International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Design AES Algorithm Based Secured Data Encryption System using Verilog

E.Devisri[1], V.UshaSri[2], G.Venkatramanan[2], N.Madhuri[2], B.Govardhana[2]

[1]Assistant Professor, Department of ECE, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India

[2]B.Tech Students, Department of ECE, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted: 03 March2024
Published: 28March 2024

Publication Issue :
Volume 11, Issue 11
March-April-2024

Page Number :
469-476

ABSTRACT

Based on Security Applications, the AES Algorithm is used. The Advanced Encryption Standard (AES) Algorithm was a Federal Information Processing Standard (FIPS),widely used for securing data. The AES Encryption algorithm is also known as the Rijndael algorithm. It is a symmetric block cipher algorithm with a block size of 128 bits. It covers theseindividual blocks using keys of 128,192,256 bits. Once it encrypts these blocks,it joins them together to form ciphertext. Parallelly, the encryption starts by XORing the key and the input data before feeding the result through the key modules. Key modules are SubBytes, ShiftRows, MixColumns, and AddRoundKey are used efficiently to decrease the complexity and optimize utilization. The architecture supports the encryption process with high accuracy, making it suitable for hardware-critical applications like wireless security, processor security, file encryption, smart cards, and mobile phones. The project utilizes Vivado software optimization tools for synthesis and implementation. A Xilinx XC3S500 Spartan Family device is employed for hardware assessment to reduce the utilization of the system by 21%of the area,41.194 ns of delay and the total power consumption is 2.664 milliwatts.

Keywords- AES Algorithm, SubBytes, ShiftRows, Mix Columns, Add Round Key, Vivado software, Power Consumption, area, Delay, Secured data application.

I. INTRODUCTION

Technically,we have seen a drastic growth in telecommunication. Through the internet, anybody can access the data present in a computer in any corner of the world. Many activities like e-commerce,data sharing, etc. will happen through the Internet.So, data authentication and secured communication have become very important.Nowadays many data encryption algorithms are available. Digital information can be encryptedby using block cipher by using cryptographic keys of 128, 192, and 256 bits. In AES encryption, There are 4 key modules such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. In SubByteseach byte of states is transformed by looking up table S-box using their value as an address, In ShiftRows, bytes in each row of the state are shifted cyclically to the left, In MixColumnsEach column is treated as a vector of bytes, and are multiplied by a fixed matrix to get the column for the modified State.Transformation in the Cipher and Inverse Cipher in which a Round Key is added to the State using an XOR operation. AES is a special kind of code that scrambles our messages in a way that only the person who has the right key can unscramble them. This means even if someone intercepts our message, they can't understand it without a Rightkey. It's like having a secret language that only you and your friendunderstand, keeping your conversations private and secure. That's why AES is so important for keeping our digital world safe and our secrets secure.

Secure applications use different methods to protect sensitive information. Encryption is like a secret code that keeps data safe from prying eyes. Access control limits who can see or change important data. Authentication checks if someone is who they say they are before letting them in. Data masking hides private details when they're not needed. Secure transmission means safely sending data so no one else can read it. Regular auditing keeps track of what's happening in the app for security. Secure coding makes sure the app is built strong and hard to break into. Backup and recovery means having extra copies of data in case something goes wrong. Security updates keep the app safe by fixing any problems. Employee training teaches everyone how to keep data safe from hackers. Following these steps helps keep sensitive information safe from attacks. It's important to keep data secure to protect privacy and prevent theft. With these measures in place, users can trust that their data is safe. Data security is everyone's responsibility, and it's crucial for building trustworthy applications.

II. LITERATURE SURVEY

The following papers have been cited during the literature survey to understand the different methodologies of computer-aided systems in allied areas of work carried out.

[1] In this study, a throughout AES algorithm-secured data encryption system using Verilog has been verified by experts, Here Output depends on different computer features but, in the computer, we have taken different features so, we faced challenges ingetting the accurate output in AES Algorithm Encryption System. This methodology uses a non-pipelined method, and conducts a comprehensive review of cryptography, focusing on its principles and applications in ensuring transmission secrecy and data integrity over insecure mediums the parameters are Power consumption typically ranges from tens of milliwatts to a few watts, while area utilization can vary from a few thousand to several tens of thousands of logic cells of 23%.

[2]This paper likely discusses the design and implementation of an AES (Advanced Encryption Standard) cryptoprocessor with advanced features, possibly within the context of the European Processor Initiative (EPI) framework. It may cover topics such as VLSI (Very Large-Scale Integration) design methodologies, cryptographic algorithms, hardware acceleration techniques, and possibly power efficiency considerations. In

this, we are using the Methodology of the design integrated into a RISC-V-based SoC, specifically tailored for the European Processor Initiative (EPI) chip. The cryptoprocessor is tested on a 7-nm CMOS standard-cells technology and the parameters are Enhance AES cryptoprocessor with security features, diverse modes, and 7-nm validation.

[3]The focus of the paper is likely on the hardware implementation aspects of AES encryption andfor real-time video streams, leveraging the parallel processing capabilities of FPGA technology and the computational power of HPS. This implementation could be useful for applications requiring secure transmission and storage of video data, such as surveillance systems, video conferencing platforms, or multimedia communication systems. In this we are using the methodologies of Optimizing AES-128 algorithm performance on Terasic DE10 FPGA for real-time video encryption/decryption, achieving over 4x faster execution than software and the parameters are Optimize AES-128 algorithm on Terasic DE10 FPGA for >4x faster real-time video encryption.

[4]Thispaper includes reviewing the Advanced Encryption Standard (AES) algorithm and its relevance to Internet of Things (IoT) applications, investigating modifications to the AES S-Box for enhanced security, and examining techniques to improve the security of cryptographic algorithms tailored for IoT devices. Additionally, the survey should encompass the analysis of IoT application scenarios, evaluating the proposed modified S-Box AES algorithm's performance and its comparison with existing implementations. Discussions on implementation considerations, security evaluation against cryptographic attacks, and future directions in IoT security are crucial. Researchers should search academic databases like IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar using relevant keywords to gather pertinent literature. Citing the Jha and Jain paper as a primary reference is imperative throughout the survey. In this we are using the Methodologies of conducting a comprehensive literature review on AES and its vulnerabilities to identify potential flaws and parameters are Measure encryption/decryption speed, resource utilization, and resistance to attacks.

III.PROPOSED METHOD

We are proposing the method as overcoming thedisadvantages of the previously existing methodsof Encryption and Key Expansion implemented using pipelined round blocks.Registers are placed between each round to pipeline the data flow.Round key signals are hardwired in each stage to minimize delay. Encrypts one 128-bit block per cycle with 11-cycle latency. Higher throughput since multiple blocks can be in the pipeline simultaneously. Decryptionis achieved by reversing the cipher flowmeter input port for key, plaintext, and control signals.

About AES Encryption Algorithm

The Advanced Encryption Standard (AES) Algorithm is widely utilized forencryption algorithms for securing data from unauthorized access. It operates with varying lengths, designated as AES-128, or AES-192, or AES-256, depending on the key size. The AES algorithm utilizes a different number of rounds for encryption: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. In each round, a unique 128-bit round key is derived from the original AES key to ease the encryption process.This method provides a reliable way to ensure the security and confidentiality of sensitive data

In this, we will explain what AES is, how it works, and why it is important for internet security. AES encryption is a method of encrypting data that uses a "symmetric block cipher" or encryption algorithm.Encryption is the process of converting plain text into code that can only be understood by someonewith the cipher (key) to decode the code.

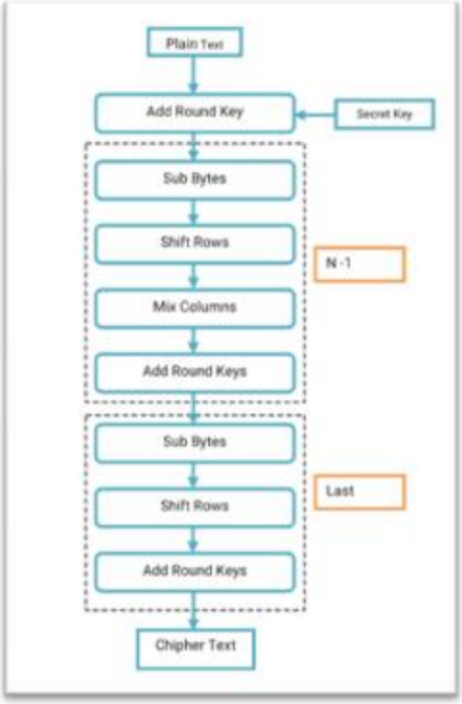


Figure 1: Diagram of AES AlgorithmEncryption System

In the AES algorithm, There arethe following steps to work the AES to secure data. Here are the steps:

1. SubBytes: It is a non-linear transformation where the byte is replaced with a value in the S-box. The S-box is predetermined for using it in the algorithm.S-box is used to substitute data. Simply we can see the S-box as a lookup table. The way to substitute bytes for the block is like each block has 8-bit data, and we can see the first 4-bit as row index and the last 4-bit as column index, using these row and column indexes we can get the value from the S-box.

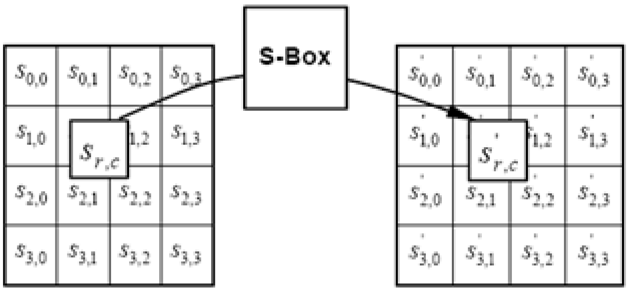


Figure 2:Process Of SubBytes

2. ShiftRows: In this operation, each row of the state is cyclically shifted to the left, depending on the row index. The 1st row is shifted 0 positions to the left and the 2nd row is shifted 1 position to the left. The 3rd row is shifted 2 positions to the left. The 4th row is shifted 3 positions to the left.

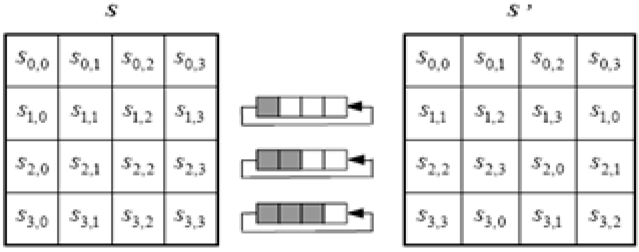


Figure 3:Process Of ShiftRows

3. MixColumns: In the mix column block, considering the state matrix shown above we have to multiply each byte of the state matrix with a predefined modulo number. So, to achieve this, the first thing is to define a multiplier. For example, if we consider x as 8-bit input, we have to generate 2x and 3x output and finally integrate in one module to generate our polynomial.

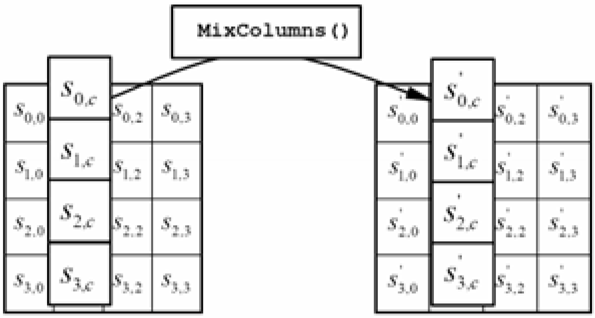


Figure 4:Process Of MixColumns

4. AddRoundKey: In the AddRoundKey() transformation, a Round Key is added to the State by a simple bitwise XOR operation. This is the first step of the AES algorithm and this is simply a XOR operation. We have 128-bit length plaintext and 128-bit length key so XOR operates bit by bit. The matrix of 16 bytes is considered as 128 bits and XORed to 128 bits of the round key. If the last round is this, then output is 128 bits of Encrypted output. Otherwise, these 128 bits will go to a similar round considering 16 bytes again.

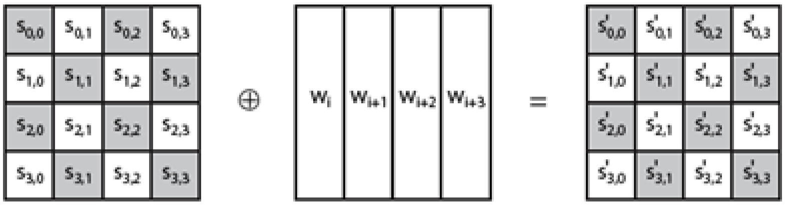


Figure 5:Process Of AddRoundKey

5. Key Expansion: The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words. Each round uses 4 linear arraywords Each word contains 32 bytes which means each sub-key is 128 bits long. Pseudo code for generating the expanded key from the original key. The key is copied into the first four words of the expanded key.

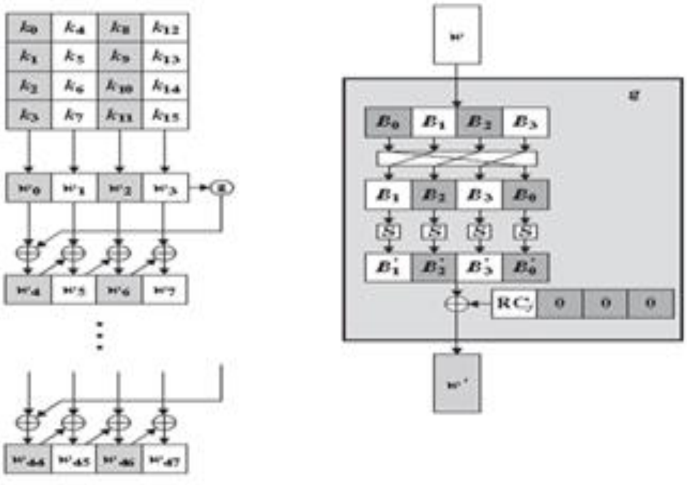


Figure 6:Process Of Key Expansion

IV. RESULT AND DISCUSSION

In this code, we develop a behavioral level using the Verilog and VHDL programming languages within theVivado software environment. The Reset is asserted (active high), and all signals are assigned to zero.The designed AES Security Algorithm has multiple sub-modules inside it, the Encryption end, based on the internal operations of the algorithm. The top module is designed, simulated, and synthesized as per the proposed algorithm. Now presenting the results of simulation.

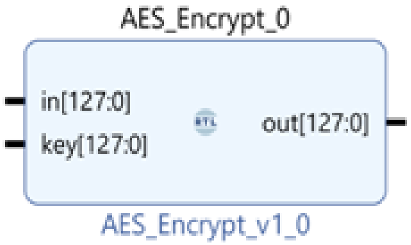


Figure 7: RTL Block diagram of AES Encryption Algorithm

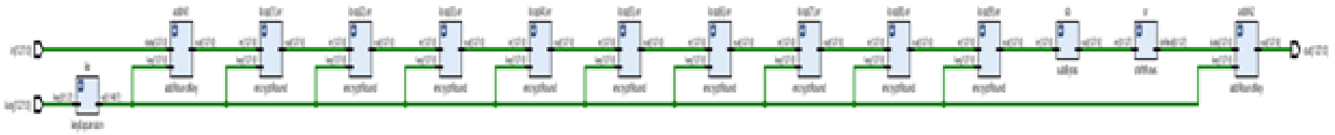
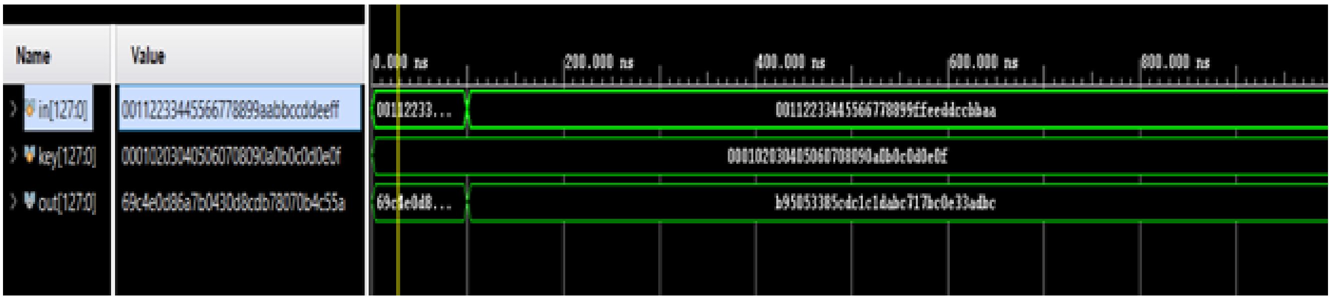


Figure 8: RTL Schematic diagram of AES Encryption Algorithm

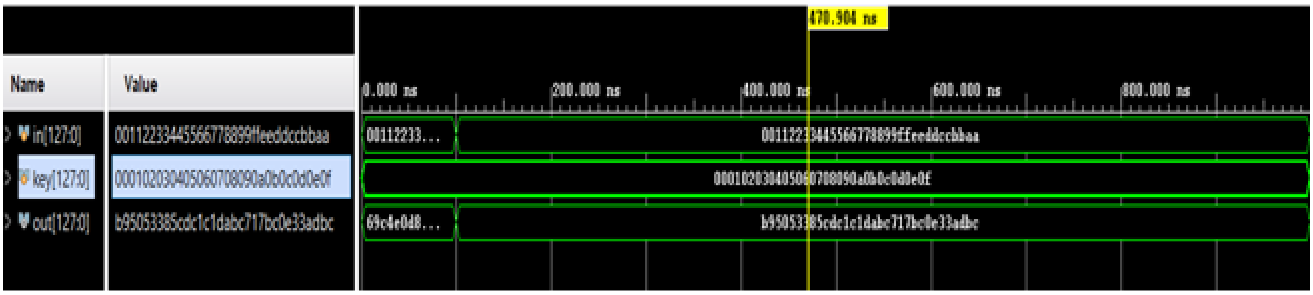
By using the Vivado software environment, the data is then encrypted with a secure key and generated cipher form of data. Showing the stimulation with two inputs of Figure8 and Figure9.



Name	Value
in[127:0]	00112233445566778899aabbccddeeff
key[127:0]	000102030405060708090a0b0c0d0e0f
out[127:0]	69c4e0d86a7b0430d8cdb78070b4c55a

0.000 ns
200.000 ns
400.000 ns
600.000 ns
800.000 ns
00112233...
00112233445566778899ffeeddccbbaa
000102030405060708090a0b0c0d0e0f
69c4e0d8...
b95053385cdc1c1dabc717bc0e33adbc

Figure 9: The plain text = 00112233445566778899aabbccddeeff is encrypted with a secure key and the cipher text = 69c4e0d86a7b0430d8cdb78070b4c55a.



Name	Value
in[127:0]	00112233445566778899ffeeddccbbaa
key[127:0]	000102030405060708090a0b0c0d0e0f
out[127:0]	b95053385cdc1c1dabc717bc0e33adbc

470.904 ns
0.000 ns
200.000 ns
400.000 ns
600.000 ns
800.000 ns
00112233...
00112233445566778899ffeeddccbbaa
000102030405060708090a0b0c0d0e0f
69c4e0d8...
b95053385cdc1c1dabc717bc0e33adbc

Figure 10: The plain text = 00112233445566778899ffeeddccbbaa is encrypted with a secure key and the cipher text = b95053385cdc1c1dabc717bc0e33adbc.

Sr No.	Parameters	Existing Method	Proposed Method
1	Software	Xilinx 14.1	Vivado 23.1
2	Methodology used	Non-pipelines	Pipelined
3	Area	23%	21%
4	Delay	52.8 ns for 11 clock cycles	41.194ns
5	Total Power	We are not considering the power so we see the delay	2.664 milli watts

Table: Result from comparison of the Proposed method with the Existing method

V. CONCLUSION

In Conclusion, Utilizing the Vivado software gives an advantage in showing the power consumption,area, and delay of the system. It is considered secure, efficient, and reliable, making it an ideal choice for securing sensitive and confidential information.the AES algorithm offers a balance between security and efficiency, making it suitable for implementation in hardware. While it may consume moderate area and power, its low latency ensures swift encryptionprocesses, which are essential for real-time applications. Additionally, advancements in hardware design and optimization techniques continue to enhance its performance, making AES a reliable choice for secure communication and data protection in modern computing systems.

VI. REFERENCES

[1]. “Design AES Algorithm based secured data Encryption system using Verilog “Aruna B Gowda, Dr Naveen,Journal of Fundamental & Comparative Research Vol. VII, No. 10(I).

[2]. “VLSI Design of Advanced-Features AES Cryptoprocessor in the Framework of the European Processor Initiative” P. Nannipieri, S. D. Matteo, L. Baldanzi, L. Crocetti, L. Zulberti, S. Saponara, L. Fanucci, IEEE Transactions on VLSI Systems, Vol. 30, No. 2 (2022).

[3]. “Implementation of an AES-based Real-time Video Encryption/Decryption using FPGA/HPS “ A. Maache, A. Touati, A. Ouali, Proceedings of the 19th International Multi-Conference on Systems, Signals & Devices(2022).

[4]. “ Design and Analysis of Modified S-Box Based AES Security Algorithm for IOT Application” Lalan Kumar Jha, Dr.Anshuj Jain, JETIR Volume 8, Issue 1 (2021).

Authors Biography

Ms. E. Devisri currently serves as an Assistant Professor in theDepartmentof Electronics and Communication Engineering at Annamacharya Institute of Technology and Sciences, Tirupati.

Ms. V. UshaSri is studying4th-yearB.Tech degree in the ECE department at Annamacharya Institute of Technology and Sciences, Tirupati. Herinterest areas are Electronics.

Mr. G. Venkatramanan is studying 4th year B.Tech degree in the ECE department at Annamacharya Institute of Technology and Sciences, Tirupati. His interest areas are Electronics.

Ms. N. Madhuri is studying 4th year B.Tech degree in the ECE department at Annamacharya Institute of Technology and Sciences, Tirupati.Herinterest areas are Electronics.

Mr. B. Govardhana is studying 4th year of a B.Tech degree in the ECE department at Annamacharya Institute of Technology and Sciences, Tirupati. His interest areas are Electronics.