IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 12, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.317

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

A Reliable Approach to Secure Data Using Cryptosystems

K.Naga Divya Bhargavi[1], Ch.Sri Naga Chandrika[2], D.N.V.D.V.Prasad[3], R.William Raju[4], B.Poojitha[5]

Assistant Professor, Dept of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India[1]

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India [2]

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India [3]

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India [4]

U.G. Student, Department of ECE, Sri Vasavi Institute of Engineering & Technology, Nandamuru, A.P, India [5]

ABSTRACT: Now a days it is very important to protect the data and to provide the security for the data in the IoT systems.There is a high demand for hardware-based cryptography methods to safeguard the security and privacy of IoT systems. But like software-based security measures, hardware-based ones can be targeted by malware, a subset of harmful code. In this paper, we employed hardware-based self-applied cryptography to safeguard the IoT systems for data security.We have created a self-implemented IP core that serves as SDRAM memory and 128-bit AES co-processors. The Internet of Things (IoT) is one of the most significant contemporary technologies that, in recent years, has drawn interest from the most intriguing sectors of life, including the industrial, academic, and other ones. The major objective is to create a seamless ecosystem that unifies the physical and digital worlds, ushering in a new era for the Internet. Due to the numerous potential it offers in a variety of applications, including those in the energy, health, and other sectors, this technology has a high commercial value to businesses.

KEYWORDS:AES 128- bits, Xilinx

I. INTRODUCTION

These days, the word IoT refers to massive systems with multiple functions that connect to a network and include sensors, electronics, and control systems. The Internet of Things (IoT) today refers to a collection of interconnected people and objects that may communicate with one another without the need for human involvement. IoT systems significantly alter and advance both peoples' daily lives and corporate sectors. With top-notch services like smart homes, smart cities, health care, and transportation, IoT transforms how we work and learn. Additionally, developments like data management, self-management systems, and industrial production automation have aided the expansion of the commercial economy.

IoT systems include excellent gadgets, and it is expected that by 2020, 30.73 billion of them will be connected. After that, the number of connected items is expected to double. IoT devices are linked to and exchange data through the Internet, which is seen as a global public space. Due to publicity, the Internet has various security flaws that make connected devices more susceptible to assaults such man-in-the-middle attacks and those that use spoofed, manipulated, or replayed routing information. In recent years, there has been a significant effort made to address security concerns in the IoT paradigm. A blockchain-based framework for industrial IoT systems was proposed by Bahga et al.oT systems include excellent gadgets, and it is expected that by 2020, 30.73 billion of them will be connected. After that, the number of connected items is expected to double.

There are many physical devices in the IoT system, including sensors and actuators, and because they are so accessible, it is very easy for them to be the subject of attacks like data forgery or command injection from unauthorised sources. Additionally, because IoT systems have limited CPU and storage capacity and cannot even be software installed, utilising software alone to secure them is insufficient. Additionally, security software may contain

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

harmful software, or malware, that can damage equipment or even switch the entire system into a privileged state under the control of the attacker.

II. METHODOLOGY

The Key Expansion, Cipher, and Inverse Cipher are the three primary components of the AES algorithm. The Cipher and Inverse Cipher technique uses a Key Schedule created by the Key Expansion. The Cipher transforms data into ciphertext, an unreadable form, whereas the Inverse Cipher transforms ciphertext back into the original data, known as plaintext.

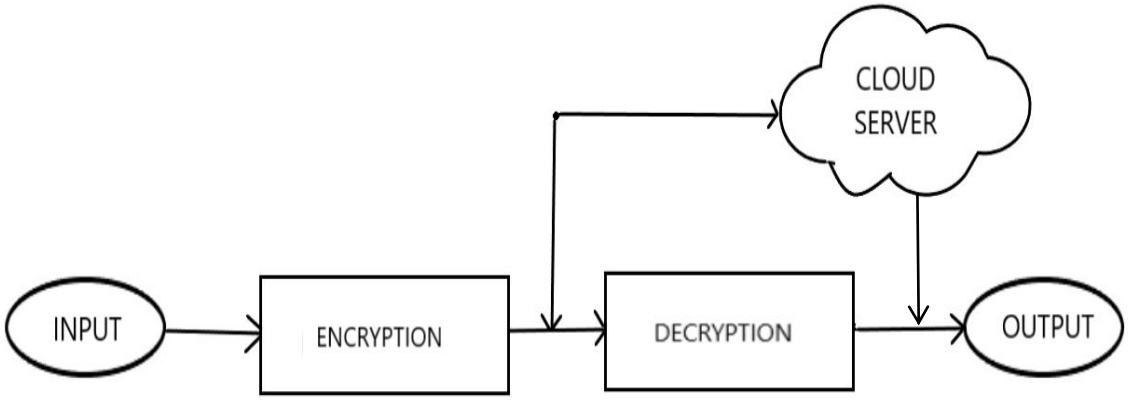


Fig.1 Block Diagram of Cryptography Process

Let us consider the input as the alphabetic, numerical or any information consisting of 128 bytes. This 128 bytes data is given as the input to the encryption block

Encrypion & Decryption:

Encryption: The encryption is the process of converting original data into confidential data. It can provide high security to the original data. The encryption consists of four steps for encrypting the given input data. They are as follows

1. Sub byte
2. Shift row
3. Mix column
4. Add round key

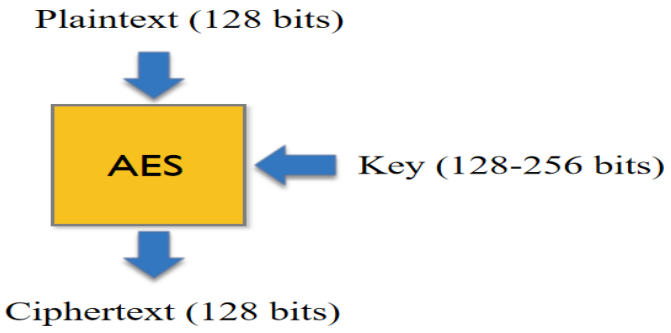


Fig: Architecture of AES Algorithm

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

- Sub-byte: The Sub Byte transformation uses an S-box table to do a nonlinear byte replacement separately on each byte of the State. S-box table has 256 numbers in it (from 0 to 255).The sub-byte transform is used to convert the original input data into the matrix form.The input given data is converted into the hexa decimal form and the hexa decimal formed data is arranged into the 4*4 matrix

- Shift Rows: The rows of the State are cyclically left-shifted over various offsets when using the ShiftRows transformation.The specific factors that determine the offset includethe row's r-index determines the order of the row, to put it another way. Rows 0 and 1 are not moved, but rows 2 and 3 are shifted two bytes to the left and three bytes to the left, respectively.

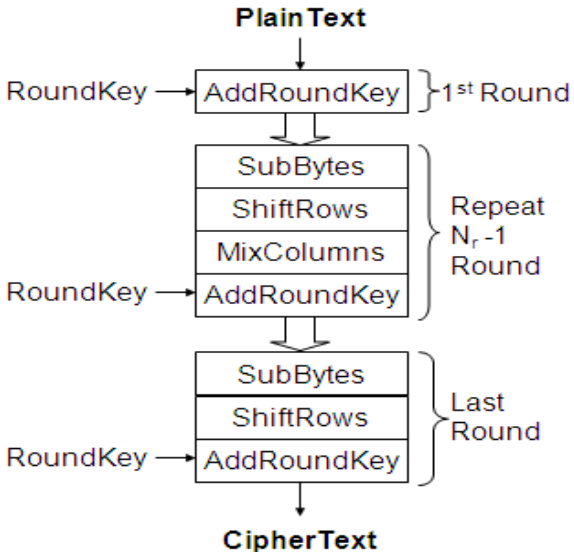


Fig: Encryption

- Mix columns: By considering each column as a four-term polynomial, the Mix Columns transformation operates on the State column by column.
- Add Round Key: One of the subkeys is used in an operation on the State during the Add Round Key phase. Each byte of the State and each byte of the subkey are simply XORed together.

The initial round, middle round, and final round are the three high-level processes that make up the encryption and decryption process.There is only the AddRoundKey operation available in the First round step.SubByte, ShiftRow, MixColumn, and AddRoundKey are the sequence operations that make up the middle round step. SubByte, ShiftRow, and AddRoundKey are the last three operations carried out in the last round stage.

As a result, the encryption and decryption processes will produce ciphertext or plain text, respectively, after 10 cycles.Nevertheless, three more inverse operations—InvSubByte, InvShiftRow, and InvMixColumn—are used during the decryption process in addition to SubByte, ShiftRow, and MixColumn. Moreover, encryption inverts the direction of this process. The decryption steps of the Middle Round are InvShiftRow, InvSubByte, AddRoundKey, and InvMixColumn.

When a 128-bit key sequence enters the Key Expansion process and generates 10 subkeys for 10 AES rounds, encryption or decryption starts. the Key Expansion process's main timetable. The four fundamental operations used in this procedure are RotWord, SubWord, XOR Rcon, and XOR.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

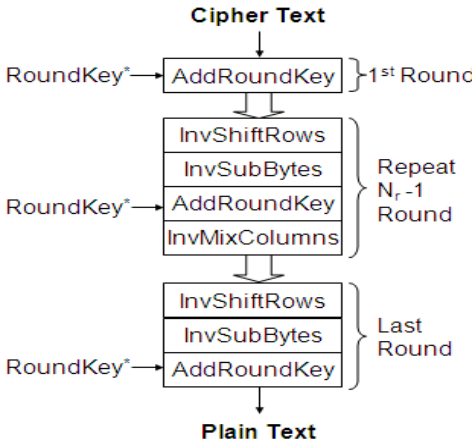


Fig: Decryption

- RotWord: RotWord is a shift operation that rotates (or circular shifts) 32-bit words [a0, a1, a2, a3] and produces newwords [a1, a2, a3, a0].
- SubWord: This operation inputs a word and a substitute for each byte in accordance with the substitution table (S-Box).
- RCon: The round contants for round I of the key expansion are 32-bit words with the form [rconi, 0, 0, 0], where the bits of rci = xi1 are regarded as the coefficients of a finite field element GF(2)[x]/(x8+x4+x3+x+1).

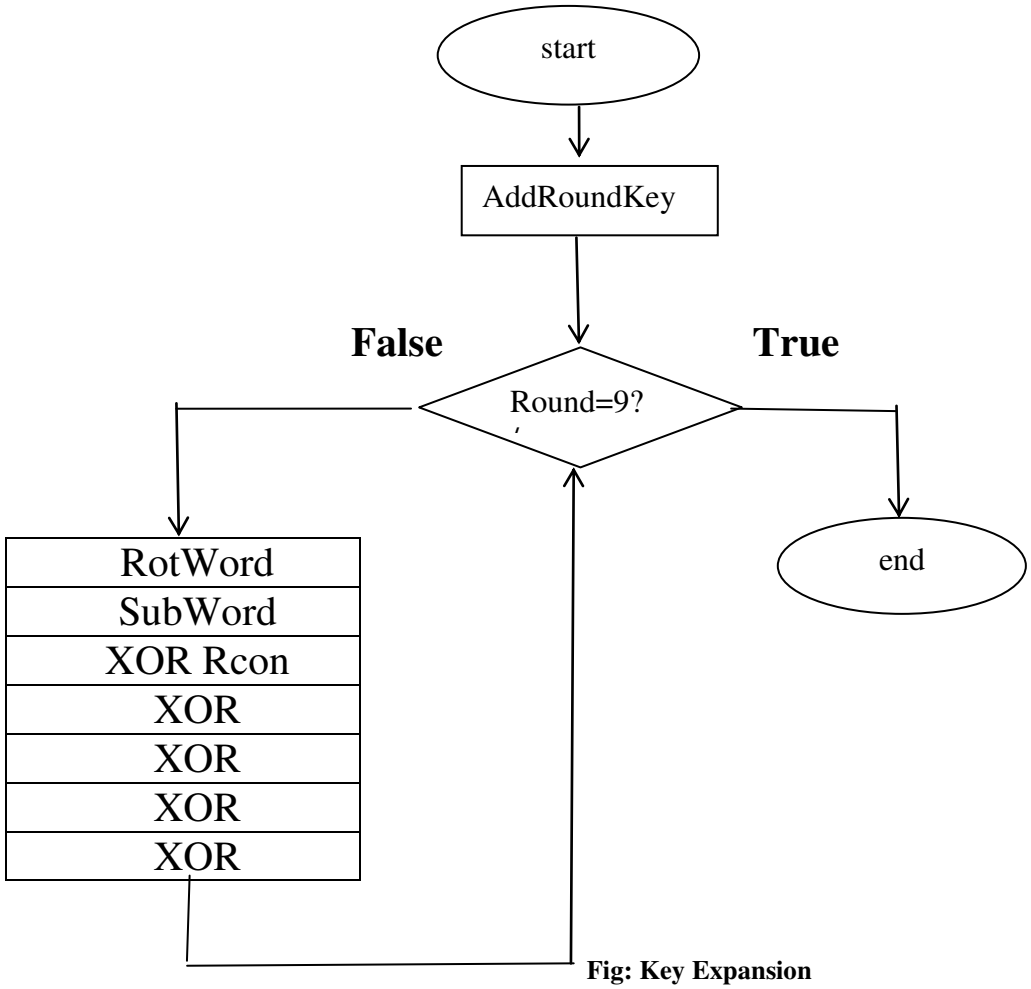


Fig: Key Expansion

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

III. SYNTHESIS & IMPLEMENT DESIGN

. The data utilised for simulation are:

- Secret key: 61626364656667686162636465666768HEX.
- Plaintext: 2067616e677320617265HEX, 507269736f6e.
- ciphertext: e7e4e1139e95ebe58caf23960a813f41HEX .

In the encryption process, Figure 6a, the input data isplaintext, and output data is ciphertext. throughout the decryptionthe output of the operation is plaintext while the input data is ciphertext,illustrated in Figure 6b. Using simulation techniques, wecan verify that the AES IP core can convert ciphertext toplaintext by the encryption, and it can convert ciphertext backto plaintext via the decoding process precisely.. Through thesimulation procedure, we have proved the function ofencryption and decoding of our IP is proper. Also, the outcomes of our simulation are contrasted with those producedby dependable software.

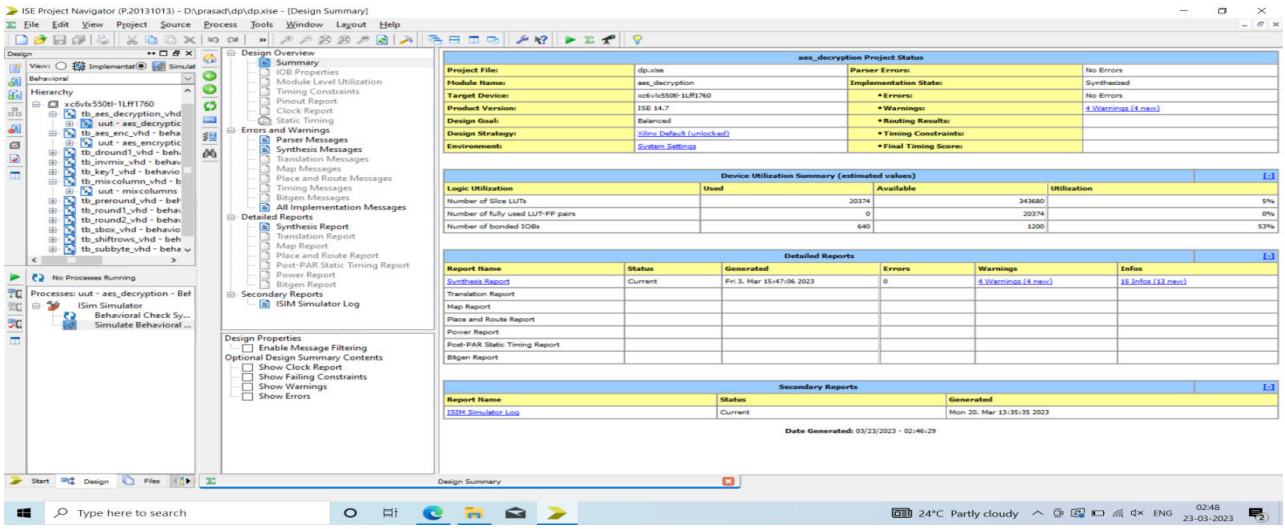


Fig: Project Navigator

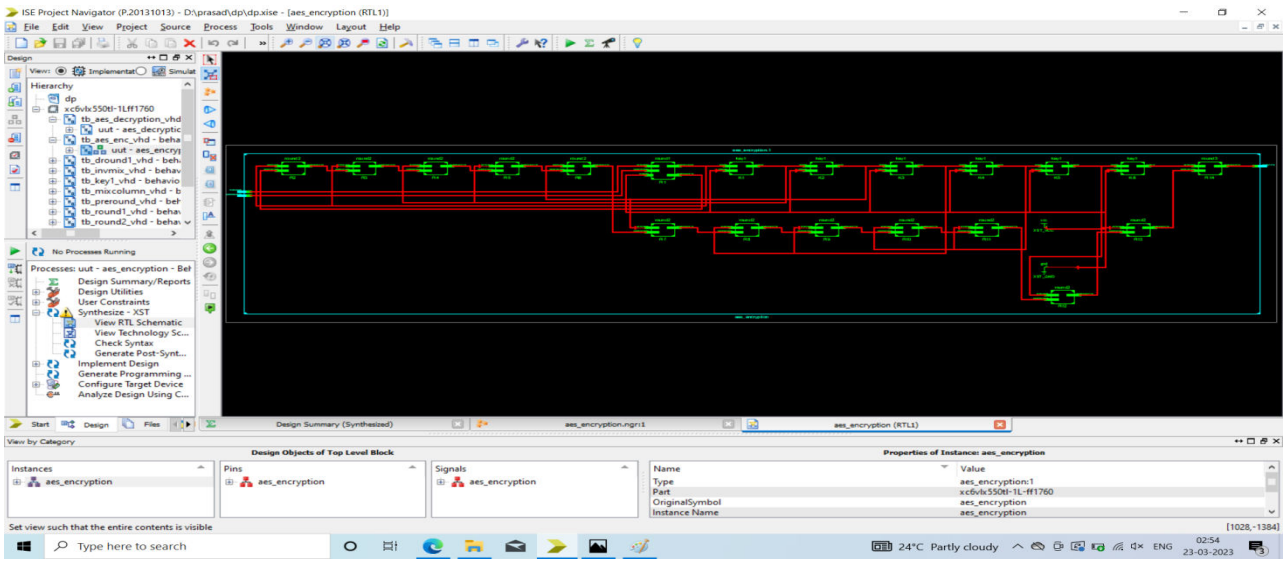


Fig:RTL Schematic of Encryption

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

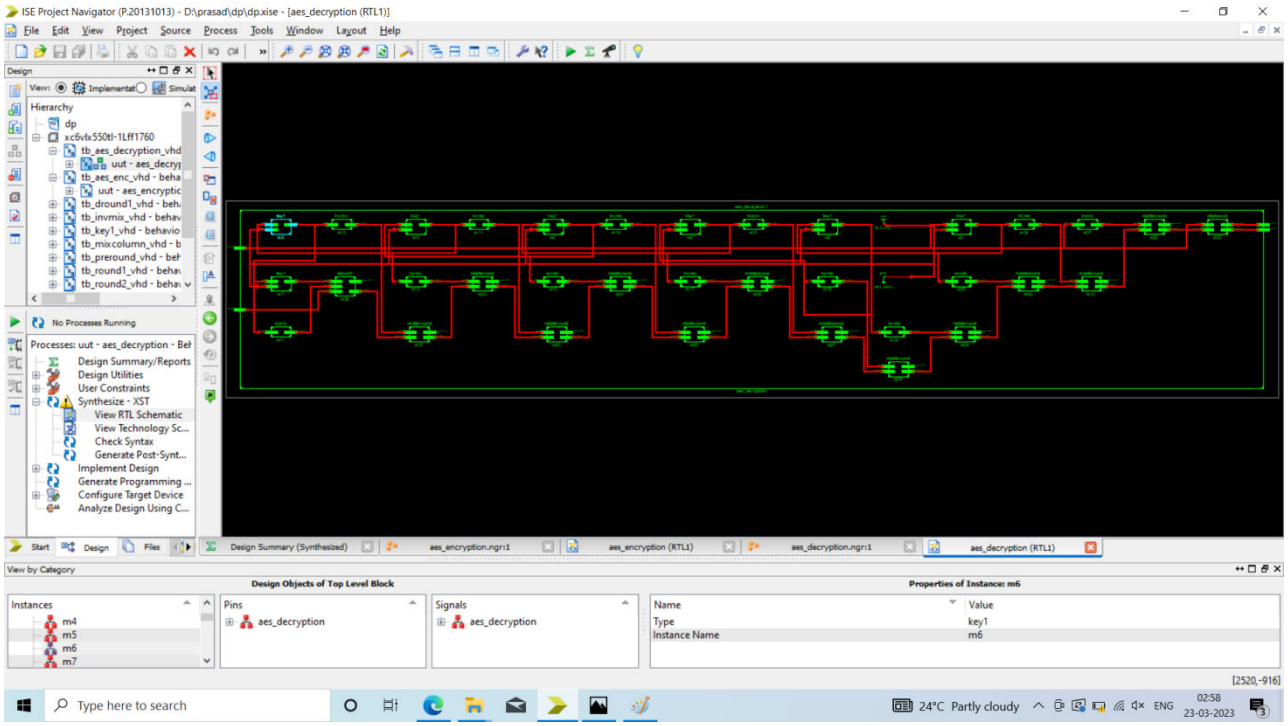


Fig:RTL Schematic of Decryption

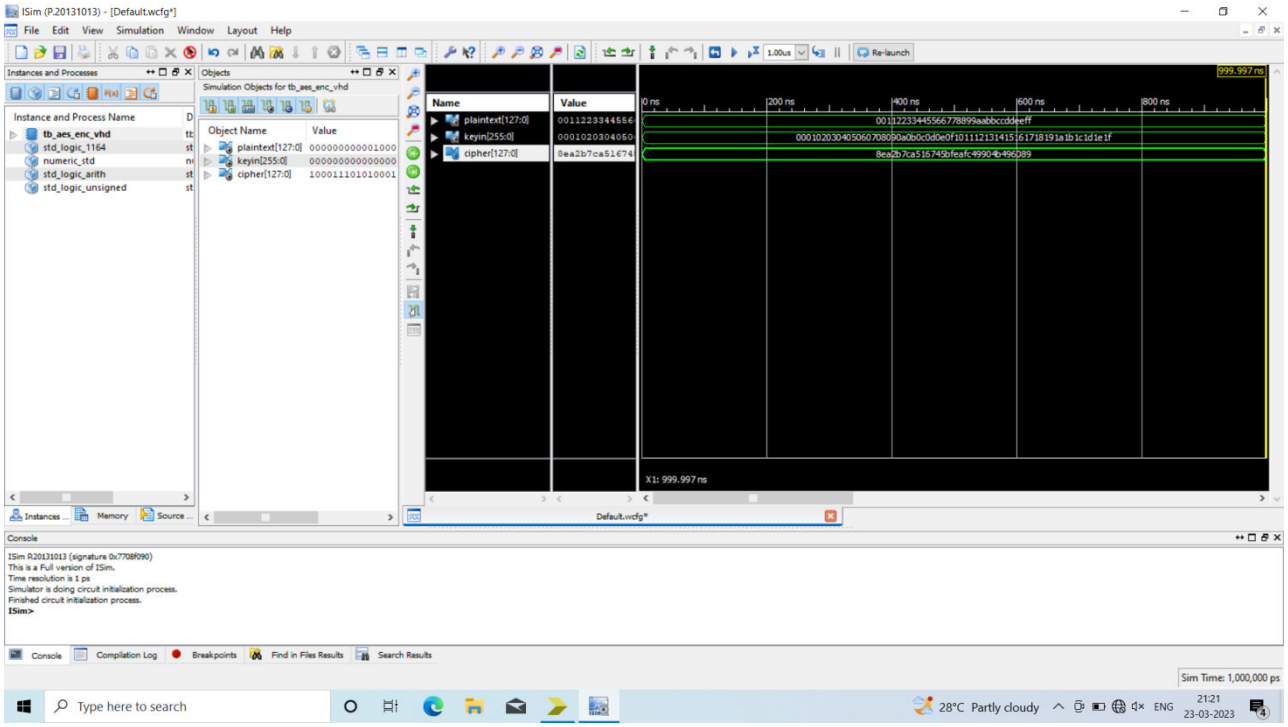


Fig:Simulation output of encryption of data

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204007 |

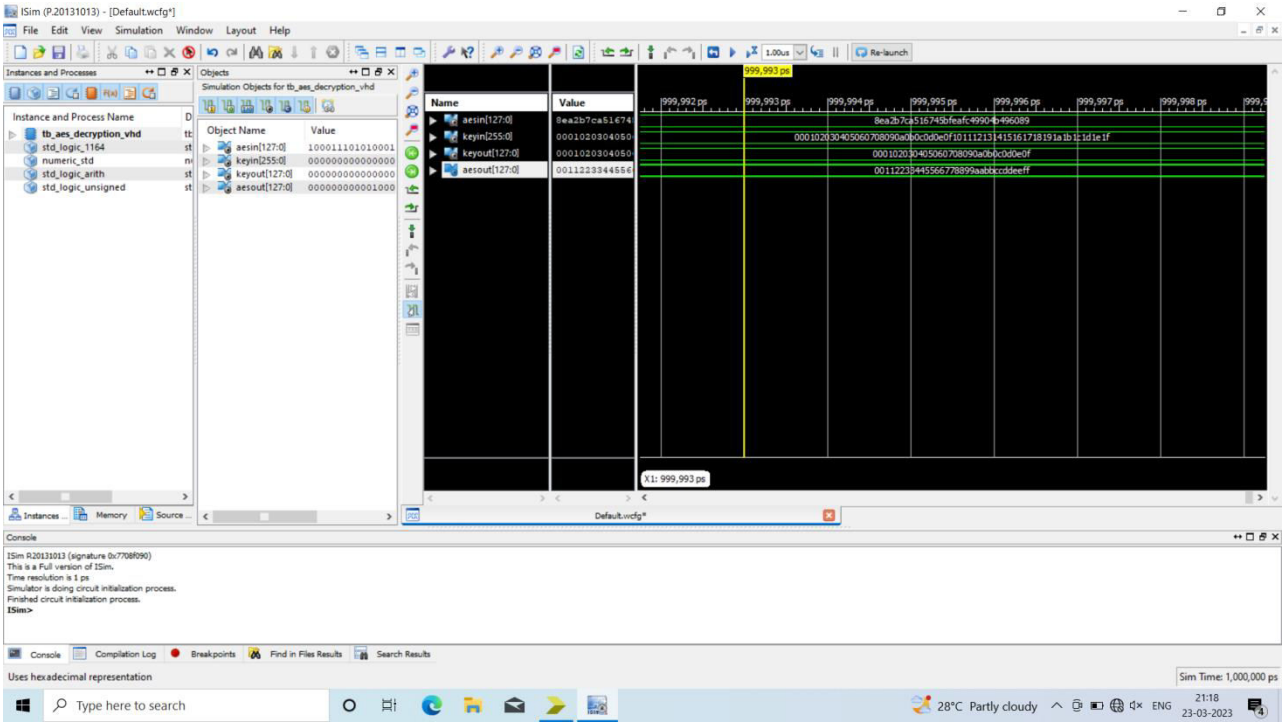


Fig: Simulation output of Decryption of data

IV. CONCLUSION

In this research, we have developed a SoC-based cryptosystem.FPGA systems to deliver a compact yet high-performancegadget that may handle the cryptographic activities of Iosystems. HPS and FPGA are the two main components of our system. Onthe FPGA side, we totally self-implemented an IP coreAES-128 is used for symmetric cryptography. On the HPSIn addition, we created a unique Linux kernel and drivers to manageand handle the hardware system. By our labour, we haveevaluated some cryptography implementation algorithms and methods for fast processing, such as custom memory modules, the Pipeline, and DMAtechniques low power consumption, and great performance hence it is appropriate for IoT systems' gateway devices or node controllers.

REFERENCES

[1] Lu, Yang, and Li Da Xu. "Internet of things (iot) cybersecurity research: A review of current research topics." *IEEE Internet of Things Journal* 6.2 (2018): 2103-2115.

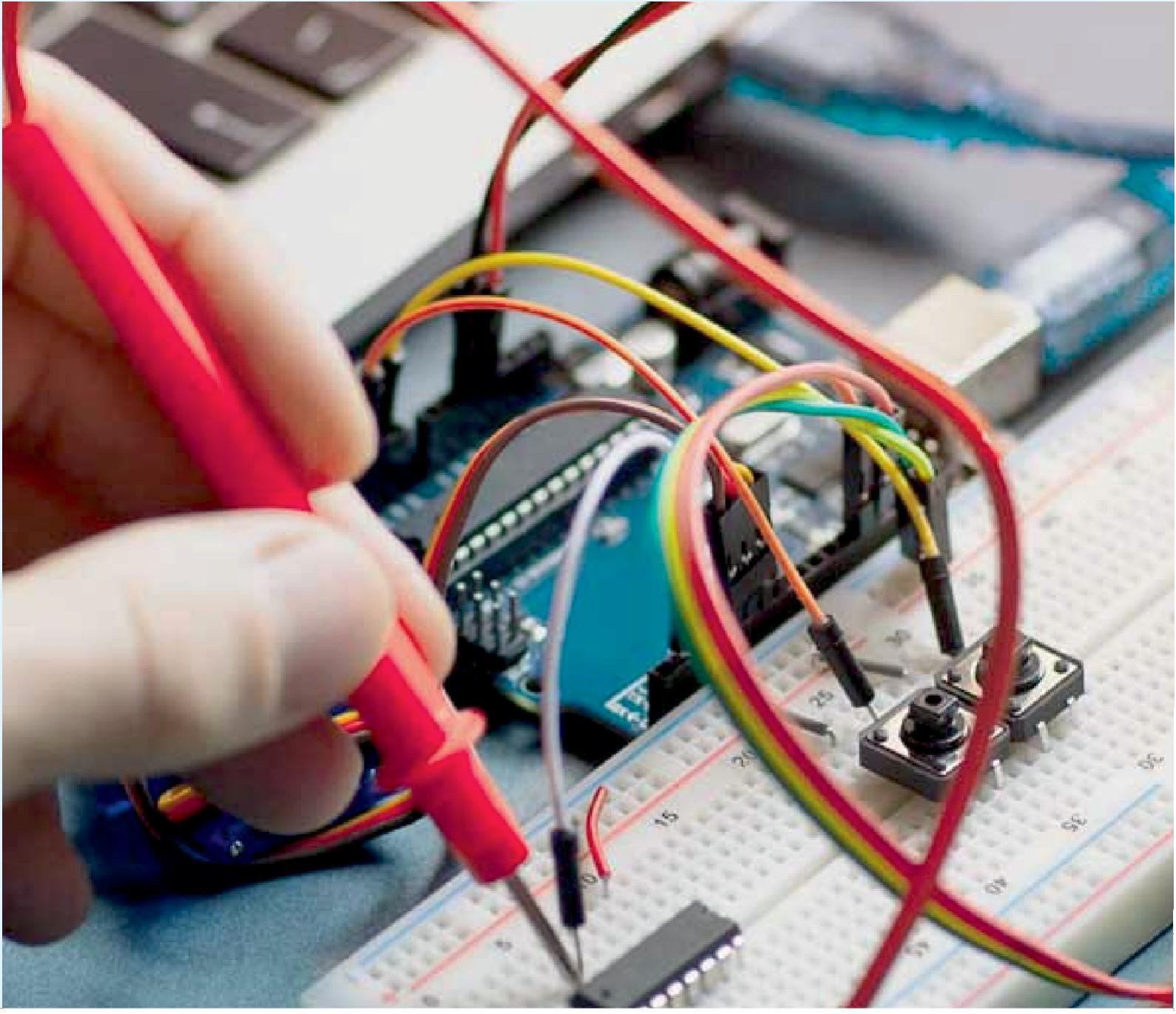
[2] Bahga, Arshdeep, and Vijay K. Madisetti. "Blockchain platform for industrial internet of things." *Journal of Software Engineering and Applications* 9.10 (2016): 533-546.

[3] Hu, Pengfei, et al. "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet
of things." *IEEE Internet of Things Journal* 4.5 (2017): 1143-1155.

[4] Zhang, Jiale, et al. "Data security and privacy-preserving in edge computing paradigm: Survey and open issues." *IEEE Access* 6 (2018): 18209-18237

[5]Xiao, Liang, et al. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." *IEEE Signal Processing Magazine* 35.5 (2018): 41-49

[6] Milosevic, Jelena, Francesco Regazzoni, and Miroslaw Malek. "Malware threats and solutions for trustworthy mobile systems design." *Hardware Security and Trust.* Springer, Cham, 2017. 149-167.



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.317

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details