IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, June 2025
Impact Factor: 7.67

Efficient Implementation of 128-Bit AES Algorithm on FPGA for Minimal Resource Utilization

Vinaya Kumar K[1] and Prof. Raji C[2]
School of Electronics and communication Engineering Reva University, Bangaluru, Karnataka, India[1,2]
kalasapuravinaykumar@gmail.com, raji.c@reva.edu.in

Abstract: *Cryptography plays a crucial role in ensuring the security and integrity of data, especially in the era of increasing cyber threats. The Advanced Encryption Standard (AES) is commonly used for secure communications, but its hardware implementations must effectively balance performance, resource use and power efficiency, particularly in FPGA-based settings. This paper presents an optimized AES-128 implementation in Verilog, crafted to minimize resource demands and power consumption while preserving encryption performance. In contrast to standard AES designs, our approach leverages optimized S-Box computations, efficient key expansion, and resource-sharing techniques to lower logic complexity. The design has been synthesized and implemented on an FPGA, achieving significant reductions in resource utilization compared to conventional AES architectures. Simulation results reveal improvements in resource utilization, area efficiency and energy savings, making our design well-suited for low-power embedded systems*

Keywords: Cyber threats, Advance encryption standard, Verilog, Logic complexity, resource utilization, energy savings

DOI: 10.48175/IJARSCT-28824