HALAMAN MOTTO

"Berinfaklah di jalan Allah, janganlah jerumuskan dirimu ke dalam kebinasaan, dan berbuat baiklah. Sesungguhnya Allah menyukai orang-orang yang berbuat baik."

Q.S Al Baqarah: 195

"Kesuksesan tidak hanya tentang tujuan, tetapi prosesnya."

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas segala karunia-Nya. Sebagai penanda dari sebuah perjuangan dan langkah awal menuju masa depan, skripsi ini penulis persembahkan sebagai ungkapan rasa syukur dan terima kasih yang mendalam kepada:

1. Allah SWT, Tuhan Yang Maha Esa, atas segala limpahan rahmat, kekuatan, dan kemudahan sehingga skripsi ini dapat terselesaikan.
2. Orang tua tercinta, Ibu dan Bapak. Terima kasih atas ketulusan doa, kasih sayang tiada batas, serta keringat dan kerja keras demi masa depan penulis. Tanpa pengorbanan kalian, penulis tidak akan mampu berdiri di titik ini.
3. Bapak Ir. Rohmatulloh Muhamad Ikhsanuddin, S.Kom, M.Cs., selaku dosen pembimbing. Terima kasih atas kesabaran, waktu, dedikasi, dan ilmu yang senantiasa diberikan selama proses bimbingan.
4. Diri penulis sendiri, terima kasih telah bertahan, berjuang, dan pantang menyerah menyelesaikan tanggung jawab ini. Semoga ini menjadi langkah awal menuju kesuksesan.
5. Adik tercinta, Nabilah Zahra, atas semangat, keceriaan, dan dukungan yang selalu menjadi penawar lelah bagi penulis.

Semoga karya ini menjadi awal dari keberkahan dan manfaat di masa depan.

ABSTRAK

Keamanan dan keaslian dokumen elektronik, khususnya e-sertifikat Praktik Kerja Lapangan (PKL) dan magang, telah menjadi kebutuhan yang sangat krusial bagi berbagai instansi pendidikan maupun dunia industri. Pada studi kasus di Cazh Academy, sistem verifikasi dokumen yang berjalan saat ini umumnya hanya memvalidasi kode QR secara visual berdasarkan tautan *database* tanpa melakukan pengujian terhadap integritas konten di dalam file dokumen itu sendiri. Celah keamanan ini menjadikan e-sertifikat dengan format PDF sangat rentan terhadap tindak pemalsuan dan manipulasi data oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penelitian ini bertujuan untuk merancang dan membangun sebuah sistem verifikasi e-sertifikat yang aman, akurat, dan tangguh dengan mengintegrasikan fungsi *hash* SHA3-512 dan algoritma kriptografi kunci asimetris RSA (*Rivest-Shamir-Adleman*) 2048-bit. Penelitian ini menggunakan metode *Research and Development* (R&D) yang dipadukan secara komprehensif dengan metode pengembangan sistem perangkat lunak *Waterfall*, meliputi tahapan analisis kebutuhan, perancangan antarmuka, implementasi, hingga pengujian. Sistem ini membagi peran pengguna menjadi pembimbing dan verifikator. Algoritma SHA3-512 digunakan untuk mengekstraksi *message digest* dari dokumen guna menjamin integritas data (*Data Integrity*), sedangkan RSA-2048 diimplementasikan untuk melakukan enkripsi tanda tangan digital (*Digital Signature*) guna memastikan autentikasi identitas penerbit (*Authentication*). Berdasarkan serangkaian evaluasi yang telah dilakukan, hasil pengujian fungsionalitas menggunakan metode *Black Box* menunjukkan bahwa seluruh fitur operasional sistem berbasis web berjalan dengan valid sebesar 100%. Lebih lanjut, pengujian keamanan menggunakan *Avalanche Effect* membuktikan bahwa algoritma kriptografi yang diterapkan memiliki tingkat sensitivitas sangat tinggi dengan persentase perubahan mencapai 51,56% saat terjadi modifikasi satu parameter nilai pada dokumen. Pengujian efisiensi komputasi juga menunjukkan waktu eksekusi kriptografi rata-rata 0,21634 detik, yang mengonfirmasi bahwa integrasi sistem ini tidak membebani kinerja server. Implementasi ini terbukti mampu menutupi celah keamanan pada sistem validasi konvensional sekaligus memberikan jaminan keaslian yang mutlak.

Kata Kunci: R&D, E-Sertifikat, Kriptografi, RSA, SHA3-512, *Waterfall*

ABSTRACT

The security and authenticity of electronic documents, particularly Field Work Practice (PKL) and internship e-certificates, have become a crucial need for various educational institutions and industries. In a case study at Cazh Academy, the current document verification system generally only validates QR codes visually based on database links without testing the content integrity within the document file itself. This security flaw makes PDF-formatted e-certificates highly vulnerable to forgery and data manipulation by irresponsible parties. Therefore, this study aims to design and build a secure, accurate, and robust e-certificate verification system by integrating the SHA3-512 hash function and the 2048-bit RSA (Rivest-Shamir-Adleman) asymmetric key cryptography algorithm. This research uses the Research and Development (R&D) method comprehensively combined with the Waterfall software development method, covering the stages of requirement analysis, interface design, implementation, and testing. This system divides user roles into supervisors and verifiers. The SHA3-512 algorithm is used to extract the message digest from the document to guarantee Data Integrity, while RSA-2048 is implemented to encrypt the Digital Signature to ensure the publisher's Authentication. Based on a series of evaluations conducted, the functionality testing results using the Black Box method show that all operational features of the web-based system are 100% valid. Furthermore, security testing using the Avalanche Effect proves that the applied cryptographic algorithm has a very high level of sensitivity, with the percentage of change reaching 51.56% when a single value parameter in the document is modified. Computational efficiency testing also shows an average cryptographic execution time of 0.21634 seconds, confirming that the integration of this system does not overburden server performance. This implementation is proven to be able to cover security vulnerabilities in conventional validation systems while providing absolute trustworthiness.

Keywords: R&D, E-Certificate, Cryptography, RSA, SHA3-512, Waterfall

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT, karena atas rahmat, hidayah, serta karunia-Nya, penulis dapat menyelesaikan penyusunan skripsi yang berjudul "*Rancang Bangun Sistem Verifikasi E-Sertifikat Menggunakan Tanda Tangan Digital RSA dan SHA3-512 Berbasis Web (Studi Kasus: Cazh Academy)*" dengan baik dan tepat pada waktunya.

Penyusunan skripsi ini ditujukan sebagai syarat akademik guna memperoleh gelar Sarjana Strata-1 pada Program Studi Ilmu Komputer, Universitas Putra Bangsa. Secara garis besar, skripsi ini membahas tentang perancangan dan pengembangan sistem keamanan dokumen digital untuk memitigasi risiko manipulasi data pada e-sertifikat, dengan mengimplementasikan kombinasi algoritma kriptografi RSA-2048 sebagai tanda tangan digital dan SHA3-512 sebagai mekanisme integritas data.

Dalam proses penyelesaian skripsi ini, penulis mendapatkan banyak bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Dr. Gunarso Wiwono, S.E., M.M., selaku Rektor Universitas Putra Bangsa.
2. Bapak Awaludin Abid, S.Kom, M.Kom., selaku Ketua Program Studi Ilmu Komputer Universitas Putra Bangsa.
3. Bapak Ir. Rohmatulloh Muhamad Ikhsanuddin, S.Kom, M.Cs., selaku Dosen Pembimbing yang telah memberikan arahan, ilmu, serta motivasi yang tak ternilai selama proses penelitian.

4. Bapak Supriyanto selaku Service Manager dan Pembimbing Magang di Cazh Academy yang telah memberikan izin, dukungan, serta kemudahan akses data selama proses penelitian berlangsung.
5. Kedua orang tua tercinta, Ibu dan Bapak, atas segala pengorbanan, dukungan moral, serta doa yang tiada henti.
6. Serta seluruh rekan-rekan mahasiswa Ilmu Komputer dan pihak-pihak lain yang tidak dapat penulis sebutkan satu per satu yang telah membantu hingga skripsi ini terselesaikan.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan kritik serta saran yang membangun demi perbaikan di masa depan. Akhir kata, penulis berharap semoga hasil penelitian ini dapat memberikan kontribusi manfaat bagi pengembangan ilmu pengetahuan serta menjadi referensi yang berguna bagi penelitian selanjutnya.

Kebumen, 6 Agustus 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN