Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Perancangan Sistem Informasi Santri Berbasis Web Menggunakan Algoritma AES Pada Yayasan Griya Fadhilah Al-Qur'an

Mohammad Badri[1*], Dodo Zaenal Abidin[2], Joni Devitra[3]

Fakultas Ilmu Komputer, Program Studi Magister Sistem Informasi, Universitas Dinamika Bangsa, Jambi, Indonesia
Email: [1]mhdbadri3@gmail.com, [2]dodozaenalabidin@gmail.com, [3]devitrajoni@yahoo.co.id
Email Penulis Korespondensi: mhdbadri3@gmail.com

Artikel Info :
Artikel History :
Submitted : 24-04-2025
Accepted : 01-02-2025
Published : 30-04-2026

Abstrak− Sistem informasi kini menjadi bagian penting dalam organisasi karena mendukung pengambilan keputusan, menyederhanakan proses kegiatan, dan membantu pengelolaan data. Proses pengelolaan data santri di Yayasan Griya Fadhilah Al-Qur'an masih dilakukan secara manual, sehingga berpotensi mengalami kerusakan, kehilangan, akses tidak sah, atau bahkan penyalahgunaan data. Absensi juga masih dilakukan secara manual menggunakan kertas, yang rentan terhadap kerusakan dan kehilangan. Pengisian penilaian dan pemantauan perkembangan santri yang menggunakan Microsoft Excel juga rentan terhadap kesalahan input, perhitungan, serta kehilangan data. Penelitian ini bertujuan untuk merancang sistem informasi santri berbasis web serta menerapkan algoritma AES *(Advanced Encryption Standard)* dalam sistem tersebut di Yayasan Griya Fadhilah Al-Qur'an. Metode pengembangan sistem yang digunakan adalah metode *Waterfall*, dengan alat bantu pemodelan UML, termasuk *use case diagram* dan *class diagram*. Sistem ini dikembangkan menggunakan bahasa pemrograman PHP dengan *framework* Laravel, dan *database* MySQL. Hasil penelitian ini adalah sistem informasi santri berbasis web dengan menerapkan algoritma AES yang dapat membantu yayasan dalam mengelola data santri serta meningkatkan keamanan data. Dengan menerapkan AES, data santri, penilaian dan perkembangan santri dapat dikonversi menjadi karakter yang tidak dapat dibaca atau diartikan secara langsung, diharapkan dapat meningkatkan keamanan dan mencegah akses tidak sah atau penyalahgunaan data.

Kata Kunci:
Perancangan; Sistem_Informasi; Santri; AES; Web

Abstract− Information systems are now an important part of an organization because they support decision making, simplify activity processes, and help manage data. The process of managing student data at the Griya Fadhilah Al-Qur'an Foundation is still done manually, which has the potential for damage, loss, unauthorized access, or even data misuse. Attendance is also still done manually using paper, which is susceptible to damage and loss. Filling in assessments and monitoring student development using Microsoft Excel is also susceptible to input errors, calculations, and data loss. This study aims to design a web-based student information system and implement the AES (Advanced Encryption Standard) algorithm in the system at the Griya Fadhilah Al-Qur'an Foundation. The system development method used is the Waterfall method, with UML modeling tools, including use case diagrams and class diagrams. This system was developed using the PHP programming language with the Laravel framework, and the MySQL database. The results of this study are a web-based student information system by implementing the AES algorithm that can help the foundation manage student data and improve data security. By implementing AES, student data, assessments and student development can be converted into characters that cannot be read or interpreted directly, which is expected to increase security and prevent unauthorized access or misuse of data.

Kata Kunci:
Design; Information System; Student; AES; Web

1. PENDAHULUAN

Seiring dengan perkembangan teknologi, sistem informasi memiliki nilai dan peran yang sangat penting bagi setiap organisasi, karena dapat meningkatkan kualitas data yang dihasilkan [1]. Sistem informasi saat ini telah menjadi elemen penting bagi setiap organisasi karena dapat mendukung pengambilan keputusan manajerial, menyederhanakan operasional harian, dan membantu mengelola data [2]. Dengan bantuan sistem informasi, data yang sebelumnya dikelola secara manual sekarang bisa diproses secara digital, sehingga menghasilkan informasi yang lebih cepat, tepat, dan mudah diakses.

Sistem informasi merupakan gabungan dari berbagai subsistem, baik yang bersifat fisik maupun nonfisik, yang saling terhubung dan berkolaborasi secara terintegrasi untuk mencapai tujuan utama, yaitu mengolah data menjadi informasi yang bermakna dan bermanfaat [3]. Salah satu contoh penerapan atau pengembangan sistem informasi adalah sistem informasi santri. Sistem informasi santri adalah kumpulan elemen terintegrasi yang dirancang untuk mengelola data santri secara efektif dan efisien [4]. Dengan adanya sistem informasi ini, organisasi atau yayasan memiliki mekanisme yang saling terhubung untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan data atau informasi guna mendukung proses organisasi [5]. Salah satu yayasan yang banyak melakukan proses organisasi setiap harinya adalah Yayasan Griya Fadhilah Al-Qur'an.

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Yayasan Griya Fadhilah Al-Qur'an adalah salah satu pusat pendidikan Tahfiz dan Tahsin Al-Qur'an di kota Medan. Yayasan Griya Fadhilah Al-Qur'an saat ini terletak di Jl. Amaliun No.181, Kota Matsum II, Kec. Medan Area, Kota Medan, Sumatera Utara, 20211. Saat ini pengelolaan data santri di Yayasan Griya Fadhilah Al-Qur'an masih dilakukan secara manual, seperti pendataan santri yang dikelola secara manual sehingga berpotensi mengalami kerusakan, kehilangan, atau akses yang tidak sah. Absensi juga masih dicatat di kertas, yang rentan terhadap kerusakan dan kehilangan. Selain itu, penilaian dan pelaporan perkembangan santri masih dikelola menggunakan Microsoft Excel, yang rentan terhadap kesalahan input data, perhitungan rumus, serta kehilangan data, yang pada akhirnya dapat memengaruhi kualitas laporan yang dihasilkan.

Data santri yang berisi informasi pribadi dan sensitif, seperti identitas pribadi, data keluarga, serta data pribadi lainnya, harus dijaga keamanannya. Jika tidak dilindungi, data berisiko disalahgunakan oleh pihak tak berwenang. Oleh karena itu, diperlukan pengamanan data untuk menjaga agar data tetap aman dan sulit diakses oleh pihak luar. AES *(Advanced Encryption Standard)* adalah salah satu algoritma pengamanan data yang dapat digunakan. AES adalah algoritma cipher blok yang dirancang oleh Daemen dan Rijmen, kemudian distandardisasi oleh NIST pada 2001. Sebagai cipher simetris, AES sangat aman untuk melindungi data rahasia dan lebih cepat dibandingkan algoritma kunci asimetris. Sejak itu, AES menjadi cipher simetris yang paling banyak digunakan dan dianalisis di seluruh dunia [6]. Algoritma ini telah dioptimalkan untuk berbagai perangkat keras dan perangkat lunak, sehingga cocok untuk aplikasi seperti komunikasi data dan penyimpanan terenkripsi.

Terdapat penelitian sebelumnya yang telah dilakukan oleh Dadang Iskandar Mulyana, dkk pada tahun 2022. Penelitian ini berfokus pada pengembangan sistem informasi santri yang sebelumnya dilakukan secara manual. Sistem informasi berbasis web yang dihasilkan ini mempermudah pengelolaan data, mempercepat proses pencatatan nilai, serta membantu dalam meminimalisir kehilangan data karena seluruh informasi disimpan secara digital [7].

Kemudian terdapat penelitian sebelumnya yang telah dilakukan oleh Faldi Rachmat Nopianto dan Ferdiansyah pada tahun 2018. Penelitian ini membahas penerapan kriptografi menggunakan algoritma AES-128 untuk mengamankan data akademik pada *database*. Pentingnya keamanan data akademik mendorong pengembangan sistem berbasis web dengan enkripsi data menggunakan AES-128 untuk mengatasi permasalahan ini. Sistem yang dihasilkan adalah aplikasi pengamanan data nilai siswa berbasis web yang menggunakan algoritma AES-128. Sistem berbasis web ini yang memiliki fitur login, pengelolaan data siswa, dan enkripsi-dekripsi data siswa dan nilai [8].

Selanjutnya terdapat penelitian sebelumnya yang telah dilakukan oleh Mayasari, dkk pada tahun 2022. Penelitian ini membahas tentang implementasi algoritma AES untuk mengamankan sistem e-aspirasi mahasiswa di Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara. Penelitian ini mengembangkan sistem informasi berbasis web dengan algoritma AES untuk mengenkripsi pesan aspirasi yang dikirimkan mahasiswa. Sistem e-aspirasi berbasis web berhasil dibangun dengan PHP dan didukung oleh AES untuk menjaga keamanan data [9].

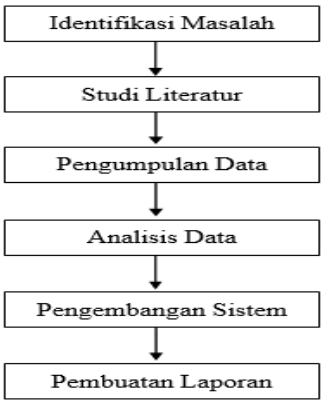
Berdasarkan penelitian terdahulu, dapat diketahui bahwa implementasi algoritma AES banyak diterapkan pada sistem informasi berbasis web untuk meningkatkan keamanan data. Merancang sistem informasi santri berbasis web dengan menerapkan algoritma AES pada Yayasan Griya Fadhilah Al-Qur'an merupakan tujuan dari penelitian ini. Sistem informasi santri ini dibangun menggunakan bahasa pemrograman PHP dengan *framework* Laravel dan *database* MySQL. Laravel merupakan salah satu *framework* PHP yang dikembangkan dengan arsitektur MVC *(Model-View-Controller)* dan dirilis dengan lisensi MIT [10]. *Framework* Laravel digunakan karena memiliki banyak *library* yang mendukung, sehingga dapat mempercepat pengembangan sistem informasi [11]. Dengan dirancangnya sistem informasi santri ini, diharapkan proses pengelolaan data santri dapat berlangsung lebih efisien dan terstruktur.

2. METODOLOGI PENELITIAN

2.1 Alur Penelitian

Alur penelitian adalah langkah atau prosedur yang akan dilakukan dalam melakukan penyusunan penelitian. Adapun alur penelitian pada penelitian ini dapat dilihat pada Gambar 1.

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

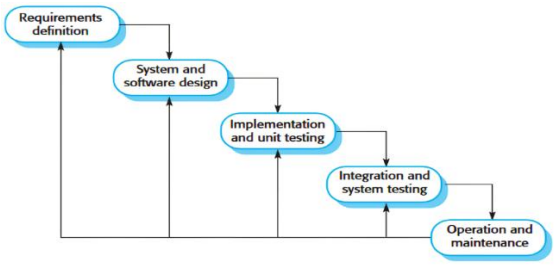


Gambar 1. Alur Penelitian

Alur penelitian pada Gambar 1 dijelaskan secara rinci sebagai berikut :

1. Identifikasi Masalah
   Pada tahap identifikasi masalah, diketahui bahwa sistem pengelolaan data santri di Yayasan Griya Fadhilah Al-Qur'an masih dilakukan secara manual. Pendataan santri dan absensi masih menggunakan kertas, yang berisiko rusak, hilang, atau disalahgunakan. Proses absensi juga masih dilakukan secara manual. Selain itu, penilaian dan pelaporan perkembangan santri masih menggunakan Microsoft Excel, yang rentan terhadap kesalahan input, perhitungan, dan kehilangan data.
2. Studi Literatur
   Pada tahap studi literatur, dilakukan pengumpulkan data dengan cara mempelajari teori dan literatur-literatur yang akurat dengan masalah yang ada pada tahap sebelumnya, yaitu mencari dan mempelajari banyak data-data dari berbagai sumber buku, laporan penelitian yang berada di perpustakaan, dan jurnal dari internet yang sesuai dengan permasalahan yang dihadapi.
3. Pengumpulan Data
   Adapun pengumpulan data dalam penelitian ini disesuaikan dengan fokus dan tujuan penelitian, dengan menggunakan beberapa teknik pengumpulan data berikut:
   a. Observasi
      Pengamatan (observasi) adalah pengamatan langsung suatu kegiatan yang sedang dilakukan. Dalam penelitian ini pengumpulan data dengan cara mengamati secara langsung sistem pengelolaan data santri yang sedang berjalan di Yayasan Griya Fadhilah Al-Qur'an.
   b. Wawancara
      Wawancara merupakan kegiatan pengumpulan data yang dilakukan dengan cara tanya jawab antara penulis dan narasumber secara lisan untuk memperoleh informasi yang akurat dan sesuai dengan fakta mengenai hal-hal yang berhubungan dengan masalah yang diteliti. Penulis melakukan wawancara langsung kepada pihak Yayasan Griya Fadhilah Al-Qur'an untuk mendapatkan data-data yang relevan agar dapat digunakan untuk merancang sistem informasi santri.
   c. Analisis Dokumen
      Dilakukan analisis dokumen guna meninjau dokumen-dokumen yang ada pada Yayasan Griya Fadhilah Al-Qur'an, seperti data santri, kelas, penjadwalan, absensi, penilaian dan perkembangan santri yang akan digunakan untuk analisis dan perancangan sistem informasi santri pada Yayasan Griya Fadhilah Al-Qur'an berbasis web.
4. Analisis Data
   Pada tahapan ini, dilakukan analisis sistem informasi santri berdasarkan hasil pengumpulan data pada objek yang diteliti, sehingga dapat dihasilkan solusi atas permasalahan yang dihadapi dalam pengelolaan data santri di Yayasan Griya Fadhilah Al-Qur'an. Pada tahap ini dilakukan analisis data yang telah dikumpulkan untuk merancang sistem agar dapat sesuai dengan yang diperlukan Yayasan Griya Fadhilah Al-Qur'an.
5. Pengembangan Sistem
   Pada tahap ini, pengembangan sistem dilakukan dengan menggunakan metode *waterfall* untuk membangun sistem informasi santri di Yayasan Griya Fadhilah Al-Qur'an, berdasarkan hasil analisis data yang telah dilakukan. SDLC *(Systems Development Life Cycle)* adalah kerangka dasar dalam pengembangan sistem. Salah satu pendekatan dalam SDLC adalah metode *Waterfall*, yang menggambarkan pengembangan perangkat lunak melalui beberapa tahapan [12]. Metode ini mengharuskan setiap fase dimulai setelah fase sebelumnya selesai, dengan hasil fase pertama menjadi input untuk fase berikutnya. Prosesnya berjalan bertahap seperti aliran air terjun *(Waterfall)*, cocok untuk proyek sistem baru atau pengembangan perangkat lunak dengan risiko rendah dan waktu pengembangan panjang [13].

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1



Gambar 2. Metode *Waterfall* [12]

Gambar 2 menunjukkan tahapan-tahapan pada metode *Waterfall*. Berikut adalah penjelasan dari masing-masing tahapan tersebut:

a. *Requirements Definition*
   Tahap *requirements definition* adalah tahap interaksi intensif antara analis sistem dengan pengguna sistem. Pada tahap ini dilakukan pendefinisian kebutuhan sistem informasi santri yaitu analisis fungsionalitas dan non fungsionalitas yang digunakan untuk merancang sistem.
b. *System and Software Design*
   Pada tahap desain sistem dan perangkat lunak dilakukan penafsiran analisis kebutuhan sistem yang dibuat pada tahap sebelumnya, menggunakan alat bantu pengembangan sistem *Unified Modelling Langauage (UML)*, seperti *use case diagram, activity diagram, class diagram* untuk menggambarkan alur sistem yang berjalan pada pengelolaan data santri di Yayasan Griya Fadhilah Al-Qur'an, serta membuat rancangan desain sistem. Desain yang dibuat ada dua, yaitu desain *interface* berupa rancangan tampilan *output* dan *input* sistem dan desain struktur data berupa rancangan *database* yang akan digunakan. Kemudian pada tahap ini juga terdapat simulasi proses enkripsi dan dekripsi AES.
c. *Implementation and Unit Testing*
   Pada tahap implementasi dan pengujian unit, dilakukan pengimplementasian desain sistem informasi santri pada Yayasan Griya Fadhilah Al-Qur'an berbasis web yang telah dirancang dengan menggunakan alat bantu pembuatan program yaitu menggunakan bahasa pemrograman *PHP* dengan *framework* Laravel, *database MySQL*, aplikasi *Visual Studio Code* untuk editor *code, XAMPP* dan *browser*. Pada tahap ini setiap perancangan dilakukan pengujian dan dicoba satu persatu dan dilakukan perbaikan apabila tidak sesuai dengan kebutuhan.
d. *Integration and System Testing*
   Pada tahap integrasi dan pengujian sistem, peneliti menggunakan metode *black-box testing* untuk memeriksa fungsionalitas dan *output* setiap bagian sistem. Tujuannya adalah memastikan keluaran sistem sesuai dengan yang diharapkan dan menemukan kesalahan untuk diperbaiki.
e. *Operation and Maintenance*
   Tahap terakhir yaitu tahap operasi dan perawatan sistem, pada tahap ini dilakukan proses pengembangan sistem yang dimana sewaktu-waktu dapat mengalami perubahan mengikuti kebutuhan perangkat lunak.

6. Pembuatan Laporan
   Pada tahap ini, dilakukan penyusunan laporan yang berguna untuk memperjelas, serta merangkum seluruh kegiatan penelitian perancangan sistem informasi santri berbasis web dengan menerapkan algoritma AES pada Yayasan Griya Fadhilah Al-Qur'an, untuk bahan evaluasi terhadap penelitian yang telah dilakukan.

3. HASIL DAN PEMBAHASAN

3.1 Simulasi Proses Algoritma AES

AES *(Advanced Encryption Standard)* adalah algoritma kriptografi simetris modern pengganti DES, yang dipublikasikan oleh NIST pada tahun 2001 [14]. Penelitian ini menggunakan AES 128-bit. Proses enkripsi dilakukan untuk mengubah data asli (*plaintext*) menjadi data terenkripsi (*ciphertext*) menggunakan kunci enkripsi. Dalam proses enkripsi menggunakan AES-128, langkah awal yaitu mengubah *state* dan *key* ke bentuk hexadecimal dengan berpedoman Tabel ASCII. Pada Tabel 1 dan Tabel 2 menunjukkan hasil konversi *state* dan *key* ke dalam bentuk hexadecimal berpedoman tabel ASCII:

Tabel 1. *State*

State	a	n	g	g	u	n		l	e	s	t	a	r	i		
Hexa	61	6E	67	67	75	6E	20	6C	65	73	74	61	72	69	02	02

Tabel 2. *Cipher Key*

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Key	y	a	y	a	s	a	n	g	f	q	o	k	e	1	2	3
Hexa	79	61	79	61	73	61	6E	67	66	71	6F	6B	65	31	32	33

Untuk mendapatkan hasil putaran pertama, caranya melakukan XOR antara *state* dengan *cipher key*. Berikut adalah tampilan hasil XOR antara *state* dengan *cipher key* ditunjukkan pada Tabel 3.

Tabel 3. Hasil XOR *State* dengan *Cipher Key*

State	61	6E	67	67	75	6E	20	6C	65	73	74	61	72	69	02	02
Chiper Key	79	61	79	61	73	61	6E	67	66	71	6F	6B	65	31	32	33
Hasil XOR	18	0F	1E	06	06	0F	4E	0B	03	02	1B	0A	17	58	30	31

Pada AES, terdapat proses ekspansi kunci yang bertujuan untuk menghasilkan sejumlah kunci tambahan *(subkey)* dari kunci utama, yang akan digunakan di setiap ronde enkripsi dan dekripsi guna meningkatkan keamanan [15]. Berikut hasil pembangkitan kunci atau *key expansion* ditampilkan pada Tabel 4.

Tabel 4. *Key Expansion Round 0-10*

Round ke-	Field
0	7961796173616e6766716f6b65313233
1	bf42ba2ccc23d44baa52bb20cf638913
2	46e5c7a68ac613ed2094a8cdeff721de
3	2a18da79a0dec994804a61596fbd4087
4	5811cdd1f8cf04457885651c1738259b
5	4f2ed921b7e1dd64cf64b878d85c9de3
6	2570c840929115245df5ad5c85a930bf
7	b674c0d724e5d5f3791078affcb94810
8	60260a6744c3df943dd3a73bc16aef2b
9	79f9fb1f3d3a248b00e983b0c1836c9b
10	a3a9ef679e93cbec9e7a485c5ff924c7

Untuk mendapatkan hasil pada tabel 4 harus melalui beberapa cara seperti berikut:

1. *Round* 0 = *Cipher Key*
2. Kolom pertama setiap round dihasilkan dengan cara melakukan Rotword (Rotasi byte) pada kolom pertama round sebelumnya. Hasil rotword disubtitusi setiap byte-nya dengan berpedoman tabel S-Box (Subbytes). Setelah itu dilakukan XOR antara hasil subbytes dengan kolom pertama round sebelumnya dan juga dengan tabel RCON yang ditunjukkan pada Tabel 5.

Tabel 5. *Rcon*

Round	1	2	3	4	5	6	7	8	9	10
Rcon[]	01	02	04	08	10	20	40	80	1b	36
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00

3. Kolom kedua sampai kolom keempat dihasilkan dengan cara melakukan XOR antara kolom keempat dengan kolom pertama di round sebelumnya.

Proses enkripsi round 1:

1. *Subbytes*
   Transformasi *SubBytes* dalam algoritma AES adalah langkah di mana setiap byte pada matriks *state* diganti dengan nilai baru menggunakan tabel substitusi yang disebut S-Box [15]. XOR antara *plaintext* dengan *cipherkey* diubah senilai dengan berpedoman tabel S-Box. Sedangkan untuk round 2 sampai *round* 10 dihasilkan dengan cara merubah hasil proses enkripsi pada *round* sebelumnya senilai dengan berpedoman tabel S-Box.

18	0F	1E	06	06	0F	4E	0B	03	02	1B	0A	17	58	30	31
Transformasi menggunakan tabel S-Box															
AD	76	72	6F	6F	76	2F	2B	7B	77	AF	67	F0	6A	04	C7

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Gambar 3. *Subbytes*

2. *Shiftrows*
   Transformasi *ShiftRows* dalam algoritma AES adalah langkah yang mengatur ulang posisi byte dalam matriks *state* dengan cara menggeser baris-barisnya ke kiri. Baris pertama tetap di tempat, baris kedua digeser satu posisi ke kiri, baris ketiga digeser dua posisi, dan baris keempat digeser tiga posisi ke kiri [15]. Contoh penerapan shiftrows seperti ditunjukkan pada Gambar 4.

AD	76	72	6F	6F	76	2F	2B	7B	77	AF	67	F0	6A	04	C7
Pergeseran *byte* pada setiap baris *state*															
AD	76	AF	C7	6F	77	04	6F	7B	6A	72	2B	F0	76	2F	67

Gambar 4. *Shiftrows*

Tahap ini hanya berlaku pada proses enkripsi round 1 sampai round 9.

3. *Mix Column*
   Melakukan perkalian antara matrix yang sudah ditentukan dengan hasil shiftrows. Berikut merupakan proses Shiftrows ditunjukkan pada Gambar 5.

02	03	01	01		AD	6F	7B	F0		B3	2C	11	29
01	02	03	01		76	77	6A	76		6C	E2	12	0A
01	01	02	03	x	AF	04	72	2F	=	CC	A1	88	71
03	01	01	02		C7	6F	2B	67		A0	1C	C3	9C

Gambar 5. *Mix Column*

4. *Add Round Key*
   Melakukan XOR antara hasil *mixcolumn* dengan *round* yang sudah didapat pada proses pembangkitan kunci. Berikut proses *add round key* pada proses *round* 1 ditunjukkan pada Gambar 6.

B3	2C	11	29		BF	CC	AA	CF		0C	E0	BB	E6
6C	E2	12	0A		42	23	52	63		2E	C1	40	69
CC	A1	88	71	⊕	BA	D4	BB	89	=	76	75	33	F8
A0	1C	C3	9C		2C	4B	20	13		8C	57	E3	8F

Gambar 6. *Add Round Key*

Pada proses *round* 2 sampai *round* 9 sama dengan *round* 1, sedangkan untuk *round* 10 proses XOR-nya dilakukan dengan hasil *shiftrows*.

Hasil akhir enkripsi
Plaintext : anggun lestari
Cipher Key : yayasangfqoke123
Cipher Text : 4452e0efc284ba08aefb09fcfbb33974

Hasil enkripsi kemudian didekripsi, proses dekripsi merupakan proses pengembalian dari proses enkripsi. Berikut merupakan langkah – langkah dekripsi:
Proses round 0 :
Proses round 0 ini hasilnya akan menjadi block yang akan digunakan pada round 1. Proses ditunjukkan pada Gambar 7.

44	C2	AE	FB		A3	9E	9E	5F		E7	5C	30	A4
52	84	FB	B3		A9	93	7A	F9		FB	17	81	4A
E0	BA	09	39	⊕	EF	CB	48	24	=	0F	71	41	1D
EF	08	FC	74		67	EC	5C	C7		88	E4	A0	B3

Gambar 7. *Round* 0 dekripsi

Proses *round* 1:
1. Invers *Shiftrows*

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

E7	5C	30	A4
FB	17	81	4A
0F	71	41	1D
88	E4	A0	B3

=

E7	5C	30	A4
4A	FB	17	81
41	1D	0F	71
E4	A0	B3	88

Gambar 8. Invers *Shiftrows*

2. Invers *Subbytes*

E7	5C	30	A4
4A	FB	17	81
41	1D	0F	71
E4	A0	B3	88

InvSubbytes →

B0	A7	08	1D
5C	63	87	91
F8	DE	FB	2C
AE	47	4B	97

Gambar 9. Invers *Subbytes*

3. Invers *Add Round Key*

B0	A7	08	1D
5C	63	87	91
F8	DE	FB	2C
AE	47	4B	97

⊕

79	3D	00	C1
F9	3A	E9	83
FB	24	83	6C
1F	8B	B0	9B

=

C9	9A	08	DC
A5	59	6E	12
03	FA	78	40
B1	CC	FB	0C

Gambar 10. Invers *Add Round Key*

4. Invers *Mix Column*

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

x

C9	9A	08	DC
A5	59	6E	12
03	FA	78	40
B1	CC	FB	0C

=

60	80	93	E3
D6	7A	AC	30
0D	11	32	60
65	1E	E8	31

Gambar 11. Invers *Mix Column*

Tahap ini hanya berlaku pada proses dekripsi *round* 1 sampai *round* 9. Pada proses *round* 2 sampai *round* 9 sama dengan *round* 1, sedangkan untuk *round* 10 proses XOR-nya dilakukan dengan hasil *shiftrows* tanpa proses *mix column*.

Hasil Akhir Dekripsi

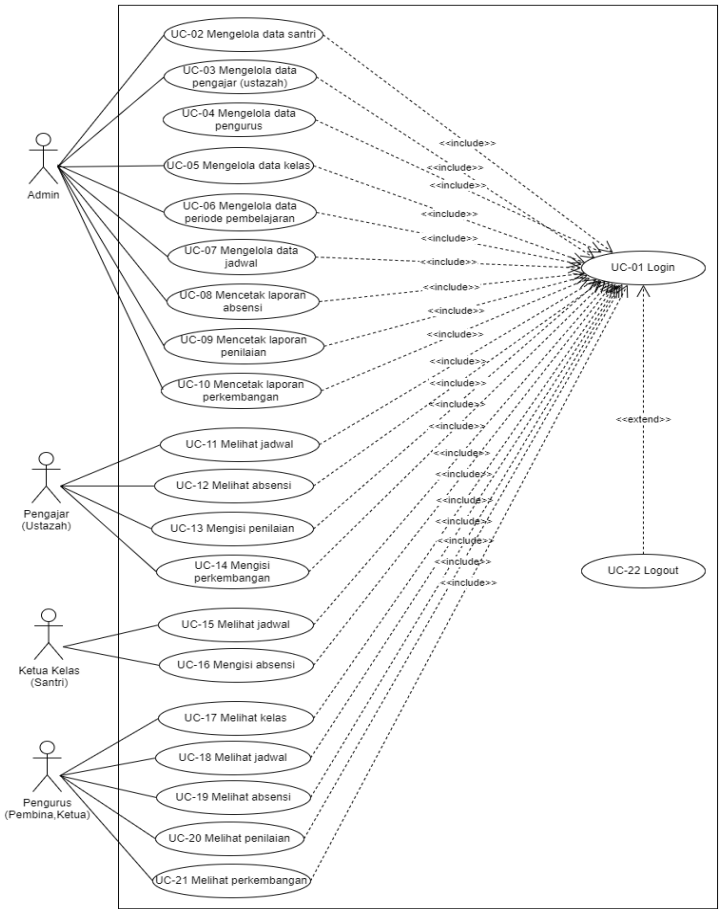
Cipher Key : yayasangfqoke123
Cipher Text : 4452e0efc284ba08aefb09fcfbb33974
Plaintext : anggun lestari

3.2 Desain Sistem

1. *Use Case Diagram*

Use case diagram menggambarkan interaksi antara pengguna *(user)* dengan sistem [16]. *Use case diagram* digunakan untuk mengilustrasikan fungsi-fungsi utama suatu sistem dan berbagai cara yang dilakukan *user* atau pengguna untuk berinteraksi dengan sistem [17]. Setiap *use case* harus memberikan hasil yang terlihat dan bernilai bagi aktor atau pihak terkait [18]. Berikut *use case diagram* sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an dapat dilihat pada Gambar 12.

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

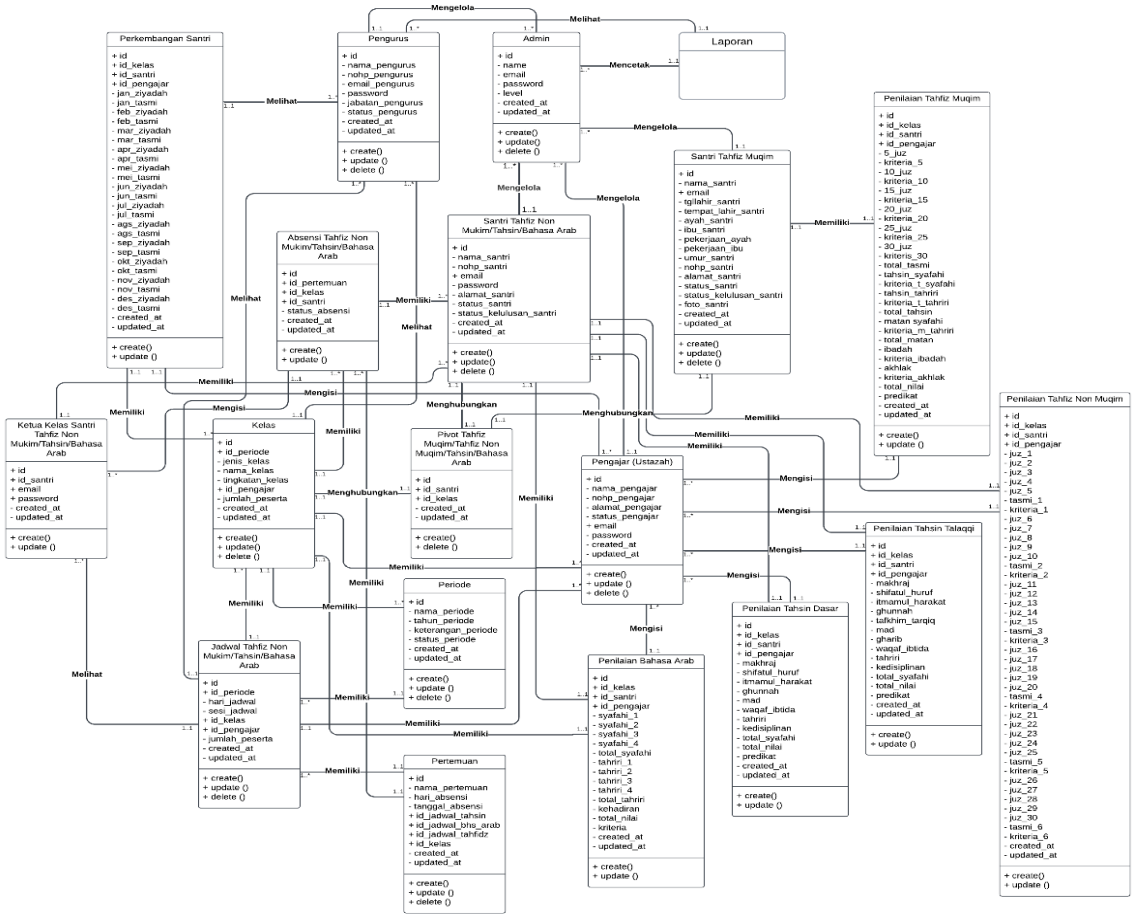


Gambar 12. *Use Case Diagram*

Gambar 12 merupakan *use case diagram* pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. *Use case diagram* tersebut menggambarkan proses pengelolaan data santri pada Yayasan Griya Fadhilah Al-Qur'an.

2. *Class Diagram*
   Diagram kelas atau *class diagram* menggambarkan struktur sistem dari segi pendefinisian *class-class* yang akan dibuat untuk membangun sistem [19]. Diagram ini memberikan pemahaman tentang sistem melalui penggambaran kelas dan hubungan antar kelas [20]. *Class diagram* untuk sistem ini dapat dilihat pada Gambar 13.

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

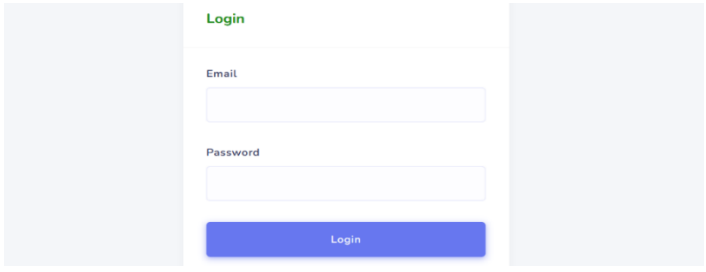


Gambar 13. *Class Diagram*

Gambar 13 merupakan *class diagram* pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. *Class diagram* menggambarkan menggambarkan struktur sistem dengan mendefinisikan kelas-kelas yang digunakan dalam pembangunan sistem.

3.3 Implementasi Sistem

1. Tampilan Halaman *Login*
   Berikut merupakan tampilan halaman *login* sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an tertera pada gambar 14.

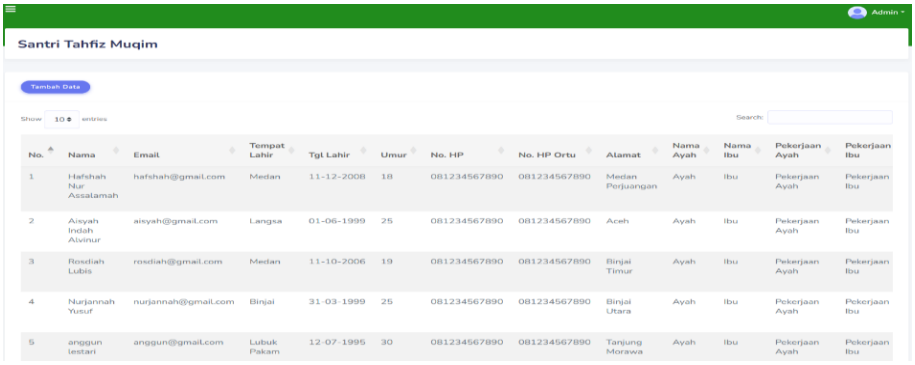


Gambar 14. Tampilan Halaman *Login*

Gambar 14 adalah tampilan halaman *login* sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman *login* merupakan halaman yang pertama kali ditampilkan saat admin, pengajar (ustazah), ketua kelas dan pengurus mengakses sistem. Pengguna dapat melakukan *login* untuk masuk ke dalam sistem.

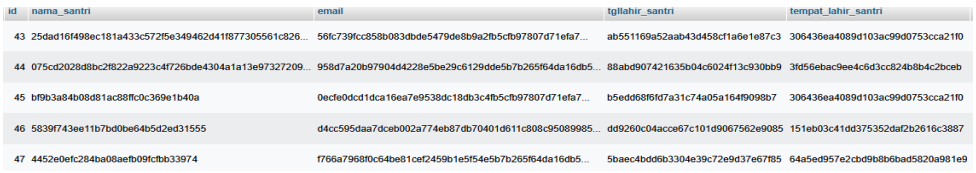
2. Tampilan Halaman Data Santri Pada Admin
   Berikut merupakan tampilan halaman data santri pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an tertera pada gambar 15.

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1



Gambar 15. Tampilan Halaman Data Santri

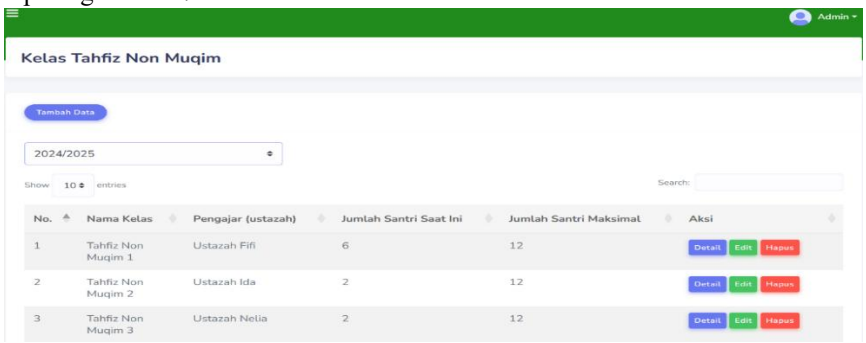
Gambar 15 adalah tampilan halaman data santri pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman data santri merupakan halaman yang ditampilkan saat admin memilih menu santri. Adapun penerapan algoritma AES 128-bit pada sistem informasi santri ini yaitu mengenkripsi data santri yang ada pada *database*. Mengenkripsi data santri pada *database* bertujuan untuk melindungi kerahasiaan dan keamanannya dari akses tidak sah. Dengan enkripsi seperti AES, data diubah menjadi format yang tidak dapat langsung diartikan atau yang hanya bisa dibaca dengan kunci dekripsi. Sedangkan pada tampilan data santri pada Gambar 15 di dalam sistem informasi santri sudah di dekripsi, sehingga admin dapat langsung melihatnya tanpa harus menginputkan kunci. Berikut hasil penerapan enkripsi data santri pada *database* dapat dilihat pada Gambar 16.



Gambar 16. Hasil Implementasi Penerapan Enkripsi Data Santri Pada *Database*

Adapun hasil ciphertext pada proses simulasi AES di pembahasan sebelumnya yaitu "4452e0efc284ba08aefb09fcfbb33974", sesuai dengan hasil enkripsi data santri di *database* sistem informasi santri pada Gambar 16.

3. Tampilan Halaman Data Kelas Pada Admin
   Berikut merupakan tampilan halaman data kelas pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an tertera pada gambar 17.

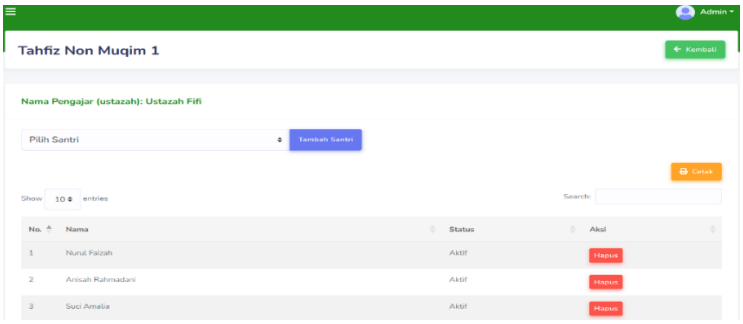


Gambar 17. Tampilan Halaman Data Kelas

Gambar 17 adalah tampilan halaman data kelas pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman data kelas merupakan halaman yang ditampilkan saat admin memilih menu kelas. Kelas pada sistem ini adalah penyebutan dalam pengelompokkan jenis kegiatan pembelajaran dan nama masing-masing kelasnya. Adapun jika admin mengklik tombol detail maka akan menampilkan halaman detail kelas yang berisi

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

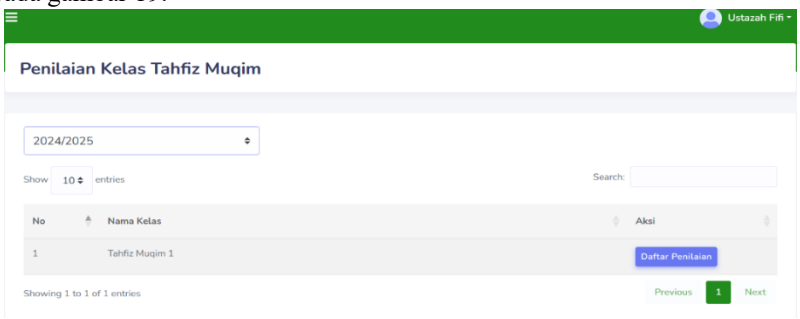
detail dari kelas tersebut yaitu nama pengajar (ustazah) dan nama santri yang terdaftar pada kelas tersebut. Adapun tampilan halaman detail kelas dapat dilihat pada Gambar 18.



Gambar 18. Tampilan Halaman Detail Kelas

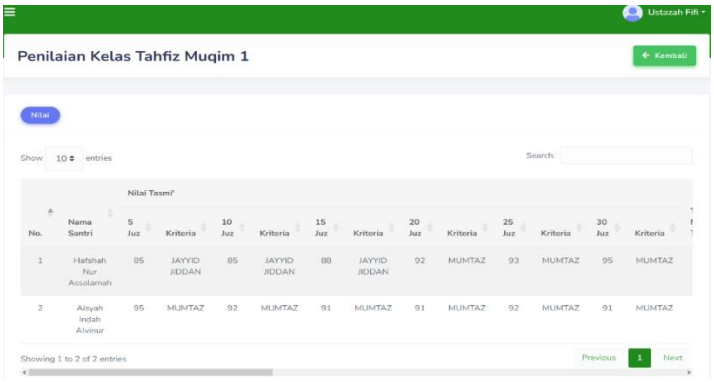
Gambar 18 adalah tampilan halaman detail kelas pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman detail kelas merupakan halaman yang menampilkan detail informasi pada kelas yang dipilih.

4. Tampilan Halaman Data Penilaian Pada Pengajar (Ustazah)
   Berikut merupakan tampilan halaman data penilaian pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an tertera pada gambar 19.



Gambar 19. Tampilan Halaman Data Penilaian

Gambar 19 adalah tampilan halaman data penilaian pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman data penilaian merupakan halaman yang ditampilkan saat pengajar (ustazah) memilih menu penilaian. Pada tampilan data penilaian terdapat tombol daftar penilaian untuk menampilkan daftar penilaian yang berisi detail nilai santri pada masing-masing kelas. Adapun tampilan halaman daftar penilaian dapat dilihat pada Gambar 20.



Gambar 20. Tampilan Halaman Daftar Penilaian

Gambar 20 adalah tampilan halaman daftar penilaian pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman daftar penilaian merupakan halaman yang menampilkan detail informasi pada penilaian santri pada kelas yang dipilih. Selain itu, pengajar (ustazah) dapat mengisi nilai santri pada halaman ini dengan mengklik tombol nilai. Data penilaian pada *database* juga dilakukan enkripsi menggunakan algoritma AES.

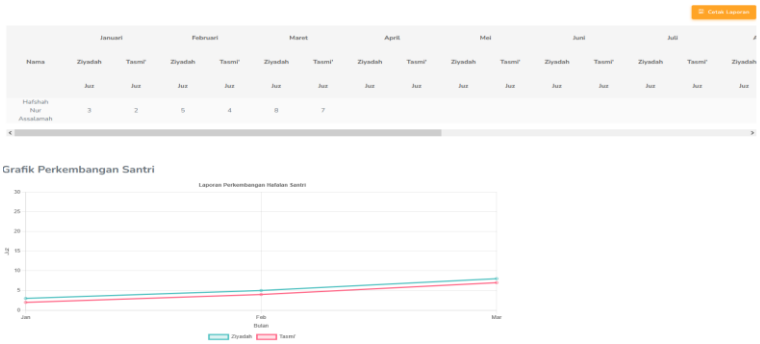
5. Tampilan Halaman Perkembangan Santri Pada Admin

Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM)
Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

Berikut merupakan tampilan halaman perkembangan santri pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an tertera pada gambar 21.

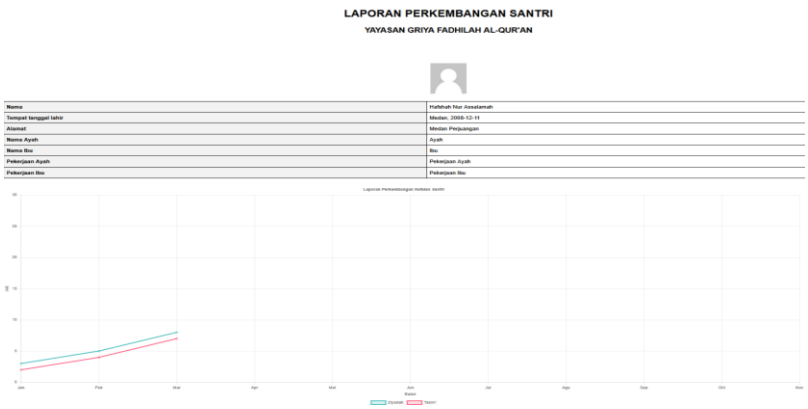
Gambar 21. Tampilan Halaman Perkembangan Santri

Gambar 21 adalah tampilan halaman perkembangan santri pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Halaman perkembangan santri merupakan halaman yang ditampilkan saat admin memilih menu perkembangan. Pada menu perkembangan terdapat laporan perkembangan santri tahfiz muqim. Pada tampilan perkembangan terdapat tombol daftar santri untuk menampilkan daftar perkembangan yang berisi detail nilai perkembangan santri tahfiz muqim yang dapat dilihat pada Gambar 22.



Gambar 22. Tampilan Halaman Daftar Perkembangan

Gambar 22 adalah tampilan halaman daftar perkembangan santri pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Data perkembangan santri pada *database* juga dilakukan enkripsi menggunakan algoritma AES. Jika admin mengklik cetak pada santri yang dipilih, maka akan muncul halaman untuk mencetak laporan perkembangan. Adapun tampilan cetak laporan perkembangan dapat dilihat pada Gambar 23.



Gambar 23. Tampilan Cetak Laporan Perkembangan

sGambar 23 adalah tampilan cetak laporan perkembangan santri pada sistem informasi santri Yayasan Griya Fadhilah Al-Qur'an. Tampilan cetak laporan perkembangan berisi detail data santri dan detail perkembangan santri. Secara keseluruhan, sistem yang dirancang dapat mengelola data santri, mengelola data pengajar (ustazah), mengelola data pengurus, mengelola data kelas, mengelola data periode, mengelola data jadwal,

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

mengelola dan mencetak laporan absensi, mengelola dan mencetak laporan penilaian, serta mengelola dan mencetak laporan perkembangan santri.

4. KESIMPULAN

Sistem pengelolaan data santri di Yayasan Griya Fadhilah Al-Qur'an masih dilakukan secara manual. Pendataan dan absensi menggunakan kertas yang berisiko rusak, hilang, atau disalahgunakan. Absensi juga masih dicatat di atas kertas, yang rentan terhadap kerusakan dan kehilangan. Penilaian dan pelaporan perkembangan santri juga masih menggunakan Microsoft Excel, yang rentan terhadap kesalahan input, perhitungan, dan kehilangan data, sehingga memengaruhi akurasi dan kualitas laporan. Sistem informasi santri berbasis web pada Yayasan Griya Fadhilah Al-Qur'an dibangun dengan menggunakan bahasa pemrograman PHP, *framework* Laravel dan *database* MySQL, sehingga menghasilkan web pengelolaan data santri yang dapat membantu yayasan untuk mengelola data santri tanpa harus menggunakan proses manual dan menumpuk berkas fisik. Sistem yang dihasilkan dapat mengelola data santri, mengelola data pengajar (ustazah), mengelola data pengurus, mengelola data kelas, mengelola data periode, mengelola data jadwal, mengelola dan mencetak laporan absensi, mengelola dan mencetak laporan penilaian, serta mengelola dan mencetak laporan perkembangan santri. Algoritma AES diterapkan dalam sistem informasi santri berbasis web pada Yayasan Griya Fadhilah Al-Qur'an untuk mengenkripsi data santri, penilaian dan perkembangan santri yang tersimpan dalam *database* sistem informasi santri. Dengan menggunakan AES, data santri penilaian dan perkembangan santri dapat dikonversi menjadi karakter yang tidak dapat dibaca atau diartikan secara langsung, sehingga diharapkan dapat meningkatkan keamanan dan mencegah akses tidak sah atau penyalahgunaan data. Proses ini mencakup enkripsi saat penyimpanan data dan dekripsi saat data dibutuhkan, memastikan hanya pihak yang berwenang yang dapat mengakses informasi secara utuh.

REFERENCES

[1] A. R. N. Malaya, E. A. Munar, F. P. Cuison, and E. G. Dacanay, "Information Management System For Research Of Don Mariano Marcos Memorial State University–South La Union Campus," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 3, pp. 1668–1675, 2022.

[2] J. Rahmadoni, R. Akbar, and U. M. Wahyuni, "Web-Based Cooperation Information System at The Science Techno Park Technology Business Development Center," *J. Appl. Eng. Technol. Sci.*, vol. 3, no. 2, pp. 156–167, Jun. 2022.

[3] D. Irmayani and M. H. Munandar, "Sistem Informasi Pengelolaan Data Siswa Pada SMA Negeri 02 Bilah Hulu Berbasis Web," *J. Inform.*, vol. 8, no. 2, pp. 65–71, 2020.

[4] Bunyamin and R. Alparisi, "Pengembangan Sistem Informasi Pengelolaan Data Santri Di Pondok Pesantren Ash - Shofi Berbasis Web," *J. Algoritm. Sekol. Tinggi Teknol. Garut*, vol. 11, no. 2, pp. 352–357, 2015.

[5] C. Gürkut, A. Elçi, and M. Nat, "An Enriched Decision-Making Satisfaction Model For Student Information Management Systems," *Int. J. Inf. Manag. Data Insights*, vol. 3, no. 2, p. 100195, 2023.

[6] C. Boura, A. Canteaut, and D. Coggia, "A General Proof Framework For Recent AES Distinguishers," *IACR Trans. Symmetric Cryptol.*, vol. 2019, no. 1, pp. 170–191, 2019.

[7] D. I. Mulyana, S. Sugiyono, S. Sutisna, H. Hartanto, A. Saepudin, and F. R. Malau, "Implementasi Sistem Informasi Santri Pada Rumah Tahfidz Pejuang Quran Duren Sawit Jakarta Timur Berbasis Web," *Swabumi*, vol. 10, no. 1, pp. 60–65, 2022.

[8] F. R. Nopianto and F. Ferdiansyah, "Aplikasi Enkripsi Data Penilaian Siswa Pada Database Menggunakan Algoritma Kriptografi (AES-128) Berbasis Web," *Skanika*, vol. 1, no. 2, pp. 669–675, 2018.

[9] M. Mayasari, S. Suendri, and M. Fakhriza, "Implementasi Algoritma Advanced Encryption Standard (AES) E-Aspirasi Mahasiswa Pada Fakultas Sains Dan Teknologi Berbasis Web," *JISTech (Journal Islam. Sci. Technol.*, vol. 7, no. 1, pp. 1–14, 2022.

[10] M. Nugraha, L. Sakinah, R. A. Setiawan, and H. Mulyani, "Rancang Bangun Sistem Informasi Penerimaan Mahasiswa Baru Berbasis Web Dengan Menggunakan Framework Laravel," *JITET (Jurnal Inform. dan Tek. Elektro Ter.*, vol. 12, no. 2, pp. 1162–1169, 2024.

[11] A. Ardi and Andriani, "Sistem Informasi Akademik Berbasis Laravel Untuk Registrasi Ulang Dan Pengajuan Cuti Mahasiswa," *INFOTECH J.*, vol. 9, no. 1, pp. 159–166, 2023.

[12] I. Sommerville, *Software Engineering*. Boston: Pearson Education, 2016.

[13] M. Prabowo, *Metodologi Pengembangan Sistem Informasi*. Salatiga: LP2M Press IAIN Salatiga, 2019.

Available Online at https://ejournal.unama.ac.id/index.php/jakakom
Volume 6, Nomor 1, April 2026
ISSN 2808-5469 (media cetak), ISSN 2808-5000 (media online)
UNAMA, DOI 10.33998/jakakom.v6i1

[14] B. Tamilarasan, R. Srinivasan, S. Dhivya, E. K. Subramanian, and C. Govindasamy, *Cryptography And Network Security: Principles And Practice*. Chennai: SK Research Group Of Companies, 2023.

[15] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Boston: Pearson Education, 2016.

[16] W. Aulia, F. Kesumaningtyas, R. Handayani, and S. Syahrinanda, "Perancangan Sistem Informasi Pengelolaan Data Santri dan Donasi Pada Surau Tahfidz Firdaus Berbasis Web," *J. Sains Dan Teknol. Keilmuan Dan Apl. Teknol. Ind.*, vol. 23, no. 1, pp. 62–27, 2023.

[17] H. Tohari, *Analisis serta Perancangan Sistem Informasi Melalui Pendekatan UML*. Yogyakarta: CV. Andi Offset, 2014.

[18] K. Budiman, *Rekayasa Perangkat Lunak*. Mungkid: Pustaka Rumah Cinta, 2022.

[19] Y. Sugiarti, *Dasar-Dasar Pemrograman Java Netbeans: Database, UML, dan Interface*. Bandung: PT Remaja Rosdakarya, 2018.

[20] N. Umar *et al.*, *Rekayasa Perangkat Lunak*. Batam: CV Rey Media Grafika, 2024.