Abstract

Secured Communication of data inside an organization is very important issue particularly when the communication is taking place outside the organization. It is very important for the organization to know the kind of data which is being shared by the employee of that organization to outside world. Encryption is an essential tool for protecting the confidentiality of data. Network security protocols such as SSL or IPSec use encryption to protect Internet traffic from eavesdropping. Encryption is also used to protect sensitive data before it is stored on non-secure disks or tapes. Encryption, however, is computationally expensive. A computer server that must encrypt data for thousands of clients before sending it over the network can easily become crypto-bound. The capacity of the server is then determined by the speed at which it can perform encryption. This is especially the case when slow encryption protocols such as the Digital Encryption Standard (DES) or Triple-DES are employed. Since DES and Triple-DES are very widely used, it is important to optimize the performance of these algorithms. Triple-DES (TDES) is basically used in various cryptographic applications and wireless protocol security layers [2]. This paper presents the design and the implementation of the Secured
Communication of Data Using Data Dictionary in Triple Data Encryption Standard (DES) algorithm. Data Dictionary is created and used by the admin for the purpose of detection of suspicious communication.

References


Index Terms

Computer Science Security

Keywords
Data Dictionary, Data Encryption Standard, Encryption System, Plaintext, Triple DES