

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian perbandingan algoritma hash SHA1, SHA2 dan SHA256 untuk mengamankan URL gambar pada studi kasus foto mahasiswa ISB Atmaluhur menyimpulkan bahwa :

1. SHA-1, SHA-2 dan SHA-256 adalah algoritme hashing yang menghasilkan intisari pesan dengan panjang berbeda. SHA-1 adalah versi dasar dari fungsi hash dan kurang aman dibandingkan SHA-2 dan SHA-256. SHA-2 adalah keluarga algoritme yang mencakup SHA-256 dan SHA-512 dan menawarkan hash yang lebih kompleks dan kode yang lebih panjang. SHA-256 adalah anggota keluarga algoritme SHA-2 dan dianggap sebagai algoritme hash paling aman di antara SHA-1, SHA-2, dan SHA-256.
2. penggunaan algoritma hash SHA256 adalah pilihan terbaik untuk melindungi integritas data gambar mahasiswa. Dalam perbandingan ini, SHA1 dianggap lemah dan tidak lagi direkomendasikan pada aplikasi untuk kepentingan keamanan. SHA2 dan SHA256 menawarkan tingkat keamanan yang lebih tinggi, dan SHA256 adalah pilihan terbaik karena menghasilkan nilai hash dengan cepats. Meskipun SHA256 dapat memengaruhi performa sistem dengan waktu komputasi yang lebih lama, keuntungan dari peningkatan keamanan akan membantu melindungi data gambar mahasiswa dari kemungkinan manipulasi atau perubahan yang tidak sah. Rekomendasi penggunaan algoritma hash SHA256 memberikan panduan bagi pengelola sistem untuk mengoptimalkan keamanan dan efisiensi sistem, serta membantu memahami dan memahami keamanan algoritma hash dalam konteks keamanan data.

5.2 Saran

Saran pada penelitian selanjutnya diharapkan untuk menganalisis mendalam tentang potensi serangan dan mekanisme hashing untuk memastikan penerapan

keamanan URL gambar yang lebih kuat. Selain itu, penting untuk meningkatkan kesadaran keamanan di antara mahasiswa dan staf, serta melakukan pemantauan keamanan yang ketat untuk melindungi data gambar mahasiswa dari potensi ancaman dan pelanggaran keamanan.

