**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:**

The main goal of this work is to implement Advanced Encryption Standard (AES) encryption using Verilog. To protect data, such as electronic devices, cryptographic algorithms are used. Each encryption cycle associated with latency can be minimized by the AES parallel design. This work proposes to implement a low-power, high-throughput AES algorithm using the key expansion method. This minimizes power consumption and critical path latency using the recommended high-performance architecture. The primary 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 latest developments in cryptographic technology will be applied in the hardware security module. by simultaneously recording a large number of HDL modules. The main purpose is to send and receive data securely without allowing data to be hacked, as well as to improve the performance of a particular parameter. Interestingly, any cryptographic algorithm works in a digital environment, and all blocks in the system handle digital data securely. Some adjustments are made in the AES 256 algorithm and it is compared with all other encryption algorithms to come up with the desired advanced encryption algorithm as the output of this project. 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