SISTEM KEAMANAN TRANSMISI DATA TERENKRIPSI DENGAN ALGORITMA OTENTIKASI ZERO KNOWLEDGE PROOF

ABSTRACT

Digital data transmission over wireless is one of the many ways done to transmit data. Transmitted data can be either privacy or data that are not privacy. Various problems arise when the data is transmitted as a way to maintain that the data sent is not read by unauthorized people, keep the data intact and not manipulated, checking identity of the sender data and etc. Various encryption techniques are developed to overcome security problems of the data. But it needed a method for authentication of data to identify the sender of the data. One of the methods used for authentication of data is Zero Knowledge Proof. This method works to identify the authenticity of a someones statement to proof without showing any knowledge of the statement mentioned. This research will mainly discuss about the security of data transmission system by combining data encryption and data authentication. The proposed data encryption is using Advanced Encryption System and method for authentication of data using the Zero Knowledge Proof. This research will conduct the development methods of authentication Zero Knowledge Proof from previous research conducted by Brandon and will be compared with the proposed method based on the simulation results transmission system client and server. Experiments will be conducted using thirty-text data, each of data will be measured on the performance of both encryption and authentication process between the previous method and proposed method. Experimental results show the performance of the proposed method is more significant in the application for security of data transmission systems, with average value of performance to authenticate 5 milliseconds from the client side and server side.(YM)

Keyword : Data transmission, Data Authentication, Data Encryption, Zero Knowledge Proof, Advanced Encryption System

ABSTRAK

Transmisi data digital merupakan salah satu cara yang banyak dilakukan untuk mengirimkan data. Data yang dikirimkan dapat berupa data yang bersifat privasi ataupun bukan privasi. Berbagai permasalahan muncul saat data tersebut dikirimkan seperti cara menjaga supaya data-data yang dikirim tidak dibaca oleh orang yang tidak berhak, data tetap utuh tidak dimanipulasi, pengenalan identitas dari pengirim data dan lain-lainnya. Berbagai teknik enkripsi dikembangkan untuk mengatasi masalah keamanan dari sebuah data. Namun dibutuhkan juga metode untuk otentikasi sebuah data untuk mengidentifikasi pengirim dari data tersebut. Salah satu metode yang digunakan untuk otentikasi data adalah Zero Knowledge Proof. Metode ini bekerja mengidentifikasi keaslian sebuah pernyataan seseorang dengan pembuktian tanpa memperlihatkan pengetahuan apapun dari pernyataan yang disebutkan. Metode Zero Knowledge Proof ini memanfaatkan perhitungan Logaritma Diskrit dalam penerapan untuk proses otentikasi seperti pada penelitian yang dilakukan Brandon untuk web authentication. Penelitian ini terutama akan membahas mengenai sistem keamanan transmisi data dengan menggabungkan enkripsi data dan otentikasi data. Enkripsi data yang diusulkan adalah Advanced Encryption System, dan untuk otentikasi data menggunakan metode Zero Knowledge Proof. Pada penelitian ini akan dilakukan pengembangan metode otentikasi Zero Knowledge Proof dari penelitian sebelumnya yang dilakukan oleh Brandon dan dibandingkan dengan metode yang diusulkan berdasarkan hasil simulasi sistem transmisi client dan server yang dibuat pada penelitian ini. Eksperimen yang dilakukan akan menggunakan tiga puluh data teks yang masing-masing akan diukur kinerja performansi baik pada proses enkripsi dan proses otentikasi antara metode sebelumnya dan metode yang diusulkan. Hasil eksperimen menunjukkan performansi kinerja dari metode yang diusulkan lebih signifikan dalam penerapan untuk sistem keamanan transmisi data, dengan nilai rata-rata performansiuntuk proses otentikasi 5 milliseconds dari sisi client dan sisi server. (YM)

Kata kunci : Transmisi data, Otentikasi Data, Enkripsi Data, Zero Knowledge Proof, Advanced Encryption System