Aes Modes of Operation

Naseema Bhanu, N.V. Chaitanya

Abstract: ***Cryptography is the science of secret codes. Previously we used DES algorithms in order to secure but cannot encrypt completely. Thus, we referred AES Algorithms to create a ciphertext in encryption and is given as an input in decryption. In present scenario, everyone sharing their data in online using internet alsoonline transactions like e-banking for money transfers, in shopping malls, restaurants, and many more. While transferring a huge amount or any confidential data there are many chances to hack the data.There are different modes of operations used in AES in accordance with the efficiency to blur the data. The design has been done in VHDL (Very High-Speed Integrated Circuit Hardware Description Language) and simulated and synthesized using Xilinx.***

Keyword: AES(Advanced Encryption Standards), Ciphertext, DES(Data Encryption Standards), e-banking.

I. INTRODUCTION

In the Advanced Encryption Standards, the Rijndael is a Block cipher, which works on fixed length group of bits, called blocks. An input is taken a certain size, usually 128 bits, the transformation requires a second input, the secret key. The secret key can be of any size depending on the cipher used while AES supports only three different key sizes of 128,192 and 256 bits.

II. DESCRIPTION OF AES ALGORITHM

The AES algorithm is a symmetric block cipher that operates onfixed block of data size 128 bits and key sizes is 128, 192 and 256 bits depending on 10, 12 and 14 rounds respectively. The AES encryption process operates on four different operations such as Substitution byte, Shift row, Mix-column and Addround key. The decryption process also has four operations are Inverse substitution byte, Inverse shift row, Inverse Mix-column and Inverse add round key. The 128bits plaintext contains 16 bytes i.e., (b0,b1,b2,….,b15).

A. AES ENCRYPTION

In this operation the plaintext is converted into the ciphertext format using the secret key.

a. Sub-bytes Transformation: Every byte in the state is replaced by another one using the Rijndael S-box given in Table 1.

b. Shift row: Every row in the 4x4 array is shifted a certain amount to the left.

c. Mix-column: A linear transformation on the columns of the state.

d. Add round key: Each byte of the state is XOR with a round key, which is a different key for each round and derived from the Rijndael key Schedule.

Table 1 Substitutional box table

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	bd	d8	4e	a9	6c	56	f4	ea	65	78	ae	8
c	ba	78	25	2e	1c	a5	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	85	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	9f	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

B. AES DECRYPTION

Decryption is the reverse operation of encryption operation i.e., the ciphertext is converted into the plaintext.

Table 2 Inverse Substitutional box table

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
7	do	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1a
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	6c	5f
d	60	51	7f	a9	19	b5	4a	od	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

a. Inverse Sub-Byte: Each byte in the state matrix is replaced with inverse S-box table given in Table 2.

b. Inverse Shift row: Every row in the 4x4 array is shifted a certain amount to right.

c. Inverse Mix-column: This is inverse operation of mix column operation. This operates on the state matrix column by column and each column is treated as a four-term polynomial.

*d. Inverse Add round key:*Inverse XOR operation is performed with each byte.

Revised Manuscript Received on July 05, 2019.

Naseema Bhanu, Electronics and Communication Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, India.

N.V. Chaitanya, Electronics and Communication Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, India.

III. ENCRYPTION AND DECRYPTION ALGORITHM

The Cryptography algorithm performs two different operations, Encryption and Decryption. In Encryption, the plaintext is converted into ciphertext using a secret key and in decryption, the ciphertext is again converted into plaintext with the help of the same secret key. In AES encryption algorithm, the 128 bits size of a key consists of 10 rounds as given in fig. 1. The operations that are applied on the state during each round are Sub byte transformation, Shift Row operation, Mixcolumn transformation and Add round key operation. The Mix-column operation is omitted in the final round.

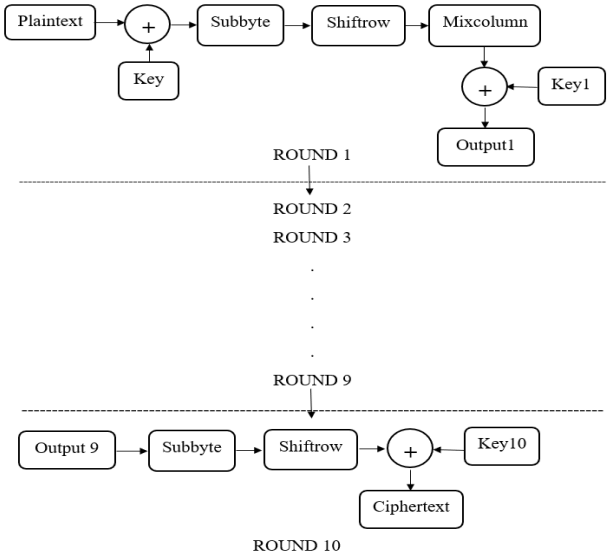

Fig. 1 AES Encryption Algorithm

AES Decryption algorithm is just the reverse operation of encryption algorithm. A key of 128 bits consists of 10 rounds as given in fig. 2.

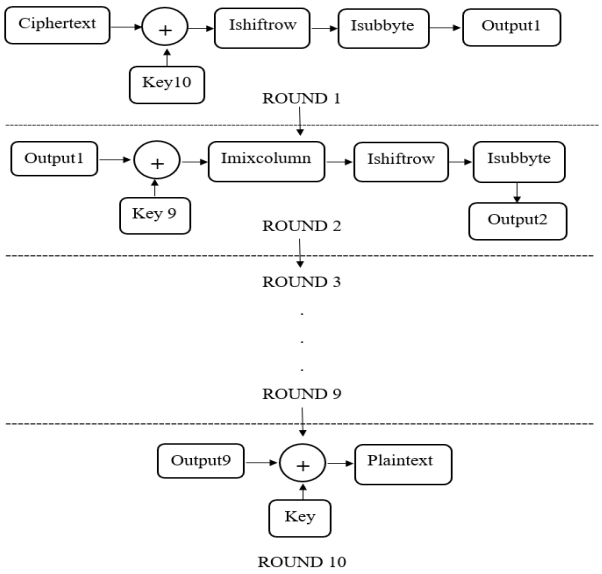

Fig. 2 AES Decryption Algorithm

The operations applied on the state during each round are inverse Sub-byte transformation, inverse shift row operation, inverse Mix-column transformation and inverse Add round key operation. In the first round Inverse Mix-column transformation operation is omitted.

IV. MODES OF OPERATION

The different modes of operation of block ciphers in AES are configuration methods that allowed to process with large data streams also without the risk of compromising the security provided. Here we provide some existing ways to blur the cipher text as a result the intruder can be avoided to break the cipher. Such modifications are known as Modes of block cipher operations.

1. ECB— (ELECTRONIC CODEBOOK) MODE

This is the simplest mode of encryption. Each plaintext block is encrypted separately. Similarly, each ciphertext block is decrypted separately. The ECB encryption and decryption given in fig. 3(a) and 3(b) respectively. In this mode, we can encrypt and decrypt by using many threads simultaneously. The only disadvantage is the created ciphertext is not blurred.

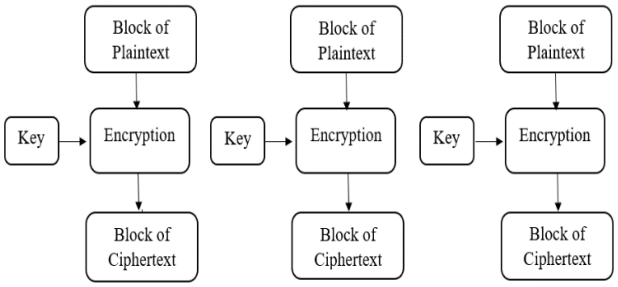

Fig. 3(a)ECB Encryption

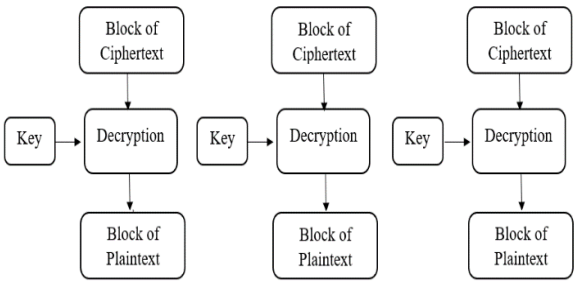

Fig. 3(b) ECB Decryption

2. PCBC— (PROPAGATING OR PLAINTEXT CIPHERBLOCK CHAINING) MODE

This mode adds XOR to the plaintext and then encrypts the data. The first plaintext block is XOR with Initialization Vector (IV). The IV has the same block size as plaintext.During decryption, the decrypted data is XOR with IV.The PCBC encryption and decryption are given in fig. 4(a) and 4(b) respectively. In this mode, both encryption and decryption can be performed using only one thread at a time. If any single ciphertext bit is damaged, the next plaintext and all subsequent blocks will be damaged and unable to decrypt correctly.

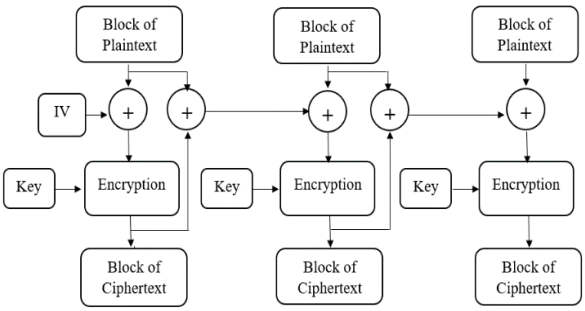

Fig. 4(a) PCBC Encryption

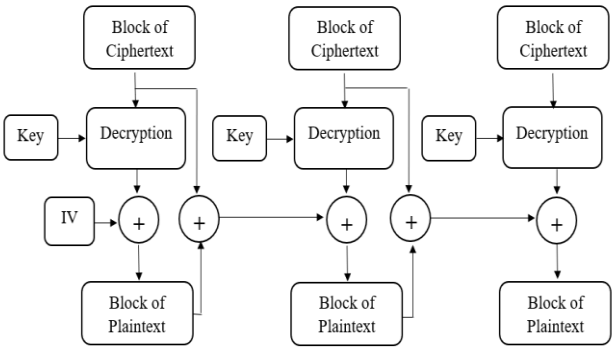

Fig. 4(b) PCBC Decryption

3. CFB— (CIPHER FEEDBACK) MODE

This is also similar as PCBC mode, except that one should encrypt cipher data from previous round, not the plaintext. The CFB encryption and decryption are given in fig. 5(a) and 5(b) respectively. Encryption in CFB mode can be performed only by using one thread and Decryption can be performed using many threads simultaneously.

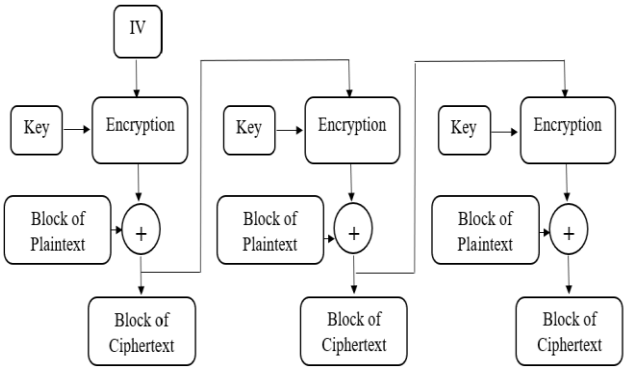

Fig. 5(a) CFB Encryption

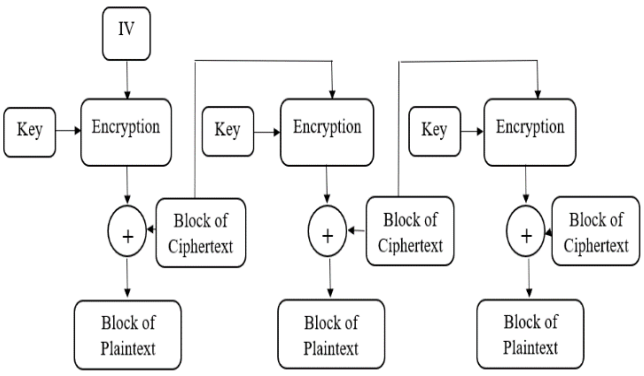

Fig. 5(b) CFB Decryption

4. OFB— (OUTPUT FEEDBACK) MODE

This creates keystream bits that are used for encrypting subsequent data blocks. In this regard, the way of working of cipher becomes similar the way of working of typical stream cipher. The OFB encryption and decryption are given in fig. 6(a) and 6(b) respectively. In OFB mode we canperform both encryption and decryption using only one thread at a time.

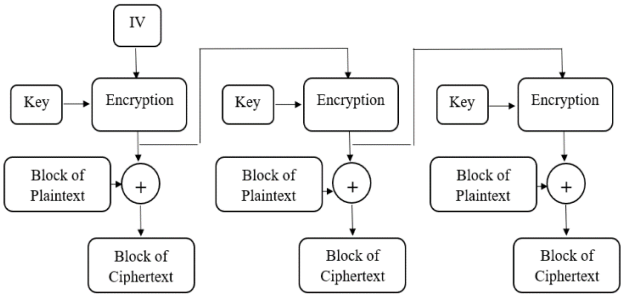

Fig. 6(a) OFB Encryption

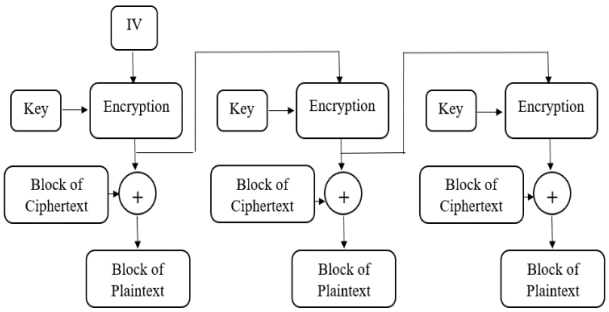

Fig. 6(b) OFB Decryption

5. CTR— (COUNTER) MODE

This is the most popular block cipher modes of operation. The CTR encryption and decryption are given in fig. 7(a) and 7(b) respectively.In this mode, Both the encryption and decryption can be performed using many threads at a time. The nonce is a unique number used once. It plays the same role as IV. The subsequent values of an increasing counter are added to nonce. CTR mode is also known as SIC (Segment Integer Counter) mode. If one plaintext bit iscorrupted, then only one corresponding output bit is damaged.

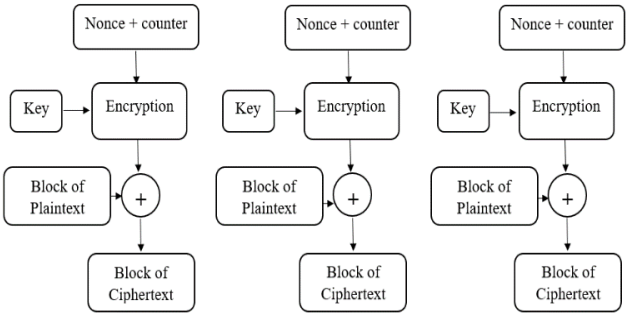

Fig. 7(a) CTR Encryption

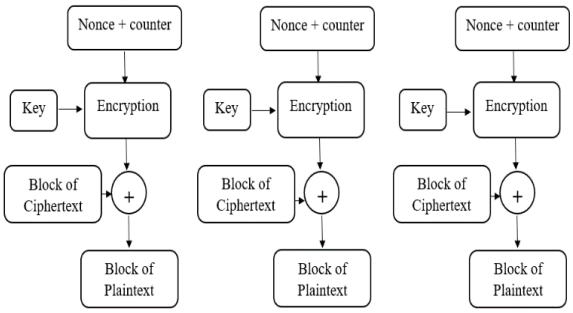

Fig. 7(b) CTR Decryption

V. SIMULATION RESULTS

The different modes of block cipher operations are coded by VHDL. The results of Encryption and decryption of every mode are synthesized and simulated on Xilinx ISE 13.2. The encryption and decryption simulation results of every mode is given below.

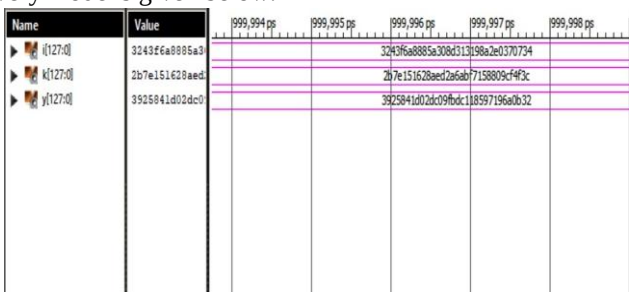

Fig. 8(a)Simulation of EBC Encryption

Fig. 8(b)Simulation of EBC Decryption

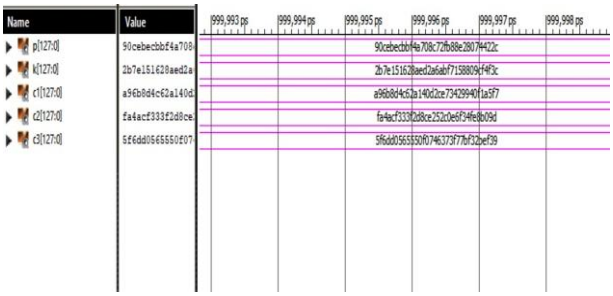

Fig. 9(a)Simulation of PCBC Encryption

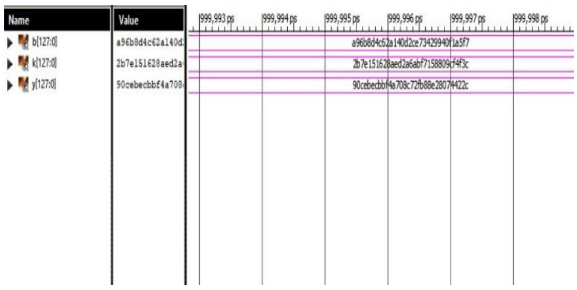

Fig. 9(b) Simulation ofPCBC Decryption

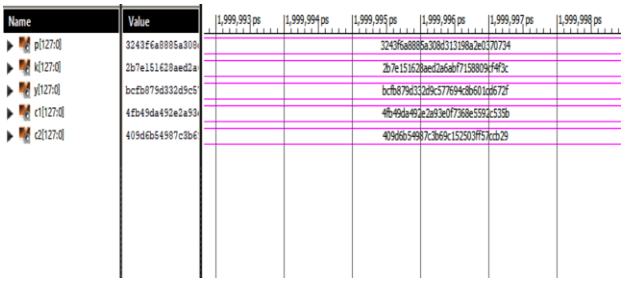

Fig. 10(a) Simulation ofCFB Encryption

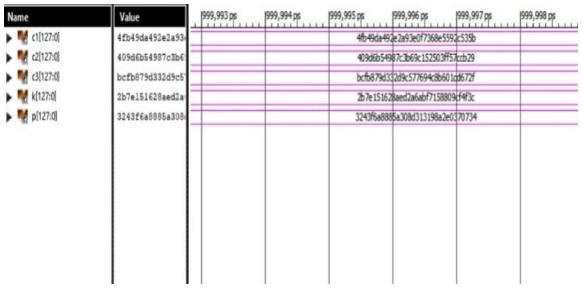

Fig. 10(b)Simulation of CFB Decryption

Fig. 11(a)Simulation of OFB Encryption

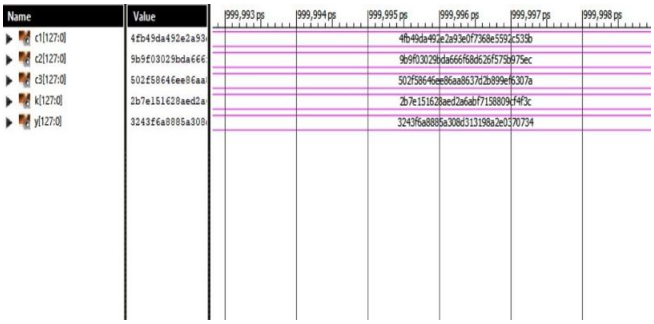

Fig. 11(b)Simulation of OFB Decryption

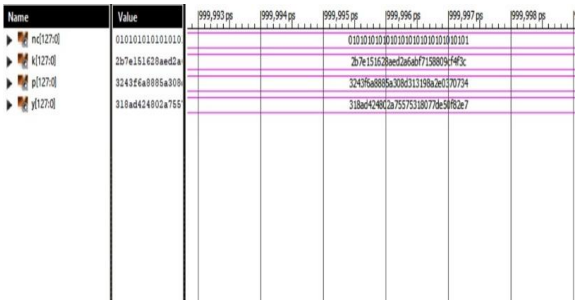

Fig. 12(a)Simulation of CTR Encryption

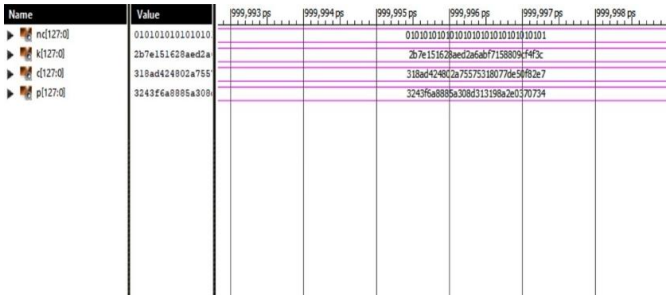

Fig.12(b)Simulation of CTR Decryption

VI. COMPARISION

The different modes of block cipher operations are performed to obtain the efficient mode to blur the ciphertext. Ciphers in the EBC mode is more vulnerable to replay attacks and cannot blur the cipher output completely. In PCBC mode, the IV should be changed after the key used many times, even this can make the system vulnerable to plaintext attacks. The drawback of OFB is the repetition of encrypting the IV may produce the same state that has occurred before. The CTR mode is the most efficient and most preferable mode as it provides quite good security and the secret code needs to be changed less often than the PCBC mode.

VII. CONCLUSION

In order to secure data, we prefer different encryption standards. Previously we used DES algorithms but unable to encrypt completely, thus we referred AES algorithm. To get the data to be encrypted most efficiently we use different Modes of Block cipher operations but the most preferred mode is CTR mode through which the data can be transmitted securely.

REFERENCES

1. Dilna.v, C. Babu “Area Optimized and high throughput AES algorithm based on permutation data scramble approach”, in International Conference on Electrical, Electronics and Optimization techniques (ICEEOT)- 2016
2. www.crypto-it.net/eng/theory/modes-of-block-ciphers.html
3. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
4.https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.html

AUTHORS PROFILE

Naseema Bhanu, M. Tech in VLSI & Embedded Systems, B.Tech in Electronics and Communication Engineering, Smart Phone Controlled Excavator with a live view.

N.V. Chaitanya, M. Tech inRADAR and Microwave Engineering in Andhra University, B.Tech in Electronics and Communication Engineering in Anna University,Microwave Engineering, Mobile Communication-5G Applications, MM Waves, VLSI.