IMPLEMENTASI *ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM* (ECDSA) UNTUK VERIFIKASI KEABSAHAN DOKUMEN BERBASIS QR CODE

Paris Al Davie[1)], Ridha Adjie Eryadi[2)], Robby Rohman Sukarya[3)]

1. Informatika, Universitas Teknologi Digital
   email: paris20122009@ digitechuniversity.ac.id
2. Informatika, Universitas Teknologi Digital
   email: ridhaadjie@digitechuniversity.ac.id
3. Informatika, Universitas Teknologi Digital
   email: robbyrohman@digitechuniversity.ac.id

Abstract

The ease of modifying digital documents increases the risk of legal data forgery due to the lack of a dual authentication mechanism. This study aims to implement a document validity verification system using the Elliptic Curve Digital Signature Algorithm (ECDSA) integrated into a Quick Response (QR) Code. The system is built on a client-server architecture, where cryptographic computation and public key storage are managed centrally on an application programming interface (API), while the Android application serves as an optical scanner. The validation process applies a dual verification mechanism, namely mathematical verification on the server side and visual verification of the original PDF document. Test results show that the system is capable of completely rejecting data manipulation attempts. The computation time for digital signing remains constant under 1 ms, while the hashing time ranges from 2 ms to 54 ms for document sizes between 500 KB and 5 MB. This system effectively guarantees the integrity and validity of digital documents.

Kata Kunci : *Document Authenticity*, ECDSA, *QR Code*, *Digital Signature*, *Client Server*

A. PENDAHULUAN

Perkembangan teknologi saat ini sangatlah pesat, bahkan telah membawa perubahan besar dalam berbagai aspek kehidupan. Salah satunya dalam pengelolaan dan pertukaran dokumen. Dikarenakan pengelolaannya yang lebih efisien, mudah diakses, serta ramah lingkungan, dokumen-dokumen yang biasanya dicetak, saat ini telah maraknya tentang transformasi menjadi dokumen digital (Enjelina & Hutabarat, 2021).

Tetapi dibalik kemudahan tersebut, muncul tantangan lain terkait keamanan, seperti pemalsuan dokumen, manipulasi isi, serta kesulitan dalam memastikan keaslian dari dokumen tersebut. Kondisi ini menimbulkan kebutuhan akan mekanisme verifikasi yang dapat menjamin bahwa suatu dokumen benar-benar asli dan tidak mengalami perubahan setelah dibuat. Ancaman pemalsuan dokumen ini bukanlah sekadar hipotesis, melainkan masalah nyata yang telah terkonfirmasi.

Sebagai bukti, Pusat Informasi Kriminal Nasional (Pusiknas) Bareskrim Polri dalam laporannya mencatat telah menerima 241 laporan terkait dokumen palsu hanya dalam kurun waktu satu bulan, yakni sepanjang September 2021 (Ratusan Dokumen Dilaporkan Palsu

Sepanjang September 2021 | Pusiknas Bareskrim Polri, 2021).

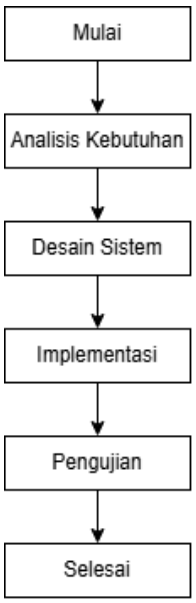
Maka dari itu, salah satu metode yang efektif untuk menjamin keabsahan dokumen adalah penggunaan tanda tangan digital (*digital signature*). Tanda tangan digital ini adalah suatu mekanisme kriptografi yang digunakan untuk memverifikasi keaslian dan integritas data digital (Nadzifarin & Asmunin, 2022).

Elliptic Curve Digital Signature Algorithm (ECDSA) merupakan salah satu algoritma tanda tangan digital yang digunakan karena memiliki keamanan yang tinggi, serta efisiensinya dalam penggunaan sumber daya. Hasil penelitian (Suantara, 2024) menunjukkan bahwa ECDSA memiliki kinerja waktu tercepat dalam implementasi sistem *multi-signature* dokumen PDF dibandingkan algoritma lainnya. Algoritma ini berfungsi untuk menjembatani antara sistem kriptografi yang kompleks di *backend*. Untuk memudahkan proses verifikasi keabsahan dokumen, hasil tanda tangan digital dapat disimpan ke dalam *Quick Response Code* (QR Code). QR Code adalah *barcode* 2 dimensi yang diperkenalkan pertama kali oleh perusahaan Jepang Denso Wave pada tahun 1994 (Dedy Irawan & Adriantantri, 2018).

Meskipun penelitian terdahulu telah menerapkan ECDSA untuk penandatanganan dokumen, sebagian besar skema masih menyatukan beban komputasi di sisi klien atau belum dilengkapi mekanisme verifikasi visual ganda untuk mencegah rekayasa dokumen fisik. Oleh karena itu, penelitian ini bertujuan mengintegrasikan algoritma ECDSA ke dalam QR Code berbasis arsitektur *client-server* dengan pendekatan *dual validation* (kriptografi dan visual) untuk menjamin keabsahan dan integritas dokumen digital.

B. METODE PENELITIAN

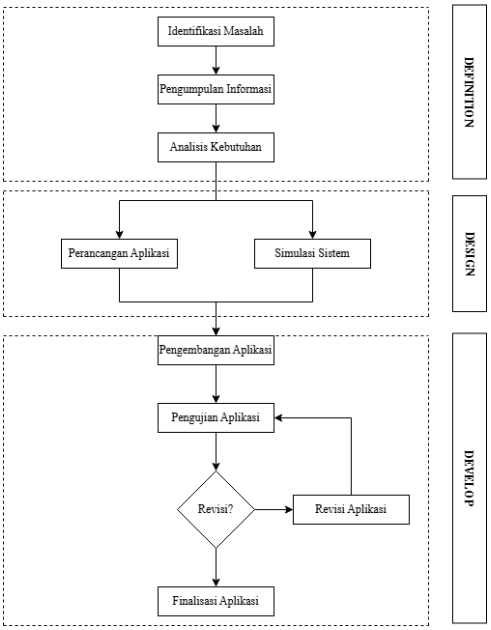
Metode penelitian ilmiah ini menggunakan jenis penelitian *Research and Development* (R&D) atau penelitian yang fokus terhadap pengembangan. *Research and Development* adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut (Sugiyono, 2011). Jenis penelitian R&D dipilih bertujuan untuk mengembangkan atau mengimplementasikan penggunaan algoritma ECDSA untuk verifikasi keabsahan dokumen.



Gambar 1. Alur Penelitian

Model Pengembangan 3D

Penelitian ini menggunakan model pengembangan 3D (*Define, Design, Develop*). Penggunaan model pengembangan 3D ini merupakan modifikasi dari model pengembangan 4D. Penetapan model pengembangan 3D dalam penelitian ini dijustifikasi berdasarkan batasan cakupan penelitian (*scope of study*), di mana fokus utama dibatasi pada perancangan, implementasi, dan pengujian kualitas perangkat lunak tanpa melibatkan tahap diseminasi produk secara luas.



Gambar 2. Diagram Prosedur Pengembangan

Definition

Tahap pendefinisian (*define*) diawali dengan mengidentifikasi potensi dan masalah mendasar terkait maraknya kasus pemalsuan dokumen digital yang merugikan berbagai pihak. Pada tahap ini, potensi penggunaan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) berbasis QR Code dirumuskan untuk memperkuat autentikasi dokumen. Selanjutnya, pengumpulan informasi dilakukan melalui studi literatur komprehensif mengenai urgensi keamanan data dan mekanisme kerja kriptografi ECDSA.

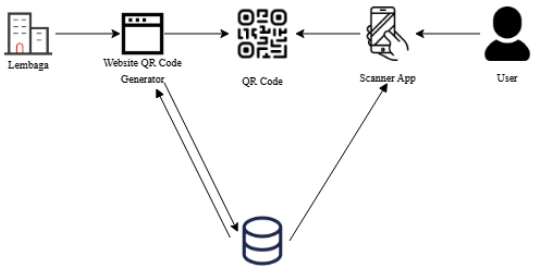
Berdasarkan informasi tersebut, analisis kebutuhan sistem dijalankan untuk menetapkan spesifikasi teknis yang diperlukan. Tahap ini menghasilkan pemetaan arsitektur perangkat lunak yang mencakup perancangan modul generator QR Code pada sisi pembuat dokumen serta pengembangan aplikasi pemindai berbasis Android untuk verifikasi keabsahan dokumen di sisi pengguna.

Design

Perancangan sistem berbasis *client-server* ini mengintegrasikan aplikasi web generator QR Code di sisi instansi penerbit dan aplikasi pemindai berbasis Android bagi pengguna umum. Aplikasi web bertugas mengelola siklus pengesahan dokumen, sementara basis data MySQL menyimpan informasi lembaga, identitas dokumen, serta pasangan kunci *Elliptic Curve Digital Signature Algorithm* (ECDSA). Alur kerja sistem melibatkan empat entitas utama melalui empat tahap terstruktur. Tahap awal mencakup manajemen pengguna oleh Superadmin, yang secara otomatis menghasilkan pasangan kunci ECDSA (*private key dan public key*) saat pendaftaran Pimpinan. Tahap berikutnya adalah pengajuan dokumen oleh Admin, yang dilanjutkan dengan pratinjau dan pengesahan oleh Pimpinan. Saat disetujui, sistem membuat nilai digest dokumen PDF menggunakan SHA-256 dan menandatanganinya dengan *private key* Pimpinan. Selanjutnya, sistem merangkai identitas dokumen, nilai *hash*, dan tanda tangan digital menjadi gambar QR Code yang disematkan langsung ke atas dokumen PDF asli untuk diunduh. Tahap akhir adalah verifikasi oleh pengguna melalui pemindaian QR Code menggunakan aplikasi Android. Aplikasi mengekstrak *payload*, mengambil *public key* dari basis data, lalu menjalankan verifikasi kriptografi ECDSA dan penyesuaian visual dokumen. Jika komputasi valid, metadata keabsahan dokumen ditampilkan, jika tidak, sistem mendeteksi manipulasi data.

Pada pengembangannya, aplikasi web dirancang menggunakan *framework* CodeIgniter 4 berbasis arsitektur MVC untuk performa yang ringan dan aman. Sementara itu, aplikasi pemindai Android dibangun menggunakan bahasa pemrograman Java dengan integrasi pustaka ZXing guna memastikan proses

pemindaian dan penerjemahan data QR Code berlangsung cepat dan akurat.



Gambar 3. Arsitektur Sistem

Develop

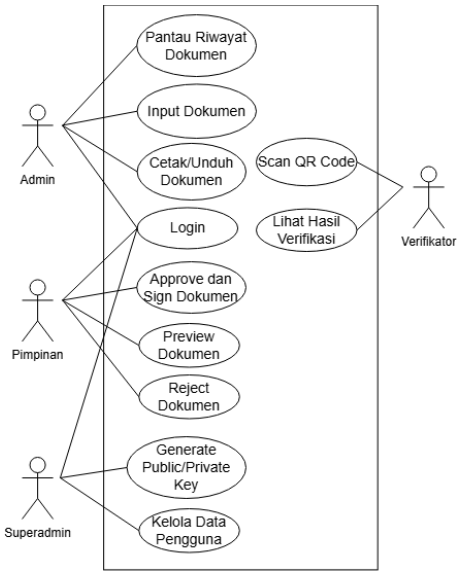
Tahap pengembangan (*develop*) diimplementasikan melalui empat fase sistematis untuk menghasilkan produk yang beroperasi secara optimal. Fase diawali dengan pengkodean sistem guna mentransformasikan rancangan menjadi prototipe aplikasi web dan Android yang fungsional. Selanjutnya, pengujian produk dilakukan pada lingkungan riil mengacu pada standar kualitas internasional ISO/IEC 25010.

Pengujian ini berfokus pada tiga karakteristik utama yang relevan dengan keamanan dokumen, yaitu efektivitas fungsionalitas, efisiensi kinerja komputasi, dan keandalan keamanan. Temuan atau kendala yang teridentifikasi selama pengujian ditindaklanjuti pada fase revisi produk guna mengoptimalkan performa, memperbaiki *bug*, serta menutup celah keamanan sistem. Terakhir, fase finalisasi dilaksanakan melalui validasi ulang terhadap produk hasil revisi. Tahap ini memastikan seluruh kriteria pengujian terpenuhi dengan baik dan sistem terbukti mampu menjawab kebutuhan verifikasi keabsahan dokumen sebelum dinyatakan siap diimplementasikan.

UML

Pemodelan sistem menggunakan *Unified Modeling Language* (UML) memvisualisasikan interaksi empat aktor utama dengan hak akses terintegrasi. Superadmin mengelola data pengguna serta membangkitkan pasangan kunci kriptografi ECDSA. Admin mengoperasikan alur kerja harian, meliputi pengunggahan dokumen PDF, pemantauan status, dan pengunduhan hasil akhir. Pimpinan memegang otoritas pengesahan dengan kewenangan meninjau, menolak, atau menyetujui dokumen melalui penandatanganan digital menggunakan private key. Sementara itu, Verifikator bertindak sebagai pihak luar tanpa otentikasi akun yang memindai QR Code untuk memvalidasi keabsahan dokumen.

Pembagian peran ini memastikan isolasi kewenangan yang jelas, di mana proses pembentukan kunci terpisah dari pengunggahan dokumen, dan eksekusi tanda tangan digital terisolasi secara aman pada tingkat otoritas tertinggi sebelum dokumen dapat diverifikasi secara publik.

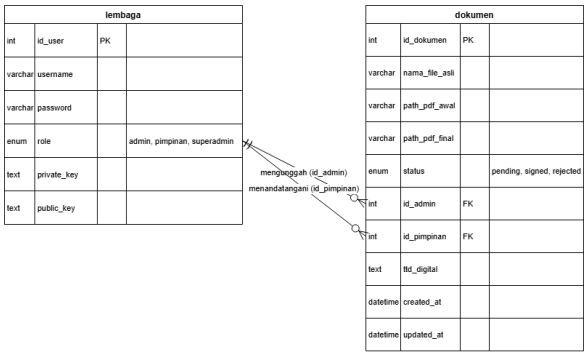


Gambar 4. Unified Modeling Language (UML)

Entity* Relationship *Diagram (ERD)

Dalam penelitian ini, ERD dirancang untuk memetakan hubungan antara tabel Lembaga dan Dokumen. Tabel Lembaga berfungsi sebagai penyimpanan data akun pengguna (Admin, Pimpinan, dan Superadmin), termasuk kredensial login dan pasangan kunci kriptografi (*private key* dan *public key*) milik Pimpinan. Tabel Dokumen berfungsi menyimpan metadata *file* dokumen PDF awal dan final, status verifikasi, nilai tanda tangan digital, serta riwayat waktu pemrosesan.

Terdapat dua relasi *One-to-Many* antara tabel Lembaga dan Dokumen. Pertama, relasi pengajuan dokumen, di mana satu entitas Admin dapat mengunggah banyak dokumen. Kedua, relasi pengesahan, di mana satu entitas Pimpinan dapat menandatangani banyak dokumen. Sebaliknya, setiap satu entitas dokumen secara spesifik hanya ditautkan pada satu Admin pengunggah dan satu Pimpinan penandatangan.



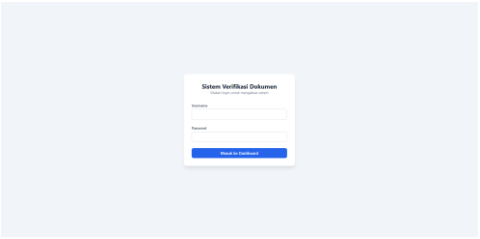
Gambar 5. Entity Relationship Diagram (ERD)

C. HASIL DAN PEMBAHASAN

Implementasi Website Generator QR Code

Teradapat empat halaman/antarmuka utama berdasarkan hak ases pengguna:

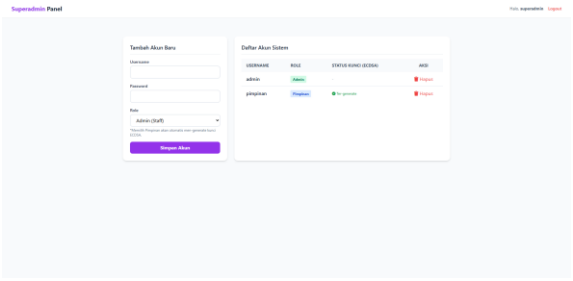
1. Login



Gambar 6. Halaman Login

Antarmuka ini berfungsi untuk memilah posisi/*role* pengguna. Setelah melakukan login, pengguna akan diarahkan menuju *dashboard* sesuai dengan hak akses.

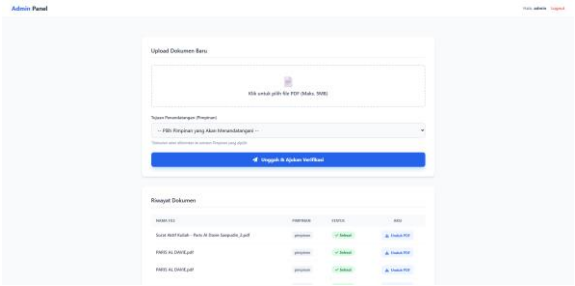
2. Dashboard Superadmin



Gambar 7. Dashboard Superadmin

Halaman *dashboard* superadmin menampilkan fitur manajemen pengguna (lembaga). Melalui halaman ini, superadmin dapat menginput data admin dan pimpinan yang secara otomatis mengenerate kunci kriptografi di backend.

3. Dashboard Admin

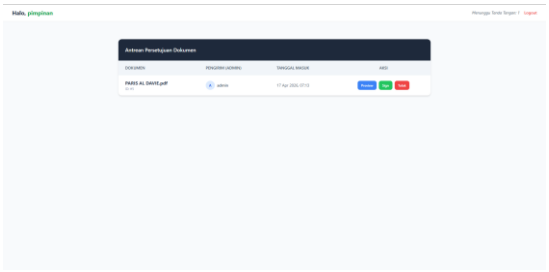


Gambar 8. Dashboard Admin

Halaman dashboard admin digunakan untuk operasional sederhana. Admin mengunggah file PDF dokumen yang

akan diberi tanda tangan digital oleh pimpinan yang dituju, dan dapat mengunduh dokumen tersebut jika sudah disetujui oleh pimpinan.

4. Dashboard Pimpinan



Gambar 9. Dashboard Pimpinan

Halaman *dashboard* pimpinan menampilkan daftar dokumen yang perlu ditanda tangani secara digital. Terdapat fitur *preview* PDF, serta tombol *Sign* yang akan mengeksekusi algoritma ECDSA menggunakan *private key* pimpinan dan juga tombol tolak untuk menolak menandatangani dokumen tersebut.

Implementasi Aplikasi Mobile

Aplikasi *Scanner* ini dibangun menggunakan bahasa Java dan *library* ZXing pada platform Android.

1. Beranda

Gambar 10. Halaman Beranda Scanner

Saat membuka aplikasi *Scanner*, aplikasi menampilkan halaman kosong dan terdapat tombol Scan QR Code untuk membuka kamera dan mendeteksi QR Code secara *real-time*.

2. Hasil

Gambar 11. Halaman Hasil Scanner

Jika proses verifikasi kriptografi bernilai *true*, antarmuka menampilkan status "Dokumen Valid" beserta memunculkan dokumen asli. Jika bernilai false, aplikasi menampilkan peringatan "Dokumen tidak valid/palsu".

Implementasi Algoritma *Hashing*

Algoritma *hashing* di-implementasikan menggunakan fungsi bawaan PHP "hash_file()". Fungsi *hash_file* membaca dokumen PDF langsung dari direktori fisik ($pdfPath) secara *streaming byte* demi *byte*. Fungsi ini tidak memuat (load) keseluruhan ukuran PDF ke dalam RAM server.

```
$fileHash = hash_file('sha256', $pdfPath);
```

Gambar 12. Potongan Kode Algoritma *Hashing* SHA-256

Implementasi Pembuatan Kunci dan Tanda Tangan

Penandatanganan di-implementasikan menggunakan *library* OpenSSL PHP. *Private key* diambil dari *database* berdasarkan sesi *login* Pimpinan. Hasil dari variabel $signature di sini adalah data biner mentah (*raw binary*). Data ini akan rusak jika langsung disatukan ke dalam QR Code, sehingga pada langkah selanjutnya akan melakukan base64_encode().

Gambar 13. Potongan Kode Penandatanganan Digital ECDSA

Proses Pembuatan Kunci ECDSA

Sistem menggunakan modul OpenSSL untuk menghasilkan pasangan kunci. Berikut adalah string mentah dari kunci yang tersimpan pada tabel lembaga untuk akun Pimpinan:

Tabel 1. Tabel Kunci Pengguna

Nama Pengguna	Private Key	Public Key
Pimpinan	MIGHAgE AMBMGB yqGSM49A g….RpyhY YT	MFkwEw YHKoZIzj 0C…aco WGEw==

Proses Hashing Dokumen Menggunakan SHA-256

File PDF yang diunggah dikomputasi menggunakan fungsi *hash* untuk mendapatkan nilai digest. Hasil komputasi SHA-256 menghasilkan string heksadesimal 64 karakter berikut:
[f2f7247030f844b8eff71e65f81abc00106 9c0c42acddf20cae4c68267e58ceb]

Proses Penandatanganan Digital

Nilai *hash* ditandatangani menggunakan *Private Key* untuk menghasilkan tanda tangan digital. Hasil penandatanganan tersebut berupa data biner mentah, sehingga dikonversi ke dalam format teks Base64 untuk mempermudah penyimpanan dan penyematan ke dalam QR Code: [MEUCIQCzzMUriG/GIw/xtcHOlDMQ +KBHleE5rpbUG76ml9MpKAIgWfkCV SfXLXcgXS4I1GyA7YKqtdHiF3BiNSN dXFd4g4o=]

Pembuatan dan Penyematan QR Code

Sistem merangkai tiga variabel utama menjadi satu string *payload* dengan format ID|Hash|Signature sebelum direnderi menjadi gambar QR Code. Payload mentah yang disematkan adalah:

Tabel 2. Tabel Format QR Code

ID	Hash	Signature
8	f2f7247030 f8…7e58ce b	MEUCIQ CzzMUri …4g4o=

Gambar QR Code tersebut disematkan secara spesifik pada halaman pertama dokumen PDF menggunakan library FPDI. Penempatan dilakukan pada koordinat X: 10 (margin kiri) dan koordinat Y yang dihitung secara dinamis berdasarkan total tinggi halaman dikurangi 40 satuan, sehingga QR Code selalu diposisikan secara konsisten di area sudut kiri bawah dokumen berukuran 30x30.

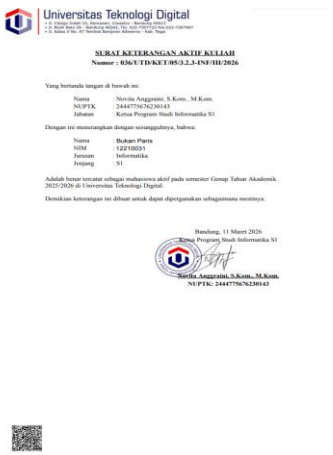
Pengujian Keamanan dan Integritas Data

Pengujian ini bertujuan menunjukkan bahwa modifikasi sekecil apa pun pada dokumen akan merusak validitas tanda tangan.

1. Pengujian Integritas Kriptografi

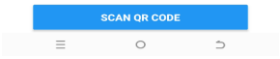
Pengujian integritas memvalidasi kemampuan ECDSA mendeteksi manipulasi data. Simulasi dilakukan dengan mengubah karakter nilai hash asli (f2f7247030f844b8eff71e65f81abc00106 9c0c42acddf20cae4c68267e58ceb) pada payload menjadi hash palsu

(37c9b2c1c092d4ade759775e952832fbd6d0d7b5e72c91aae0acf59e8fd6b4ab), lalu mengonversinya menjadi QR Code rekayasa. Hasilnya, sistem secara mutlak menolak dokumen akibat ketidakcocokan nilai kriptografi.



Gambar 14. Dokumen Yang Sudah Diubah Isi dan QR Code

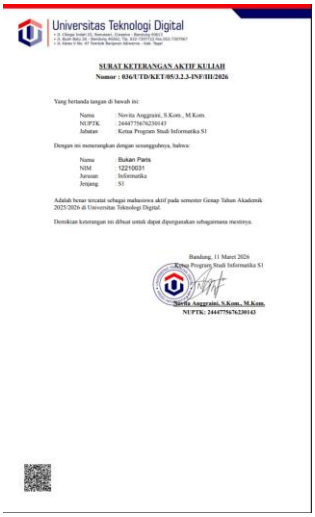
Akibat ketidakcocokan nilai hash, fungsi openssl_verify mengembalikan nilai 0 karena signature sah tidak tervalidasi pada hash yang direkayasa. Aplikasi pun menampilkan peringatan "Dokumen Tidak Valid", membuktikan bahwa integritas payload dilindungi secara penuh oleh algoritma ECDSA.



Gambar 15. Hasil Scan Pada Pengujian Rekayasa A

2. Pengujian Integritas Dokumen

Pengujian ini mengevaluasi sensitivitas sistem terhadap pemalsuan konten dokumen melalui pendekatan verifikasi ganda. Simulasi dilakukan dengan memanipulasi teks pada berkas PDF sah menggunakan PDF Editor, sementara gambar QR Code asli dipertahankan tanpa modifikasi sebelum dipindai kembali oleh aplikasi.



Gambar 16. Dokumen Yang Sudah Diubah Isi

Verifikasi kriptografi memberikan status "Valid" karena QR Code terbukti asli dan sesuai tanda tangan Pimpinan. Namun, sistem secara otomatis mengunduh serta menampilkan berkas PDF asli dari server guna memfasilitasi verifikasi visual terhadap manipulasi konten.

Gambar 17. Hasil Scan Pada Pengujian Rekayasa B

Mekanisme *dual validation* ini memungkinkan Verifikator membandingkan konten dokumen fisik dengan berkas asli yang diunduh secara otomatis dari server. Ketidakcocokan informasi di antara keduanya membatalkan keabsahan dokumen, membuktikan ketahanan sistem dalam melindungi integritas data digital sekaligus konten fisik.

Pengujian Efisiensi Kinerja

Pengujian performa komputasi algoritma dilakukan sebanyak 5 (lima) kali percobaan untuk mendapatkan waktu rata-rata eksekusi.

Tabel 3. Tabel Pengujian Efisiensi Kinerja

Dokumen	Proses	Waktu Eksekusi
Dokumen PDF 500KB	*Hashing File* PDF	2,22 ms
	Signing Menggunakan *Private Key*	0,21 ms
	Pemindaian & Verifikasi di Aplikasi Android	213 ms
Dokumen PDF 2MB	*Hashing File* PDF	16,84 ms
	Signing Menggunakan *Private Key*	0,17 ms
	Pemindaian & Verifikasi di Aplikasi Android	407 ms
Dokumen PDF 5MB	*Hashing* File PDF	30,38 ms
	Signing Menggunakan *Private Key*	0,12 ms
	Pemindaian & Verifikasi di Aplikasi Android	8573 ms

Berdasarkan hasil pengujian pada tabel di atas, waktu komputasi untuk menghasilkan nilai intisari (SHA-256) berbanding lurus dengan ukuran *file* dokumen. Sebaliknya, waktu yang dibutuhkan untuk mengeksekusi algoritma penandatanganan ECDSA mencatatkan waktu konstan, yaitu stabil pada rentang 0,14 milidetik terlepas dari besarnya file PDF. Hal ini menunjukkan sistem berjalan sangat efisien.

D. KESIMPULAN DAN SARAN

Kesimpulan

Algoritma ECDSA berhasil diintegrasikan pada QR Code melalui arsitektur *client-server* yang memisahkan beban komputasi. Isolasi proses *signing* dan verifikasi kriptografi pada *backend* (API) memastikan aplikasi Android beroperasi murni sebagai pemindai optik yang efisien tanpa mengekspos *private key* ke perangkat klien. Selanjutnya, sistem menerapkan metode validasi ganda secara kriptografis dan visual

untuk memverifikasi keaslian dokumen. Ekstraksi *payload* (ID, *hash*, *signature*) memastikan penolakan mutlak terhadap manipulasi data digital, sedangkan pengunduhan otomatis berkas PDF asli dari server memfasilitasi pencocokan visual untuk mencegah rekayasa konten fisik. Kinerja sistem terbukti sangat efisien, di mana waktu pembuatan *hash* berjalan *linier* sesuai ukuran berkas (2–54 ms untuk dokumen 500 KB – 5 MB), sementara proses penandatanganan (*signing*) ECDSA berlangsung konstan di bawah 1 ms tanpa dipengaruhi oleh ukuran file PDF.

Saran

Meskipun sistem beroperasi sesuai rancangan, terdapat beberapa keterbatasan yang perlu dikembangkan pada penelitian selanjutnya. Pertama, pengimplementasian algoritma kompresi data diperlukan jika variabel *payload* QR Code bertambah, guna mencegah kerapatan gambar yang menyulitkan kamera beresolusi rendah. Kedua, kunci ECDSA perlu diintegrasikan dengan *Application Programming Interface* (API) Penyelenggara Sertifikasi Elektronik (PSrE) resmi seperti BSrE untuk mencapai keabsahan hukum penuh. Ketiga, penyimpanan *public key* dapat diintegrasikan dengan teknologi *blockchain* untuk mencegah peretasan basis data terpusat. Terakhir, penerapan langsung pada instansi pemerintahan atau pendidikan diperlukan guna mengevaluasi performa sistem dalam lingkungan produksi skala besar.

E. REFERENSI

[1] Dedy Irawan, J., & Adriantantri, E. (2018). Pemanfaatan QR-code sebagai media promosi toko. Jurnal Mnemonic, 1(2), 58–61. https://doi.org/10.36040/mnemonic.v1i2.39

[2] Enjelina, S., & Hutabarat, E. (2021). Aspek hukum penggunaan tanda tangan digital dalam menyelesaikan penandatanganan dokumen-dokumen bisnis perusahaan-perusahaan yang dikembangkan oleh PrivyID [Skripsi, Universitas HKBP Nommensen]. Repository Universitas HKBP Nommensen. https://repository.uhn.ac.id/handle/123456789/5517

[3] Fitriyadi, M. N., & Senubekti, M. A. (2024). Implementasi prototyping dalam pengembangan aplikasi keuangan Yayasan Assalaam Al Madani Sumedang sebagai upaya meningkatkan akuntabilitas kinerja. JATI (Jurnal Mahasiswa Teknik Informatika), 8(6), 12844–12851. https://doi.org/10.36040/jati.v8i6.12148

[4] Nadzifarin, A., & Asmunin, A. (2022). Penerapan Elliptic Curve Digital Signature Algorithm pada tanda tangan digital dengan studi kasus dokumen surat-menyurat. Journal of Informatics and Computer Science (JINACS), 4(1), 1–9. https://doi.org/10.26740/jinacs.v4n01.p1-9

[5] Pusiknas Bareskrim Polri. (2021, 29 September). Ratusan dokumen dilaporkan palsu sepanjang September 2021. https://pusiknas.polri.go.id/detail_artikel/ratusan_dokumen_dilaporkan_palsu_sepanjang_september_2021

[6] Senubekti, M. A., Anggraini, N., Rusghana, F., & Mahatma, K. (2025). Pengembangan aplikasi E-Bale Sunda untuk digitalisasi peminjaman arsip di Pengadilan Negeri Bale Bandung Kelas 1A menggunakan CodeIgniter 4.

TEKNO: Jurnal Penelitian Teknologi dan Peradilan, 3(1), 61–74.

[7] Sopandi, H., & Anggraini, N. (2021). Aplikasi perpustakaan berbasis web menggunakan framework CodeIgniter (Studi kasus: SMPN 3 Pacet). Nuansa Informatika, 15(1), 38–46. https://doi.org/10.25134/nuansa.v15i1.4321

[8] Suantara, Y. (2024). Perbandingan kinerja waktu algoritma ECDSA, EdDSA, RSA, dan implementasinya pada sistem multi-signature dokumen PDF. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 11(1), 1–12. https://jurnal.mdp.ac.id/index.php/jatisi/article/view/6752

[9] Sugiyono. (2011). Metode penelitian pendidikan: Pendekatan kuantitatif, kualitatif, dan R&D. Alfabeta.

[10] Valentino, M. R., Fitriyadi, M. N., Senubekti, M. A., & Darsiti, D. (2025). Penerapan metode prototyping dalam implementasi aplikasi pemesanan makanan online menggunakan barcode pada Kedai Mas Gunarto. JATI (Jurnal Mahasiswa Teknik Informatika), 9(5), 8125–8132. https://doi.org/10.36040/jati.v9i5.15045