Hardware Implementation of a Hybrid data encryption algorithm using AES and Blowfish for IoT devices

Arya Tripathi
Department of Electronics and Communications Engineering, Institute of Technology, Nirma University. Ahmedabad, Gujarat, India – 382481

20BEC130@nirmauni.ac.in

Yash Purohit
Department of Electronics and Communications Engineering, Institute of Technology, Nirma University. Ahmedabad, Gujarat, India – 382481

20BEC137@nirmauni.ac.in

***Abstract* – The scope of this paper revolves around the hardware implementation of a hybrid symmetric data encryption algorithm that uses 128-bit, 10 round AES and 64-bit, 16 round Blowfish encryption techniques to convert 128-bit plain information into 128-bit cipher. The goal is to utilize the advantages offered by both AES and Blowfish algorithms like the former is more secure and can be used in wide applications whereas the latter is faster. Hardware Implementation of the hybrid algorithm on FPGA has been carried out and the same was simulated to derive the advantages as well as limitations offered by the same.**

Keywords – AES, Blowfish, cipher, encryption, substitution box, Feistel structure, Rijndael, Verilog HDL.

I. INTRODUCTION

Data encryption refers to transforming a data from plain text to ciphertext. The encrypted data and decrypted data can only be accessed by encryption key and decryption key respectively. Data encryption is done to provide data security and protect the data against unauthorized access and man in the middle attacks. Data encryption can be either software or hardware based, the latter is considered safer than the previous one. Many symmetric and asymmetric algorithms are used for data encryption and decryption.

AES and Blowfish are two such algorithms. Both of them are symmetric encryption techniques. Performance analysis shows that the Blowfish algorithm is faster than most of the other algorithms. It is one of the most power and processing time efficient techniques. It is used in many applications such as backup software, E-mail encryption tool and password management tools.

On the other hand, AES is one of the most secure algorithm techniques used in government computer security and electronic data protection. Though AES is secure, it can still be improved to avoid the attacks that can occur due to the vulnerability of its S-Box. Hybrid algorithms are used to overcome the limitations of Cryptographic algorithms. A hybrid of AES and Blowfish Algorithms has been discussed in this paper. Both of the algorithms combined together provides a better throughput than individual implementation of AES and Blowfish Algorithms.

II. AES ALGORITHM

Advanced Encryption Standard (AES) or Rijndael is a symmetric key cryptographic algorithm developed by National Institute of Standards and Technology in the year 2001 to protect classified information which was implemented on both hardware as well software throughout the world. AES is a symmetric block cipher technique. The size of the plain and the cipher text is the same. Since it is a private key encryption technique, only a single key can encrypt and decrypt the data. AES is very much in application today as it has enhanced strength as compared to both DES and 3DES despite being harder to implement.

A. *Features of AES Algorithm:*

1) Block size : 128, 192, 256 bits
2) Key Size : 128, 192, 256 bits
3) No. of Rounds : 10 (9 with mix columns)
4) No. of S-Boxes : 1 (maps 8-bit input to 8-bit output)

B. *AES Structure and Working:*

First of all, AES converts the block of 128-bit data in the form of a 4x4 matrix of bytes. All the operations are then carried out in matrix form and the intermediate outputs are stored in the form of state matrix. The plain data is taken as an input and passed through a pre-round transformation block where it is simply XORed with the 128-bit Key. This output now goes to the input of the first round where the data goes through the following for steps:

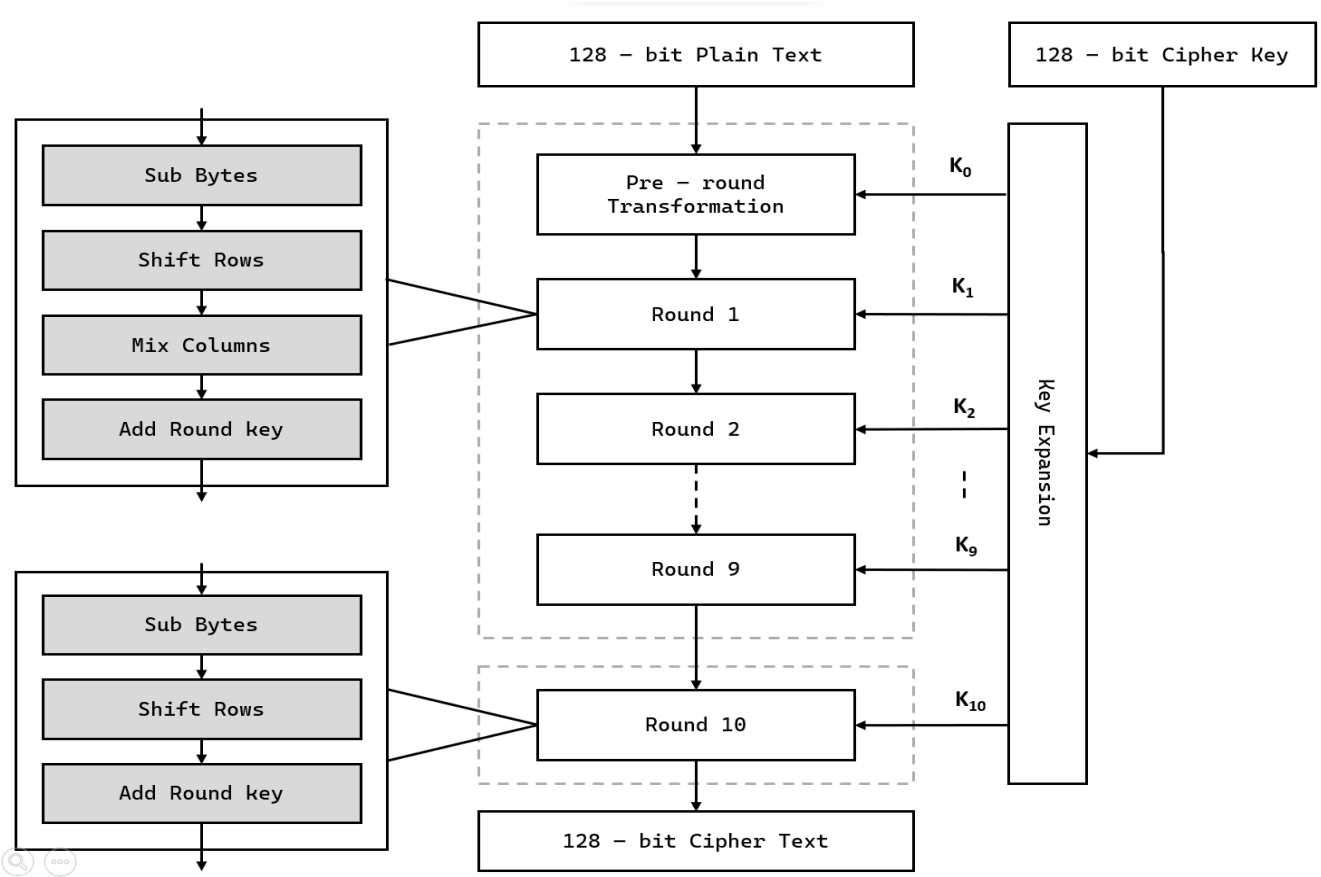

Fig. 1 AES : Flow of Algorithm

1) Substitution bytes: A predefined S-Box is used as a look table where the bytes are mapped according to their values. The data stored in the matrix is in Hexadecimal form, The first digit corresponds to the row and next corresponds to the column number. These rows and columns serve as indexes into the S-Box to select a unique byte.

2) Shift Row Operation: There is a cyclic left shift of the row elements. The first row is shifted by 0 bytes, the next row is shifted by 1 byte, the third row is shifted by 2 bytes and the last row is shifted by 3 bytes.

3) Mix Columns: Every Column of the state array is multiplied by a constant matrix and the new column matrix obtained replaces the original one.

4) Add Round Key: The state matrix obtained now is XORed with the 128 bits of the respective round key obtained through key expansion.

These steps remain the same till the 9th round. In the last round, the Mix Column step is discarded.

C. Key Expansion:

There are a total of 11 sub keys, one for the pre round transformation and the remaining ones for the next 10 rounds. The first key K0 is expanded through a series of steps and the key for next round K1 is obtained. This follows till the next round.

The last Column of the previous key is cyclically shifted by 1 byte (RotWord), bytes of which are then substituted by mapping with the AES S-Box (SubWord) and finally the SubWord is XORed with a round constant.

Column 1 of the new round is obtained by XORing the obtained column with the first column of the previous round. Column 2 is obtained by XORing column 1 with the second column of the previous round.

Column 3 obtained by XORing column 2 with the third column of the previous round and column 4 of the new round is obtained by XORing column 3 with the fourth column of the previous round. Thus, each round key has its new key obtained from the previous key.

III. BLOWFISH ALGORITHM

Blowfish encryption and decryption technique, developed by Bruce Schneier in 1993 is a 64-bit block size and variable key length ciphering method, which happens to be an alternative to the DES (Data Encryption Standard) technique as it provides enhanced encryption rate and improved speed as compared to DES and 3DES. Its variable key length of maximum 446 bits enables high security layers and hence it becomes difficult to crack. Till date no deciphering or cryptanalysis method for Blowfish has been found.

A. *Features of Blowfish Algorithm:*

1) Block size : 64 bits
2) Key Size : 32 – 446 bits (variable size).
3) No. of Subkeys : 18 (16 for each round and 2 for post processing)
4) No. of Rounds : 16
5) No. of S-Boxes : 4 (each with 256 entries of 32 bits)
6) Structure : Feistel Network

B. *Blowfish Structure:*

Blowfish Algorithm encrypts the data in the series iterations of 16 rounds and each requires a sub-key (here, 32-bit) which is used in both encryption and decryption. After the 16 rounds, the final post processing generates the 64-bit cipher text utilizing 2 sub-keys.

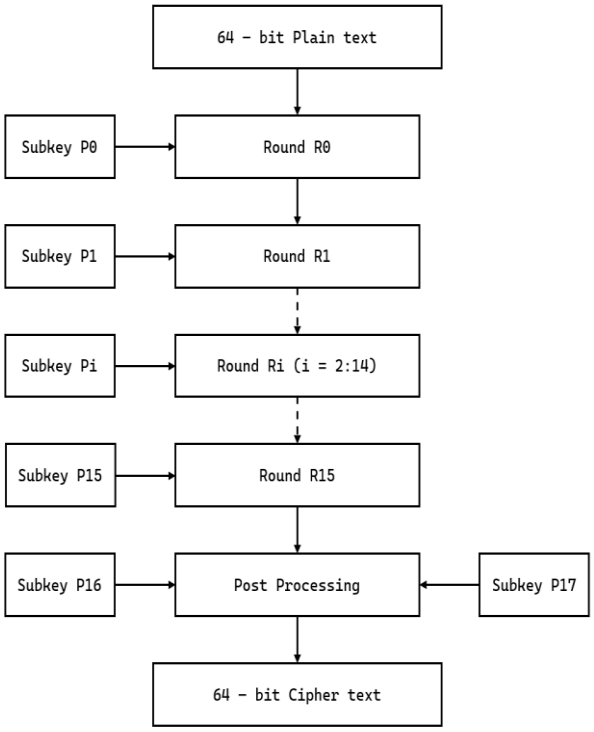

Fig. 2 Blowfish : Flow of Algorithm

C. *Rounds:*

Each round in the Blowfish Structure divides the input into 32-bit higher and lower double words. The higher double-word (X_L) is XORed with the subkey of the respective round and the result is fed into the Feistel function, the output of which is again XORed with the lower double-word (X_R) and is fed into the higher 32-bit double word of the round's output. The lower 32-bit double word of the output is simply equal to the higher double-word (X_L) of input.

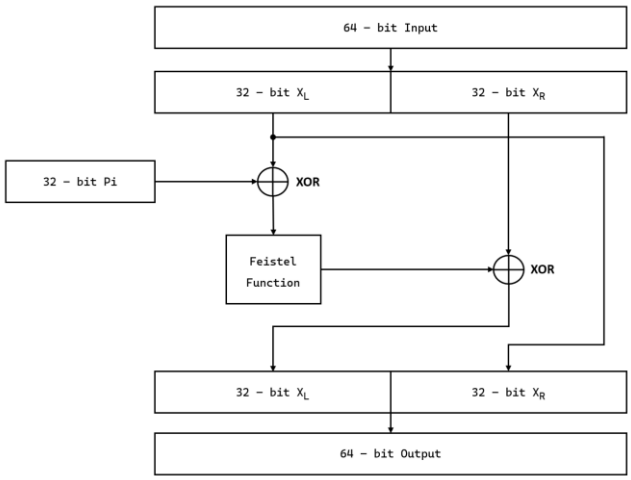

Fig. 3 Blowfish : Flow Diagram of Round R_i

D. *Feistel Function:*

The 32-bit input is divided into four 8-bit quarters by the Feistel function, which then feeds the quarters into the S-boxes. The S-boxes generate 32-bit output from 8-bit input. The final 32-bit output is created by adding the outputs and XORing them.

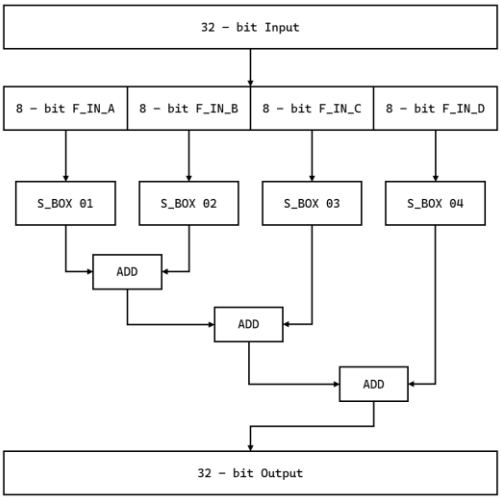

Fig. 4 Blowfish : Feistel Function

E. Key Schedule:

The key schedule of Blowfish starts by initializing the P-Array and the S-Boxes.

1) P – Array:

The P-Array is an 18-element array consisting of the 18 symmetric (private) subkeys, each of 32 – bits, initialized with digits of π, that are required in the processing and the post-processing rounds. The same array of 18 subkeys is utilized in the decryption process as well.

2) S – Boxes:

Both the encryption and decryption processes require 4 substitution boxes (S-boxes), each of which has 256 entries with a 32-bit length. These are initialized after the P-Array with digits of π. These boxes accept the 8-bit quarter and return a 32-bit double word which is then processed in the Feistel function.

F. Post Processing:

The final post processing block accepts input from the 16th round and swaps the higher and lower 32-bit double words XORing with subkey P17 and P18 respectively, to generate the 64-bit Cipher text.

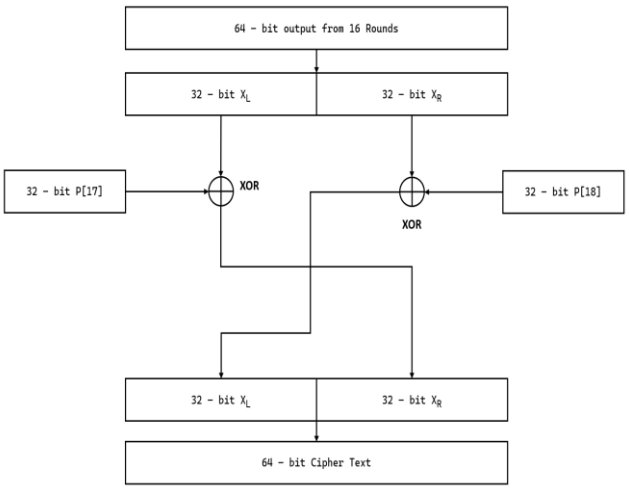

Fig. 5 Blowfish : Post – Processing Block

Blowfish decryption uses the exact same structure and operations. Only difference is that the subkeys are used in the reverse order in the deciphering process.

IV. 2BF – 1AES HYBRID TECHNIQUE

The proposed Hybrid Encryption Method employs a single round of 128-bit AES, 10-round encryption technique and two rounds of 64-bit, 16-round Blowfish encryption to generate a 128-bit cipher text from 128-bit input. The input is firstly fed in the AES block to generate a 128-bit AES cipher and then the upper and lower 64-bit words of generated cipher are fed into the input of separate 64-bit Blowfish blocks. The Blowfish outputs are then combined to generate 128-bit 2BF-1AES cipher text. At the other end, the opposite flow is followed to recover the 128-bit plain text.

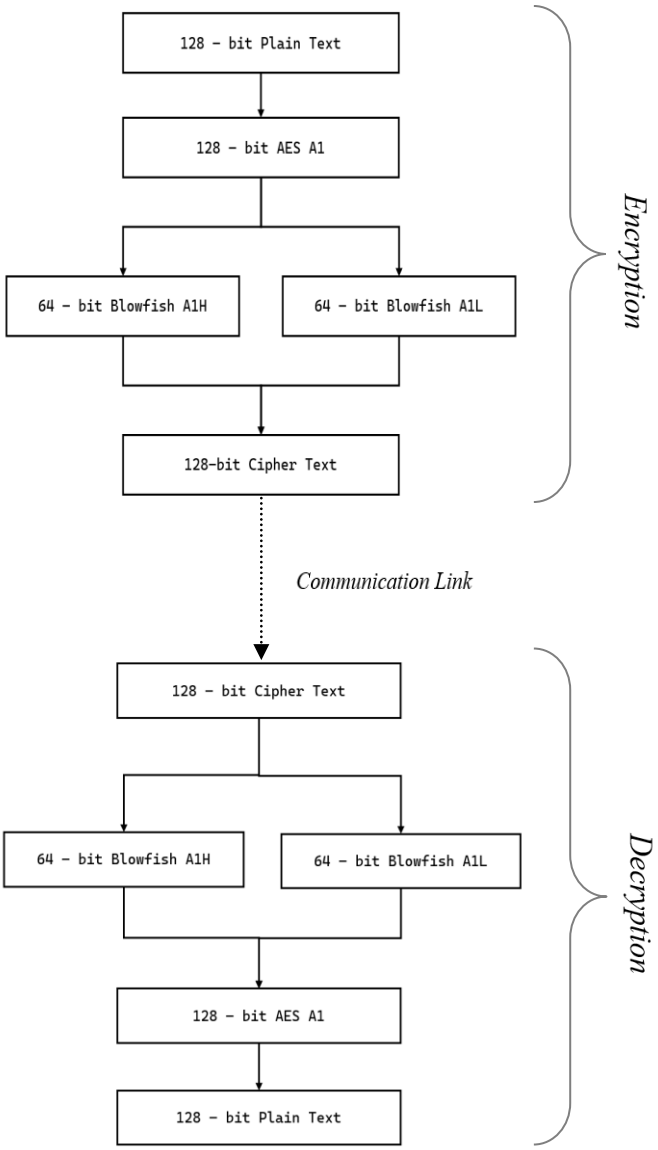

Fig. 6 2BF – 1AES Hybrid Encryption : Flow Diagram

V. Hardware Implementation

To verify and test the functioning of the above algorithm, the same has been modelled using Verilog HDL and implemented on FPGA.

TABLE I
DEVICE AND TOOL SPECIFICATIONS

Device and Tool Specifications	
Device	Cyclone II
Chip Name	EP2C35F672C6
HDL Used	Verilog HDL
Design Tool	Quartus II Web Edition by Intel
Simulation Tool	Modelsim Altera by Mentor Graphics
Modelling Style	Structural Modelling
FPGA Kit	DE2 FPGA Kit by Altera

The implementation has been carried out using Structural Style of Modelling, in which a series of modules as stated below have beem defined for both AES and Blowfish Structures. Both the modules are then combined in the top module HYB_BF_AES which uses the SSD module to drive the seven segment displays.

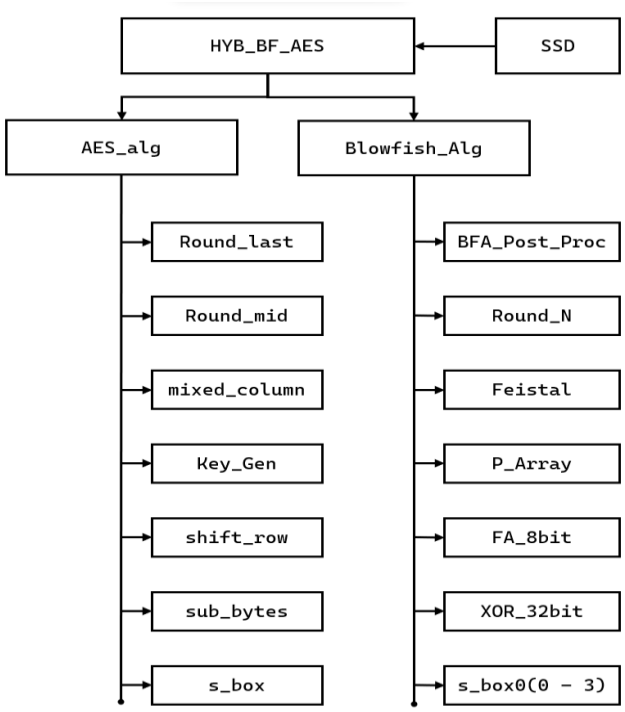

Fig. 7 2BF – 1AES Hybrid Encryption : Structural Modules

VI. Implementation Results

Upon successful implementation of the proposed design using Verilog HDL, it's RTL level diagram as well as RTL simulation have been studied and based on that, the results have been derived. The data and the key have been fed from within the program owing to the limitations of the hardware available.

TABLE II
IMPLEMENTATION RESULTS

Implementation Results	
Logic Elements Used	11 / 33216
Pins Used	59 / 475
Memory Bits Used	0 / 483,840
Build Time	3 minutes 10 seconds

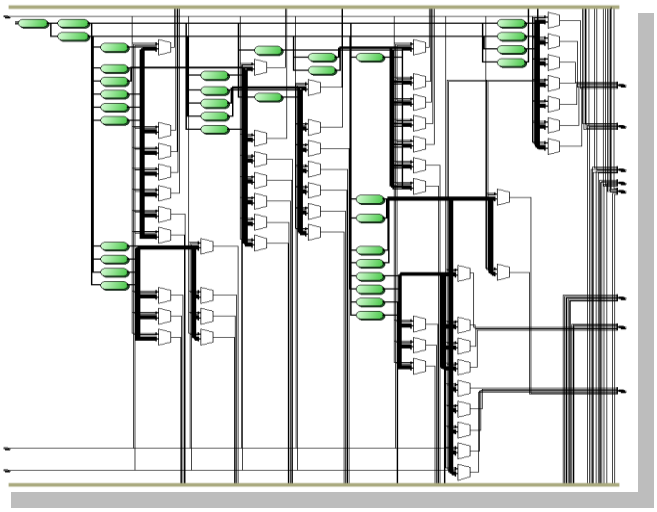

Fig. 8 2BF – 1AES Hybrid Encryption : RTL View

TABLE III
IMPLEMENTATION RESULTS

Simulation Results	
Input Data	00000101_03030707_0F0F1F1F_3F3F7F7F
Input Key	00000000_00000000_00000000_00000000
AES Output	C7D12419_489E3B62_33A2C5A7_F4563172
Blowfish B1 output	C31546AC_A54029EB
Blowfish B2 output	34F2EEC8_F14EE2D
2BF-1AES output	C31546AC_A54029EB_34F2EEC8_F14EE2D

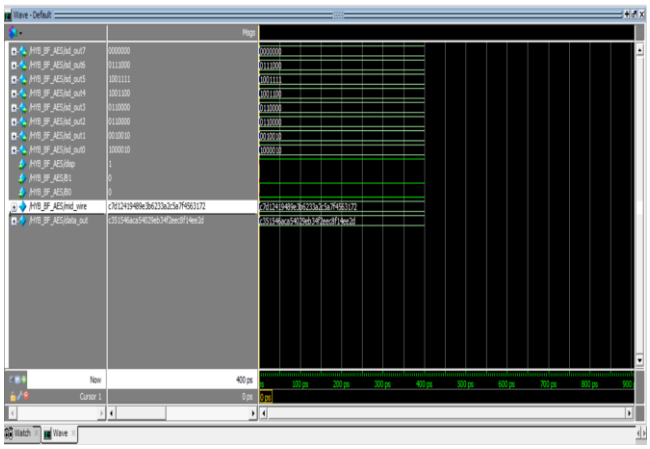

Fig. 9 2BF – 1AES Hybrid Encryption : RTL Simulation

VII. CONCLUSION

This paper elaborates the design and hardware implemenation of a hybrid encryption algorithm made using 128-bit, 10 round AES encryption and 64-bit, 16 round Blowfish encryption techniques using Verilog HDL and has been simulated to verify the functionality as well as test it's effectiveness in the domain.

Simulations show the round-by-round encryption of data as per the algorithm steps. Comparison of encrypted data with already available encrypted data of respective cryptographic algorithms confirms the accuracy of the code and its implementation. Due to constraints in the number of input ports on the Altera DE2 board, inputs have been given directly through the code. The FPGA implementation shows the decrypted data on the Seven Segment Display.

The plain data has been encrypted in two stages; AES encryption followed by Blowfish encryption algorithm thereby making it more robust and secure. Blowfish is a fit choice for AES to make a hybrid algorithm as the security of AES is enhanced without much compromise of the speed. Both of them are a symmetric key algorithm making their hybrid symmetric too. Thus, the final encrypted data can only be accessed using the private key. This hybrid algorithm can easily be incorporated in IoT devices and mobile applications as well as can be modified in different ways to achieve enhanced functioning.

REFERENCES

[1] Advanced encryption standard (2022) Wikipedia. Wikimedia Foundation. Available at: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard (Accessed: November 25, 2022).

[2] Blowfish algorithm with examples (2021) GeeksforGeeks. Available at: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/ (Accessed: November 27, 2022).

[3] S. U. Jonwal and P. P. Shingare, "Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 2017, pp. 64-67, doi: 10.1109/ICOEI.2017.8300776.

[4] T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE Region 10 Conference, 2009, pp. 1-4, doi: 10.1109/TENCON.2009.5396115.