Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
5 (3) 2025, Page: 52236-52240

Penerapan Digital Signature Berbasis Algoritma RSA-2048 dan SHA-256 untuk Verifikasi Keaslian Dokumen Akademik Siswa pada Sistem Berbasis Web

Khairul Fikri[1], Hadi Kurnia Saputra[2]

[1,2]Program Studi Pendidikan Teknik Informatika, Departemen Elektronika, Fakultas Teknik, Universitas Negeri Padang, Indonesia

Penulis Korespondensi: Khairul Fikri, e-mail: fikrikhairul53@gmail.com

Published: Juli , 2025

ABSTRAK

Pengelolaan dokumen akademik siswa di Sekolah Menengah Kejuruan masih sering dilakukan secara manual menggunakan dokumen fisik dan file spreadsheet yang terpisah, sehingga pencarian dokumen memakan waktu dan dokumen rentan dipalsukan karena belum tersedia mekanisme verifikasi keaslian secara digital.

Tujuan penelitian ini adalah merancang dan menerapkan mekanisme digital signature berbasis algoritma RSA-2048 dan fungsi hash SHA-256 untuk menjamin keaslian dan integritas dokumen akademik siswa, serta menguji fungsionalitas dan kelayakan sistem pada lingkungan sekolah yang sebenarnya.

Bahan dan metode. Sistem dikembangkan menggunakan metode Research and Development (R&D) dengan model Waterfall yang terdiri atas tahap analisis, desain, pengodean, dan pengujian. Mekanisme digital signature diimplementasikan melalui ekstensi OpenSSL bawaan PHP pada framework Laravel dengan basis data MySQL, membangkitkan pasangan kunci RSA 2048 bit untuk setiap penanda tangan yang berwenang dan nilai hash SHA-256 untuk setiap dokumen sebelum ditandatangani. Setiap dokumen yang telah ditandatangani dilengkapi QR Code yang terhubung ke halaman verifikasi publik.

Hasil. Pengujian Black-box Testing terhadap 14 skenario menunjukkan 11 skenario berjalan sesuai harapan, 2 skenario yang berkaitan dengan pemindaian QR Code berhasil sebagian, dan 1 skenario belum diuji. Pengujian kelayakan menggunakan kuisioner Skala Likert terhadap 6 responden menghasilkan persentase kelayakan sebesar 77,33% yang termasuk kategori layak.

Simpulan. Mekanisme digital signature berbasis RSA-2048 dan SHA-256 berhasil diterapkan dan mampu menjamin autentikasi, integritas, dan non-repudiation dokumen akademik secara matematis, meskipun fitur pemindaian QR Code masih memerlukan pengujian lanjutan sebelum sistem diterapkan secara produksi.

Kata kunci: digital signature, algoritma RSA, SHA-256, QR Code, keaslian dokumen

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Perkembangan teknologi informasi mendorong institusi pendidikan, termasuk Sekolah Menengah Kejuruan (SMK), untuk memiliki sistem pengelolaan dokumen akademik yang akurat, aman, dan mudah diverifikasi oleh berbagai pihak terkait. Di SMK Negeri 1 Lembah Melintang, pengelolaan dokumen akademik siswa seperti laporan hasil belajar, sertifikat kompetensi, dan dokumen pendukung lainnya masih dilakukan secara manual dan terpisah menggunakan dokumen fisik serta file spreadsheet. Kondisi ini menimbulkan beberapa persoalan, yaitu lamanya proses pencarian dokumen, potensi kesalahan pencatatan dan duplikasi data, serta tingginya risiko pemalsuan dokumen akademik yang beredar.

Berdasarkan data Dapodik Kementerian Pendidikan, SMK Negeri 1 Lembah Melintang memiliki jumlah siswa aktif sebanyak 1.070 siswa pada tahun ajaran 2026/2027, dengan estimasi lebih dari 2.100 dokumen rapor yang perlu diterbitkan setiap tahun ajaran, di luar dokumen akademik lain seperti sertifikat kompetensi dan surat keterangan lulus. Berdasarkan keterangan Kepala Tata Usaha, pencarian dokumen dari arsip fisik yang diterbitkan dalam kurun waktu 5 tahun terakhir membutuhkan waktu sekitar 5 menit, sementara dokumen yang diterbitkan lebih dari 10 tahun lalu seringkali tidak dapat ditemukan kembali. Permasalahan mendasar lain yang dihadapi adalah belum adanya mekanisme verifikasi keaslian dokumen akademik secara digital, sehingga dokumen fisik rentan dipalsukan oleh pihak eksternal dan berdampak pada rendahnya kepercayaan pihak industri maupun perguruan tinggi terhadap dokumen yang diterbitkan sekolah.

Digital signature atau tanda tangan digital merupakan mekanisme kriptografi yang memungkinkan sebuah dokumen digital diberi tanda tangan secara elektronik sehingga keaslian dan integritasnya dapat diverifikasi secara matematis. Mekanisme ini bekerja berdasarkan prinsip kriptografi asimetris, yaitu penggunaan sepasang kunci yang berbeda namun saling berkaitan, berupa kunci privat yang digunakan untuk menandatangani dokumen dan kunci publik yang digunakan untuk memverifikasi tanda tangan tersebut. Digital signature memiliki tiga sifat utama, yaitu autentikasi, integritas, dan non-repudiation, yang menjadikannya berbeda dari tanda tangan basah karena keasliannya dapat dibuktikan tanpa memerlukan kehadiran fisik pihak penandatangan.

Tujuan penelitian ini adalah merancang dan menerapkan mekanisme digital signature berbasis algoritma RSA dengan panjang kunci 2048 bit dan fungsi hash SHA-256, dilengkapi QR Code sebagai media verifikasi publik, pada aplikasi manajemen dokumen akademik siswa berbasis web, serta menguji fungsionalitas dan tingkat kelayakannya pada lingkungan sekolah yang sebenarnya.

METODE

Metode Penelitian

Penelitian ini menggunakan metode Research and Development (R&D) yang diterapkan pada bidang rekayasa perangkat lunak, dengan model pengembangan Waterfall yang terdiri atas empat tahap berurutan, yaitu analisis, desain, pengodean, dan pengujian. Model Waterfall dipilih karena seluruh kebutuhan fungsional dan non-fungsional sistem sudah terdefinisi lengkap sejak tahap analisis awal, penelitian dikerjakan oleh satu orang peneliti dengan tenggat waktu yang jelas, dan mekanisme kriptografi digital signature membutuhkan rancangan yang matang dan diverifikasi sebelum diimplementasikan.

Perancangan Digital Signature

Mekanisme digital signature dibangun melalui empat tahapan utama, yaitu pemilihan teknologi kriptografi, pembangkitan pasangan kunci RSA, proses penandatanganan dokumen (signing), dan proses verifikasi tanda tangan (verification). Algoritma kriptografi asimetris yang digunakan adalah RSA, diimplementasikan melalui ekstensi OpenSSL bawaan PHP, bukan pustaka pihak ketiga, karena ekstensi ini telah teruji pada sistem berskala produksi dan terintegrasi langsung dengan framework Laravel. Pasangan kunci RSA dibangkitkan oleh Admin melalui fungsi openssl_pkey_new() dengan panjang kunci 2048 bit, sesuai standar minimum yang direkomendasikan untuk menjamin keamanan sekaligus menjaga beban komputasi yang wajar. Kunci privat dienkripsi menggunakan fasilitas Crypt bawaan Laravel sebelum disimpan ke basis data, sedangkan kunci publik disimpan dalam bentuk teks biasa. Setiap akun penanda tangan yang berwenang, baik Kepala Sekolah, Wakil Kepala Sekolah, Waka Kurikulum, Kepala Jurusan, Wali Kelas, maupun Guru Mata Pelajaran, memiliki pasangan kunci RSA tersendiri sehingga setiap tanda tangan digital dapat ditelusuri hingga pemilik akun yang bersangkutan.

Proses penandatanganan dokumen diawali dengan pembangkitan nilai ringkasan pesan (message digest) dari isi dokumen menggunakan fungsi hash satu arah SHA-256, yang dipilih karena memiliki sifat collision resistance tinggi sehingga perubahan sekecil apa pun pada dokumen menghasilkan nilai hash yang jauh berbeda. Nilai hash tersebut selanjutnya dienkripsi menggunakan kunci privat penanda tangan melalui fungsi openssl_sign() dengan algoritma OPENSSL_ALGO_SHA256, menghasilkan tanda tangan digital yang di-encode ke format base64. Secara matematis, proses ini dapat dinyatakan sebagai s = H(m)^d mod n, dengan H(m) adalah nilai hash dokumen m, serta d dan n merupakan bagian dari kunci privat. Pada proses verifikasi, sistem

menghitung ulang nilai hash dokumen yang diterima, mendekripsi tanda tangan digital menggunakan fungsi openssl_verify() dengan kunci publik penanda tangan, lalu membandingkan kedua nilai hash tersebut; dokumen dinyatakan valid apabila kedua nilai identik, dan tidak valid apabila berbeda. Setiap dokumen yang telah ditandatangani dilengkapi QR Code yang dibangkitkan sebelum proses hashing, berisi tautan menuju halaman verifikasi publik sehingga pihak eksternal seperti industri dan perguruan tinggi dapat memeriksa keaslian dokumen secara daring tanpa perlu login maupun mendatangi sekolah secara langsung.

Metode Pengujian

Pengujian fungsional sistem dilakukan menggunakan metode Black-box Testing, yaitu metode pengujian yang berfokus pada verifikasi keluaran (output) sistem terhadap suatu masukan (input) tertentu tanpa memeriksa struktur kode program secara internal. Pengujian dilakukan terhadap 14 skenario pengujian yang mencakup proses autentikasi, pengelolaan dokumen dan pengguna, pembangkitan serta verifikasi digital signature berbasis algoritma RSA, hingga verifikasi dokumen secara publik melalui QR Code. Selain pengujian fungsional, dilakukan pula pengujian kelayakan (usability testing) menggunakan kuisioner Skala Likert dengan lima alternatif jawaban, yaitu Sangat Setuju (skor 5), Setuju (skor 4), Netral (skor 3), Tidak Setuju (skor 2), dan Sangat Tidak Setuju (skor 1), yang melibatkan 6 responden terdiri dari siswa, Admin, Kepala Sekolah, dan Wali Kelas/Guru Mata Pelajaran. Persentase kelayakan dihitung dengan membandingkan skor total yang diperoleh terhadap skor maksimal yang mungkin dicapai, dikalikan 100%.

HASIL DAN PEMBAHASAN

Mekanisme digital signature berhasil diimplementasikan pada sistem yang diberi nama e-MDADS (Elektronik Manajemen Dokumen Akademik Digital Sekolah), yang dibangun menggunakan framework Laravel, bahasa pemrograman PHP, basis data MySQL, serta Tailwind CSS. Setiap dokumen akademik yang diinput ke dalam sistem, baik yang diterbitkan langsung oleh sistem (seperti Rekap Nilai) maupun hasil unggahan pemindaian dokumen fisik yang dilegalisasi (seperti Ijazah dan Sertifikat Kompetensi), melalui proses hashing SHA-256 kemudian ditandatangani secara digital menggunakan kunci privat RSA-2048 milik penanda tangan yang berwenang. Untuk dokumen jenis kedua, digital signature berfungsi sebagai legalisasi digital, yaitu pengesahan bahwa salinan hasil pemindaian telah diverifikasi kesesuaiannya dengan dokumen fisik asli, bukan menggantikan tanda tangan asli yang telah ada sebelumnya. Hasil akhir berupa dokumen yang dilengkapi QR Code unik yang terhubung ke halaman verifikasi publik.

Pengujian Black-box Testing dilakukan untuk memastikan setiap fungsi sistem berjalan sesuai dengan kebutuhan fungsional yang telah dirancang. Ringkasan hasil pengujian terhadap 14 skenario pengujian ditampilkan pada Tabel 1 berikut.

Tabel 1. Ringkasan Hasil Pengujian Black-box Testing

No	Fokus Pengujian	Jumlah Skenario	Status
1	Autentikasi, manajemen pengguna, dan manajemen dokumen	11	Berhasil sesuai harapan
2	Pemindaian QR Code pada dokumen (skenario 7 dan 8)	2	Berhasil sebagian, perlu pengujian lanjutan
3	Penolakan dokumen yang telah dimodifikasi (skenario 11)	1	Belum diuji

Dari 14 skenario pengujian, 11 skenario (sekitar 78,6%) berjalan sesuai harapan, mencakup fungsi autentikasi, pengelolaan akun pengguna dan data siswa, pengelolaan dokumen akademik, pembangkitan kunci RSA, serta akses dokumen oleh siswa. Dua skenario yang berkaitan dengan pemindaian QR Code berhasil sebagian dan memerlukan pengujian lebih lanjut menggunakan aplikasi pembaca QR Code yang berbeda, sedangkan satu skenario terkait penolakan dokumen yang telah dimodifikasi belum sempat diuji. Hasil ini menunjukkan bahwa mekanisme inti digital signature, yaitu pembangkitan kunci, penandatanganan, dan perhitungan hash, telah berfungsi sebagaimana mestinya, sementara aspek pendukung berupa pemindaian QR Code pada berbagai perangkat masih memerlukan validasi tambahan sebelum sistem diterapkan secara produksi.

Pengujian kelayakan (usability testing) dilakukan terhadap 6 responden yang terdiri dari 3 siswa, 1 Admin, 1 Kepala Sekolah, dan 1 Wali Kelas/Guru Mata Pelajaran, menggunakan 10 pernyataan kuisioner yang mencakup kemudahan penggunaan, tanda tangan digital, QR Code dan verifikasi, notifikasi, legalisasi dokumen, kerahasiaan identitas, efisiensi, dan kepuasan keseluruhan. Skor maksimal keseluruhan adalah 5 × 10 pernyataan × 6 responden = 300. Total skor yang diperoleh adalah 232, sehingga persentase kelayakan keseluruhan sebesar 77,33% dan termasuk kategori layak. Persentase tertinggi (80,00%) diperoleh pada pernyataan terkait portal verifikasi publik, sistem notifikasi, legalisasi dokumen hasil pemindaian, dan percepatan pengelolaan dokumen akademik, sedangkan persentase terendah (70,00%) diperoleh pada pernyataan mengenai kemudahan QR Code dalam memverifikasi keaslian dokumen, yang selaras dengan hasil Black-box Testing pada dua skenario pemindaian QR Code yang masih memerlukan pengujian ulang.

Secara keseluruhan, hasil implementasi dan pengujian menunjukkan bahwa mekanisme digital signature berbasis algoritma RSA-2048 bit dan fungsi hash SHA-256 mampu menjamin tiga aspek utama keamanan dokumen akademik, yaitu autentikasi, integritas, dan non-repudiation, secara matematis tanpa memerlukan kehadiran fisik penanda tangan. Penerapan QR Code sebagai media verifikasi terbukti memudahkan pihak eksternal memeriksa keaslian dokumen secara daring, sekaligus menjaga kerahasiaan dokumen karena nilai hash dan data pribadi tidak ditampilkan secara eksplisit pada halaman verifikasi publik. Meskipun demikian, hasil pengujian black-box dan kuisioner sama-sama mengindikasikan bahwa mekanisme pemindaian QR Code pada dokumen hasil legalisasi masih memerlukan pengujian lanjutan menggunakan berbagai aplikasi pembaca QR Code dan perangkat yang berbeda, serta pengujian skenario dokumen yang dimodifikasi untuk memastikan sistem secara konsisten menolak dokumen yang tidak sah.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah diuraikan, mekanisme digital signature berbasis algoritma RSA dengan panjang kunci 2048 bit dan fungsi hash SHA-256 berhasil diterapkan pada aplikasi manajemen dokumen akademik siswa berbasis web, baik untuk dokumen yang diterbitkan langsung oleh sistem maupun dokumen hasil unggahan fotokopi yang dilegalisasi secara digital. Sistem mampu membangkitkan QR Code secara otomatis sebagai media verifikasi yang terhubung ke halaman verifikasi publik, memungkinkan pihak eksternal memeriksa keaslian dokumen tanpa login maupun mendatangi sekolah secara langsung, sekaligus menjaga kerahasiaan identitas pemilik dokumen. Hasil pengujian Black-box Testing menunjukkan 11 dari 14 skenario fungsional berjalan sesuai harapan, sedangkan hasil pengujian kelayakan terhadap 6 responden menghasilkan persentase kelayakan sebesar 77,33% dengan kategori layak. Pengembangan selanjutnya disarankan untuk melakukan pengujian lanjutan terhadap mekanisme pemindaian QR Code pada berbagai perangkat dan aplikasi pembaca, serta pengujian skenario dokumen yang dimodifikasi guna memastikan konsistensi penolakan dokumen yang tidak sah oleh sistem.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing atas bimbingan yang diberikan selama penelitian ini berlangsung, serta kepada kepala sekolah, guru, dan staf SMK Negeri 1 Lembah Melintang atas izin dan dukungan yang diberikan selama proses pengambilan data dan pengujian sistem.

REFERENCES

Kadir, A. (2014). Pengenalan sistem informasi. Yogyakarta: CV Andi Offset.

Connolly, T., & Begg, C. (2015). Database systems: A practical approach to design, implementation, and management (6th ed.). Pearson.

ISO/IEC 27001. (2013). Information technology — Security techniques — Information security management systems requirements. Geneva: ISO/IEC.

Laudon, K. C., & Laudon, J. P. (2018). Management information systems: Managing the digital firm (Global ed.). Pearson.

Lubis, B. O., dkk. (2021). Sistem informasi pengelolaan sertifikasi kompetensi online pada SMK dengan metode web base engineering. Journal of Information System, Informatics and Computing, 5(2).

Pressman, R. S., & Maxim, B. (2015). Software engineering: A practitioner's approach (8th ed.). New York: McGraw-Hill Education.

Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.). John Wiley & Sons.

Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson Education.

Sugiyono. (2013). Metode penelitian pendidikan: Pendekatan kuantitatif, kualitatif, dan R&D. Bandung: Alfabeta.