

Sistem *E-Payroll* pada Karyawan Yayasan Pendidikan Islam An-Nadwah Menggunakan Algoritma *Advanced Encryption Standard (AES)* Berbasis Web

Linda Fitriyani ¹, Dwipa Handayani ^{1,*}, Tyastuti Sri Lestari ¹, Agus Hidayat ¹

* Korespondensi: e-mail: dwipa.handayani@dsn.ubharajaya.ac.id

¹ Informatika, Fakultas Ilmu Komputer; Universitas Bhayangkara Jakarta Raya, Jl. Perjuangan No. B1, Marga Mulya, Bekasi utara, Bekasi, Jawa Barat 17143, Telp/Fax: (021) 88955882; e-mail: 202110715007@mhs.ubharajaya.ac.id, dwipa.handayani@dsn.ubharajaya.ac.id, tyas@ubharajaya.ac.id, agus.hidayat@dsn.ubharajaya.ac.id

Submitted : **11 September 2025**
Revised : **9 Oktober 2025**
Accepted : **12 November 2025**
Published : **30 November 2025**

Abstract

The rapid development of information technology encourages educational institutions to improve efficiency and security in administrative management, including payroll systems. This research aims to design a web-based E-Payroll system implemented at the Islamic Education Foundation An-Nadwah by applying the Advanced Encryption Standard (AES) algorithm to ensure the confidentiality of employee salary data. The system was developed using the Rapid Application Development (RAD) method to enable fast and user-responsive development. The implementation results show that the system can effectively encrypt and decrypt salary data, as well as provide real-time and secure payroll reports. System testing using the blackbox method demonstrates that all system functionalities work as expected. This system is expected to enhance efficiency, accuracy, and security in the payroll process within the foundation.

Keywords: AES Encryption, Data Security, E-Payroll, Rapid Application Development, Website

Abstrak

Perkembangan teknologi informasi yang pesat mendorong institusi pendidikan untuk meningkatkan efisiensi dan keamanan dalam pengelolaan administrasi, salah satunya adalah sistem penggajian. Penelitian ini bertujuan untuk merancang sistem E-Payroll berbasis web yang diterapkan pada Yayasan Pendidikan Islam An-Nadwah dengan menerapkan algoritma Advanced Encryption Standard (AES) guna menjaga kerahasiaan data gaji karyawan. Sistem dibangun menggunakan metode Rapid Application Development (RAD) untuk memastikan pengembangan yang cepat dan responsif terhadap kebutuhan pengguna. Hasil dari implementasi menunjukkan bahwa sistem mampu mengenkripsi dan mendekripsi data gaji secara efektif, serta menyajikan laporan penggajian secara real-time dan aman. Pengujian sistem menggunakan metode blackbox membuktikan bahwa seluruh fungsi sistem berjalan sesuai dengan yang diharapkan. Sistem ini diharapkan dapat meningkatkan efisiensi, akurasi, dan keamanan dalam proses penggajian di lingkungan yayasan.

Kata kunci: E-Payroll, Enkripsi AES, Keamanan Data, Rapid Application Development, Website

1. Pendahuluan

Teknologi saat ini mulai ada perkembangan, dimana bisa diterapkan diberbagai bidang pendidikan, ekonomi, kesehatan, hingga sosial budaya. Perkembangan ini telah mengubah banyak aspek kehidupan manusia, menjadikan berbagai aktivitas lebih efisien, mudah diakses, dan inovatif.

Dengan kemajuan teknologi informasi akan berdampak perubahan yang signifikan di berbagai sektor, khususnya pengelolaan sistem penggajian. Sistem penggajian yang efisien dan aman menjadi kebutuhan utama bagi organisasi dalam memastikan kelancaran administrasi keuangan serta kesejahteraan karyawan. Namun, banyak institusi masih menghadapi kendala dalam implementasi sistem penggajian yang belum optimal, seperti kesalahan perhitungan, keterlambatan pembayaran, serta ancaman keamanan data keuangan. Oleh karena itu, transformasi ke sistem penggajian berbasis web yang dilengkapi dengan teknologi keamanan data menjadi solusi strategis dalam meningkatkan efisiensi dan perlindungan informasi (Syukron & Abdurrazaq, 2021).

Gaji merupakan salah satu kompensasi upah yang diberikan kepada karyawan sebagai imbalan atas kontribusi kepada perusahaan atau lembaga. Sistem penggajian yang dirancang dengan baik sangat penting untuk memastikan pelayanan yang memadai bagi karyawan serta menyediakan informasi berkualitas bagi manajemen dalam pengambilan keputusan. Informasi ini biasanya disajikan dalam bentuk laporan yang akurat dan tepat waktu (Pahlawan & Zulfikar, 2023).

Yayasan Pendidikan Islam An-Nadwah adalah yayasan di bidang pendidikan di Kabupaten Bekasi khususnya Kecamatan Tambun Selatan. berdiri sejak tahun 1992. Yayasan Pendidikan Islam An-Nadwah terdiri dari Play Group, TK Islam (RA), SD Islam Terpadu, SMP Islam dan SMK Plus. Memiliki sebanyak 142 karyawan dan terdiri dari beberapa jabatan dalam perusahaan.

Untuk mengatasi masalah tersebut, diperlukan sistem *E-Payroll* berbasis web yang dapat meningkatkan efisiensi dan akurasi dalam pengelolaan gaji. Dengan sistem ini, proses penggajian dapat berjalan secara efektif dan efisien, sehingga dapat mempercepat distribusi gaji kepada karyawan.

Selain itu, sistem ini juga meningkatkan keamanan data gaji, yang bersifat sensitif dan perlu dilindungi dari penyalahgunaan. Penggunaan algoritma AES dalam sistem informasi dapat memberikan keamanan tambahan terhadap data sensitif, termasuk informasi penggajian (Wiharto & Mufti, 2022).

Metode *Rapid Application Development (RAD)* yang memungkinkan proses perancangan dilakukan secara iteratif dan cepat, dengan melibatkan pengguna dalam setiap tahap pengembangan. Pendekatan ini diharapkan dapat menghasilkan sistem yang sesuai dengan kebutuhan yayasan dan mudah diadaptasi oleh penggunanya.

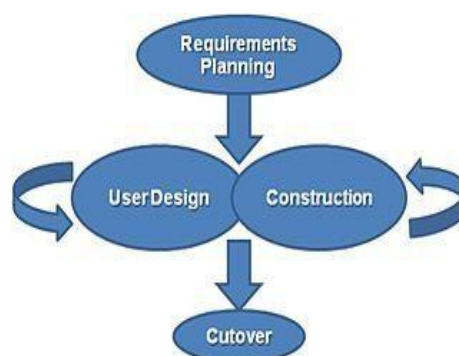
2. Metode Penelitian

2.1. Sistem Penggajian

Sistem penggajian adalah proses untuk menentukan, memonitor, mengembangkan, serta mengontrol gaji karyawan pada perusahaan. Model penggajian misalnya harian, bulanan, atau lainnya (Arisandy et al., 2023). Pendapat lain menjelaskan bahwa, Sistem penggajian adalah salah satu hal yang berkaitan dengan pengelolaan kesejahteraan tenaga kerja sehingga harus diberi perhatian khusus oleh perusahaan dalam rangka mencapai tujuannya (Setiawan et al., 2024). Berdasarkan referensi diatas, bahwa sistem penggajian berfungsi untuk menentukan, mengelola, dan mengendalikan gaji karyawan serta memperhatikan kesejahteraan tenaga kerja. Sistem ini penting untuk diperhatikan oleh perusahaan karena berpengaruh pada pencapaian tujuan perusahaan. Berbagai model penggajian, seperti harian atau bulanan, dapat dipilih sesuai kebutuhan perusahaan untuk memastikan kesejahteraan karyawan tetap terjaga.

2.2. Rapid Application Development (RAD)

Rapid Application Development (RAD) adalah metode pengembangan aplikasi yang kerap dipakai saat ini. Metode ini menekankan pada proses pembuatan aplikasi berdasarkan pembuatan *prototype*, iterasi, dan *feedback* yang berulang-ulang (Aditia et al., 2023). Pendapat lain menjelaskan bahwa. *Rapid Application Development (RAD)* adalah metodologi pengembangan dan perangkat lunak terkait yang menggunakan pendekatan berorientasi objek untuk membuat sistem komputer baru (Rizal et al., 2023). Berdasarkan kutipan diatas *Rapid Application Development (RAD)* adalah metode pengembangan aplikasi yang menekankan pada pembuatan prototype secara cepat, iterasi berulang, serta penggunaan *feedback* untuk penyempurnaan sistem. Metode ini menggunakan pendekatan berorientasi objek dalam proses pengembangan perangkat lunak agar hasilnya lebih efisien dan sesuai kebutuhan. Adapun tahapan-tahapan pada Gambar 1.



Sumber: Pahlawan & Zulfikar (2023)

Gambar 1. Tahapan RAD

a. Requirement Planning

Tahap perencanaan kebutuhan sistem, mencakup analisis proses bisnis, ruang lingkup, dan model yang digunakan. Tujuannya adalah mencapai kesepakatan antara pengguna, manajer, dan tim terkait.

b. *User Design*

Tahap perancangan sistem menggunakan alat bantu seperti UML (*use case*, *activity*, *class*, dan *sequence diagram*). Pengguna terlibat langsung dalam proses desain input dan output.

c. *Construction*

Tahap pembangunan sistem berdasarkan desain dan kesepakatan sebelumnya. Pengguna masih dapat memberikan masukan jika ada yang perlu disesuaikan. Diakhiri dengan integrasi dan pengujian sistem.

d. *Cutover*

Tahap akhir berupa konversi data, pelatihan pengguna, dan evaluasi implementasi sistem. Prosesnya cepat karena pendekatan RAD mempercepat seluruh siklus pengembang (Kosidin et al., 2020).

2.3. Algoritma *Advanced Encryption Standard (AES)*

Algoritma AES adalah sistem penyandian blok yang memiliki sifat *non-feistel* karena AES menggunakan komponen yang memiliki invers dengan panjang blok 256 bit. Penyandian AES menggunakan proses yang berulang yang disebut dengan ronde. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya, kunci ronde dibangkitkan berdasarkan kunci yang diberikan (Mustika, 2020).

Pendapat lain menjelaskan bahwa, Algoritma *Advanced Encryption Standard* merupakan sebuah algoritma simetris yang dimana menggunakan kunci yang sama untuk proses enkripsinya (Lesmana et al., 2021). Berdasarkan kutipan diatas. Algoritma AES yaitu algoritma enkripsi simetris berbasis blok *non-Feistel* dengan panjang blok 256 bit, menggunakan kunci yang sama untuk enkripsi dan dekripsi, serta bekerja melalui beberapa ronde yang bergantung pada panjang kunci. Berikut adalah rumus dasar yang digunakan dalam setiap ronde AES:

a. *AddRoundKey (Initial State)*

AddRoundKey adalah langkah pertama dan terakhir dalam setiap ronde enkripsi AES, yang menggabungkan data yang akan dienkripsi dengan kunci ronde melalui operasi XOR.

$$\text{State} = \text{State} \oplus \text{RoundKey} \quad (1)$$

Di mana: State adalah blok data 256-bit; *RoundKey* adalah kunci ronde yang dihasilkan dari kunci utama yang sudah diperluas.

b. *SubBytes*

Proses *SubBytes* adalah proses pengolahan dengan substitusi tidak linear dengan mengganti setiap *byte* dari initial state hasil langkah *AddRoundKey* (initial state) dengan *byte* pada sebuah tabel yang SBox.

$$S(x) = \text{S-box}[x] \quad (2)$$

Di mana: *x* adalah *byte* yang akan disubstitusi dalam blok data; *S(x)* adalah *byte* yang digantikan dengan nilai yang sesuai dalam S-box.

3. Hasil dan Pembahasan

3.1. Perancangan Algoritma *Advanced Encryption Standard* (AES)

Pada bagian ini dijelaskan tahapan-tahapan dalam penerapan algoritma AES (*Advanced Encryption Standard*) yang digunakan untuk mengamankan data sensitif pada sistem penggajian. Dalam implementasi AES-256 pada sistem ini, proses enkripsi diterapkan pada informasi penting seperti nama karyawan, NIK, email, nomor telepon, alamat, hingga data gaji dan tunjangan. Langkah-langkah dalam proses enkripsi meliputi konversi teks ke bentuk heksadesimal, pembentukan blok data, serta transformasi data melalui tahapan *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns* sebelum akhirnya disimpan dalam bentuk ciphertext. Proses dekripsi dilakukan dengan metode kebalikan, menggunakan kunci yang sama. Tabel 1 contoh proses enkripsi dan dekripsi menggunakan data testing.

Tabel 1. Data Testing

Atribut	Nilai
Nama	Dede Patimah
NIK	3211233
Email	dedefatimah@gmail.com
No HP	081290528338
Alamat	Sukabumi kp.rawa sapi Jatimulya Kec. Tambun Selatan Bekasi
Join Date	Selasa, 11 Februari 2020
Jabatan	Guru Kelas

Sumber: Hasil Penelitian (2025)

a. Konversi *Plaintext* ke *Hexadecimal*

Setiap karakter dalam *plaintext* dikonversi ke nilai ASCII *hexadecimal*. Jika jumlah karakter kurang dari 16 *byte*, maka dilakukan *padding* menggunakan *byte* 0x04 untuk mencapai panjang 16 *byte* sesuai blok AES.

Tabel 2 menunjukkan proses konversi setiap karakter pada nama “Dede Patimah” menjadi kode ASCII dan nilai HEX, sebagai tahap awal enkripsi AES. Hasil konversi memperlihatkan karakter huruf, spasi, serta penambahan padding 0x04 untuk memenuhi ukuran blok 16 *byte* sesuai standar AES.

Tabel 2. Konversi Nama ke HEX

Karakter	ASCII	HEX
D	68	44
e	101	65
d	100	64
e	101	65
	32	20
P	80	50

Karakter	ASCII	HEX
a	97	61
t	116	74
i	105	69
m	109	6D
a	97	61
h	104	68
	4	04
	4	04
	4	04
	4	04

Sumber: Hasil Penelitian (2025)

Tabel 3 menampilkan hasil konversi nomor HP “081290528338” ke dalam bentuk ASCII dan HEX sebagai langkah awal proses enkripsi AES. Setiap digit angka dikonversi menjadi nilai heksadesimal yang sesuai, kemudian ditambahkan empat *byte* padding 0x04 untuk memenuhi panjang blok 16 *byte*.

Tabel 3. Konversi No HP ke HEX

Karakter	ASCII	HEX
0	48	30
8	56	38
1	49	31
2	50	32
9	57	39
0	48	30
5	53	35
2	50	32
3	51	33
8	56	38
3	51	33
8	56	38
	4	04
	4	04
	4	04
	4	04

Sumber: Hasil Penelitian (2025)

Tabel 4 memperlihatkan proses konversi email “dedefatimah@gmail.com” menjadi kode ASCII dan HEX sebagai bagian dari tahap awal enkripsi AES. Setiap karakter, termasuk

simbol @, dipetakan ke nilai heksadesimal sehingga seluruh teks siap diolah dalam bentuk blok data.

Tabel 4. Konversi *Email* ke HEX

Karakter	ASCII	HEX
d	100	64
e	101	65
d	100	64
e	101	65
p	112	70
a	97	61
t	116	74
i	105	69
m	109	6D
a	97	61
h	104	68
@	64	40
g	103	67
m	109	6D
a	97	61
i	105	69

Sumber: Hasil Penelitian (2025)

b. Matriks State 4x4

Data heksadesimal disusun ke dalam bentuk matriks 4 baris × 4 kolom, yang disebut sebagai *state*. Penyusunan dilakukan dari kiri ke kanan, atas ke bawah. Matriks ini akan menjadi dasar setiap proses transformasi selanjutnya.

Tabel 5 menunjukkan penyusunan data HEX hasil konversi nama ke dalam bentuk matriks 4x4, sesuai struktur state AES. Setiap nilai ditempatkan secara berurutan dari kiri ke kanan dan dari baris atas ke baris bawah.

Tabel 5. *Matriks State* Nama

44	65	64	65
20	50	61	74
69	6D	61	68
04	04	04	04

Sumber: Hasil Penelitian (2025)

Tabel 6 menampilkan penyusunan 16 *byte* data HEX dari nomor HP ke dalam bentuk matriks state 4x4. Penataan matriks ini memastikan bahwa seluruh *byte* siap melewati proses transformasi AES secara sistematis.

Tabel 6. Matriks State No HP

30	38	31	32
39	30	35	32
33	38	33	38
04	04	04	04

Sumber: Hasil Penelitian (2025)

Tabel 7 menyusun seluruh 16 *byte* hasil konversi email ke dalam matriks 4x4 sebagai state AES. Penyusunan ini dilakukan secara berurutan sehingga setiap nilai berada pada posisi kolom dan baris yang tepat.

Tabel 7. Matriks State Email

64	65	64	65
70	61	74	69
6D	61	68	40
67	6D	61	69

Sumber: Hasil Penelitian (2025)

c. *AddRoundKey*

Pada tahap ini, kunci enkripsi yang telah dibuat sebelumnya akan di-XOR-kan dengan blok data (*state array*). Proses awal menggabungkan data dengan kunci, langkah awal pengamanan. Tabel 8 hasil operasi XOR antara matriks state nama dengan kunci ronde pertama. Nilai-nilai HEX merupakan kombinasi awal antara plaintext dan key untuk enkripsi.

Tabel 8. *AddRoundKey* Nama

Baris 0	Baris 1	Baris 2	Baris 3
0F	07	61	F0
8D	18	07	97
99	B9	6B	E5
27	67	24	12

Sumber: Hasil Penelitian (2025)

Tabel 9 menunjukkan hasil pencampuran nilai state nomor HP dengan key enkripsi melalui operasi XOR. Proses ini menghasilkan blok data baru yang sudah terikat dengan kunci ronde.

Tabel 9. *AddRoundKey* No HP

Baris 0	Baris 1	Baris 2	Baris 3
1B	31	5E	48
82	7F	23	9D
81	9B	67	F9
2D	67	24	12

Sumber: Hasil Penelitian (2025)

Tabel 10 menampilkan hasil XOR antara matriks state email dan kunci ronde, menghasilkan nilai HEX baru yang aman. Tahap ini memastikan bahwa seluruh *byte* email

telah terikat langsung dengan key yang digunakan. Blok hasil XOR ini menjadi masukan untuk proses SubBytes.

Tabel 10. *AddRoundKey* Email

Baris 0	Baris 1	Baris 2	Baris 3
08	27	06	76
92	51	40	87
B5	B9	6B	A1
0F	67	24	0F

Sumber: Hasil Penelitian (2025)

d. *SubBytes*

Setiap nilai dalam matriks akan digantikan dengan nilai baru berdasarkan tabel substitusi (S-Box). Proses ini menambah kompleksitas enkripsi karena penggantinya tidak bersifat linear dan sulit ditebak. Tabel 11 hasil substitusi setiap *byte* state menggunakan S-Box menghasilkan nilai baru yang non-linear. Transformasi memperkuat keamanan karena memutus hubungan langsung antara input dan output.

Tabel 11. Hasil *SubBytes* Nama

6B	09	C6	28
09	2F	C2	A4
3F	50	D1	4F
9C	B5	83	A4

Sumber: Hasil Penelitian (2025)

Tabel 12 menampilkan penggantian setiap elemen state nomor HP dengan nilai dari tabel S-Box. Menambahkan kerumitan enkripsi setiap *byte* berubah ke bentuk yang sulit ditebak.

Tabel 12. Hasil *SubBytes* No HP

73	0B	86	62
13	63	37	77
3F	4D	2D	30
87	B5	83	A4

Sumber: Hasil Penelitian (2025)

Tabel 13 menunjukkan perubahan seluruh *byte* state email melalui substitusi S-Box untuk meningkatkan non-linearitas cipher. Proses ini membuat pola data asli tidak lagi dapat dikenali.

Tabel 13. Hasil *SubBytes* Email

D1	4A	75	57
D3	1F	6E	51
E5	50	D1	0D
90	B5	83	3B

Sumber: Hasil Penelitian (2025)

e. *ShiftRows*

Baris-baris dalam matriks akan digeser ke kiri sebanyak jumlah barisnya. Baris pertama tidak digeser, baris kedua digeser 1 *byte*, baris ketiga 2 *byte*, dan baris keempat 3 *byte*. Ini menciptakan difusi, sehingga data tersebar lebih merata dalam blok. Tabel 14 memperlihatkan hasil pergeseran baris state nama, di mana baris kedua digeser 1 *byte*, baris ketiga 2 *byte*, dan baris keempat 3 *byte* ke kiri. Pergeseran ini menghasilkan difusi sehingga *byte* saling berpindah posisi.

Tabel 14. *ShiftRows* Nama

Baris 0	Baris 1	Baris 2	Baris 3
6B	09	C6	28
2F	C2	A4	09
D1	4F	3F	50
A4	9C	B5	83

Sumber: Hasil Penelitian (2025)

Tabel 15 menunjukkan hasil penggeseran baris pada state nomor HP sesuai aturan *ShiftRows* AES. Proses ini merombak posisi *byte* tanpa mengubah nilainya, menghasilkan penyebaran data yang lebih luas dalam kolom.

Tabel 15. *ShiftRows* No HP

Baris 0	Baris 1	Baris 2	Baris 3
73	0B	86	62
63	37	77	13
2D	30	3F	4D
A4	87	B5	83

Sumber: Hasil Penelitian (2025)

Tabel 16 menampilkan state email setelah proses *ShiftRows*, di mana baris-baris telah digeser sesuai jumlah offset masing-masing. Pergeseran ini menciptakan distribusi *byte* yang lebih acak dalam kolom.

Tabel 16. *ShiftRows* Email

D1	4A	75	57
1F	6E	51	D3
D1	0D	E5	50
3B	90	B5	83

Sumber: Hasil Penelitian (2025)

f. *MixColumns*

Setiap kolom dalam matriks diolah menggunakan operasi matematika tertentu (di bidang Galois) untuk mencampur data di dalamnya. Proses ini membuat perubahan kecil dalam data awal menghasilkan efek yang luas terhadap output akhir.

Tabel 17 memperlihatkan output dari proses MixColumns untuk data nama, yang mencampurkan setiap kolom dengan operasi aritmatika Galois. Proses ini menghasilkan nilai yang sangat berbeda dari inputnya, memperkuat penyebaran data.

Tabel 17. Hasil *MixColumns* Nama

8A	35	B7	1A
2E	FA	C6	6F
91	8E	0F	95
DA	9A	E6	10

Sumber: Hasil Penelitian (2025)

Tabel 18 menunjukkan hasil pencampuran kolom pada state nomor HP menggunakan transformasi GF(2⁸). Setiap kolom diolah sehingga perubahan satu *byte* berdampak pada seluruh kolom.

Tabel 18. Hasil *MixColumns* No HP

8E	76	9B	93
3F	0B	B1	61
84	59	14	20
7E	C2	56	B7

Sumber: Hasil Penelitian (2025)

Tabel 19 memperlihatkan hasil MixColumns pada state email, menghasilkan nilai baru yang berasal dari kombinasi matematis setiap elemen kolom. Proses ini memastikan bahwa output menjadi semakin sulit dilacak dari data aslinya.

Tabel 19. Hasil *MixColumns* Email

F5	12	3B	5D
9C	D1	61	9F
69	A3	D3	44
7B	10	F4	32

Sumber: Hasil Penelitian (2025)

g. Hasil Ciphertext

Setelah melewati seluruh *round*, output akhirnya berupa data heksadesimal yang merupakan ciphertext. Data ini tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi yang sesuai.

Tabel 20. Hasil *Ciphertext*

Karakter	Ciphertext
Dede Patimah	eyJkZWRIliwiUGF0aW1haCJ9
081290528338	eylwODEyOTA1MjIzODM4In0=
dedefatimah@gmail.com	eyJkZWRIcGF0aW1haEBnbWpC5jb20ifQ==

Sumber: Hasil Penelitian (2025)

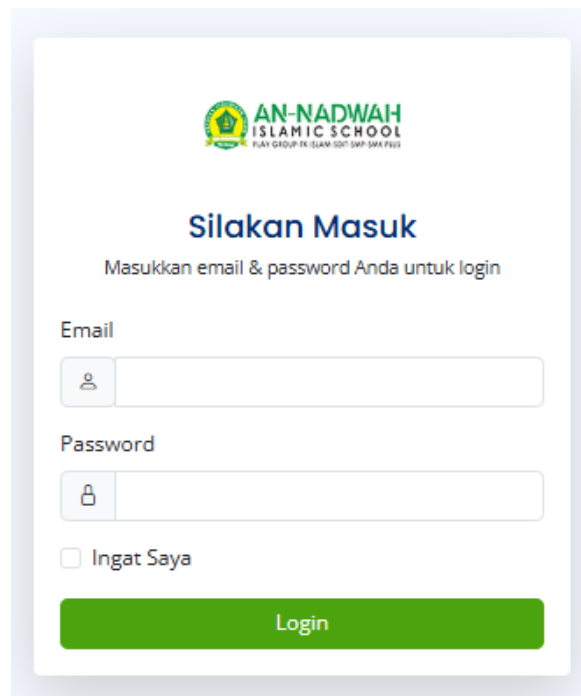
Tabel 20 menampilkan hasil akhir enkripsi berupa ciphertext untuk nama, nomor HP, dan email dalam format Base64. *Ciphertext* ini merupakan data terenkripsi yang tidak dapat

dibaca tanpa kunci dekripsi AES yang sesuai. Hasil ini menunjukkan bahwa seluruh proses enkripsi berhasil mengubah plaintext menjadi bentuk aman.

3.2. Implementasi

a. Halaman Login

Halaman login merupakan gerbang utama bagi pengguna untuk mengakses sistem. Pengguna harus memasukkan email dan password yang valid. Setelah berhasil, sistem akan mengarahkan pengguna ke *dashboard* utama.

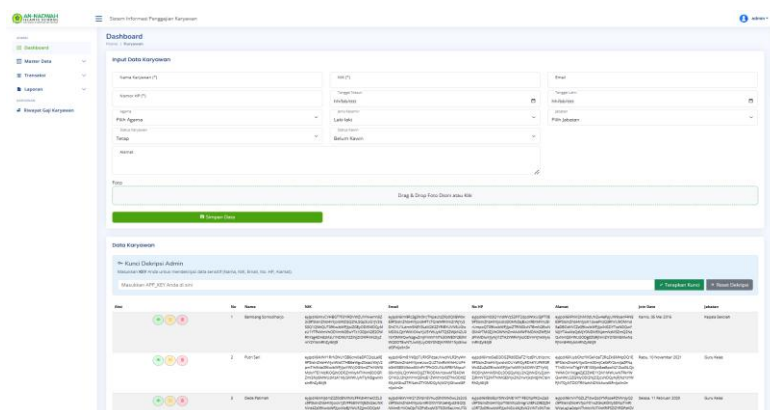


Sumber: Hasil Penelitian (2025)

Gambar 2. Halaman Login

b. Halaman Data Karyawan

Pada halaman ini admin dapat menginput data karyawan seperti nama, NIK, email, nomor HP, alamat, agama, status, dan jabatan. Halaman ini menampilkan daftar karyawan yang telah tersimpan di sistem.



Sumber: Hasil Penelitian (2025)

Gambar 3. Halaman Data Karyawan

Sistem E-Payroll pada Karyawan Yayasan Pendidikan Islam An-Nadwah Menggunakan Algoritma Advanced Encryption Standard (AES) Berbasis Web

Tabel dilengkapi dengan fitur dekripsi, yang hanya dapat diakses jika admin memasukkan key dekripsi. Hal ini memastikan bahwa data sensitif tetap aman dari akses tidak sah.

c. Halaman Data Jabatan

Admin dapat menambahkan dan melihat data jabatan seperti nama jabatan, gaji pokok, dan tunjangan. Informasi gaji dan tunjangan juga dienkripsi dan hanya bisa dilihat jika key dekripsi dimasukkan.

Sumber: Hasil Penelitian (2025)

Gambar 4. Halaman Data Jabatan

d. Halaman *Generate Gaji*

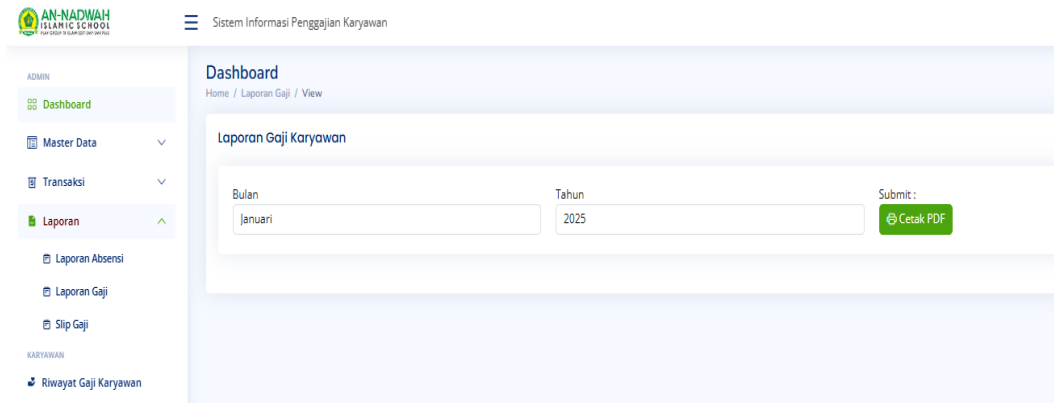
Fitur ini digunakan untuk menghitung gaji karyawan secara otomatis berdasarkan data absensi, potongan, bonus, dan data jabatan.

Sumber: Hasil Penelitian (2025)

Gambar 5. Halaman Generate Gaji

e. Halaman Laporan Gaji

Laporan ini menampilkan rekapitulasi gaji semua karyawan dalam periode tertentu. Laporan ini dapat dicetak dan digunakan untuk dokumentasi atau pelaporan internal.

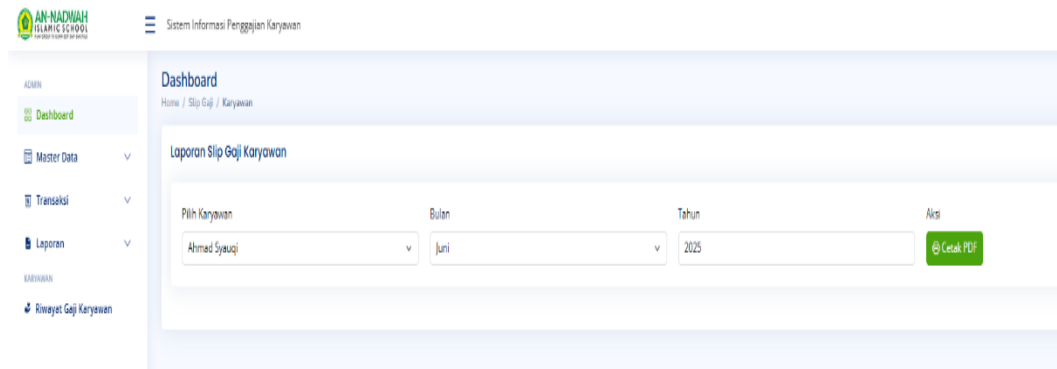


Sumber: Hasil Penelitian (2025)

Gambar 6. Halaman Laporan Gaji

f. Halaman Slip Gaji

Slip gaji karyawan disediakan dalam bentuk individual dan dapat dicetak. Slip ini berisi rincian gaji pokok, tunjangan, potongan, bonus, dan total gaji yang diterima.

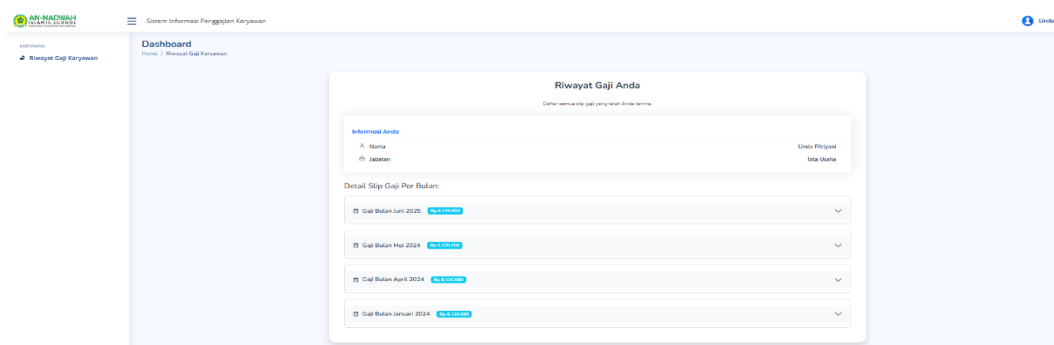


Sumber: Hasil Penelitian (2025)

Gambar 7. Halaman Slip Gaji

g. Halaman Riwayat Gaji Karyawan

Halaman ini menampilkan daftar riwayat slip gaji yang telah diterima oleh karyawan. Terdapat informasi nama, jabatan, dan daftar gaji bulanan lengkap dengan nominal yang diterima untuk setiap bulannya. Slip gaji dapat dilihat per bulan dan dirinci lebih lanjut sesuai kebutuhan karyawan.



Sumber: Hasil Penelitian (2025)

Gambar 8. Halaman Riwayat Gaji Karyawan

4. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan sistem informasi penggajian berbasis web yang mengintegrasikan algoritma Advanced Encryption Standard (AES) 256-bit sebagai metode pengamanan data sensitif. Sistem yang dikembangkan terbukti mampu meningkatkan efisiensi dan keamanan dalam pengelolaan data penggajian di lingkungan instansi atau lembaga pendidikan. Penerapan algoritma AES 256-bit berhasil mengenkripsi informasi penting seperti nama karyawan, NIK, email, nomor HP, alamat, gaji pokok, dan tunjangan jabatan, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengakses data tersebut. Proses enkripsi menghasilkan representasi data yang tidak dapat dibaca tanpa otorisasi, memberikan jaminan terhadap kerahasiaan dan integritas data.

Daftar Pustaka

- Aditia, S., Miharja, M. N. D., & Aguswin, A. (2023). Implementasi Sistem Kehadiran Praktikum Berbasis Qr_Code Dengan Whatsapp Gateway Menggunakan Metode Rapid Application Development (RAD). *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, Vol,9, No(e-ISSN 2502-8995 p-ISSN 2460-8181), 82–88.
- Arisandy, D., Ratnasari, A. D., Hosashi, F., & Angel, A. (2023). Perancangan Sistem Informasi Penggajian pada Top Remit. *Remik*, 7(1), 85–93. <https://doi.org/10.33395/remik.v7i1.11955>
- Kosidin, Firdaus, E., & Rusmana, A. (2020). Penerapan Metode Rapid Application Development (RAD) Dalam Pengembangan Aplikasi Simpan Pinjam Koperasi Syariah. *Jurnal Informatika Dan Komputer (INFOKOM)*, 8(No. 1), 24–36.
- Lesmana, H. F., Aditiawan, F. P., & Mumpuni, R. (2021). Rancang Bangun Sistem Penggajian Karyawan PT. X Menggunakan Algoritma Advanced Encryption Standard. *Prosiding Seminar Nasional Informatika Bela Negara*, 2, 54–63. <https://doi.org/10.33005/santika.v2i0.103>
- Mustika, L. (2020). Implementasi Algoritma AES Untuk Pengamanan Login dan Data Customer Pada E-Commerce Berbasis Web. *JURIKOM (Jurnal Riset Komputer)*, 7(1), 148. <https://doi.org/10.30865/jurikom.v7i1.1943>
- Pahlawan, H., & Zulfikar, A. F. (2023). Sistem Informasi Payroll Pada Yayasan Pendidikan Sandol Nusantara Menggunakan Metode Rapid Application Development (RAD). *LOGIC : Jurnal Ilmu Komputer Dan Pendidikan*, 1(6), 1591–1600.
- Rizal, C., Iqbal, M., Rian Putra, R., & Israr Fathoni, M. (2023). Rancang Bangun Sistem Informasi Posyandu Ibu Dan Anak Berbasis Web Web-Based Information System of Mother and Child Posyandu Design. *Jurnal Testing Dan Implementasi Sistem Informasi*, 1(2), 102–110.
- Setiawan, D., Ario, K., Wibowo, T., & Naury, C. (2024). Perancangan Sistem Informasi Penggajian Di Artngang Studio Berbasis Website. *Indonesian Journal of Information Technology and Computing (IMAGING)*, 4(1), 176–186.

<https://journal.polhas.ac.id/index.php/imaging/article/view/259/0>

- Syukron, A., & Abdurrazaq, M. H. (2021). Perancangan Sistem Informasi Penggajian Karyawan Berbasis Website Dengan Metode Waterfall. *Jurnal Sistem Informasi Akuntansi (JASIKA)*, 1(2), 74–83. <https://doi.org/10.31294/jasika.v1i2.624>
- Wiharto, Y., & Mufti. (2022). Implementasi Advanced Encryption Standard 128 Sebagai Pengamanan Basis Data Obat-obatan Apotek. *Jurnal Teknik Informatika Dan Sistem Informasi*, 8(2), 335–350. <https://doi.org/10.28932/jutisi.v8i2.4817>