IMPLEMENTASI ALGORITMA PAILLIER CRYPTOSYSTEM PADA FITUR SHORTLINK BERBASIS WEB

Abstrak

Dalam era digital saat ini, shortlink telah menjadi alat yang populer untuk mempersingkat tautan URL dan memfasilitasi berbagi tautan secara efisien. Namun, penggunaan shortlink sering kali membawa risiko terhadap keamanan dan privasi, terutama ketika tautan tersebut mengarah ke konten sensitif atau pribadi. Untuk mengatasi masalah ini, pendekatan kriptografi dapat diadopsi untuk melindungi tautan asli dengan menggunakan teknik enkripsi. Artikel ini mengusulkan penerapan solusi keamanan untuk shortlink dengan memanfaatkan Paillier Cryptosystem, sebuah sistem kriptografi publik yang dapat digunakan untuk melindungi informasi sensitif. Metode ini memungkinkan tautan asli dienkripsi sebelum diubah menjadi shortlink, sehingga hanya penerima yang memiliki kunci dekripsi yang tepat yang dapat mengakses tautan yang sebenarnya. Oleh karena itu, tautan yang disingkat tetap aman dari akses yang tidak sah. Melalui penggunaan Paillier Cryptosystem, tautan yang telah dienkripsi dapat diubah menjadi shortlink tanpa mengorbankan keamanan. Proses enkripsi dan dekripsi yang dilakukan oleh sistem Paillier memastikan bahwa informasi sensitif tetap terlindungi dan hanya dapat diakses oleh pihak yang berwenang. Selain itu, kemampuan Paillier Cryptosystem dalam melakukan operasi homomorfik juga memungkinkan penghitungan pada data terenkripsi tanpa perlu mendekripsinya terlebih dahulu. Penelitian ini akan membahas implementasi praktis dari solusi shortlink yang aman dengan menggunakan Paillier Cryptosystem, serta menganalisis tingkat keamanan yang dapat dihasilkan. Dengan menggabungkan efisiensi shortlink dan keamanan kriptografi Paillier, artikel ini mengusulkan pendekatan yang inovatif untuk memenuhi kebutuhan akan pengiriman tautan yang cepat dan efisien tanpa mengabaikan aspek keamanan dan privasi.

Kata kunci : Shortlink, Kriptografi, Paillier Cryptosystem

IMPLEMENTASI ALGORITMA PAILLIER CRYPTOSYSTEM PADA FITUR SHORTLINK BERBASIS WEB

Abstract

In today's digital era, shortlinks have become a popular tool for abbreviating URL links and facilitating efficient link sharing. However, the use of shortlinks often brings about security and privacy risks, especially when the links direct to sensitive or private content. To address this issue, cryptographic approaches can be adopted to protect the original links by employing encryption techniques. This paper proposes the implementation of a security solution for shortlinks by leveraging the Paillier Cryptosystem, a public-key cryptography system that can be used to safeguard sensitive information. This method allows the original links to be encrypted before being transformed into shortlinks, ensuring that only authorized recipients with the appropriate decryption key can access the actual link. As a result, the shortened links remain secure from unauthorized access. Through the utilization of the Paillier Cryptosystem, the encrypted links can be converted into shortlinks without compromising security. The encryption and decryption processes performed by the Paillier system ensure that sensitive information remains protected and accessible only to authorized parties. Additionally, the homomorphic capabilities of the Paillier Cryptosystem enable computations on encrypted data without requiring prior decryption. This study will discuss the practical implementation of a secure shortlink solution using the Paillier Cryptosystem, along with an analysis of the achievable level of security. By combining the efficiency of shortlinks with the cryptographic security of the Paillier system, this paper proposes an innovative approach to fulfill the need for swift and efficient link sharing without disregarding the aspects of security and privacy.

Keywords : *Shortlink, Kriptografi, Paillier Cryptosystem*