Secure Data Storage in The Cloud With Enhanced Symmetric Block Cipher Design

Authors:

Waleed Kareem ,Omar A. Dawood, Hussein Almulla

Abstract

Cloud storage become most widely contemporary storage that used by the big companies through applying their services and their commercial activities. The security threats increased dramatically with the accelerating of increasing the volume of data on remote servers. The encryption-based methods are used to trust the data on remote servers securely with encrypted form. In this paper developed a new modern symmetric cipher under Substitution Permutation Network (SPN) structure with three strong variable ciphering keys of 128,192 and 256 bit of changeable rounds. The proposed algorithm involves a new algebraic theories and concrete mathematical principles that completely depend on Galois Field GF(2 8). The present cipher works to trust the cloud storage through encrypting the data to ensure the confidentiality. The proposed cipher enhanced the security metric and solve numerous type of internet-based storage problems for cloud services. Standard (AES), Feistel Structure (FS).

Keyword

Block Cipher, Cloud Storage, Galois Field (28), Substitution and Permutation Network (SPN), Advance Encryption Standard (AES), Feistel Structure (FS).