BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis, perancangan, implementasi, dan pengujian pada sistem verifikasi e-sertifikat CAZHSECURE yang telah diuraikan pada bab-bab sebelumnya, maka dapat ditarik kesimpulan yang menjawab rumusan masalah dan tujuan penelitian sebagai berikut:

1. Rancang bangun sistem verifikasi e-sertifikat berbasis web telah berhasil dikembangkan menggunakan *framework* Laravel. Sistem ini secara efektif mengatasi kelemahan validasi visual pada sistem *QR Code* sebelumnya di Cazh Academy dengan menyediakan mekanisme verifikasi ganda, yaitu pemindaian *QR Code* untuk validasi identitas dan fitur unggah (*upload*) dokumen PDF untuk validasi integritas konten secara menyeluruh.
2. Kombinasi algoritma kriptografi RSA 2048-bit dan fungsi *hash* SHA3-512 telah berhasil diimplementasikan ke dalam alur penerbitan dokumen. Fungsi SHA3-512 terbukti andal dalam menghasilkan message digest untuk menjaga keutuhan data, sementara algoritma RSA berhasil mengelola kunci asimetris untuk menyandikan hash tersebut menjadi tanda tangan digital (*digital signature*) guna memastikan autentikasi dokumen.
3. Hasil pengujian secara empiris membuktikan ketangguhan sistem dalam mendeteksi manipulasi data. Pengujian *Avalanche Effect*

menghasilkan persentase sebesar 51,56% saat terjadi modifikasi 1 digit pada isi dokumen, yang menandakan sensitivitas algoritma sangat tinggi. Sistem secara mutlak berhasil membedakan dan menolak e-sertifikat yang telah dimanipulasi.

5.2 Saran

Sistem yang dibangun dalam penelitian ini telah berfungsi dengan baik sesuai spesifikasi, namun masih memiliki ruang untuk pengembangan lebih lanjut. Berdasarkan hasil penelitian dan kesimpulan di atas, beberapa saran yang dapat diberikan untuk pengembangan secara praktis maupun akademis di masa mendatang adalah:

1. Mengingat sistem CAZHSECURE saat ini masih berstatus sebagai *Proof of Concept* (PoC) yang berdiri sendiri (*standalone*), peluang pengembangan ke depannya dapat diarahkan pada proses integrasi modul kriptografi ini ke dalam ekosistem Sistem Informasi Manajemen (SIM) yang sudah ada. Hal ini bertujuan agar siklus penerbitan oleh pembimbing dan pengunduhan e-sertifikat oleh peserta dapat berjalan lebih efisien melalui satu pintu.
2. Dari segi fungsionalitas dan skalabilitas, pengembangan sistem selanjutnya dapat difokuskan pada penambahan fitur *template builder* dinamis. Fitur ini memungkinkan untuk menyesuaikan tata letak dan desain visual dokumen secara fleksibel melalui antarmuka dasbor tanpa perlu melakukan perubahan pada kode

program. Selain itu, ruang lingkup implementasi sistem pengamanan ini memiliki potensi besar untuk diperluas, tidak hanya terbatas pada e-sertifikat, tetapi juga dapat diaplikasikan untuk menjamin integritas dan autentikasi dokumen legal lain yang bersifat krusial, seperti *Memorandum of Understanding* (MoU) atau surat perjanjian kerja sama.

3. Untuk penelitian akademis selanjutnya, disarankan untuk mengimplementasikan atau membandingkan metode RSA dengan algoritma kriptografi asimetris alternatif lainnya. Penggunaan algoritma yang memiliki ukuran kunci lebih efisien berpotensi dapat mempercepat proses komputasi kriptografi.