PRC6: Hybrid Lightweight Cipher for Enhanced Cloud Data Security in Parallel environment

Zahraa A. Mohammed[1] and Khalid Ali Hussein[2]

[1]University of Babylon
[2]Mustansiriyah University

March 11, 2024

Abstract

Modern technologies of computing cloud are showing great promise, but at the same time create new security challenges that hinder full acceptance. Given that most of these services often use cloud networks as channels for communication, securing data transmission is crucial. This paper proposes a hybrid encryption algorithm, the proposed two-layered PRC6 cipher, developed to achieve high security in cloud computing environments with minimal resource constraints. The PRC6 cipher incorporates enhancements from Cha-cha into an extension of the RC6 cipher. PRC6 implements double encryption. At the first level, the plain text is divided into four equal parts, each encrypted by processes derived from RC6, which include shifting, summation, modulo arithmetic, and XOR with a generated key. The second level incorporates a Quarter round function, among others, to further obscure the encoded message. PRC6 is implemented in a parallel computing model to significantly reduce overall computation time, especially important for lightweight applications. Experimental results show that the algorithm can achieve a high level of security for cloud workloads in only a few encryption rounds. Performance evaluations against popular encryption standards also indicate that PRC6 offers promising security benefits when computational resources are limited. This hybrid approach presents a viable solution for strengthening data protection in modern cloud systems.

Hosted file

`PRC6.docx` available at https://authorea.com/users/753834/articles/723923-prc6-hybrid-lightweight-cipher-for-enhanced-cloud-data-security-in-parallel-environment