

BAB V

KESIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan mengenai "Perancangan Sistem Sertifikat Berbasis Web Menggunakan Algoritma SHA-256, Salt dan QR-Code sebagai Verifikasi Digital", dapat disimpulkan beberapa hal sebagai berikut:

1. Sistem web berhasil dirancang dan dibangun untuk menghasilkan sertifikat lomba dalam format PDF secara otomatis berdasarkan kode unik yang dibuat saat proses *hashing*. Selain itu, sistem mampu menampilkan QR Code yang berisi nilai *hash* sebagai sarana verifikasi keaslian. Pengujian *black box* menunjukkan bahwa seluruh fitur mulai dari *hashing* data, pembuatan sertifikat digital, hingga verifikasi QR Code berjalan sesuai dengan fungsionalitas yang telah dirancang.
2. Implementasi algoritma *hash* SHA-256 yang dikombinasikan dengan nilai *salt* dalam sistem web menghasilkan *hash* yang unik dan acak. Hal ini dibuktikan melalui pengujian menggunakan metode korelasi *Pearson* terhadap 10 data peserta, yang menunjukkan nilai korelasi sangat rendah hingga mendekati nol, sehingga membuktikan bahwa *output hash* bersifat acak dan tidak berkorelasi langsung dengan inputnya. Ini sesuai dengan karakteristik ideal dari algoritma kriptografi *hash* untuk mengamankan dan menjamin keaslian dari sertifikat tersebut.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang diperoleh, beberapa saran yang dapat dijadikan masukan untuk pengembangan selanjutnya antara lain:

1. Sistem dapat dikembangkan lebih lanjut agar mendukung desain sertifikat yang dinamis berdasarkan kategori kegiatan, jenis peserta, maupun instansi penyelenggara. Selain itu, perlu ditambahkan fitur manajemen pengguna berdasarkan *role* (misalnya admin, panitia, dan peserta), agar hak akses setiap pengguna dapat dibatasi sesuai fungsinya. Hal ini akan meningkatkan keamanan serta efektivitas penggunaan sistem.

2. Selanjutnya, sistem verifikasi ini dapat diperluas ke dalam bentuk aplikasi *mobile* agar lebih mudah diakses oleh pengguna. Dengan adanya versi aplikasi, proses pembuatan maupun verifikasi sertifikat dapat dilakukan secara fleksibel dan cepat melalui perangkat seluler, tanpa bergantung pada platform web saja.