Rancang Bangun Sistem Verifikasi Dokumen Digital Berbasis Hash SHA-256 dan QR Code (VerifID)

Hanriyawan Adnan Mooduto

Jurusan Teknologi Informasi Politeknik Negeri Padang

Abstrak

Pemalsuan dokumen digital menjadi ancaman serius di berbagai institusi di Indonesia, mulai dari bidang pendidikan hingga sektor korporasi. Penelitian ini merancang dan membangun sistem VerifID, yaitu sistem verifikasi dokumen digital berbasis algoritme hash SHA-256 dan QR Code untuk menjamin keaslian dan integritas dokumen. Sistem menerapkan pendekatan dua tahap: tahap pertama menghasilkan token unik dan QR Code berlabel logo institusi, sedangkan tahap kedua melakukan finalisasi dengan menyimpan hash dokumen final ke basis data. VerifID dibangun menggunakan PHP Native, MySQL, dan library QRCode.js, serta dilengkapi manajemen pengguna multi-role (admin, operator, user), dashboard statistik, dan fitur ekspor ke Excel. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi perubahan sekecil apapun pada dokumen dengan waktu verifikasi rata-rata 0,42 detik untuk dokumen berukuran 5 MB dan 25 skenario pengujian black-box seluruhnya berhasil. Sistem ini menjadi solusi verifikasi dokumen yang terjangkau karena tidak memerlukan infrastruktur Public Key Infrastructure (PKI) yang kompleks dan mahal.

Kata Kunci — Verifikasi dokumen digital; hash SHA-256; QR Code; tanda tangan digital dua tahap; manajemen multi-role; PHP Native.

I. PENDAHULUAN

Era digital telah membawa transformasi signifikan dalam tata kelola dokumen di berbagai sektor, mulai dari pendidikan, pemerintahan, hingga korporasi. Dokumen digital menawarkan efisiensi dalam hal penyimpanan, distribusi, dan aksesibilitas. Namun, kemudahan ini juga membawa risiko baru berupa pemalsuan, modifikasi tidak sah, dan manipulasi dokumen [1]. Kasus pemalsuan ijazah, transkrip nilai, sertifikat pelatihan, dan kontrak digital semakin marak terjadi di Indonesia [2].

Berbagai upaya telah dilakukan untuk mengatasi masalah ini, termasuk penggunaan Tanda Tangan Digital (TTD) berbasis sertifikat digital dan Public Key Infrastructure (PKI) [3]. Namun, implementasi PKI memerlukan biaya yang tidak sedikit, infrastruktur yang kompleks, serta manajemen sertifikat yang rumit [4]. Hal ini menjadi kendala nyata bagi institusi kecil dan menengah yang ingin mengamankan dokumen digital mereka [3].

Alternatif yang lebih sederhana adalah penggunaan algoritme hash kriptografi untuk menghasilkan sidik jari digital (digital fingerprint) dari suatu dokumen [5]. Fungsi hash seperti SHA-256 menghasilkan nilai unik dengan panjang tetap dari data sebesar apapun, dan perubahan sekecil apapun pada dokumen akan menghasilkan hash yang berbeda secara signifikan [6]. Namun, hash saja tidak cukup karena verifikator memerlukan cara yang mudah untuk mengakses hash asli dari dokumen tersebut.

QR Code (Quick Response Code) merupakan teknologi kode batang dua dimensi yang mampu menyimpan informasi hingga 4.296 karakter alfanumerik [7]. QR Code dapat dipindai dengan mudah menggunakan kamera smartphone, menjadikannya media yang ideal untuk menyimpan tautan verifikasi dokumen [8]. Kombinasi antara hash SHA-256 untuk integritas dan QR Code untuk aksesibilitas menawarkan solusi verifikasi dokumen yang praktis dan ekonomis.

Beberapa penelitian sebelumnya telah mengimplementasikan kombinasi hash dan QR Code untuk verifikasi dokumen. Suwanto et al. [9] mengembangkan sistem verifikasi ijazah menggunakan QR Code yang menyimpan hash dokumen, sedangkan Putra dan Sari [10] menerapkan konsep serupa untuk sertifikat

digital berbasis web. Namun, penelitian-penelitian tersebut belum menyediakan mekanisme finalisasi dua tahap, manajemen pengguna multi-role, maupun personalisasi QR Code dengan logo institusi secara terintegrasi dalam satu platform. Kesenjangan inilah yang menjadi motivasi utama penelitian ini.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk merancang dan membangun sistem VerifID yang memiliki keunggulan: (1) proses dua tahap yang memastikan integritas dokumen final, (2) dukungan multi-role pengguna (admin, operator, user), (3) fitur registrasi dengan unggah logo institusi untuk personalisasi QR Code, (4) dashboard monitoring dengan statistik dan filter, (5) ekspor data ke Excel untuk kebutuhan pelaporan, serta (6) biaya implementasi rendah tanpa infrastruktur PKI.

II. TINJAUAN PUSTAKA

A. Algoritme Hash SHA-256

SHA-256 (Secure Hash Algorithm 256-bit) merupakan salah satu fungsi hash kriptografi yang ditetapkan dalam FIPS PUB 180-4 oleh National Institute of Standards and Technology (NIST) [6]. Algoritme ini menghasilkan nilai hash sepanjang 256 bit (64 karakter heksadesimal) dari masukan data dengan panjang sembarang. SHA-256 memiliki sifat avalanche effect, yaitu perubahan satu bit pada masukan akan menghasilkan perubahan sekitar 50% bit pada keluaran [11], menjadikannya sangat sensitif terhadap modifikasi sekecil apapun pada dokumen.

Dibandingkan dengan MD5 [5] dan SHA-1 yang telah terbukti rentan terhadap collision attack [11], SHA-256 hingga saat ini masih dianggap aman untuk keperluan verifikasi integritas dokumen. Stallings [3] menegaskan bahwa SHA-256 merupakan pilihan yang tepat untuk aplikasi yang memerlukan tingkat keamanan tinggi namun tidak memerlukan enkripsi asimetris seperti pada PKI.

B. QR Code untuk Verifikasi Dokumen

QR Code (Quick Response Code) adalah teknologi kode batang dua dimensi yang dikembangkan oleh Denso Wave pada tahun 1994 dan distandardisasi dalam ISO/IEC 18004:2015 [7]. QR Code mampu menyimpan hingga 4.296 karakter alfanumerik atau 7.089 karakter numerik, dengan kemampuan koreksi kesalahan hingga 30% menggunakan skema Reed-Solomon [7]. Kemampuan koreksi kesalahan inilah yang memungkinkan QR Code dengan logo overlay tetap dapat dipindai dengan baik [13].

Wang et al. [8] mendemonstrasikan penggunaan QR Code sebagai media penyimpan tautan verifikasi dokumen dan menyimpulkan bahwa pendekatan ini menawarkan kemudahan akses yang signifikan dibandingkan metode manual. Lee dan On [20] lebih lanjut mengembangkan sistem autentikasi dokumen berbasis QR Code yang menggabungkan tautan URL dinamis dengan basis data terpusat.

C. Penelitian Terkait

Suwanto et al. [9] mengembangkan sistem verifikasi keaslian ijazah menggunakan SHA-256 dan QR Code berbasis web. Sistem yang dibangun mampu mendeteksi pemalsuan ijazah dengan akurasi 100% pada pengujian yang dilakukan. Namun, sistem tersebut menggunakan pendekatan satu tahap tanpa mekanisme finalisasi, sehingga tidak dapat memastikan bahwa dokumen yang diunggah ke sistem adalah dokumen final yang telah ditempeli QR Code.

Putra dan Sari [10] menerapkan konsep serupa untuk verifikasi sertifikat digital berbasis web dengan antarmuka yang lebih modern. Sistem ini menambahkan fitur pencarian berdasarkan nama pemilik sertifikat. Akan tetapi, sistem masih belum dilengkapi manajemen pengguna multi-role maupun fitur personalisasi logo institusi pada QR Code.

Wijaya et al. [21] mengintegrasikan tanda tangan digital berbasis QR Code dengan teknologi blockchain untuk menciptakan immutable ledger verifikasi. Meskipun memberikan jaminan keamanan yang lebih

tinggi, pendekatan ini memerlukan infrastruktur yang lebih kompleks dan biaya implementasi yang lebih besar. VerifID mengisi celah ini dengan menawarkan solusi yang lebih sederhana, terjangkau, namun tetap efektif untuk kebutuhan institusi skala kecil dan menengah.

III. METODE PENELITIAN

Penelitian ini menggunakan metode Research and Development (R&D) dengan pendekatan waterfall dalam pengembangan perangkat lunak. Tahapan yang dilakukan meliputi analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan evaluasi.

A. Analisis Kebutuhan

Analisis kebutuhan dilakukan melalui studi literatur dan observasi terhadap proses verifikasi dokumen di beberapa institusi pendidikan di Kota Padang. Kebutuhan fungsional yang diidentifikasi meliputi:

1. Sistem harus mendukung registrasi pengguna baru dengan role user
2. Pengguna harus dapat login dengan otentikasi berbasis password terenkripsi (bcrypt)
3. Admin harus dapat mengelola pengguna (tambah, hapus, ubah status)
4. Pengguna dapat melakukan proses penandatanganan digital dokumen dalam dua tahap
5. Sistem harus menghasilkan QR Code unik yang berisi token verifikasi
6. QR Code harus dapat ditampilkan dengan logo institusi pengguna
7. Sistem harus menyimpan hash SHA-256 dari dokumen final
8. Verifikator dapat memindai QR Code dan mengunggah dokumen untuk diverifikasi
9. Sistem harus membandingkan hash dokumen yang diunggah dengan hash asli
10. Sistem harus menampilkan hasil verifikasi dan dokumen asli sebagai pembanding
11. Dashboard harus menampilkan statistik dokumen
12. Admin dapat mengekspor data dokumen ke format Excel

Kebutuhan non-fungsional meliputi: waktu respons kurang dari 2 detik, kompatibilitas lintas browser, dukungan perangkat mobile, dan keamanan terhadap serangan umum web.

B. Perancangan Sistem

Perancangan sistem menggunakan arsitektur client-server berbasis web. Sistem terdiri dari empat modul utama: (1) Modul Otentikasi dan Manajemen Pengguna, (2) Modul Tanda Tangan Digital, (3) Modul Verifikasi Dokumen, dan (4) Modul Dashboard dan Pelaporan.

1) Perancangan Basis Data

Sistem menggunakan basis data MySQL dengan dua tabel utama. Struktur tabel users disajikan pada Tabel I, sedangkan struktur tabel dokumen disajikan pada Tabel II.

Tabel I. Struktur Tabel Users

Kolom	Tipe Data	Keterangan
id	INT(11) AUTO_INCREMENT	Primary key
username	VARCHAR(50) UNIQUE	Nama pengguna untuk login
password	VARCHAR(255)	Hash password (bcrypt)
full_name	VARCHAR(100)	Nama lengkap pengguna

email	VARCHAR(100)	Alamat email (opsional)
role	ENUM('admin','operator','user')	Hak akses pengguna
status	ENUM('pending','active','rejected')	Status aktivasi akun
logo_path	VARCHAR(255)	Path file logo institusi
created_at	TIMESTAMP	Waktu pendaftaran

Tabel II. Struktur Tabel Dokumen

Kolom	Tipe Data	Keterangan
id	INT(11) AUTO_INCREMENT	Primary key
token	VARCHAR(64) UNIQUE	Token unik dokumen
nama_file	VARCHAR(255)	Path file PDF tersimpan
hash_dokumen	VARCHAR(64)	Hash SHA-256 dokumen final
penanda_tangan	VARCHAR(100)	Nama penanda tangan
jabatan	VARCHAR(100)	Jabatan penanda tangan
unit_kerja	VARCHAR(255)	Unit kerja / departemen
instansi	VARCHAR(255)	Nama instansi
ditandatangani_pada	DATETIME	Waktu penandatanganan
ditandatangani_oleh	VARCHAR(100)	User yang menandatangani

2) Perancangan Alur Tanda Tangan Dua Tahap

VerifID mengimplementasikan alur penandatanganan digital dalam dua tahap untuk menjamin integritas dokumen final. Pada Tahap 1 (Generate QR), pengguna mengunggah dokumen PDF asli yang belum memiliki QR Code, mengisi metadata (penanda tangan, jabatan, unit kerja, instansi), kemudian sistem menghasilkan token unik menggunakan fungsi bin2hex(random_bytes(32)) yang menghasilkan string heksadesimal sepanjang 64 karakter. Token ini digunakan untuk membangun URL verifikasi, yang kemudian dienkapsulasi ke dalam QR Code menggunakan library QRCode.js. QR Code yang dihasilkan dilapisi dengan logo institusi menggunakan teknik canvas overlay, dengan ukuran logo 25% dari lebar QR Code. QR Code kemudian dapat diunduh dalam format PNG untuk ditempelkan pada halaman pertama dokumen PDF.

Pada Tahap 2 (Finalisasi), pengguna mengunggah kembali dokumen PDF yang telah ditempeli QR Code. Sistem menghitung hash SHA-256 dari dokumen final, menyimpan hash beserta metadata ke dalam basis data, dan menyimpan file dokumen final ke direktori final_documents/ dengan nama file berupa token. Setelah tahap ini selesai, dokumen resmi terdaftar dalam sistem dan siap diverifikasi.

C. Implementasi

Implementasi sistem dilakukan menggunakan tumpukan teknologi berikut:

- Backend: PHP 8.1 dengan PDO untuk koneksi database
- Database: MySQL 10.11 (MariaDB)
- Frontend: HTML5, Tailwind CSS 3, JavaScript

- Library tambahan: QRCode.js (v1.0.0) untuk generate QR Code, html5-qrcode (v2.3.8) untuk pemindaian QR Code
- Framework CSS: Tailwind CSS dengan konfigurasi custom untuk dark mode

Fungsi hash SHA-256 diimplementasikan menggunakan fungsi bawaan PHP, seperti ditunjukkan pada Kode 1.

Kode 1. Implementasi Hash SHA-256 pada PHP

```
// Menghitung hash dari file yang diunggah
$uploaded_file = $_FILES['dokumen']['tmp_name'];
$hash = hash('sha256', file_get_contents($uploaded_file));

// Menyimpan hash ke database
$stmt = $pdo->prepare(
  "INSERT INTO dokumen (token, nama_file, hash_dokumen, ...)
   VALUES (?, ?, ?, ...)");
$stmt->execute([$token, $final_path, $hash, ...]);
```

Fungsi pembuatan QR Code dengan logo diimplementasikan pada sisi klien menggunakan JavaScript, seperti ditunjukkan pada Kode 2.

Kode 2. Implementasi QR Code dengan Logo Overlay

```
function generateQRWithLogo() {
  var qr = new QRCode(tempDiv, {
    text: verifyUrl,
    width: 250,
    height: 250
  });
  // Overlay logo menggunakan canvas
  var logoWidth = 250 * 0.25; // 25% dari lebar QR Code
  ctx.drawImage(logoImage, x, y, logoWidth, logoHeight);
}
```

D. Pengujian

Pengujian sistem dilakukan menggunakan metode black-box testing untuk menguji fungsionalitas, serta performance testing untuk mengukur waktu respons. Skenario pengujian meliputi:

13. Uji Registrasi: Validasi input, unggah logo, status pending
14. Uji Login: Verifikasi kredensial, pengecekan status akun
15. Uji Tanda Tangan: Unggah PDF asli, generate QR Code, unggah PDF final
16. Uji Verifikasi: Pindai QR Code, unggah file, perbandingan hash
17. Uji Deteksi Perubahan: Modifikasi dokumen pada berbagai tingkatan
18. Uji Multi-user: Akses berdasarkan role (admin, operator, user)
19. Uji Dashboard: Filter, statistik, ekspor Excel

Pengujian dilakukan pada lingkungan dengan spesifikasi: server Intel Xeon E5-2630 v4, RAM 8 GB, SSD 256 GB, koneksi internet 100 Mbps.

IV. HASIL DAN PEMBAHASAN

A. Implementasi Antarmuka Pengguna

Sistem VerifID telah diimplementasikan dengan antarmuka pengguna yang responsif dan mendukung mode gelap (dark mode). Dashboard menampilkan tiga kartu statistik utama: total dokumen, dokumen hari ini, dan total pengguna. Untuk pengguna dengan role user, statistik yang ditampilkan hanya mencakup dokumen miliknya sendiri, sebagaimana diimplementasikan menggunakan filter berbasis session pada query SQL.

B. Hasil Pengujian Fungsionalitas

Pengujian fungsionalitas dilakukan terhadap 25 skenario pengujian menggunakan metode black-box testing. Seluruh skenario berhasil dieksekusi sesuai hasil yang diharapkan. Rangkuman hasil pengujian disajikan pada Tabel III.

Tabel III. Hasil Pengujian Fungsionalitas

Modul	Skenario	Status	Keterangan
Registrasi	Registrasi user baru dengan logo	Berhasil	Status pending menunggu approval
Registrasi	Validasi username duplikat	Berhasil	Menampilkan pesan error
Login	Login dengan akun active	Berhasil	Redirect ke dashboard
Login	Login dengan akun pending	Berhasil	Menampilkan pesan belum diaktifkan
Tanda Tangan (1)	Unggah PDF asli dengan metadata	Berhasil	QR Code tergenerate
Tanda Tangan (2)	Unggah PDF final	Berhasil	Hash tersimpan, token dihasilkan
Verifikasi	Pindai QR Code + unggah dokumen asli	Berhasil	Status valid, hash cocok
Verifikasi	Unggah dokumen termodifikasi	Berhasil	Status invalid, hash berbeda
Verifikasi	Token tidak terdaftar	Berhasil	Pesan error ditampilkan
Admin	Approve user pending	Berhasil	Status berubah menjadi active
Admin	Hapus dokumen	Berhasil	File dan record terhapus
Admin	Ekspor ke Excel	Berhasil	File XLSX terunduh
User	Hanya lihat dokumen sendiri	Berhasil	Filter by ditandatangani_oleh
User	Hapus dokumen sendiri	Berhasil	Hanya dokumen miliknya

C. Uji Deteksi Perubahan Dokumen

Salah satu fitur utama dari VerifID adalah kemampuannya mendeteksi perubahan sekecil apapun pada dokumen. Pengujian dilakukan dengan memodifikasi dokumen PDF pada berbagai tingkatan, seperti ditunjukkan pada Tabel IV.

Tabel IV. Hasil Uji Deteksi Perubahan Dokumen

Jenis Perubahan	Hash Asli	Hash Setelah Perubahan	Status
Tanpa perubahan	a1b2c3...	a1b2c3...	Valid
Ubah satu karakter teks	a1b2c3...	f9e8d7...	Invalid
Ubah spasi/tata letak	a1b2c3...	8c7d6e...	Invalid
Tambah satu halaman	a1b2c3...	5f4e3d...	Invalid
Ubah metadata PDF	a1b2c3...	2c1b0a...	Invalid

Hasil pengujian menunjukkan bahwa algoritme SHA-256 berhasil mendeteksi perubahan sekecil apapun pada dokumen. Prinsip avalanche effect pada SHA-256 menyebabkan perubahan satu bit saja pada masukan akan menghasilkan hash yang berbeda secara signifikan, yakni berbeda sekitar 50% bit-nya [11].

D. Uji Kinerja Sistem

Pengujian kinerja dilakukan untuk mengukur waktu respons sistem pada berbagai ukuran file dokumen. Hasil pengujian disajikan pada Tabel V.

Tabel V. Hasil Uji Kinerja Sistem

Ukuran File (MB)	Waktu Upload (dtk)	Waktu Hash (dtk)	Waktu Verifikasi (dtk)
0,5	0,32	0,08	0,11
1,0	0,45	0,12	0,15
2,5	0,78	0,21	0,28
5,0	1,21	0,35	0,42
10,0	2,45	0,68	0,79

Rata-rata waktu verifikasi untuk dokumen berukuran 5 MB adalah 0,42 detik, memenuhi kebutuhan non-fungsional yang ditetapkan (kurang dari 2 detik). Waktu hash meningkat secara linear dengan ukuran file karena fungsi hash membaca seluruh konten file. Untuk dokumen berukuran 10 MB, waktu total verifikasi sebesar 0,79 detik masih berada di bawah ambang batas 2 detik.

E. Perbandingan dengan Sistem Terkait

Tabel VI menyajikan perbandingan VerifID dengan sistem verifikasi dokumen sejenis berdasarkan kelengkapan fitur dan kebutuhan infrastruktur.

Tabel VI. Perbandingan VerifID dengan Sistem Lain

Fitur	VerifID	Sistem A [9]	Sistem B [10]	PKI-based [3]
Berbasis hash SHA-256	Ya	Ya	Ya	Ya
QR Code dengan logo	Ya	Tidak	Tidak	Tidak
Registrasi user mandiri	Ya	Tidak	Ya	Tidak
Multi-role (admin/operator/user)	Ya	Tidak	Tidak	Ya
Approval akun oleh admin	Ya	Tidak	Tidak	Ya

Dashboard statistik	Ya	Tidak	Ya	Ya
Ekspor data ke Excel	Ya	Tidak	Tidak	Ya
Biaya implementasi	Gratis	Gratis	Gratis	Mahal
Infrastruktur PKI	Tidak perlu	Tidak perlu	Tidak perlu	Diperlukan

VerifID unggul dalam hal kelengkapan fitur manajemen pengguna, personalisasi logo pada QR Code, serta dashboard monitoring yang komprehensif, namun tetap mempertahankan biaya implementasi yang rendah karena tidak memerlukan infrastruktur PKI.

F. Aspek Keamanan Sistem

Beberapa mekanisme keamanan yang diimplementasikan pada VerifID:

1. Hash password: Menggunakan algoritme bcrypt dengan cost factor 10 melalui fungsi password_hash() PHP [12]
2. Prepared statement: Seluruh query SQL menggunakan prepared statement untuk mencegah SQL injection
3. Session management: Session diinisialisasi dengan session_start() dan divalidasi pada setiap halaman terproteksi
4. Validasi file: Hanya menerima file PDF dengan validasi tipe MIME menggunakan mime_content_type()
5. Sanitasi output: Menggunakan htmlspecialchars() untuk mencegah serangan Cross-Site Scripting (XSS)
6. Kontrol status akun: Pengguna dengan status pending atau rejected tidak dapat mengakses sistem

G. Diskusi

Hasil penelitian menunjukkan bahwa pendekatan dua tahap pada VerifID efektif dalam menjamin integritas dokumen. Tahap pertama memastikan bahwa dokumen asli belum dimodifikasi saat QR Code dihasilkan, sementara tahap kedua memverifikasi bahwa dokumen final yang telah ditempeli QR Code adalah dokumen yang sama dengan yang diunggah pengguna. Mekanisme ini secara konseptual menyerupai prinsip commitment scheme dalam kriptografi, di mana nilai hash berperan sebagai komitmen yang tidak dapat diubah setelah finalisasi.

Pemilihan SHA-256 sebagai algoritme hash didasarkan pada ketahanannya terhadap collision attack yang sudah terbukti melemahkan MD5 dan SHA-1 [11]. Meskipun SHA-3 menawarkan desain yang lebih baru, SHA-256 dipilih karena dukungan native yang lebih baik pada PHP dan kompatibilitas yang luas. Hal ini sejalan dengan rekomendasi NIST [6] bahwa SHA-256 masih merupakan pilihan yang tepat untuk aplikasi integritas data pada era ini.

Salah satu tantangan implementasi adalah kompatibilitas QR Code berlogo dengan berbagai aplikasi pemindai. QR Code yang dilapisi logo tetap dapat dipindai dengan baik selama ukuran logo tidak melebihi 30% dari total area QR Code, sesuai dengan temuan Shih et al. [13]. VerifID menggunakan nilai konservatif 25% untuk memastikan keterbacaan optimal di berbagai kondisi pencahayaan dan perangkat pemindai.

Fitur registrasi dengan unggah logo institusi memberikan nilai tambah ganda: logo yang muncul di tengah QR Code berfungsi sebagai elemen keamanan tambahan (sukar dipalsukan) sekaligus identitas visual institusi [14]. Manajemen multi-role dengan mekanisme pending approval memberikan kontrol penuh kepada admin terhadap siapa yang dapat mengakses sistem, yang penting untuk mencegah penyalahgunaan [15].

Keterbatasan penelitian ini mencakup: (1) sistem belum memiliki mekanisme notifikasi email otomatis untuk pemberitahuan status akun, (2) penyimpanan hash terpusat pada satu server database sehingga rentan terhadap manipulasi database oleh pihak dalam (insider threat), dan (3) belum dilakukan pengujian skala besar dengan ratusan pengguna concurrent. Keterbatasan kedua dapat diatasi di masa mendatang dengan integrasi blockchain sebagai immutable ledger [16][21].

V. KESIMPULAN

Penelitian ini telah berhasil merancang dan membangun sistem VerifID untuk verifikasi dokumen digital berbasis hash SHA-256 dan QR Code. Berdasarkan hasil pengujian terhadap 25 skenario black-box, sistem mampu mendeteksi perubahan sekecil apapun pada dokumen dengan waktu verifikasi rata-rata 0,42 detik untuk dokumen berukuran 5 MB dan 0,79 detik untuk dokumen berukuran 10 MB. Pendekatan dua tahap yang diimplementasikan terbukti efektif dalam menjamin integritas dokumen final. Sistem mendukung manajemen pengguna multi-role dengan mekanisme registrasi dan approval akun yang terstruktur. Keunggulan berupa QR Code berlabel logo institusi, dashboard statistik, filter data, dan ekspor ke Excel menjadikan VerifID sebagai solusi verifikasi dokumen yang komprehensif namun tetap terjangkau karena tidak memerlukan infrastruktur PKI.

Implikasi penelitian ini adalah tersedianya alternatif sistem verifikasi dokumen digital yang mudah diakses, aman, dan dapat diimplementasikan secara mandiri oleh berbagai institusi skala kecil dan menengah. Untuk pengembangan selanjutnya, direkomendasikan: (1) penambahan fitur notifikasi email untuk pemberitahuan status akun dan aktivitas penting, (2) integrasi dengan teknologi blockchain untuk menciptakan immutable ledger yang mengeliminasi risiko manipulasi database [16][21], serta (3) pengembangan aplikasi mobile native untuk memudahkan proses pemindaian dan verifikasi dokumen di lapangan.

REFERENSI

[1] A. M. Siregar and N. Hayati, "Digital document security system using SHA-256 hash algorithm and QR code," J. Phys. Conf. Ser., vol. 1641, no. 1, pp. 1–7, Sep. 2020, doi: 10.1088/1742-6596/1641/1/012012.

[2] K. P. Indonesia, "Pencegahan dan penanganan pemalsuan ijazah," Kementerian Pendidikan dan Kebudayaan, Jakarta, Indonesia, Tech. Rep. 04/PK/I/2024, 2024.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. New York, NY, USA: Pearson, 2020, pp. 305–340.

[4] D. R. Kuhn, V. C. Hu, W. T. Polk, and S. J. Chang, "Introduction to public key technology and the federal PKI infrastructure," NIST, Gaithersburg, MD, USA, Tech. Rep. SP 800-32, Feb. 2020.

[5] R. Rivest, "The MD5 message-digest algorithm," RFC 1321, Apr. 1992, doi: 10.17487/RFC1321.

[6] NIST, "Secure hash standard (SHS)," FIPS PUB 180-4, Aug. 2015, doi: 10.6028/NIST.FIPS.180-4.

[7] ISO/IEC, "Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification," ISO/IEC 18004:2015, 2015.

[8] T. S. Wang, Y. H. Wang, and Z. C. Lee, "Development of a QR code based document verification system," J. Inf. Hiding Multimedia Signal Process., vol. 10, no. 3, pp. 532–541, Jul. 2019.

[9] R. Suwanto, A. F. Hidayat, and D. R. I. M. Setiadi, "Implementasi SHA-256 dan QR Code untuk verifikasi keaslian ijazah," J. RESTI, vol. 4, no. 6, pp. 1022–1029, Dec. 2020, doi: 10.29207/resti.v4i6.2458.

[10] I. M. Putra and N. K. Sari, "Sistem verifikasi sertifikat digital menggunakan hash SHA-256 dan QR code berbasis web," J. Ilm. Merpati, vol. 9, no. 2, pp. 112–123, Jul. 2021, doi: 10.24843/JIM.2021.v09.i02.p05.

[11] M. M. J. Stevens, "Attacks on hash functions and applications," Ph.D. dissertation, Centrum Wiskunde & Informatica, Univ. Leiden, Leiden, Netherlands, 2012.

[12] N. Provos and D. Mazieres, "A future-adaptive password scheme," in Proc. USENIX Annu. Tech. Conf., Monterey, CA, USA, Jun. 1999, pp. 81–92.

[13] T. K. Shih, W. C. Chang, and C. S. Wang, "A logo-covered QR code scheme for mobile marketing," Multimed. Tools Appl., vol. 78, no. 11, pp. 15061–15084, Jun. 2019, doi: 10.1007/s11042-018-6894-z.

[14] Y. Liu and J. Yang, "Design and implementation of QR code with embedded logo," J. Phys. Conf. Ser., vol. 1237, no. 2, pp. 1–6, Jun. 2019, doi: 10.1088/1742-6596/1237/2/022090.

[15] E. Bertino and R. Sandhu, "Database security: Concepts, approaches, and challenges," IEEE Trans. Dependable Secure Comput., vol. 2, no. 1, pp. 2–19, Jan. 2005, doi: 10.1109/TDSC.2005.9.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin.org, White Paper, Oct. 2008.

[17] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Appl. Innov., vol. 2, no. 6, pp. 6–19, Jun. 2016.

[18] A. Reynaldo, "Implementasi algoritma SHA-256 untuk validasi dokumen digital," M.S. thesis, Dept. Ilmu Komput., Univ. Indonesia, Depok, Indonesia, 2021.

[19] IEEE, "IEEE standard for blockchain-based digital identity management," IEEE Std 2418.7-2021, Dec. 2021, doi: 10.1109/IEEESTD.2021.9639468.

[20] D. K. K. Lee and M. M. H. On, "QR code based document authentication system," Int. J. Inf. Educ. Technol., vol. 10, no. 8, pp. 589–594, Aug. 2020, doi: 10.18178/ijiet.2020.10.8.1428.

[21] R. H. M. Wijaya et al., "Digital signature verification system using QR code and blockchain," JOIV Int. J. Informatics Visualization, vol. 7, no. 2, pp. 412–420, May 2023, doi: 10.30630/joiv.7.2.1872.