms. *Internet of Things and Artificial Intelligence Journal*, *4*(4), 616–624. https://doi.org/10.31763/iota.v4i4.804

Nugrahantoro, A., Fadlil, A., & Riadi, I. (2020). Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC). *Jurnal Ilmiah FIFO*, *12*(1), 12. https://doi.org/10.22441/fifo.2020.v12i1.002

Pressman, R. S. (2020). *Software Engineering: A Practitioner's Approach.* McGraw-Hill.

Putra, J. S., Ardianto, R., & Purwono, P. (2024). Tinjauan Terhadap Implementasi Advanced Encryption Standard 256 Dalam Keamanan Data. *Device : Journal of Information System, Computer Science and Information Technology*, *5*(2), 335–355. https://doi.org/10.46576/device.v5i2.4621

Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan the Implementation of Advanced Encryption Standard on the Encryption and Decryption of the Confidential Documents At. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21