BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang pesat mengubah kebiasaan manusia dalam berkegiatan. Transformasi digital mendorong perubahan dari proses konvensional menjadi otomatis, di mana kemudahan dan kecepatan menjadi alasan utama digitalisasi dokumen. Dokumen fisik saat ini telah bertransformasi menjadi dokumen digital, dan tanda tangan basah beralih menjadi tanda tangan digital untuk mengatasi batasan jarak dan waktu. Keamanan dari tanda tangan digital menjadi tantangan baru untuk menjaga integritas pesan dan meyakini bahwa tanda tangan yang dibubuhkan merupakan tanda tangan asli dari pengirim (Nurjaman, 2024).

Peningkatan penggunaan dokumen digital di organisasi memerlukan metode validasi yang efisien. Metode konvensional yang mengharuskan pencetakan dokumen untuk tanda tangan basah dianggap tidak efektif dari segi waktu. Alternatif menggunakan citra tanda tangan hasil pindai (*scan*) memiliki risiko keamanan tinggi (Gunawan et al., 2024). Penelitian oleh R. Kurniawan et all. (2020) yang menyoroti risiko keamanan dokumen yang telah dibubuhi tanda tangan sehingga sangat rentan dipalsukan. Celah ini memungkinkan pihak yang tidak bertanggung jawab untuk mengambil citra tanda tangan tersebut dan menggunakannya kembali pada dokumen lain yang tidak sah. Solusi preventif, penggunaan *Quick Response* (QR) diterapkan

untuk menggantikan fungsi tanda tangan konvensional, di mana data identitas surat di dalam *QR Code* dilindungi menggunakan teknik kriptografi agar sulit dimanipulasi.

Permasalahan keamanan dokumen ini sangat relevan pada Cazh Academy, yang merupakan sebuah unit bisnis yang dikembangkan dari program magang di PT Cazh Teknologi Inovasi sejak 2021. Awalnya kegiatan magang yang dilakukan oleh pelajar dan mahasiswa di PT Cazh Teknologi Inovasi tidak dikelola oleh unit apapun, karena keterbatasan personil dan divisi. Namun sejak 2023, Cazh Academy digagas sebagai sebuah wadah unit bisnis baru yang mengelola kegiatan magang, sekaligus menjadi inkubator karya-karya pilot project aplikasi berbasis *web* dan *mobile* yang potensial dikembangkan dan dipasarkan, serta berperan sebagai lembaga yang menerbitkan dokumen digital penting berupa e-sertifikat, seperti sertifikat PKL/Magang. Hingga tahun 2026, Cazh Academy telah menerbitkan lebih dari 300 e-sertifikat kepada peserta PKL/Magang, sehingga keamanan dan keaslian dokumen digital menjadi aspek yang sangat penting untuk dijaga. Cazh Academy saat ini telah menerapkan fitur verifikasi menggunakan *QR Code* yang tertera pada e-sertifikat. Sistem yang berjalan memungkinkan pengguna memindai *QR Code* untuk diarahkan ke tautan data di server. Namun, sistem yang ada saat ini hanya memvalidasi keberadaan data ID di *database* dan belum memiliki fitur validasi terhadap integritas file dokumen itu sendiri.

Kelemahan sistem yang berjalan tersebut adalah belum adanya fitur untuk mengunggah (*upload*) file guna pengecekan konten. Format dokumen PDF tedapat celah keamanan yang serius karena sangat rentan terhadap manipulasi. Penelitian oleh Afandi et al. (2024), isi dokumen PDF dapat dimodifikasi dengan mudah menggunakan perangkat lunak gratis. Artinya, jika seseorang merubah nilai pada file sertifikatnya tetapi membiarkan *QR Code*-nya utuh, sistem yang hanya melakukan validasi berdasarkan data ID tanpa pengecekan integritas file akan tetap menampilkannya sebagai data yang valid saat dipindai, sehingga dapat mengecoh verifikator. Kondisi ini berpotensi merugikan perusahaan penerima kerja dan mencoreng kredibilitas Cazh Academy. Perlunya pengembangan sistem yang mampu memvalidasi integritas file secara matematis.

Sistem keamanan dokumen digital memerlukan mekanisme yang mampu menjamin keaslian, keutuhan, serta mencegah terjadinya manipulasi data oleh pihak yang tidak berwenang. Hal ini sejalan dengan penelitian A. R. Harahap & Salim (2023) yang menyatakan bahwa sistem kriptografi berperan dalam menjaga keaslian, kerahasiaan, dan keamanan dokumen elektronik. Penelitian (Nurjaman (2024) mengindikasikan bahwa penggunaan algoritma RSA (Rivest-Shamir-Adleman) secara tunggal belum memadai untuk menjamin dokumen bebas dari modifikasi, sehingga mutlak diperlukan integrasi dengan fungsi *hash* yang andal. Studi tersebut membuktikan bahwa kombinasi RSA dan SHA3-512 efektif dalam memvalidasi keaslian dokumen PDF serta memitigasi serangan manipulasi.

SHA3-512 merupakan salah satu varian dari keluarga algoritma SHA-3 yang distandarisasi oleh NIST, yang terdiri atas beberapa fungsi *hash* dengan panjang keluaran berbeda, yaitu SHA3-224, SHA3-256, SHA3-384, dan SHA3-512 (NIST, 2015). Oleh karena itu, penelitian ini mengadopsi varian SHA3-512 yang berbasis struktur *Keccak* dengan mekanisme *sponge construction*, yaitu arsitektur yang dirancang untuk menghasilkan fungsi *hash* dengan tingkat ketahanan integritas yang lebih tinggi dibandingkan algoritma *hash* generasi sebelumnya.

Pemilihan algoritma RSA dalam penelitian ini didasarkan juga pada karakteristik asimetrisnya yang unggul dalam mekanisme autentikasi. Penelitian oleh Depo Sadrila Hadi et al. (2025) menegaskan bahwa meskipun algoritma simetris seperti AES lebih unggul dalam kecepatan enkripsi data massal, algoritma RSA tetap memegang peranan krusial dan tak tergantikan dalam implementasi tanda tangan digital. Algoritma RSA menyediakan mekanisme kunci publik yang memungkinkan verifikasi integritas dan autentikasi dokumen dilakukan secara terbuka tanpa mengorbankan keamanan kunci privat pemilik tanda tangan, sebuah fitur yang tidak dimiliki oleh skema enkripsi simetris biasa.

Beberapa penelitian terdahulu yang menjadi landasan implementasi sistem berbasis *website* ini antara lain dilakukan oleh Syahfira Chairunnisa Lubis, Khairi Ibnutama, (2022) dengan judul "Implementasi *Digital Signature* Pada Faktur Dengan Menggunakan Kombinasi Algoritma SHA-256 Dan RSA-CRT". Penelitian ini berhasil menerapkan tanda tangan digital

untuk mencegah manipulasi data transaksi pada dokumen bisnis sehingga integritasnya tetap terjaga.

Selanjutnya, pengembangan pada sektor pendidikan dilakukan oleh Ajif et al. (2025) melalui penelitian berjudul "Implementasi Modul Tanda Tangan Digital dengan Superenkripsi RSA-ECDSA dan SHA-512 Pada Sistem Informasi Akademik Sekolah". Studi ini sukses membangun modul verifikasi nilai siswa pada sistem berbasis web, yang membuktikan bahwa platform web efektif digunakan untuk distribusi dokumen akademik yang aman.

Djuandadesta et al. (2025) dalam penelitiannya yang berjudul "Autentikasi Dokumen Digital Pada *Cloud* Menggunakan Algoritma *Hashing* BLAKE2 dan RSA", menyimpulkan bahwa integrasi algoritma kriptografi pada penyimpanan berbasis *cloud* mampu menjamin autentikasi dokumen digital secara *real-time* dan efisien. Ketiga penelitian tersebut mempertegas bahwa implementasi metode kriptografi pada platform berbasis web memberikan keunggulan dalam hal aksesibilitas dan verifikasi data yang lebih praktis.

Keberhasilan implementasi berbasis web dalam penelitian-penelitian tersebut, penelitian ini difokuskan untuk mengatasi permasalahan autentikasi dokumen di Cazh Academy yang saat ini masih rentan terhadap risiko pemalsuan dan inefisiensi akibat proses manual. Integrasi keandalan algoritma RSA untuk tanda tangan digital dan SHA3-512 untuk integritas data ke dalam sebuah platform *website*, diharapkan sistem ini dapat memberikan solusi verifikasi dokumen yang aman, akurat, dan mudah diakses secara *real-*

time. Berdasarkan latar belakang permasalahan dan solusi teknis yang telah dipaparkan, maka penelitian ini mengambil judul: '*Rancang Bangun Sistem Verifikasi E-Sertifikat Menggunakan Tanda Tangan Digital RSA dan SHA3-512 Berbasis Web (Studi Kasus: Cazh Academy)'*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang dan membangun sistem verifikasi e-sertifikat berbasis *website* yang dapat mengatasi kelemahan validasi visual pada sistem *QR Code* yang sudah berjalan di Cazh Academy?
2. Bagaimana mengimplementasikan kombinasi algoritma kriptografi RSA dan SHA3-512 guna mendeteksi modifikasi pada isi file sertifikat elektronik?
3. Bagaimana hasil pengujian fungsionalitas sistem menggunakan *Black Box Testing* serta analisis tingkat sensitivitas algoritma menggunakan *Avalanche Effect* dalam mendeteksi manipulasi pada e-sertifikat?

1.3 Batasan Masalah

Agar pembahasan dalam penelitian ini lebih terarah dan fokus, maka penulis menetapkan batasan masalah sebagai berikut:

1. Objek e-sertifikat yang diteliti Adalah sertifikat PKL/Magang yang diterbitkan oleh Cazh Academy dalam format digital (PDF).

2. Proses pengamanan menggunakan fungsi *hash* SHA-3 512-bit untuk integritas data dan algoritma RSA 2048-bit untuk tanda tangan digital.
3. Proses Verifikasi keaslian dokumen berbasis web dilakukan melalui dua metode, yaitu pemindaian *QR Code* dan pengunggahan (*upload*) file PDF.
4. Penelitian ini tidak membahas Pembangunan Infrastruktur Kunci (PKI) yang kompleks atau melibatkan Otoritas Sertifikat (CA) eksternal. Manajemen kunci publik dan privat dilakukan secara internal pada *server* aplikasi.
5. Aplikasi dibangun berbasis web (menggunakan *Framework* Laravel/PHP) dan ditujukan untuk penggunaan oleh Pembimbing (penerbit e-sertifikat) dan Publik/Verifikator (pengguna umum).
6. Sistem verifikasi e-sertifikat yang dibangun dalam penelitian ini bersifat *Proof of Concept* (PoC) yang berfokus pada pembuktian fungsionalitas dan keamanan algoritma SHA3-512 serta RSA. Sistem ini berdiri sendiri (*standalone*) dan tidak terintegrasi secara langsung dengan Sistem Informasi Manajemen (SIM) utama milik Cazh Academy.
7. Fokus utama sistem hanya pada tahapan *generate* (pembuatan) dokumen PDF otomatis berdasarkan input nilai serta penerapan kriptografinya. Oleh karena itu, sistem tidak mencakup modul administrasi operasional magang (seperti pendaftaran peserta,

approval kegiatan, dan pengisian jurnal harian). Data peserta magang yang digunakan dalam sistem diasumsikan telah valid dan direpresentasikan menggunakan data *dummy* untuk keperluan pengujian.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menghasilkan rancang bangun sistem verifikasi e-sertifikat berbasis web yang mampu mengatasi kelemahan validasi visual pada sistem e-sertifikat di Cazh Academy.
2. Mengimplementasikan kombinasi algoritma RSA dan SHA3-512 untuk mendukung proses autentikasi serta mendeteksi perubahan atau manipulasi data pada file e-sertifikat.
3. Membuktikan secara empiris bahwa sistem yang dibangun mampu membedakan e-sertifikat yang telah dimanipulasi dan menerima e-sertifikat yang asli (valid).

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoritis
    a. Memberikan kontribusi wawasan mengenai implementasi gabungan algoritma kriptografi modern (SHA3-512) dan standar (RSA) dalam studi kasus pengamanan dokumen pendidikan vokasi.

b. Menjadi referensi bagi peneliti selanjutnya yang ingin mengembangkan sistem keamanan dokumen dengan metode verifikasi berbasis konten (*content-based verification*).

2. Manfaat Praktis

a. Meningkatkan kredibilitas institusi dengan menjamin bahwa sertifikat yang diterbitkan aman dari pemalsuan, serta melindungi reputasi lembaga dari risiko penggunaan sertifikat palsu oleh oknum tidak bertanggung jawab.

b. Memberikan kemudahan dan kepastian hukum bagi pihak industri (HRD) atau institusi lain dalam memverifikasi keaslian sertifikat pelamar kerja secara akurat, cepat, dan mandiri tanpa perlu menghubungi pihak instansi secara manual.

c. Menerapkan ilmu kriptografi dan rekayasa perangkat lunak yang telah dipelajari dalam solusi nyata di dunia kerja.