

An advanced AES algorithm using swap and 400 bit data block with flexible S-Box in Cloud Computing

Publisher: IEEE

Cite This

 PDF

Chinnakandukuri Paul Pramod ; Manjit Jaiswal **All Authors**

1

Paper

Citation

154

Full

Text Views



Abstract

Abstract:

This paper suggests a new Advance Encryption Standard (AES) encryption technique. New Algorithm uses 400 bit block encryption scheme and a key dependent rotated S-Box which varies according to the 200 bit key provided by the user. Fixed S-box allows hackers to study S-box and find weaker points, whereas using key-dependent S-Box, it is harder for attacker to do any offline analysis of an attack on one particular set of S-boxes. This helps to store data in

Document Sections

I. Introduction

II. Literature Survey