

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 Cahz 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 Czh 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: Cazz 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 Cazzh 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

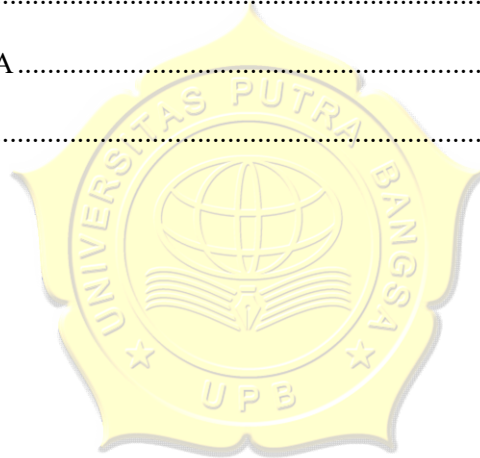
DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN UJIAN	iii
HALAMAN BEBAS PLAGIARISME	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
ABSTRAK.....	vii
ABSTRACT.....	viii
KATA PENGANTAR.....	ix
DAFTAR ISI	xi
DAFTAR TABEL.....	xv
DAFTAR GAMBAR	xvi
DAFTAR LAMPIRAN	xixi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	6
1.3 Batasan Masalah.....	6
1.4 Tujuan Penelitian.....	8
1.5 Manfaat Penelitian	8
BAB II KAJIAN PUSTAKA	10
2.1 Landasan Teori	10

2.1.1	Kriptografi.....	10
2.1.2	Keamanan Informasi	14
2.1.3	E-Sertifikat	15
2.1.4	Tanda Tangan Digital	15
2.1.5	Website.....	16
2.1.6	<i>Framework</i>	16
2.1.7	Metode Pengembangan Sistem	17
2.1.8	Pengujian Sistem.....	18
2.1.9	<i>Avalanche Effect</i>	19
2.2	Hasil Penelitian Terdahulu	21
2.3	Kerangka Pemikiran.....	24
2.4	Keaslian Penelitian.....	26
BAB III METODOLOGI PENELITIAN.....		28
3.1	Tahapan Penelitian	28
3.2	Objek dan Subjek Penelitian.....	31
3.2.1	Objek Penelitian.....	31
3.2.2	Subjek Penelitian.....	32
3.3	Metode Penelitian.....	33
3.3.1	Pendekatan Penelitian	33
3.3.2	Metode Pengembangan Sistem	33
3.4	Metode Pengumpulan Data	36
3.5	Perancangan Sistem	37
3.5.1	Analisis Kebutuhan Sistem	38

3.5.2	<i>Use case Diagram</i>	46
3.5.3	<i>Flowchart Sistem</i>	40
3.5.4	<i>Activity Diagram</i>	51
3.5.5	<i>Data Flow Diagram</i>	47
3.5.6	<i>Entity Relationship Diagram</i>	50
3.5.7	<i>Perancangan Database</i>	57
3.5.8	<i>Wireframe</i>	62
3.6	<i>Alat dan Bahan</i>	71
3.6.1	<i>Perangkat Keras</i>	71
3.6.2	<i>Perangkat Lunak</i>	72
3.6.3	<i>Bahan Penelitian</i>	72
3.7	<i>Prosedur Pengujian</i>	73
BAB IV HASIL DAN PEMBAHASAN.....		74
4.1	<i>Implementasi Perancangan</i>	74
4.1.1	<i>Fitur Autentikasi Pengguna</i>	74
4.1.2	<i>Fitur Pemulihan Kata Sandi</i>	77
4.1.3	<i>Fitur Dashboard</i>	79
4.1.4	<i>Fitur Tambah Sertifikat</i>	82
4.1.5	<i>Fitur Riwayat Sertifikat</i>	86
4.1.8	<i>Fitur Manajemen Kunci Kriptografi</i>	89
4.1.9	<i>Fitur Verifikasi Keaslian Dokumen</i>	91
4.2	<i>Hasil Pengujian</i>	94
4.2.1	<i>Black Box Testing</i>	95

4.2.2	Hasil Pengujian <i>Avalanche Effect</i>	114
4.3	Pembahasan.....	117
4.3.1	Analisis Keamanan Berdasarkan CIA Triad	118
4.3.2	Perbandingan dengan Penelitian Terdahulu	119
4.3.3	Pemeliharaan dan Perbaikan Sistem	121
4.3.4	Keterbatasan Sistem.....	123
BAB V PENUTUP.....		124
5.1	Kesimpulan	124
5.2	Saran.....	125
DAFTAR PUSTAKA		127
LAMPIRAN.....		132



DAFTAR TABEL

Tabel II-1 Penelitian Terdahulu.....	22
Tabel III-1 Kebutuhan Fungsional	38
Tabel III-2 Kebutuhan Non-Fungsional	40
Tabel III-3 Users	58
Tabel III-4 Participants.....	59
Tabel III-5 Rsa_keys	60
Tabel III-6 Certificates	61
Tabel IV-1 Pengujian Fitur Autentikasi Pengguna.....	95
Tabel IV-2 Pengujian Fitur Pemulihan Kata Sandi	97
Tabel IV-3 Pengujian Fitur Dashboard.....	100
Tabel IV-4 Pengujian Fitur Tambah Sertifikat	102
Tabel IV-5 Pengujian Fitur Riwayat Sertifikat.....	105
Tabel IV-6 Pengujian Fitur Manajemen Kunci Kriptografi	108
Tabel IV-7 Pengujian Fitur Verifikasi Internal	110
Tabel IV-8 Pengujian Fitur Verifikasi Publik	113
Tabel IV-9 Pengujian Avalanche Effect	115

DAFTAR GAMBAR

Gambar II-1 Skema Algoritma RSA	12
Gambar II-2 Fungsi <i>Hash Keccak</i> SHA3-512	14
Gambar II-3 Kerangka Pemikiran.....	26
Gambar III-1 Tahapan Penelitian	28
Gambar III-2 Metode <i>Waterfall</i>	36
Gambar III-3 <i>Flowchart</i> Autentikasi.....	41
Gambar III-4 <i>Flowchart</i> Menerbitkan Sertifikat.....	42
Gambar III-5 <i>Flowchart</i> Pengelolaan E-Sertifikat.....	43
Gambar III-6 <i>Flowchart</i> Pembangkitan Kunci	44
Gambar III-7 <i>Flowchart</i> Verifikasi	45
Gambar III-8 <i>Use Case Diagram</i>	46
Gambar III-9 DFD Level 0	48
Gambar III-10 DFD Level 1	49
Gambar III-11 ERD.....	50
Gambar III-12 <i>Activity Diagram</i> Login.....	52
Gambar III-13 <i>Activity Diagram</i> Menerbitkan E-Sertifikat.....	53
Gambar III-14 <i>Activity Diagram</i> Pengelolaan Riwayat E-Sertifikat	54
Gambar III-15 <i>Activity Diagram</i> Manajemen Kunci Kriptografi	55
Gambar III-16 <i>Activity Diagram</i> Verifikasi	56
Gambar III-17 <i>Wireframe</i> Fitur Autentikasi Pengguna	63
Gambar III-18 <i>Wireframe</i> Permintaan Tautan.....	64
Gambar III-19 <i>Wireframe</i> Pembaruan Kata Sandi	64

Gambar III-20 Wireframe Fitur <i>Dashboard</i>	65
Gambar III-21 Wireframe Fitur Tambah Sertifikat	66
Gambar III-22 Wireframe Fitur Riwayat Sertifikat	67
Gambar III-23 <i>Wireframe</i> Fitur Manajemen Kriptografi	68
Gambar III-24 <i>Wireframe</i> Fitur Verifikasi Internal	70
Gambar III-25 <i>Wireframe</i> Fitur Verifikasi Publik	71
Gambar IV-1 Antarmuka Autentikasi Pengguna	75
Gambar IV-2 Implementasi Kode Autentikasi Pengguna	76
Gambar IV-3 Antarmuka Permintaan Tautan	77
Gambar IV-4 Antarmuka Pembaruan Kata Sandi	78
Gambar IV-5 Implementasi Kode Permintaan Tautan	79
Gambar IV-6 Implementasi Kode Pembaruan Kata Sandi.....	79
Gambar IV-7 Antarmuka Fitur <i>Dashboard</i>	80
Gambar IV-8 Implementasi Kode <i>Dashboard</i>	81
Gambar IV-9 Antarmuka Tambah Sertifikat	82
Gambar IV-10 Implementasi Kode Tambah Sertifikat.....	84
Gambar IV-11 Antarmuka Konfirmasi Sukses.....	85
Gambar IV-12 Antarmuka Riwayat Sertifikat.....	86
Gambar IV-13 Implementasi Kode Riwayat dan Filter	88
Gambar IV-14 Antarmuka Manajemen Kunci Kriptografi	89
Gambar IV-15 Implementasi Kode Manajemen Kunci.....	90
Gambar IV-16 Antarmuka Verifikasi Internal	92
Gambar IV-17 Antarmuka Verifikasi Publik	92

Gambar IV-18 Implementasi Kode Validasi Token.....	93
Gambar IV-19 Implementasi Kriptografi RSA dan <i>Hash</i> SHA3-512.....	94
Gambar IV-20 Eksekusi Perhitungan menggunakan Laravel Tinker.....	117



DAFTAR LAMPIRAN

Lampiran I. Kartu Bimbingan	133
Lampiran II. Kartu Seminar Proposal	134
Lampiran III. Surat Permohonan Izin Penelitian	135
Lampiran IV. Wawancara	136
Lampiran V. <i>AuthController.php</i>	138
Lampiran VI. <i>DashboardController.php</i>	140
Lampiran VII. <i>PasswordResetController.php</i>	143
Lampiran VIII. <i>SertifikatController.php</i>	146
Lampiran IX. <i>VerifikasiController.php</i>	154

