VLSI IMPLEMENTATION IN HARDWARE SECURITY MODULE BASED ON AES ENCRYPTION METHOD

BATCH NUMBER : C10

PROJECT CODE :

BATCH MEMBER : A. AKASH

P. JAIGANESH

M.MAHIZHAN

SUPERVISOR : Mr .K. SRINIVASAN

SDG GOALS : 9

Department of Electronics and Communication Engineering ECE
Sri Sairam College of Engineering Chennai, India.

Abstract:

Cryptography is very important now-a-days for data security and integrity as the ecommerce and internet applications has increased. But, it has least importance in many cases because of extra memory and other requirements needed for the implementation. The main aim of this work is to implement Advanced Encryption Standard (AES) Encryption using Verilog. To protect data like electronics, cryptographic algorithms are used. Each round of encryption associated with delay can be reduced by AES parallel design. This work proposes a low power and high throughput implementation of AES algorithm using key expansion approach. We minimize the power consumption and critical path delay using the proposed high-performance architecture. The fundamental goal of the initiative is to increase data flow, although security considerations have become increasingly important over time. The use of encryption and decryption techniques inside VLSI has recently increased since cryptography can convert plaintext to cipher and vice versa. The most recent developments in cryptography technology will be applied in the hardware security module. by simultaneously writing a lot of HDL modules. The main objective is to send and receive data securely without allowing data to be hacked, as well as to improve the performance of a specific parameter. The methodology involved in this system is Verilog code. To support both analog and digital circuit designing, Xilinx provides analog and digital platform. It is interesting to note that any encryption algorithm works in a digital environment and all the blocks in the system will handle digital data in security.

Guide Signature