

INTISARI

Pencurian dan penyadapan data sudah menjadi suatu permasalahan yang cukup serius dan sangat merugikan untuk para korban peretasannya. Untuk menjaga data tetap aman, diperlukannya keamanan bertingkat/berlapis dengan beberapa cara dan teknik yang digunakan dengan cara membuat suatu pengamanan dokumen berbasis website menggunakan algoritma SHA-1 dan AES 128. Metode pengembangan sistem yang digunakan pada penelitian ini menggunakan metode pengembangan secara Waterfall. Hasil dari penelitian ini berupa aplikasi pengamanan dokumen berbasis website yang pengamanannya menggunakan algoritma SHA-1 dan Algoritma AES 128 dengan bahasa pemrograman PHP, aplikasi yang dibagun dapat melakukan proses enkripsi dan dekripsi kunci serta konten dari dokumen yang telah ditentukan menggunakan algoritma SHA 1 dan algoritma AES 128 dan hasil dari penguiannya telah teridentifikasi aman dan cepat dalam proses pengamanan dokumen. Penelitian ini diharapkan dapat digunakan untuk mengamankan berbagai jenis dokumen-dokumen penting guna menghindari penyadapan atau pencurian data oleh pihak yang tidak bertanggung jawab.

Kata kunci: SHA-1, AES 128, PHP, Waterfall dan Dokumen

ABSTRACT

Data theft and eavesdropping has become a serious and very detrimental problem for the victims of the hack. To keep data safe, multilevel / layered security is needed in several ways and techniques used by creating a website-based document security using the SHA-1 and AES 128 algorithms. The system development method used in this study uses the waterfall development method. The results of this study are in the form of a website-based document security application whose security uses the SHA-1 algorithm and the AES 128 Algorithm with the PHP programming language, the application that is studied can carry out the process of encrypting and decrypting keys and the content of predetermined documents using the SHA 1 algorithm and the AES 128 algorithm and the results of the quenching have been identified as safe and fast in the document security process. This research is expected to be used to secure various types of important documents to avoid eavesdropping or data theft by irresponsible parties.

Keywords: SHA-1, AES 128, PHP, Waterfall and Documents

