PT Mekar Research and Publishing
Journal Information System and Computer Application
ISSN : 3110-1887 (Online)

DIGITALISASI PERPUSTAKAAN BERBASIS QR CODE MENGGUNAKAN ALGORITMA AES

Aprilia Cahyanti[1*], Fauzan Masykur[1], Adi Fajaryanto Cobantoro[1]
[1]Prodi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Ponorogo
Jl. Budi Utomo no.10 Ponorogo

Author Email: aprilyacahyanti155@gmail.com

Abstract: - Perpustakaan adalah lembaga sosial yang didirikan dan dipertahankan oleh masyarakat, sehingga perpustakaan merupakan barometer kemajuan suatu negara, proses peminjaman buku seperti registrasi dan penginputan masih bersifat manual, memakan waktu, rawan kesalahan, dan tidak efisien dalam mengelola data peminjaman. barcode telah terbukti efektif dalam mengelola pencatatan dan inventaris di banyak sektor, termasuk bisnis dan layanan publik, namun penggunaannya masih belum meluas. digitalisasi perpustakaan memberikan banyak manfaat dalam bidang keamanan, efisiensi, dan keakuratan data. Karena itu, sangat dianjurkan untuk menerapkan algoritma AES dalam sistem digitalisasi perpustakaan yang modern. Berbeda dengan sistem yang tidak menggunakan algoritma AES, data buku lebih rentan terhadap manipulasi atau kerusakan yang tidak terdeteksi. Risiko kesalahan manusia dalam proses pencatatan data masih tinggi karena masih memerlukan input manual. Sistem juga harus membandingkan semua data buku, yang memakan waktu cukup lama untuk diambil. Selain itu, kemungkinan terjadinya duplikasi data buku juga bisa terjadi bila tidak ada mekanisme untuk mendeteksi duplikat.

Key-Words: - Perpustakaan, Digitalisasi, AES, QR Code

Received: November 5, 2025. Revised: December 4, 2025. Accepted: December 30, 2025. Published: January 7, 2026.

1 Pendahuluan

Perpustakaan adalah lembaga sosial yang didirikan oleh masyarakat dan dipertahankan melalui dukungan masyarakat, sehingga perpustakaan merupakan barometer kemajuan suatu negara, dan perpustakaan dapat mengetahui apakah suatu negara mengalami kemajuan atau kemunduran [1]. Proses peminjaman buku seperti registrasi dan penginputan masih bersifat manual, memakan waktu, rawan kesalahan, dan tidak efisien dalam mengelola data peminjaman yang jumlahnya terus bertambah [2]. Sistem peminjaman buku di perpustakaan-perpustakaan di Indonesia yang masih bersifat manual menjadi kendala utama dalam pengelolaan koleksi dan pemberian layanan kepada pengguna, sehingga menurunkan minat membaca siswa dan melemahkan potensi perpustakaan sebagai pusat pembelajaran yang belum mampu ditampilkan secara maksimal [3].

Teknologi barcode telah terbukti efektif dalam mengelola pencatatan dan inventaris di banyak sektor, termasuk bisnis dan layanan publik, namun penggunaannya masih belum meluas. Jenis kode batang berbeda dalam hal struktur, kapasitas data, dan penggunaan. di antaranya adalah *QR Code*. *QR code* ialah evolusi dari *barcode* atau kode batang, menawarkan fleksibilitas dan kapasitas data yang jauh lebih besar. Pilihan antara *QR Code* dan kode batang bergantung pada persyaratan spesifik aplikasi.

Advanced Encryption Standard (AES) adalah teknik kriptografi yang digunakan untuk keamanan data. Algoritma AES adalah cipher blok simetris yang digunakan untuk enkripsi dan dekripsi data. Proses enkripsi mengubah data menjadi format yang tidak dapat dipahami, yang disebut *ciphertext*, sedangkan dekripsi melibatkan pengembalian *ciphertext* ke bentuk aslinya, yang disebut plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, atau 256 bit untuk tujuan enkripsi dan dekripsi data. [5]

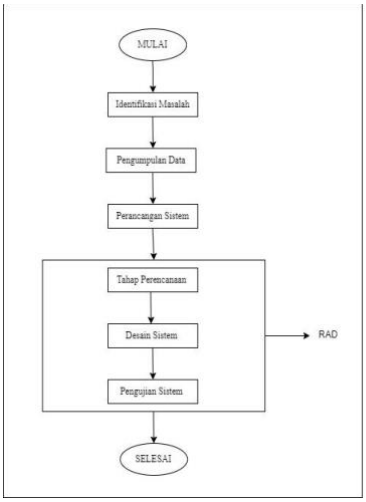
Menggunakan algoritma hashing dalam proses digitalisasi perpustakaan memberikan banyak manfaat dalam bidang keamanan, efisiensi, dan keakuratan data. Karena itu, sangat dianjurkan untuk menerapkan algoritma hashing dalam sistem digitalisasi perpustakaan yang modern. Berbeda dengan sistem yang tidak menggunakan algoritma

hashing, data buku lebih rentan terhadap manipulasi atau kerusakan yang tidak terdeteksi [6][7][8]. Risiko kesalahan manusia dalam proses pencatatan data masih tinggi karena masih memerlukan input manual. Sistem juga harus membandingkan semua data buku, yang memakan waktu cukup lama untuk diambil. Selain itu, kemungkinan terjadinya duplikasi data buku juga bisa terjadi bila tidak ada mekanisme untuk mendeteksi duplikat.

2 Metode Penelitian

2.1 Tahapan Penelitian

Tahapan penelitian menguraikan perkembangan proses penelitian. untuk digitalisasi perpustakaan menggunakan barcode dengan algoritma Hashing yang dirujuk pada gambar 2.1.



2.2 Pengumpulan Data

Tahap pengumpulan data bertujuan mengidentifikasi secara langsung permasalahan yang dihadapi, mengumpulkan informasi faktor-faktor yang mempengaruhi permasalahan tersebut, dan mencari solusi yang relevan berdasarkan keadaan sebenarnya di lapangan yang dilakukan melalui observasi lapangan.

3 Hasil dan Pembahasan

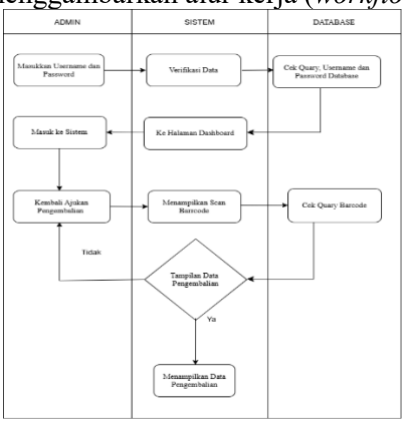
3.1 Perancangan Sistem

Pembuatan sistem diperlukannya rancangan terlebih dahulu, perancangan dapat disusun menggunakan metode RAD, metode yang digunakan ditujukan pada gambar 3.1

Gambar 3. 1 Rancangan Sistem

3.1.1 Activity Diagram

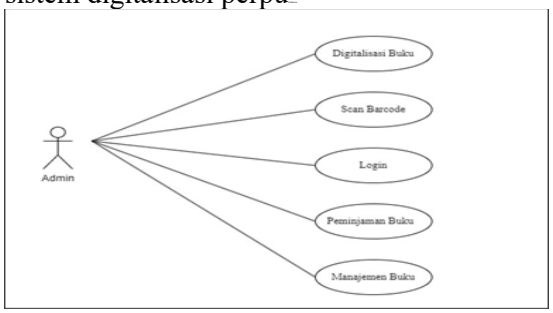
Aktivitas Diagram adalah diagram dalam *Unified Modeling Language* (UML) yang digunakan untuk menggambarkan alur kerja (*workflow*).



Gambar 3.2 Diagram Activity

3.1.2 Use Case Diagram

Use Case Diagram adalah alat visual dalam *Unified Modeling Language* (UML) yang menggambarkan interaksi antara pengguna (aktor) dan sistem. Dalam konteks digitalisasi perpustakaan, diagram kasus penggunaan dengan jelas menunjukkan interaksi antara pengguna dan sistem digitalisasi perpu



Gambar 3. 2 Diagram Use Case

3.1.3 Rancangan Database

a.Tabel Siswa

Primary Key : Id

Foreign Key :

Total : 45 bytes

Tabel 3. 1 Tabel Database User

No	Nama Kolom	Tipe Data	Panjang	Keterangan
1	Id_User	INT	5	*Primary Key*
2	Nama	VARCHAR	15	
3	Username	VARCHAR	15	
4	Password	INT	10	
5	Alamat	VARCHAR		

Gambar 3. 3 Database untuk user

3.2.2 Perhitungan Algoritma

3.2.2.1 Algoritma AES

AES harus digunakan sebagai fungsi hash karena AES dapat memiliki panjang kunci yang berbeda, sehingga jumlah ronde dalam Rijndael juga berbeda.

	Key Length (Nb Words)	Block Size (Nb Words)	Number of Rounds (Nr)
AES 128	4	4	10
AES 192	6	4	12
AES 256	8	4	14

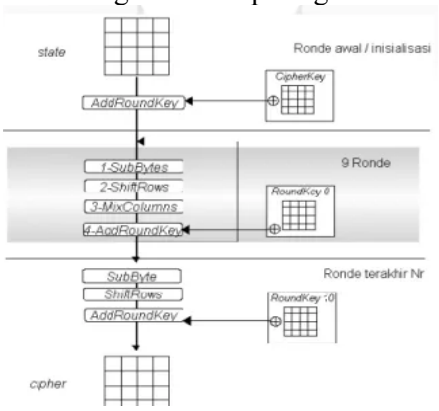
Gambar 3. 5 Tabel AES

Dari tabel 3.5 dapat dilihat dari desainnya, AES-128 menggunakan panjang kunci sebesar 128 bit, yang sesuai dengan 4 word, masing-masing terdiri dari 32 bit, menghasilkan panjang kunci 128 bit. Ukuran blok input adalah empat kata (128 bit), dan jumlah rondenya adalah (N_r) Sedangkan pada **AES-256**, panjang kunci ditingkatkan menjadi 256 bit, namun ukuran blok masukan tetap 128 bit; jumlah ronde enkripsi juga meningkat menjadi 14, dengan plaintext tetap 128 bit, sehingga ronde menjadi 14 ronde. Operasi AES dilakukan pada struktur byte dua dimensi yang dikenal sebagai state. State tersebut terdiri dari 4 baris byte. Setiap baris terdiri dari N_b byte, di mana N_b adalah hasil dari panjang blok dibagi dengan 32. Oleh karena itu, ketika ukuran plaintext adalah 128 bit, N sama dengan 128/32, menghasilkan 4 byte (32 bit). Dalam state tersebut, struktur array direpresentasikan oleh simbol s, dengan setiap byte memiliki dua indeks. Yang pertama (r) memiliki nilai dalam rentang 0 hingga 3 yang menunjukkan nomor baris. Indeks kedua (c) mewakili nomor kolom yang berada dalam rentang 0 hingga N_b. Berdasarkan tabel 5, N_b adalah 4. Setiap elemen dalam state dianggap dalam bentuk S_(r,c) atau S[r,c]. Empat langkah utama dalam algoritma AES mencakup yang berikut [4]:

1. SubBytes
2. ShiftRow
3. MixColumns
4. AddRoundKey

Algoritma AES (Standar Enkripsi Lanjutan) memiliki tiga parameter, yang terdiri dari [4]:

1. Plainteks merupakan blok data masukan yang berukuran 16 *byte*, berisi data asli yang akan diproses melalui enkripsi.
2. Cipherteks merupakan blok data keluaran yang berukuran 16 *byte*, menyimpan hasil dari proses enkripsi.
3. Kunci merupakan array berukuran 16 byte, yang mencakup kunci enkripsi yang digunakan (sering disebut juga sebagai kunci cipher).Ilustrasi algoritma AES digambarkan pada gambar 3.6



Gambar 3. 6 Ilustrasi Algoitma AES

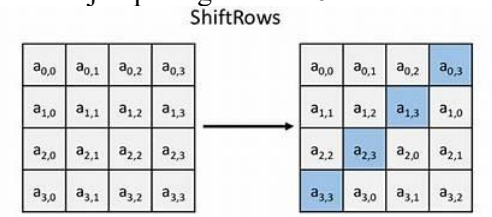
Langkah-langkah dalam proses enkripsi sebagai berikut:

a. Transformasi SubBytes

Transformasi SubBytes adalah transformasi byte di mana setiap segmen status diganti sesuai dengan tabel substitusi tertentu yang disebut S-Box. Untuk setiap byte dalam array status, katakanlah S[r, c] = xy, di mana xy menunjukkan digit heksadesimal dari nilai S[r, c]. Nilai substitusi, yang direpresentasikan sebagai S′[r, c], adalah elemen yang ditemukan dalam tabel substitusi pada persimpangan baris x dan kolom y. Gambar 2 menggambarkan dampak pemetaan byte pada setiap byte di dalam status.

b. Shiftrows

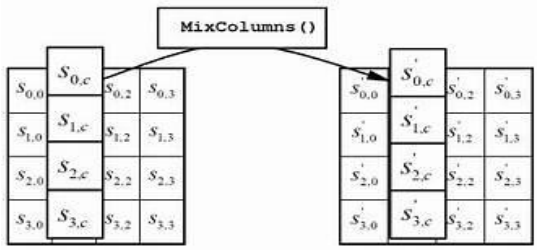
Shiftrow pada dasarnya adalah operasi pergeseran bit di mana bit paling kiri dipindahkan ke posisi paling kanan, mirip dengan rotasi bit. Proses ShitfRows Dirujuk pada gambar 4.6



Gambar 3. 7 Proses ShitfRows

c. MixColumns

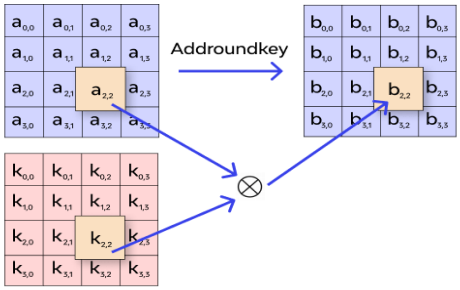
Menjalankan operasi pada setiap elemen di dalam kolom tunggal dari state. Transformasi MixColumns memodifikasi setiap elemen di dalam kolom tersebut. Ilustrasi MixColumns dirujuk pada gambar 3.8



Gambar 3.8 Proses MixColumns

d. AddRound Key

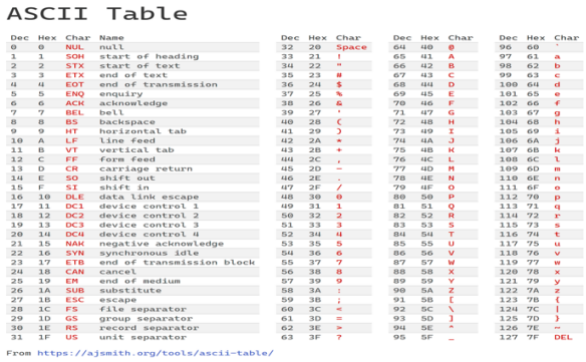
Melakukan operasi XOR antara state saat ini dan kunci putaran. Proses AddRoundKey dapat dilihat pada ilustrasi gambar 3. 9



Gambar 3. 9 Proses ilustrasi AddRoundKey

Secret Key dalam algoritma AES (*Advanced Encryption Standard*) adalah Kunci yang sama digunakan dalam operasi enkripsi dan dekripsi data. Karena AES merupakan algoritma kriptografi simetris, keamanan keseluruhan sistem sangat bergantung pada kerahasiaan kunci rahasia ini. *Secret key* adalah serangkaian bit acak dengan panjang tertentu yang menjadi input utama untuk algoritma AES dalam mengubah plaintext menjadi ciphertext (proses enkripsi) mengubah *ciphertext* kembali menjadi *plaintext* (proses dekripsi) jika kunci rahasia tersebut bocor, maka informasi dapat diakses sepenuhnya. Semakin panjang *secret key*, semakin tinggi tingkat keamanannya, tetapi waktu pemrosesan menjadi sedikit lebih berat.

Algoritma AES berperan untuk mengenkripsi serta mendekripsi data dengan metode simetris, sedangkan hashing berupa metode verifikasi satu arah yang digunakan untuk memastikan keutuhan dan keaslian data. Fungsi hash konseptual merupakan Hasil nilai hash tidak dapat didekripsi kembali, dan fitur ini dimanfaatkan untuk menjamin kerahasiaan data. Ada berbagai macam algoritma yang digunakan untuk menghasilkan hash. Namun, seiring berjalannya waktu, banyak ahli kriptanalisis telah menemukan kelemahan pada algoritma terdahulu yang awalnya dianggap kuat (*strong*). Pada gambar 3.10 di bawah ini terdapat tabel ASCII, yang digunakan sebagai acuan untuk mengetahui nilai desimal dari setiap karakter dalam teks sebelum proses enkripsi atau hashing dilakukan. Di bawah ini terdapat tabel ASCII, yang digunakan sebagai acuan untuk mengetahui nilai desimal dari setiap karakter dalam teks sebelum proses enkripsi atau hashing dilakukan.



Gambar 3.10 Tabel ASCII

4 Kesimpulan

Dalam konteks keamanan data, kombinasi antara AES dan fungsi hash memberikan perlindungan berlapis AES untuk mengenkripsi dan mendekripsi data, sedangkan hashing untuk memastikan data tidak diubah. Berdasarkan penelitian Hamdani Santoso, fungsi hash bersifat satu arah — hasil *hash value* tidak dapat dikembalikan ke bentuk aslinya, sehingga cocok untuk menjaga kerahasiaan data. Meskipun terdapat banyak algoritma hash, perkembangan kriptanalisis membuat sebagian algoritma lama tidak lagi aman. Oleh karena itu, penggunaan AES sebagai dasar fungsi hash dapat memberikan kekuatan dan keandalan yang lebih baik dalam sistem keamanan data modern.

DAFTAR PUSTAKA

[1] F. Siyasih, "RANCANG BANGUN SISTEM PERPUSTAKAAN DIGITAL (STUDI KASUS : SMK 1 BANDAR LAMPUNG)," Jurnal Informatika dan Rekayasa Perangkat Lunak (JATIKA), vol. 2, September 2021.

[2] Rustiana, Yamin, A., & Elviantari, A, "PERANCANGAN APLIKASI BARCODE TERHADAP PENGARSIPAN SKRIPSI DAN PEMINJAMAN BUKU PADA PERPUSTAKAAN FAKULTAS ILMU DAN TEKNOLOGI HAYATI," SEMINAR

NASIONALMANAJEMEN INOVASI, vol. 8, pp. 54-62, 2 Juli 2024.

[3] M. W. Saputra, "DESAIN DAN IMPLEMENTASI SISTEM INFORMASI PERPUSTAKAAN BERBASIS WEB DENGAN MENGGUNAKAN BARCODE," Teknologipintar.org, vol. 3, 2023.

[4] Muhammad Anum Fadhillah, Latief Mulyarahim, Kayla Nadira, "ALGORITME HASHING SHA-512 PADASISTEM HALAMAN SIGN UP JAVA," TRIPLE A: Jurnal Pendidikan Teknologi Informasi, vol. 2, Juli 2023.

[5] Andilala Andilala, Agung Kharisma Hidayah, AR Walad Mahfuzy, M Oki, "Implementasi Kombinasi Enkripsi Base64 Dengan Hashing Sha-1 Dan Md5 Pada Aplikasi Perpustakaan Universitas Muhammadiyah Bengkulu," Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD, vol. 6, Juli 2023.

[6] A. A. Ibrahim, "Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)," JURNAL TEKNIK INFORMATIKA STMIK ANTAR BANGSA, vol. Vol. III no. 10, pp. 53 - 60, 2017.

[7] A. A. Ibrahim, "Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)," JURNAL TEKNIK INFORMATIKA STMIK ANTAR BANGSA, vol. Vol. III no. 10, pp. 53 - 60, 2017.F. Siyasih, "RANCANG BANGUN SISTEM PERPUSTAKAAN DIGITAL (STUDI KASUS : SMK 1 BANDAR LAMPUNG)," *Jurnal Informatika dan Rekayasa Perangkat Lunak (JATIKA),* vol. 2, September 2021.

[8] F. Masykur, A. Prasetyo, I. Abdurrozaq, E. Kumalasari, and P. Utomo, “Yolo-Drone : Detection Paddy Crop Infected Using Object Detection Algorithm Yolo and Drone Image,” vol. 9, no. September, 2025