



162162

Encryption System for Confidential Data Transmission

Abstract

The ubiquitous and borderless Internet has greatly increased connectivity between people. Together with its popularity as a commercial activities platform, the Internet has also become a popular target for cyber criminals who intentionally exploit on the Internet's numerous vulnerabilities. Perpetrators exploit the vulnerability of computer systems with malicious software programs designed specifically to steal confidential information such as user names, passwords and credit card numbers by recording keystrokes from the computer keyboard. The two most common methods used are keystroke recording and phishing scams. Phishing is a means of fraudulently acquiring confidential information through deception, for example, by masquerading as an official email or website for requesting such information. Online services relying on password challenges alone for authentication are the most vulnerable to keystroke recording as well as to other means of obtaining passwords. Multi-conditional authentication can be deployed to replace Password Challenge. However, these solutions incur high implementation cost and bring forth privacy issues. Embodiments of the invention describe an encryptor and a method for implementation thereof for encrypting data input and a dynamic variable obtainable by the encryptor into encrypted data. The encryptor data communicatively interfaces an input device and a computing system wherein a user is able to interact with the input device for generating the data input. The encrypted data is transmitted to and relayed by the computer system for subsequent reception and decryption by a decryptor for comparing with a reference dynamic variable obtainable by the decryptor for verifying validity of data decrypted therefrom.

FIG. 2



G00002