INTISARI

Dalam era digital yang semakin berkembang, layanan pemendek URL telah menjadi solusi praktis untuk membagikan tautan ke dokumen penting atau data sensitif dengan lebih efisien. Namun, di balik kemudahannya, banyak layanan pemendek URL konvensional tidak memiliki mekanisme keamanan yang memadai, sehingga tautan yang dihasilkan rentan terhadap eksploitasi, penyalahgunaan, atau akses oleh pihak yang tidak berwenang. Risiko ini semakin meningkat seiring dengan meningkatnya ancaman siber. Oleh karena itu, penelitian ini bertujuan untuk meningkatkan keamanan data pada aplikasi pemendek URL berbasis website bernama "Linky" dengan menerapkan algoritma Advanced Encryption Standard (AES) 256-bit. Dengan metode enkripsi ini, setiap data yang dimasukkan oleh pengguna akan dienkripsi sebelum disimpan ke dalam database, memastikan perlindungan optimal terhadap informasi yang tersimpan. Proses enkripsi ini bertujuan untuk mencegah akses tidak sah, bahkan jika data yang tersimpan berhasil diakses oleh pihak yang tidak berwenang. Pengujian dilakukan dengan memanfaatkan software CrackStation untuk menguji ketahanan enkripsi terhadap metode serangan berbasis dictionary attack, serta pengujian Blackbox untuk mengevaluasi fungsionalitas dan keamanan sistem secara keseluruhan. Hasil pengujian menunjukkan bahwa algoritma AES 256-bit mampu memberikan perlindungan data yang kuat tanpa mengorbankan efisiensi pemrosesan. Dengan demikian, implementasi enkripsi ini dapat menjadi solusi efektif dalam meningkatkan keamanan layanan pemendek URL, memastikan bahwa data pengguna tetap aman, dan memberikan pengalaman berbagi tautan yang lebih terpercaya.

Kata Kunci: Kriptografi, AES 256-bit, Keamanan Data, Pemendek URL, Enkripsi

ABSTRACT

In the rapidly evolving digital era, URL shortening services have become a practical solution for efficiently sharing links to important documents or sensitive data. However, despite their convenience, many conventional URL shorteners lack adequate security mechanisms, making the generated links vulnerable to exploitation, misuse, or unauthorized access. This risk is further heightened by the increasing number of cyber threats. Therefore, this study aims to enhance data security in a web-based URL shortening application called "Linky" by implementing the Advanced Encryption Standard (AES) 256-bit algorithm. With this encryption method, all user-inputted data is encrypted before being stored in the database, ensuring optimal protection of stored information. This encryption process is designed to prevent unauthorized access, even if stored data is compromised. The system's security was tested using CrackStation software to assess encryption resilience against dictionary attacks, as well as Blackbox testing to evaluate overall system functionality and security. The test results demonstrate that the AES 256-bit algorithm provides strong data protection without compromising processing efficiency. Thus, this encryption implementation offers an effective solution for enhancing the security of URL shortening services, ensuring user data remains secure, and providing a more reliable link-sharing experience.

Keywords: Cryptography, AES 256-bit, Data Security, URL Shortener, Encryption