TECHNOVATAR Jurnal Teknologi, Industri dan Informasi
Vol. 4, No. 4, Oktober 2026, pp. 1 – 12
Open Access:
https://journal.awatarapublisher.com/index.php/technovatar
ISSN: 3031-8874, **DOI**: 10.61434/technovatar.vXiX.XXX

RANCANGAN VERIFIKASI INTEGRITAS DOKUMEN PDF BERBASIS QR CODE DAN SHA-256 DENGAN EVALUASI LOKAL

Ade Sutriyono[1*]
[1] Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika, Cirebon, Indonesia
Email: ade@mahardika.ac.id

INFO ARTIKEL
Sejarah Artikel:
Diterima, 25 September 2026
Direvisi, 30 September 2026
Disetujui, 2 Oktober 2026

KEYWORDS
PDF integrity
QR Code
SHA-256
Document verification
Synthetic evaluation

ABSTRACT

Document verification requires distinguishing issuance records, file equality, and signatory identity. This study designs a PDF verification mechanism using QR codes and SHA-256 and evaluates its comparison component locally. The method combines a targeted literature search, architecture and decision-model design, and testing with 12 synthetic PDFs containing 1, 3, or 10 pages. Demonstration QR codes are embedded before PDF finalization and hashing to prevent circular hash dependencies, ensuring strict byte-level integrity verification. Seventy-two comparisons cover identical controls, text changes, numeric changes, added pages, metadata changes, and different documents carrying the same QR code. All 12 controls yield matching hashes, whereas all 60 variants yield different hashes. Extracted text remains unchanged in the metadata cases. Six status-decision cases produce the specified local outcomes. These findings support byte comparison within the tested scope while identifying its limits: scanning a QR code without submitting the PDF does not check the user-held file, and a hash does not authenticate the signatory. The Google Workspace architecture remains an undeployed design. Cloud security, network performance, and usability are not evaluated. The contribution consists of a finalization procedure, distinct verification labels, and a reproducible test package.

This work is licensed under a Creative Commons Attribution 4.0 International License.

KATA KUNCI
Integritas PDF
QR Code
SHA-256
Verifikasi dokumen
Evaluasi sintetis

ABSTRAK

Verifikasi dokumen memerlukan pembedaan antara rekaman penerbitan, kecocokan berkas, dan identitas penanda tangan. Penelitian ini merancang mekanisme verifikasi PDF berbasis QR Code dan SHA-256 serta mengevaluasi komponen pembanding secara lokal. Metode meliputi penelusuran literatur terarah, perancangan arsitektur dan model keputusan, serta pengujian 12

CORRESPONDING AUTHOR

Ade Sutriyono
Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika
Jl. Taman Pemuda No. 2, Cirebon 45153, Jawa Barat, Indonesia
Email: ade@mahardika.ac.id

PDF sintetis dengan jumlah halaman 1, 3, dan 10. QR demonstrasi disisipkan sebelum finalisasi PDF dan penghitungan hash guna menghindari dependensi hash melingkar (circular reference). Sebanyak 72 pembandingan mencakup kontrol identik, perubahan teks, angka, halaman, metadata, dan dokumen lain dengan QR yang sama. Seluruh 12 kontrol memiliki hash sama, sedangkan seluruh 60 variasi memiliki hash berbeda. Pada perubahan metadata, teks hasil ekstraksi tetap sama. Enam kasus keputusan status menghasilkan keluaran yang sesuai dengan kebijakan lokal. Temuan menunjukkan kegunaan pembandingan byte pada cakupan uji, sekaligus memperlihatkan batasnya: QR yang dipindai tanpa unggahan belum memeriksa file pengguna, dan hash tidak membuktikan identitas penanda tangan. Arsitektur Google Workspace merupakan rancangan yang belum di-deploy. Penelitian tidak mengukur keamanan cloud, kinerja jaringan, atau usability. Kontribusi berupa prosedur finalisasi, pemisahan label keputusan, dan paket uji yang dapat direproduksi.

PENDAHULUAN

Verifikasi dokumen akademik memerlukan pembedaan antara keberadaan rekaman penerbitan, kecocokan berkas, dan identitas pihak yang mengesahkan dokumen. Literatur pengelolaan kredensial mengembangkan berbagai arsitektur untuk menghubungkan penerbit, pemilik, dan pemeriksa. Delgado-von-Eitzen et al. (2021) menempatkan privasi serta skalabilitas sebagai persoalan rancangan sertifikasi, sedangkan Caramihai dan Severin (2023) membahas pengelolaan diploma pada lingkungan universitas. Kedua kajian tersebut menunjukkan bahwa penyimpanan catatan saja belum menyelesaikan seluruh kebutuhan tata kelola.

Rustemi et al. (2023) memetakan penelitian verifikasi sertifikat akademik berbasis *blockchain*. Pengembangan DIAR kemudian memperlihatkan alternatif arsitektur penerbitan serta verifikasi diploma (Rustemi et al., 2024). Penelitian ini mengambil konteks yang lebih terbatas: bagaimana institusi dengan registri terpusat dapat membedakan hasil pemeriksaan metadata dan hasil pemeriksaan *byte* dokumen. Pilihan terpusat merupakan asumsi rancangan, bukan temuan bahwa arsitektur tersebut lebih murah atau lebih aman daripada *blockchain*.

QR Code menyediakan representasi data yang dapat dibaca perangkat. Variasi penggunaannya bahkan mencakup instruksi yang dapat dieksekusi dalam pendekatan eQR (Scanzio et al., 2024). Akan tetapi, kode yang dapat dipindai tidak otomatis menjadi bukti otentik. Njuguna dan Ndia (2025) membahas ancaman seperti pemalsuan kode dan pengalihan menuju tujuan berbahaya. QsecR secara khusus mengembangkan pemeriksaan URL berbahaya (Rafsanjani et al., 2023). Implikasinya, pemeriksaan *hash* PDF dan pemeriksaan keamanan tujuan tautan adalah masalah yang berbeda.

Pemisahan tersebut juga relevan terhadap istilah tanda tangan digital. SHA-256 merupakan fungsi *hash* yang ditetapkan dalam Secure *Hash* Standard (National Institute of Standards and Technology [NIST], 2015). Tanda tangan digital menggunakan mekanisme tambahan untuk autentikasi asal data (NIST, 2023). Penelitian sertifikat profesional oleh Sintyaningrum et al. (2021) mengintegrasikan QR dan tanda tangan digital, sementara Yuliana dan Walidaniy (2024) meneliti integrasi *multi-signature* dengan EdDSA. Rancangan yang hanya membandingkan *hash* dengan registri tidak boleh mengambil klaim autentikasi penanda tangan dari sistem tersebut.

Persoalan penelitian dirumuskan sebagai tiga pertanyaan. Pertama, bagaimana merancang urutan penerbitan serta keputusan verifikasi yang memisahkan identitas rekaman, status dokumen, dan kecocokan PDF? Kedua, bagaimana perilaku pembandingan SHA-256 pada perubahan terkontrol terhadap PDF final yang telah memuat QR? Ketiga, ancaman apa yang tetap berada di luar jangkauan pembandingan tersebut? Tujuannya adalah menghasilkan rancangan model tripartit yang memisahkan status registri, integritas berkas byte, dan autentikasi penanda tangan, pembanding lokal yang dapat direproduksi, serta batas klaim yang proporsional dengan bukti empiris.

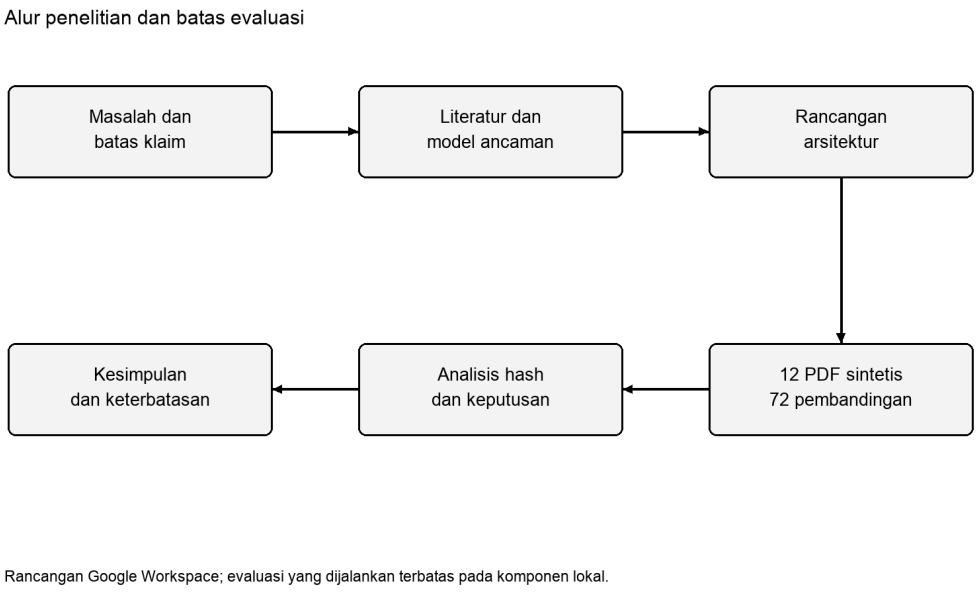
Kontribusi artikel berupa model keputusan, urutan finalisasi PDF sebelum pencatatan *hash*, dan paket uji sintetis dengan sumber yang dapat dijalankan ulang. Kontribusi ini merupakan sintesis rekayasa dalam lingkup penelitian, bukan klaim bahwa kombinasi QR dan SHA-256 pertama kali ditemukan. Penelusuran bersifat terarah dan tidak dimaksudkan sebagai tinjauan sistematis atas seluruh penelitian terdahulu.

METODE PENELITIAN

Pendekatan dan unit analisis

Penelitian menggunakan pendekatan rekayasa berorientasi desain dengan evaluasi komponen secara lokal. Artefak desain terdiri atas rancangan arsitektur, prosedur penerbitan, dan keputusan verifikasi. Artefak implementasi terdiri atas pembangkit PDF sintetis serta pembanding SHA-256. Pemisahan desain dan bukti evaluasi mengikuti perhatian terhadap transparansi proses, pembangunan, evaluasi, dan kontribusi dalam penelitian desain (Hevner et al., 2024). Penetapan mutu evaluasi juga perlu disesuaikan dengan lingkup artefak yang diteliti (Prochner & Godin, 2022).

Unit analisis ialah pasangan *byte* PDF dan *hash* referensinya. Sampel dasar terdiri atas 12 PDF sintetis: empat variasi identitas untuk masing-masing jumlah halaman 1, 3, dan 10. Angka pada dokumen merupakan nilai sintetis, bukan nilai transaksi atau data pribadi. Pemilihan 12 dokumen sintetis dengan variasi jumlah halaman (1, 3, dan 10 halaman) bertujuan mencakup skenario berkas akademik satu lembar hingga multi-halaman pada kombinasi kasus yang ditentukan, bukan mewakili populasi dokumen perguruan tinggi secara statistik. Alur penelitian ditampilkan pada Gambar 1.



Gambar 1. Alur penelitian dan batas evaluasi

Penelusuran sumber

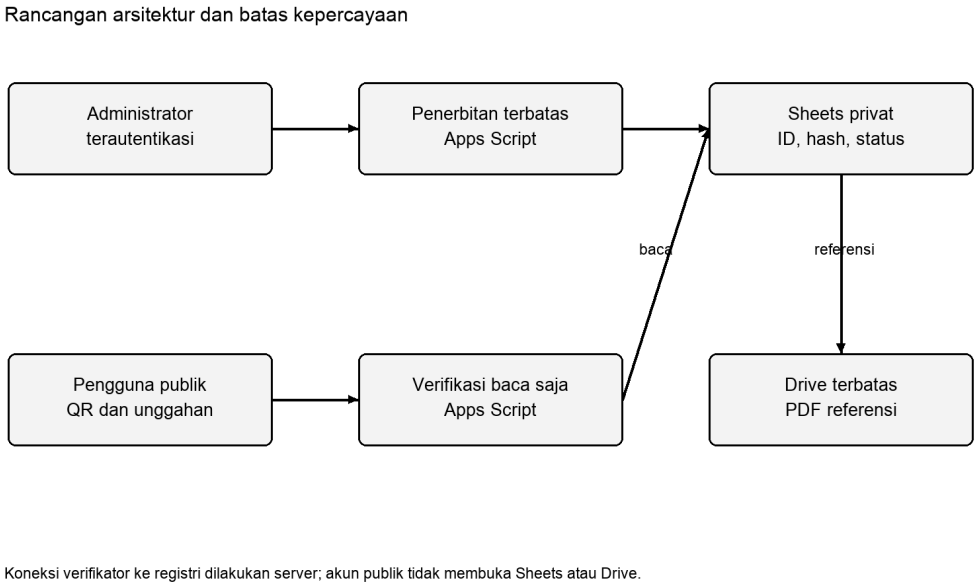
Penelusuran dilakukan pada 24 Maret 2026 melalui pencarian web, laman penerbit, serta registri Crossref. Percobaan pencarian Consensus tidak menghasilkan rekaman karena kuota akun telah habis. Tidak digunakan layanan Deep Research atau Pro Research terpisah. Sumber penelitian dibatasi pada publikasi Januari 2021 sampai Oktober 2025. Standar teknis yang lebih lama digunakan hanya untuk definisi normatif yang relevan.

Kueri menggabungkan istilah QR Code, SHA-256, document verification, academic certificate, digital signature, dan design research evaluation. Artikel dipilih berdasarkan kesesuaian dengan rancangan, ketersediaan DOI, kecocokan metadata registri dan penerbit, serta tanggal publikasi. Informasi yang hanya tersedia sebagai abstrak dibatasi pada kontribusi yang dinyatakan dalam abstrak. Tidak dilakukan penggabungan ukuran efek, penghitungan prevalensi pemalsuan, ataupun

penilaian kelengkapan korpus. Catatan sumber dan pembatasan akses disimpan bersama bahan penelitian.

Arsitektur dan model ancaman

Gambar 2 memperlihatkan rancangan pemisahan aplikasi administrasi terbatas dan layanan verifikasi baca saja. Google Sheets direncanakan sebagai registri privat berisi ID, *hash*, status, dan versi. Google Drive direncanakan untuk menyimpan PDF referensi dengan akses terbatas. Google Apps Script ditempatkan sebagai lapisan layanan. Pemilihan komponen tersebut belum diuji sebagai *deployment*; pengujian yang dilaporkan dalam artikel hanya berjalan lokal.



Gambar 2. Rancangan arsitektur dan batas kepercayaan

Administrator diasumsikan berwenang menerbitkan serta mencabut dokumen. Pengguna publik diasumsikan hanya memeriksa metadata terbatas dan kecocokan berkas. Penyerang dapat mengubah PDF, menyalin QR, atau mengarahkan pengguna menuju laman palsu. Kompromi akun administrator dan registri dimasukkan sebagai ancaman residu. Rancangan mensyaratkan domain verifikasi yang diketahui, pemisahan izin tulis, pembatasan data yang ditampilkan, dan audit perubahan. Persyaratan ini belum menjadi bukti bahwa kontrol telah diterapkan atau mampu menolak serangan.

Tabel 1. Ancaman, persyaratan desain, dan batas evaluasi

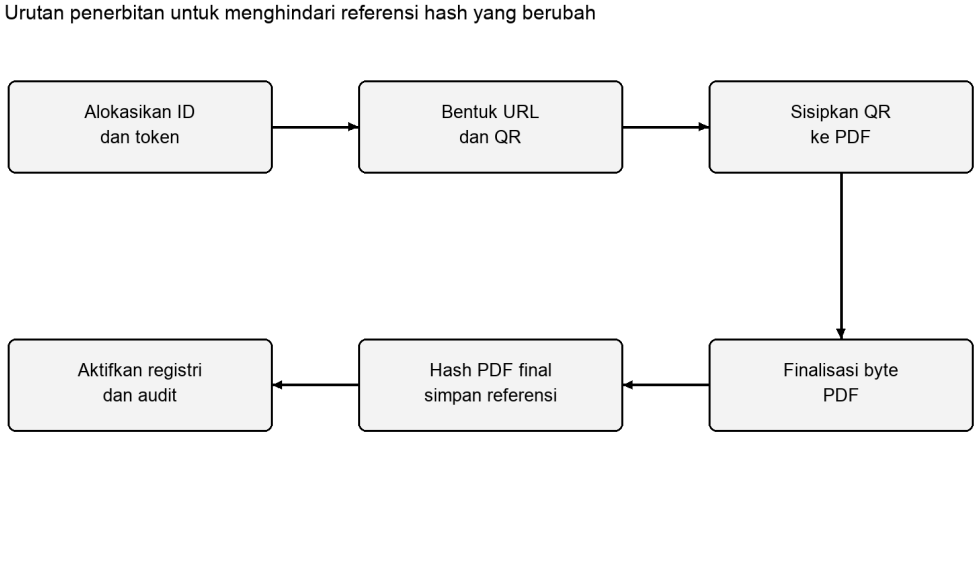
Ancaman	Persyaratan desain	Bukti yang tersedia
PDF berubah	Bandingkan hash PDF final	Uji lokal perubahan teks, angka, halaman, metadata
QR disalin	Metadata saja tidak cukup; bandingkan file	Uji lokal QR sama pada dokumen lain
QR menuju laman palsu	Domain resmi dan pemeriksaan tujuan	Tidak diuji
Registri atau akun dikuasai	Izin terbatas, audit, pemulihan	Tidak diuji
Dokumen dicabut	Keputusan pencabutan terpisah	Model keputusan lokal

Tabel 1 merangkum ancaman dan batas bukti. Perlindungan terhadap pengambilalihan akun, perubahan registri, serta kebocoran metadata memerlukan evaluasi tersendiri. Pengujian perubahan

PDF tidak dapat menggantikan pengujian tersebut. Pengungkapan batas artefak dan proses diperlukan agar pembaca tidak menyamakan keberhasilan komponen dengan keamanan sistem secara keseluruhan (Barata et al., 2023).

Prosedur penerbitan dan pembandingan

Gambar 3 memperlihatkan urutan yang diusulkan: alokasi ID, pembentukan URL dan QR, penyisipan QR, finalisasi PDF, penghitungan *hash*, kemudian aktivasi rekaman. *Hash* disimpan di luar PDF. Menyisipkan *hash* seluruh file ke dalam file yang sama akan mengubah *byte* yang menjadi masukan *hash*; oleh sebab itu rancangan secara tegas menggunakan registri eksternal guna menghindari ketergantungan hash melingkar (circular hash dependency). Perubahan setelah finalisasi memerlukan versi dan *hash* referensi baru.



Gambar 3. Urutan penerbitan PDF sebelum pencatatan hash

Untuk *byte* PDF final B, *hash* referensi didefinisikan sebagai h_ref = SHA256(B). Pada unggahan U, pembanding menghitung h_u = SHA256(U). Hasil cocok diperoleh jika kedua *digest* sama. Definisi fungsi berasal dari NIST (2015), sedangkan kebijakan keputusan merupakan rancangan penelitian ini. Tidak dilakukan ekstraksi teks atau normalisasi PDF sebelum pembandingan, sehingga kesetaraan makna dan tampilan berada di luar kriteria kecocokan.

Dalam eksperimen, QR dibangkitkan secara lokal dan ditambahkan pada halaman pertama sebelum penghitungan *hash*. QR berisi URL demonstrasi pada *example.org* dengan token uji tetap yang diturunkan dari ID sintetis. Token tetap dipakai untuk reproduksibilitas, bukan sebagai contoh pembangkitan token acak aman pada produksi. Domain tersebut bukan layanan verifikasi institusi. Penelitian tidak mengukur keberhasilan pemindaian atau *decoding* QR.

Formulasi dan langkah perhitungan SHA-256

SHA-256 memetakan pesan menjadi 256 bit, atau 64 karakter heksadesimal, secara deterministik. Fungsi ini bukan enkripsi dan tidak memiliki operasi dekripsi. Rumus berikut mengikuti FIPS 180-4 (NIST, 2015). Simbol $\oplus$ menyatakan XOR, $\wedge$ AND, $\neg$ NOT, $\vee$ OR, ROTR rotasi kanan pada kata 32 bit, dan SHR pergeseran kanan logis. Semua penjumlahan kata dilakukan modulo 2^{32}.

$$\ell + 1 + k \equiv 448 \,(mod\ 512)\,;\ pesan\ akhir = M \parallel 1 \parallel 0^{k} \parallel [\ell]_{64} \quad (1)$$

Panjang pesan ℓ kurang dari 2^{64} bit. Bilangan k adalah jumlah nol terkecil yang memenuhi (1); panjang asli ditambahkan sebagai bilangan 64 bit big-endian. Setiap blok 512 bit dipecah menjadi 16 kata 32 bit lalu diperluas menjadi 64 kata.

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z) \quad (2)$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (3)$$

$$\Sigma_0(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \quad (4)$$

$$\Sigma_1(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \quad (5)$$

$$\sigma_0(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \quad (6)$$

$$\sigma_1(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \quad (7)$$

$$W_t = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} \, (mod\ 2^{32}) \quad (8)$$

Persamaan (8) berlaku untuk t = 16 sampai 63; W_0 sampai W_{15} berasal dari blok pesan. Delapan nilai awal heksadesimal adalah 6a09e667, bb67ae85, 3c6ef372, a54ff53a, 510e527f, 9b05688c, 1f83d9ab, dan 5be0cd19. Konstanta K_0 sampai K_{63} ditentukan standar, bukan dipilih secara acak ketika menjalankan algoritma.

$$T_1 = h + \Sigma_1(e) + Ch(e,f,g) + K_t + W_t \, (mod\ 2^{32}) \quad (9)$$

$$T_2 = \Sigma_0(a) + Maj(a,b,c) \, (mod\ 2^{32}) \quad (10)$$

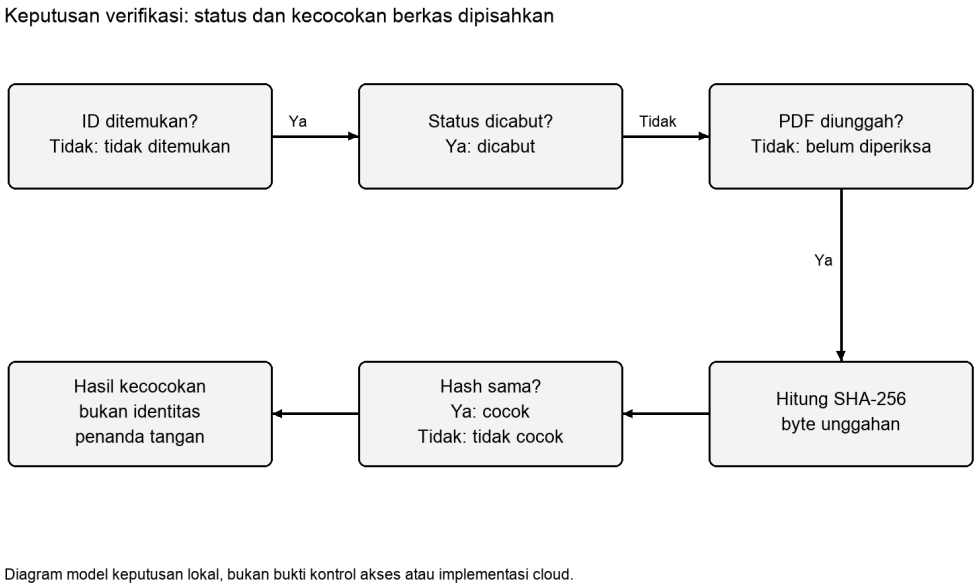
Dalam setiap putaran, a baru = $T_1 + T_2$, b baru = a, c baru = b, d baru = c, e baru = d + T_1, f baru = e, g baru = f, dan h baru = g; sisi kanan menggunakan nilai sebelum pembaruan. Setelah 64 putaran, masing-masing kata kerja ditambahkan ke kata keadaan sebelumnya, modulo 2^{32}. Delapan kata hasil digabungkan untuk memperoleh *digest*. Berkas PDF diperlakukan sebagai seluruh *byte* berkas, bukan hanya teks hasil ekstraksi. Implementasi pedagogis dan jejak putaran disertakan serta dibandingkan dengan hashlib; contoh ini tidak menggantikan pustaka kriptografi produksi.

Desain eksperimen

Setiap PDF dasar menghasilkan enam kasus: salinan *byte* identik, perubahan teks, perubahan angka, tambahan satu halaman, perubahan metadata, dan dokumen lain yang memakai token serta QR yang sama. Dengan demikian terdapat 72 pembandingan, terdiri atas 12 kontrol identik dan 60 variasi. Perubahan halaman dan metadata dilakukan melalui serialisasi ulang PDF; perlakuan tersebut menguji perubahan berkas hasil operasi, bukan mengisolasi satu *byte* atau mengukur *avalanche effect*.

PDF dibangkitkan menggunakan ReportLab 4.4.9, dimodifikasi dan diperiksa keterbacaannya menggunakan pypdf 6.10.0, serta dibandingkan dengan hashlib pada Python 3.12.14. Pemeriksaan metadata mencocokkan teks hasil ekstraksi sebelum dan sesudah modifikasi. Kesamaan teks ekstraksi tidak disamakan dengan bukti kesamaan tampilan piksel. Manifest mencatat nama file, jumlah halaman, ukuran *byte*, token uji, kedua *digest*, dan hasil pembandingan. Pelaksanaan eksperimen berlangsung pada 24 Maret 2026; tanggal tersebut diselaraskan sebelum penerimaan naskah dan tidak merupakan riwayat editorial atau tanggal terbit final.

Ukuran hasil utama ialah jumlah pasangan dengan *hash* sama atau berbeda pada setiap kategori. Tidak dihitung estimasi akurasi populasi, interval kepercayaan binomial, atau uji signifikansi karena kasus bersifat deterministik dan tidak merupakan sampel acak independen. Enam pengujian keputusan tambahan memeriksa kombinasi status aktif, dicabut, ID tidak ditemukan, tidak ada unggahan, perubahan file, dan penyalinan QR. Gambar 4 menampilkan model keputusan yang diimplementasikan secara lokal.



Gambar 4. Pemisahan status registri dan kecocokan berkas

DISKUSI DAN PEMBAHASAN

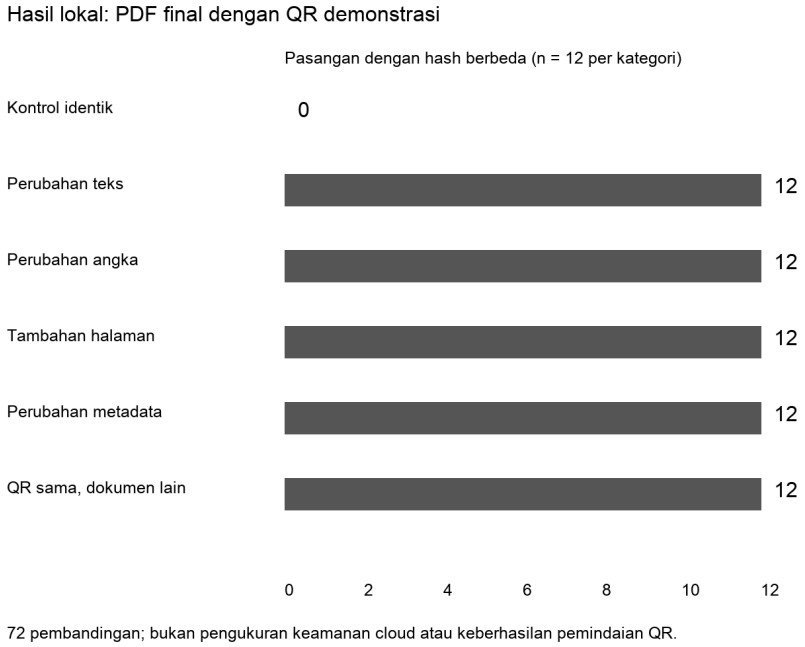
Hasil pembandingan byte PDF

Tabel 2 menyajikan seluruh hasil. Dua belas kontrol identik memiliki *hash* sama. Setiap kategori perubahan menghasilkan 12 *hash* berbeda, sehingga seluruh 60 variasi terdeteksi sebagai ketidakcocokan terhadap referensi. Pemeriksaan *parser* berhasil untuk semua berkas keluaran. Jumlah ini hanya mencerminkan cakupan eksperimen yang dijalankan; keberhasilan pada kasus terkontrol tidak menyatakan bahwa sistem mendeteksi semua bentuk pemalsuan.

Tabel 2. Pembandingan hash pada PDF sintetis final

Kategori	Pasangan	Hash sama	Hash berbeda
Kontrol identik	12	12	0
Perubahan teks	12	0	12
Perubahan angka	12	0	12
Tambahan halaman	12	0	12
Perubahan metadata	12	0	12
QR sama, dokumen lain	12	0	12
Total	72	12	60

Gambar 5 memvisualisasikan jumlah ketidakcocokan per kategori. Kontrol identik menyediakan pemeriksaan bahwa pembandingan tidak menolak salinan *byte* yang sama. Perubahan teks dan angka menunjukkan bahwa keluaran PDF hasil perubahan konten tidak lagi cocok dengan referensi. Penambahan halaman juga menghasilkan ketidakcocokan. Karena operasi pembangkitan atau serialisasi ulang dapat mengubah lebih dari satu bagian PDF, hasil tidak digunakan untuk menilai sensitivitas terhadap satu lokasi *byte* tertentu.



Gambar 5. Jumlah ketidakcocokan hash pada eksperimen lokal

Perubahan metadata menghasilkan *hash* berbeda pada seluruh 12 kasus, sementara teks hasil ekstraksi tetap sama. Temuan ini menegaskan sifat kriteria penelitian: identitas *byte*. Pada penggunaan administrasi, perubahan yang tidak mengubah isi substantif dapat tetap menimbulkan peringatan ketidakcocokan. Pesan antarmuka verifikasi sebaiknya secara presisi menyebutkan berkas berbeda dari referensi byte, bukan langsung memvonis dokumen palsu. Hal ini krusial karena perubahan metadata non-substantif tetap mengubah nilai hash, sehingga penilaian motif perubahan atau keabsahan administratif tetap membutuhkan klarifikasi penerbit.

Penyalinan QR dan keputusan status

Pada kategori salinan QR, dokumen dengan identitas isi berbeda memakai QR yang sama dengan dokumen referensi. Seluruh 12 file menghasilkan *hash* berbeda. Hal ini menunjukkan bahwa penggunaan token identik tidak membuat *byte* file lain cocok. Namun, keberhasilan proteksi tersebut berlaku mutlak hanya ketika pengguna mengunggah berkas PDF untuk dibandingkan secara penuh. Apabila pengguna sekadar memindai QR tanpa mengunggah berkas, sistem hanya memverifikasi keberadaan rekaman di registri tanpa memvalidasi keaslian berkas yang dipegang pengguna.

Enam kasus keputusan pada Tabel 3 memberikan hasil yang sesuai dengan keluaran yang ditentukan. Dokumen yang dicabut tetap menghasilkan status dicabut walaupun *byte* berkas cocok. ID yang tidak ada menghasilkan status tidak ditemukan. Tanpa unggahan, hasilnya terdaftar tetapi integritas berkas belum diperiksa. Implementasi lokal tidak menguji kebijakan akses jaringan maupun autentikasi administrator.

Tabel 3. Hasil enam kasus keputusan lokal

Kasus	Keluaran aktual	Sesuai
Aktif, file identik	Cocok	Ya
Aktif, file diubah	Tidak cocok	Ya
Dicabut, file identik	Dicabut	Ya
ID tidak ditemukan	Tidak ditemukan	Ya
Aktif, tanpa unggahan	Terdaftar; belum diperiksa	Ya

Kasus	Keluaran aktual	Sesuai
QR sama, dokumen lain	Tidak cocok	Ya

Pemisahan status memberikan informasi yang lebih tepat daripada satu label valid. Kecocokan berkas tidak membatalkan pencabutan. Keberadaan rekaman tidak membuktikan bahwa file pengguna identik. Lebih lanjut, pencocokan terhadap registri yang telah diubah penyerang dapat menghasilkan penerimaan yang salah secara substantif meskipun fungsi *hash* bekerja benar. Karena itu, integritas referensi adalah asumsi kepercayaan utama, bukan keluaran dari fungsi *hash*.

Contoh keputusan rektor dan perhitungan aktual

Contoh tambahan ini terpisah dari 72 pembandingan utama. Dokumen berlabel "CONTOH SINTETIS, BUKAN KEPUTUSAN RESMI" memuat Keputusan Rektor Kampus X, Nomor 001/SK/KX/2025, tentang Penetapan Tim Verifikasi Dokumen Akademik. Isinya menetapkan Ketua tim adalah Pejabat Contoh, dengan masa tugas 1 tahun. Kampus dan pejabat tersebut bersifat fiktif; tidak disertakan tanda tangan. Teks lengkap, tiga PDF contoh, dan hasil komputasi tersedia dalam paket data.

Sebagai perhitungan pendek, pesan ASCII "abc" tanpa tanda kutip dan tanpa baris baru memiliki $\ell = 24$, $k = 423$, $W_0 = 61626380$, dan $W_{15} = 00000018$ setelah padding. Pada putaran pertama, $\Sigma_1(e) = 3587272b$, $Ch(e,f,g) = 1f85c98c$, $\Sigma_0(a) = ce20b47e$, dan $Maj(a,b,c) = 3a6fe667$. Karena $K_0 = 428a2f98$, persamaan (9) menghasilkan $T_1 = 54da50e8$; persamaan (10) menghasilkan $T_2 = 08909ae5$. Nilai a baru adalah 5d6aebcd dan e baru fa2a4622. Setelah seluruh 64 putaran dan penambahan keadaan, hasilnya:

```
ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad
```

Teks keputusan asli menggunakan UTF-8 dengan baris baru LF, termasuk LF terakhir: 205 *byte* atau 1.640 bit, sehingga diproses dalam empat blok. Pada blok pertama $W_0 = 4b455055$, $T_1 = 3ebd3dbd$, $T_2 = 08909ae5$, a baru = 474dd8a2, dan e baru = e40d32f7. *Hash* akhir bukan hanya hasil putaran pertama; seluruh blok harus diselesaikan. Tabel 5 memperlihatkan *digest* lengkap yang benar-benar dihitung.

Tabel 5. Hash aktual contoh keputusan sintetis

Variasi	SHA-256 teks UTF-8	SHA-256 seluruh PDF
Asli-contoh	0537f7defe69034600fe44947f1d18ab 6c61cfc3785d69e831a1fbcc08731145	163b7c9b960cc4336a72818bca907426 6f7b42c58c4c0c30a7323ad9163feb1a
Diubah-masa-tugas	245aedd0a6fe9d22f5b310a988828070 d30c638e9d28095ac54e2186976c8b11	dbb0116f2e70355e9d8bedd09efaf777 6fd13520e9fec1795736b33093bccaec
QR-token-acak	0537f7defe69034600fe44947f1d18ab 6c61cfc3785d69e831a1fbcc08731145	7722edfe1f4246f27d1613ec2de135d7 eb0bf2ed3baed4da845acb093a1ec7ef

Pada variasi kedua hanya "Masa tugas: 1 tahun." diganti menjadi "Masa tugas: 2 tahun." QR tetap sama. Dibandingkan dengan aslinya, 143 dari 256 bit *hash* teks dan 131 dari 256 bit *hash* PDF berubah. Ini adalah ilustrasi satu pasangan, bukan estimasi statistik *avalanche effect*. Mengunggah PDF asli menghasilkan status cocok; mengunggah versi masa tugas yang diubah menghasilkan tidak cocok terhadap *hash* asli yang didaftarkan.

Variasi ketiga mempertahankan teks keputusan, tetapi memakai token QR acak 128 bit yang dihasilkan dengan generator acak kriptografis. Token contoh adalah f18cef355ca3db247c5f5d0a23d74b34 dan disimpan agar pengulangan eksperimen mereproduksi berkas. *Hash* teks tetap sama, sedangkan *hash* PDF berubah karena *byte* QR berubah. Token acak digunakan untuk identifikasi, bukan sebagai keluaran SHA-256. SHA-256 sendiri selalu menghasilkan *hash* yang sama untuk input *byte* yang sama. PDF bertoken baru perlu didaftarkan dengan *hash* finalnya sendiri; membandingkannya dengan *hash* PDF asli akan menghasilkan tidak cocok. Perubahan token setelah pencatatan *hash* melanggar urutan finalisasi yang dirancang.

Perbandingan dengan penelitian terdahulu

Tabel 4 menempatkan artefak penelitian terhadap beberapa pendekatan yang berdekatan. Rancangan berbasis registri terpusat memperjelas prosedur pengelolaan referensi, sedangkan penelitian *blockchain* membahas persoalan penerbitan serta pencatatan kredensial dengan model kepercayaan berbeda. Tidak terdapat eksperimen biaya, skalabilitas, atau keamanan komparatif dalam penelitian ini; karena itu tabel tidak memberikan peringkat keunggulan.

Tabel 4. Posisi artefak terhadap penelitian terkait

Sumber	Fokus	Perbedaan lingkup
Delgado-von-Eitzen et al. (2021)	Sertifikasi dan privasi	Artikel ini tidak mengevaluasi kepatuhan regulasi
Caramihai dan Severin (2023)	Pengelolaan diploma blockchain	Registri artikel ini dirancang terpusat
Rustemi et al. (2024)	Penerbitan dan verifikasi DIAR	Tidak ada deployment blockchain atau cloud di sini
Yuliana dan Walidaniy (2024)	Multi-signature EdDSA dan QR	Hash lokal tidak mengautentikasi penanda tangan
Rafsanjani et al. (2023)	Deteksi URL berbahaya	Pemeriksaan URL tidak dijalankan di sini

Yuliana dan Walidaniy (2024) memanfaatkan tanda tangan EdDSA untuk autentikasi dokumen. Sintyaningrum et al. (2021) juga menempatkan tanda tangan digital dalam penerbitan sertifikat profesional. Sebaliknya, eksperimen ini hanya memeriksa *hash* terhadap referensi. Penambahan EdDSA merupakan arah pengembangan yang membutuhkan pembangkitan kunci, perlindungan kunci privat, pengaitan identitas, dan kebijakan pencabutan. RFC 8032 menjelaskan algoritma EdDSA, tetapi keberadaan algoritma tersebut tidak dengan sendirinya menjamin keamanan aplikasi yang memakainya (Josefsson & Liusvaara, 2017).

QsecR menangani deteksi URL berbahaya, sedangkan kajian Njuguna dan Ndia merangkum ancaman QR yang lebih luas. Kedua sumber itu mendukung pemisahan pemeriksaan tujuan tautan dari pemeriksaan file. Untuk implementasi institusi, domain resmi harus dapat dikenali pengguna dan perubahan tujuan QR perlu diperiksa tersendiri. Tidak ada data dalam penelitian ini yang mengukur kemampuan pengguna mengenali domain palsu atau keberhasilan mitigasi *phishing*.

Implikasi desain dan keterbatasan

Hasil menghasilkan tiga implikasi desain dalam lingkup artefak. Pertama, penerbit harus mempertahankan PDF final yang persis sama dengan file yang digunakan untuk mencatat *hash*. Kedua, antarmuka perlu menyatakan apakah pemeriksaan hanya menyangkut rekaman atau juga *byte* unggahan. Ketiga, pencabutan harus menjadi keputusan terpisah dari kecocokan *hash*. Ketiga implikasi tersebut diturunkan dari prosedur serta kasus uji, bukan dari pengamatan pengguna atau evaluasi organisasi.

Dokumen cetak dan hasil scan tidak diharapkan cocok dengan *hash* PDF digital sumber, sebab keduanya merupakan representasi *byte* berbeda. Rancangan ini mengharuskan akses pada PDF digital untuk pemeriksaan *byte*. Verifikasi dokumen fisik hasil cetak atau pemindaian dapat memanfaatkan pemeriksaan metadata atau tanda air fisik, namun tidak dapat mengklaim kecocokan integritas byte PDF digital; pengembangan masa depan diarahkan pada integrasi tanda tangan elektronik tersertifikasi sesuai regulasi nasional. Pembatasan yang dinyatakan secara konkret membantu memisahkan mutu artefak dari jangkauan generalisasinya, sejalan dengan perhatian terhadap pelaporan keterbatasan penelitian desain (Barata et al., 2023).

Evaluasi terbatas pada PDF sintetis sederhana, satu lingkungan perangkat lunak, dan lima jenis variasi. Tidak tersedia pengujian PDF terenkripsi, lampiran, formulir kompleks, pembaruan bertahap, maupun interoperabilitas lintas editor. Tidak dilakukan *cryptanalysis*, pengukuran waktu respons cloud, pengujian beban, kontrol akses jarak jauh, atau studi *usability*. QR hanya dibangkitkan dan ditanamkan; keterbacaan setelah pencetakan, kerusakan gambar, dan berbagai

kamera tidak dievaluasi. Arsitektur Google Workspace tetap merupakan rancangan untuk pengembangan berikutnya.

Penelitian berikutnya perlu menjalankan *deployment* yang dapat diaudit, memeriksa izin administrator dan pembatasan data publik, menguji perilaku perubahan status serentak, serta mengukur waktu respons pada ukuran file yang berbeda. Studi pengguna dapat memeriksa apakah perbedaan terdaftar, cocok, dan dicabut dipahami secara benar. Evaluasi tersebut harus melaporkan data yang benar-benar dikumpulkan dan tidak dapat digantikan oleh keberhasilan pembanding lokal.

KESIMPULAN

Penelitian menghasilkan rancangan verifikasi yang memisahkan rekaman penerbitan, status pencabutan, dan kecocokan *byte* PDF. Pada 72 pembandingan lokal terhadap PDF sintetis yang telah memuat QR demonstrasi, 12 kontrol identik memiliki *hash* sama dan seluruh 60 variasi memiliki *hash* berbeda. Enam kasus keputusan status memberikan hasil sesuai kebijakan lokal yang ditentukan. Perubahan metadata dengan teks ekstraksi tetap sama memperlihatkan bahwa kecocokan *hash* merupakan kriteria *byte*, bukan kriteria kesamaan makna.

Kontribusi praktisnya adalah urutan finalisasi PDF sebelum pencatatan *hash*, label keputusan yang tidak berlebihan, dan paket uji yang dapat direproduksi. Penyalinan QR dapat diungkap melalui pembandingan file yang berbeda, tetapi pemindaian QR saja belum memeriksa file pengguna. SHA-256 tidak membuktikan identitas penanda tangan, dan keamanan bergantung pada referensi serta registri yang dipercaya. Kesimpulan tidak mencakup kelayakan *deployment* Google Workspace, penghematan biaya, *usability*, atau tanda tangan elektronik tersertifikasi.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika Cirebon atas penyediaan fasilitas komputasi riset dan dukungan kelembagaan selama pelaksanaan penelitian ini.

KONTRIBUSI PENULIS

Ade Sutriyono: *Conceptualization*, *Methodology*, *Software*, *Validation*, *Formal analysis*, *Visualization*, Writing – original draft, dan Writing – review and editing. Penulis telah memeriksa dan menyetujui versi akhir naskah.

PERNYATAAN KETERSEDIAAN DATA

Seluruh skrip Python pembangkit PDF sintetis, 72 berkas uji, manifes digest SHA-256, dan kode pembanding lokal tersedia dari para penulis atas permintaan yang wajar untuk tujuan verifikasi akademik dan replikasi ilmiah.

PERNYATAAN BEBAS KONFLIK KEPENTINGAN

Deklarasi konflik kepentingan perlu dikonfirmasi oleh seluruh penulis sebelum pengajuan naskah.

PERNYATAAN ETIKA PENELITIAN DAN PUBLIKASI

Para penulis menyatakan bahwa penelitian dan penulisan naskah ini telah mematuhi standar etika penelitian dan publikasi, sesuai dengan prinsip ilmiah, serta bebas dari plagiasi.

PERNYATAAN PEMANFAATAN TEKNOLOGI ASISTIF

Teknologi AI generatif, melalui Codex, digunakan untuk membantu perumusan rancangan, penelusuran dan pemeriksaan referensi, penyusunan kode eksperimen, pembuatan diagram, penulisan draf, dan penataan naskah. Hasil numerik berasal dari kode yang dijalankan pada PDF sintetis, bukan angka yang dihasilkan sebagai narasi. Penulis perlu menelaah dan menyetujui seluruh isi sebelum pengajuan serta bertanggung jawab atas keakuratan dan integritas versi akhir.

REFERENSI

Barata, J., da Cunha, P. R., & de Figueiredo, A. D. (2023). Self-reporting Limitations in Information Systems Design Science Research. *Business & Information Systems Engineering, 65(2), 143-160*. https://doi.org/10.1007/s12599-022-00782-8

Caramihai, M., & Severin, I. (2023). A *Blockchain*-Based Solution for Diploma Management in Universities. *Sustainability, 15(20), 15169*. https://doi.org/10.3390/su152015169

Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021). Application of *Blockchain* in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information. *Applied Sciences, 11(10), 4537*. https://doi.org/10.3390/app11104537

Hevner, A. R., Parsons, J., Brendel, A. B., Lukyanenko, R., Tiefenbeck, V., Tremblay, M. C., & vom Brocke, J. (2024). Transparency in design science research. *Decision Support Systems, 182, 114236*. https://doi.org/10.1016/j.dss.2024.114236

Josefsson, S., & Liusvaara, I. (2017). Edwards-Curve Digital Signature Algorithm (EdDSA) (RFC 8032). *RFC Editor*. https://www.rfc-editor.org/rfc/rfc8032

N*ational Institute of Standards and Technology. (2015). Secure Hash Standard (SHS) (FIPS PUB 180-4)*. https://doi.org/10.6028/NIST.FIPS.180-4

N*ational Institute of Standards and Technology. (2023). Digital Signature Standard (DSS) (FIPS 186-5)*. https://doi.org/10.6028/NIST.FIPS.186-5

Njuguna, D., & Ndia, J. (2025). Quick Response Code Security Attacks and Countermeasures: A Systematic Literature Review. *Journal of Cyber Security, 7(1), 1-20*. https://doi.org/10.32604/jcs.2025.059398

Prochner, I., & Godin, D. (2022). Quality in research through design projects: Recommendations for evaluation and enhancement. *Design Studies, 78, 101061*. https://doi.org/10.1016/j.destud.2021.101061

Rafsanjani, A. S., Kamaruddin, N. B., Rusli, H. M., & Dabbagh, M. (2023). QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework. *IEEE Access, 11, 92523-92539*. https://doi.org/10.1109/ACCESS.2023.3291811

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A Systematic Literature Review on *Blockchain*-Based Systems for Academic Certificate Verification. *IEEE Access, 11, 64679-64696*. https://doi.org/10.1109/ACCESS.2023.3289598

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2024). DIAR: a *blockchain*-based system for generation and verification of academic diplomas. *Discover Applied Sciences, 6(6), 297*. https://doi.org/10.1007/s42452-024-05984-1

Scanzio, S., Rosani, M., Scamuzzi, M., & Cena, G. (2024). QR Codes: From a Survey of the State of the Art to Executable eQR Codes for the Internet of Things. *IEEE Internet of Things Journal, 11(13), 23699-23710*. https://doi.org/10.1109/JIOT.2024.3385542

Sintyaningrum, D. E., Muladi, & Ashar, M. (2021). The Encryption of Electronic Professional Certificate by Using Digital Signature and QR Code. *2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE), 19-24*. https://doi.org/10.1109/ICCTEIE54047.2021.9650641

Yuliana, M., & Walidaniy, W. D. (2024). Efficient *Multi-signature* and QR Code Integration for Document Authentication Using EdDSA-based Algorithm. *International Journal of Intelligent Engineering and Systems, 17(2), 390-401*. https://doi.org/10.22266/ijies2024.0430.32