International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Generating Cipher Text using BLOWFISH Algorithm for Secured Data Communications

Ch. Usha Kumari, T. Pavani, A. Sampath Dakshina Murthy, B. Lakshmi Prasanna, M. Pala Prasad Reddy

Abstract*: Cryptography plays a major role in the network security. In order to secure the data one must do encryption of the original message. In this paper, the design and analysis of high speed and high performance BLOWFISH algorithm is implemented in VHDL coding and compared with AES (Advanced Encryption Standard) algorithm. The BLOWFISH algorithm involves the process of giving the data and key as input to the encryption block. BLOWFISH encryption algorithm is designed and programmed in VHDL coding. Then it is implemented in Xilinx 10.1. This research is carried in the following steps: designing of encryption algorithm, writing VHDL code, simulating the code on "ModelSim altera 6.5e", synthesizing and implementing the code using Xilinx's ISE 10.1.This research aims in developing flexible and technology independent architectures in the areas of VPN software, file compression, public domain software such as smart cards, etc. Also presents the comparison of BLOWFISH and AES algorithms. Experimental results show that BLOWFISH algorithm runs faster than AES algorithm while both of them consume almost the same Power.

***Keywords*: BLOWFISH algorithm, AES algorithm, Cryptography, Feistel Networks, Encryption.**

I. INTRODUCTION

The secure data communication is directly attributed to the nature of the Cryptosystems. Cryptosystems use cryptographic algorithms, with keys and different protocols to work effectively. The security of encrypted data is entirely dependent on two things, one, the strength of the cryptographic algorithm and the other the secrecy of the key while under the transmission over a channel. Advancement in this direction is the newly approved and widely adopted secret-key algorithm known as Rijndael Algorithm, has been selected as a standard algorithm by the National Institute of Standards and Technology (NIST).

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Ch. Usha Kumari*, Dept. of ECE, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India
T. Pavani, Dept. of ECE, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India
A. Sampath Dakshina Murthy, Dept. of ECE, Vignan's Institute of Information Technology, VIIT, Visakhapatnam, India
B. Lakshmi Prasanna, Dept. of ECE, Institute of Aeronautical Engineering, Hyderabad, Telangana, India,
M Pala Prasad Reddy, , Dept. of EEE, Institute of Aeronautical Engineering Hyderabad, Telangana, India

Though there are several designs and implementations of this algorithm in Software and Hardware, many lack coordination, optimization and justification among the parameters of interest-Throughput, Speed, Power, Cost, etc.

Cryptology is the art of secret writing. Cryptography allows storing secret information and transmitting it across insecure networks so that it is not possible to read by any other person except the intended recipient. Data which is read and understandable without any special methods is said to be plaintext/clear text. The method of separating plaintext in such a way as to hide its contents is called encryption.

Encrypting plaintext in an unreadable text or understandable language called cipher text. Encryption helps in hiding the information from anyone for whom it is not intended, even those who can see the encrypted data. The procedure for reverting cipher text to its original plaintext is called decryption.

In this research, the design and analysis of high speed and high performance BLOWFISH algorithm is implemented in VHDL coding and compared with A-E-S algorithm. The BLOWFISH algorithm gives the data and key to the encryption block as input, later implementing many blocks as Fiestal network block shown in Figure.2. Initially, the BLOWFISH encryption algorithm is designed and programmed in VHDL coding. Then it is implemented in Xilinx 10.1.

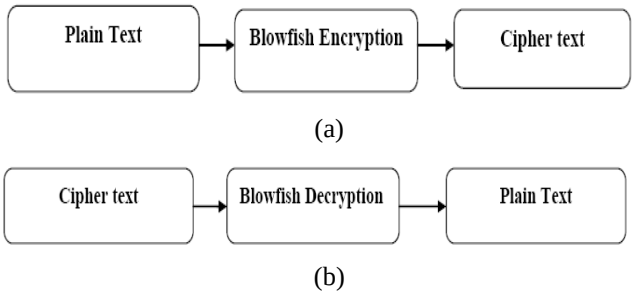

Fig.1. (a) Encryption (b) Decryption

Figure 1 is the block diagram of blowfish Encryption and Decryption. In this research Blowfish, is a block cipher secret-key method, designed and analyzed. It is a Feistel network, repeating encryption function for about 16 times. The size of block is 64 bits, and size of key is of 448 bits. Blowfish is a block cipher key of variable length.

It is very fast compared to AES when applied with 32-bit microprocessors. The comparison of two algorithms AES and Blowfish is carried out in this research.

Blowfish is observed as most effective in execution time and in terms of transmission speed. This research proposes to design and simulate Blow fish and AES by using VHDL coding.

The steps included in the research are encryption algorithm designing, writing VHDL code, simulating the code on "ModelSim altera 6.5e", synthesizing and implementing (i.e., translate, map and place and route) the code using Xilinx's ISE 10.1. The HDL (VHDL/Verilog) ultimately aims at developing flexible and technology independent architectures. Thus, the project ultimately aims at implementing the BLOWFISH encryption and AES algorithm on Xilinx's IES 10.1 to achieve that which algorithm is more effective. Application areas include VPN software, file compression, public domain software such as smart cards, etc.

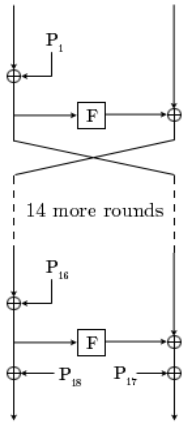

Fig.3. Fiestal Network

II. RELATED WORKS

A cryptographic algorithm is used in the encryption and decryption process. It works with a key either word or number to encrypt into cipher text. The security is dependent on accuracy of cryptographic algorithm and key secrecy. The cryptosystem comprises of many keys and protocols. PGP is a example cryptosystem. Rosen, E., at.al. [1] proposed side channel attack based on the analysis of power traces for obtaining the encryption key. Power traces can be used to detect bit flips which secure the key. Balancing the bit flips with opposite bit flips has been proposed, by the use of opposite logic.

RSA and El method is implemented for mobile systems because of its ease of operation and faster. Cryptographic algorithms are very accurate in the security of wireless sensor networks (WSNs). The energy efficient block cipher algorithm is needed, as these operate without human interference for a prolong period with a very little energy.

Symmetrical key uses two keys one for encryption and other for decryption to communicate. Conventional encryption has incredible benefits. It is very fast. It is especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution since they are vulnerable to major attacks while transmission. Asymmetric key encryption uses two keys; when one key is used to encrypt, the other is used to decrypt. It solves the problem of secure key-distribution by adopting a public key for encryption and a private key for decryption. Examples include Elliptic Curve Cryptography (ECC). But they are more complex than their symmetric counterparts and require more processing power.

Hash function is a one way encryption technique and cannot preserve the integrity by converting back. The combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption. Conventional encryption is about 1,000 times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.

Symmetric and Asymmetric key encryption technique offer confidentiality for the privacy of data. Authentication is also provided where a key acts as identity proof. Hash functions the data integrity where is not altered. Asymmetric key encryption is used for non-repudiation. AES is the Advanced Encryption Standard. AES algorithm and Rijndael algorithm are used interchangeably. There are several algorithms proposed for AES, including RC6, Blowfish, and skipjack. However, Rijndael is selected because of its flexibility and simplicity.

III. METHODOLOGY

The AES specifies the algorithm to support variable key sizes of 128, 192, and 256 bits. The algorithm operates as a 2D array consisting of four rows of bytes. Each row contains Ni bytes, where Ni is length of the block divided by 32.

The array is denoted with symbol A and each byte has two indices, with row number R_i in the range $0 <= R_i < 4$ and its column number Ci in the range $0 <= Ci < Ni$. This permits an individual byte denoted to as A[Ri,Ci]. Since AES specifies Ni = 4, the range for Ci, the column number of the State, is $0 <= Ci < 4$. Number rounds to be executed in AES algorithm depends on key size.

The number of rounds is represented by Nγ, where Nγ = 10 when $N_{ƙ} = 4$, Nγ = 12 when $N_{ƙ} = 6$, and Nγ = 14 when $N_{ƙ} = 8$ shown in Table:1.

	Key Length (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES128	4	4	10
AES192	6	4	12
AES256	8	4	14

Table:1 Key Length, Block Size and Rounds numbers

The AES algorithm has 128 bits for input and output with 0 and 1. The cipher key has a sequence of 128, 192 or 256 bits. The sequences are numbers with 0 and 1, starting and ending.

The AES algorithm processes as sequence of eight bytes.

The byte values are represented as concatenation of individual bits 0 and 1 in AES algorithm in the order {b7-b0}. These bytes are represented as polynomial expression.

$b^7 \times^7 + b^6 \times^6 + b^5 \times^5 + b^4 \times^4 + b^3 \times^3 + b^2 \times^2 + b^1 \times^1 + b0 = \Sigma b^i \times^i$

The various operational blocks required and the state flow in this design consideration of the AES-128 algorithm is shown in Figure.3.

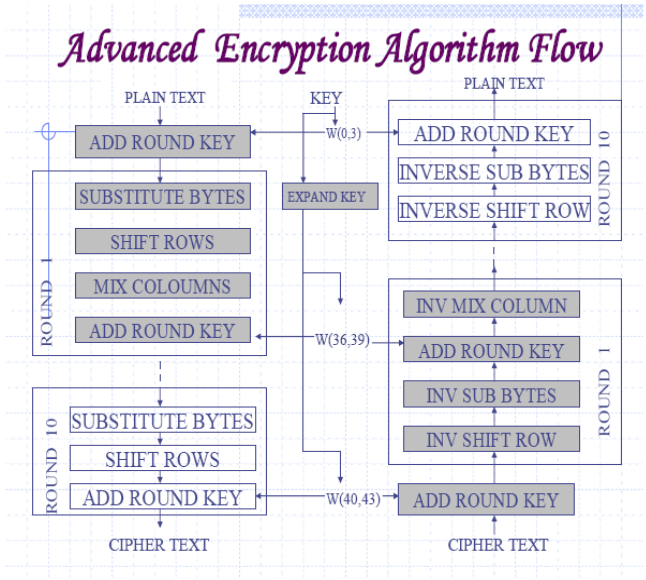

Fig.3. AES Algorithm Flow

The other algorithm used in this research is BLOWFISH. This is compared with AES algorithm. BLOWFISH is used effectively for protecting data from intruders. It takes variable key length of 32 to 448 bits for securing the data. BLOWFISH algorithm is used on communication link and for file encryption where key does not change frequently. BLOWFISH algorithm is very fast encryption algorithm implemented on 32-bit microprocessors.

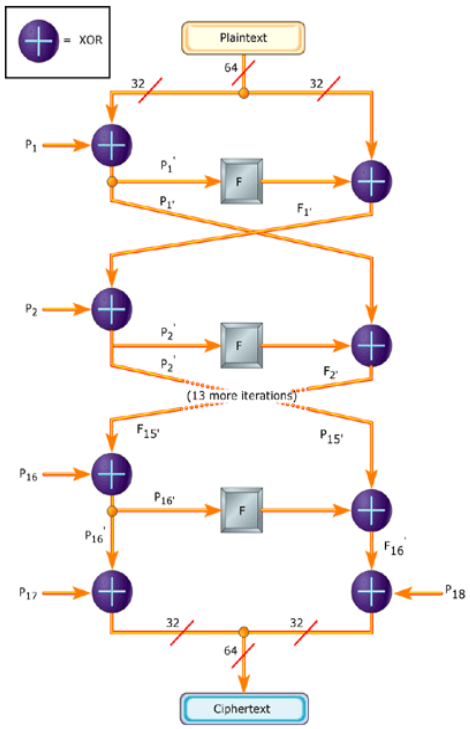

Fig.4. Blowfish Algorithm Fiestel Network

Data encryption takes place with 16-round Feistel network. Every single round comprises of a key-dependent permutation and key-data dependent substitution. All operations are XORs and additional operations are four indexed array data.

A Feistel network is a method of converting any function into a permutation. It has many block cipher designs. The Feistal Network working is described below:

- Divide every block into halves
- Every right half converts into new left half
- Then this new right half is the final result when the left half is XOR'ed with the result of applying f to the right half and the key.
- Note that previous rounds can be derived even if the function f is not invertible

Blowfish uses a large number of sub-keys. These keys must be pre-computed before any data encryption or decryption. The sub-keys are calculated as follows:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3). For example:

   P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3. Encrypt the all-zero string with the Blowfish algorithm, using the sub-keys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub-keys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P- array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

IV. RESULT AND DISCUSSION

The AES algorithm is coded in VHDL and simulated on modelsim to check the desired functionality. The input message, plaintext and keygive are 128 bits. The rounds performed are N-1. The simulation result is shown in the below Figure 5. The inputs given are keygive and plaintext, the out is cipher text. (127:0) shown in Figure 6.

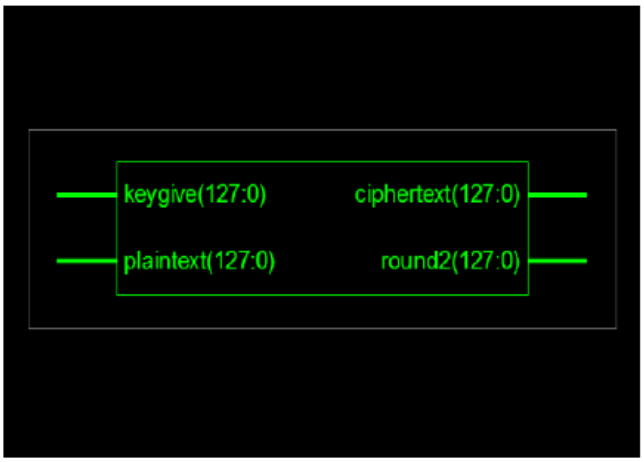

Fig.6. AES RTL Schematic

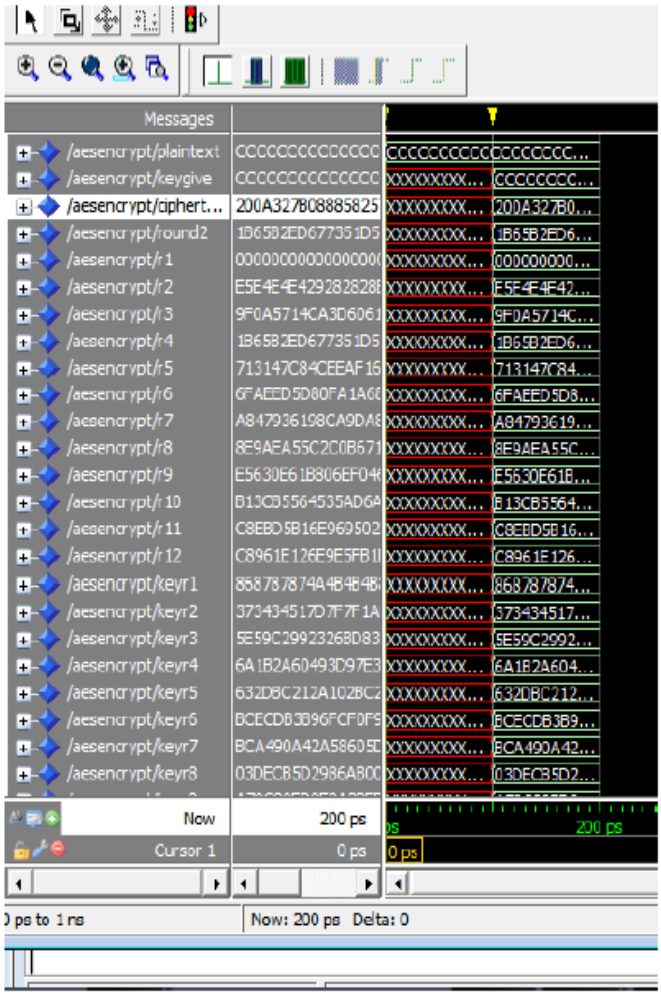

Fig.5. AES Output

The BLOWFISH algorithm result is shown in Figure 7. The input message; key1 to key18, lisource and resource taken are 32 bits. The inputs given are key1 to key18,lisource and resource. The outs are lifinal and rifinal. (31:0) is the number of bits used.

The Blowfish cryptographic algorithm without pipelining, was rated at 590 Mbits/sec maximal throughput, which is 204% as fast as the leading (pipelined) competitor. With pipelining, this design reachs 10.667 Gbits/sec throughput. The power consumed during operation is 63 mW.

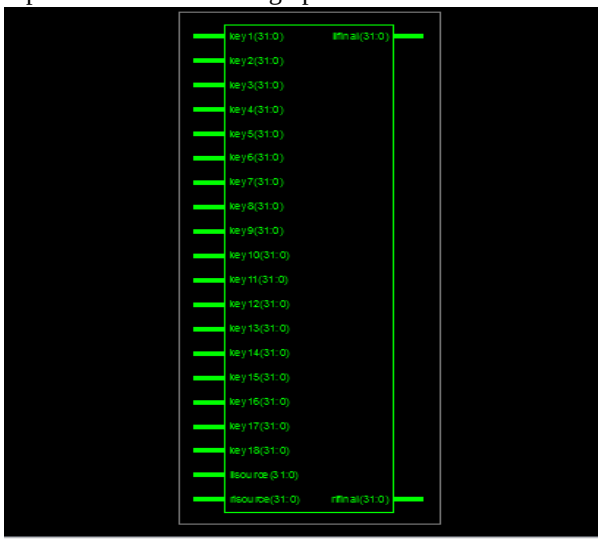

Fig.7. BLOWFISH RTL Schematic

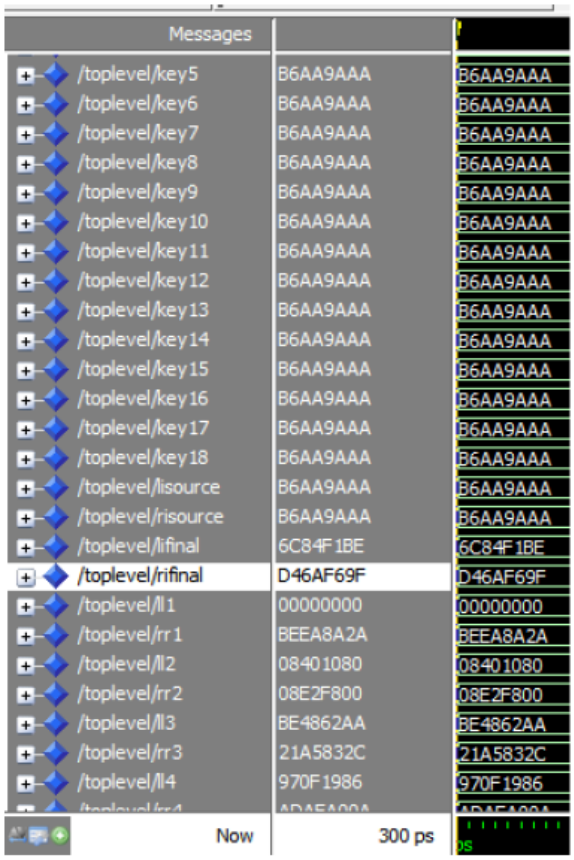

Fig.8. BLOWFISH Algorithm output

V. CONCLUSION

In this research high speed BLOWFISH cryptographic algorithm is presented. This method has maximum throughput of 590 Mbits/sec which very fast without pipelining. With pipelining it is observed that the throughput has reached to 10.667 Gbits/sec. The power consumed with this design is 63 mW during operation which is very less. This algorithm has high speed encryption than AES algorithm. This algorithm provides more security in internet and networking applications. The encryption speed, accuracy and power consumption is compared for AES and BLOWFISH. Experimental results proven Blowfish algorithm runs with faster encryption speed than AES algorithm while both of them consume almost the same Power.

REFERENCES

1. Rosen, E., Viswanathan, A., and Callon, R. "Multiprotocol Label Switching Architecture," IETF RFC 3031, January 2001.
2. Behringer, M., "Analysis of the Security of the MPLS Architecture," Internet Draft, IETF Network Working Group, February 2001.
3. Senevirathne, T. and Paridaens, O., "Secure MPLS – Encryption and Authentication of MPLS.
4. Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol," IETF RFC 2401, November 1998.
5. Rivest, R., " The MD5 Message-Digest Algorithm," IETF RFC 1321, April 1992.
6. Stallings, W., Cryptography and Network Security Principles and Practice, 2nd Edition, Prentice Hall, New Jersey, 1999.
7. Schneier, B., Blowfish symmetric block cipher, 1993.
8. Counterpane Internet Security Web Site, Copyright Counterpane Internet Security, Inc., 2001.

9. Kumari, C.U. and Padma, T., 2019. Energy-Efficient Routing Protocols for Wireless Sensor Networks. In Soft Computing and Signal Processing (pp. 377-384). Springer, Singapore.
10. Kumari, C.U., 2018, April. Investigation: Life-Time and Stability Period in Wireless Sensor Network. In 2018 3rd International Conference for Convergence in Technology (I2CT) (pp. 1-5). IEEE.
11. Kumari, C.U., Prasad, S.J. and Mounika, G., 2019, March. Leaf Disease Detection: Feature Extraction with K-means clustering and Classification with ANN. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1095-1098). IEEE.
12. Kumari, C.U. and Krishna, R., M.: High performance wireless communication channel using LEACH protocols. Pak. J. Biotechnol, 13, pp.52-56.

AUTHORS PROFILE

Dr Ch Usha Kumari is presently working as a professor in Department of ECE, Gokaraju Rangaraju Institute of Engineering and Technology (GRIET), Hyderabad. She completed her Ph.D from Jawaharlal Nehru Technological University, Hyderabad. She completed her M.Tech from Andhra University Visakhapatnam. She had 14years of teaching experience. She published many journals and research papers in national and international conferences. She is life associate member of IETE and fellow member of IEEE.

Dr T. Pavani received her AMIE with first class from The Institution of Engineers (India), M.Tech and PhD from Andhra University College of Engineering, Andhra University. She is having 12 years of teaching and research experience. Her areas of interest are Antennas, Electromagnetics, EMI/EMC. and Applications of Soft computing. She is a life member of the Institution of Engineers and SEMCE. Presently working for a project sanctioned under collaborative Research Scheme, with the Grant No: JNTUH/TEQIP-III/CRS/2019/ECE/9.

Sampath Dakshina Murthy Achanta received his BTech Degree in Electronics and Communication Engineering Degree in 2013 and MTech Degree in Digital Electronics and Communication Engineering 2015. He is pursuing PhD in Electronics and Communication Engineering from Koneru Lakshmaiah Education Foundation Deemed University in Guntur, Andhra Pradesh. His research interest includes image and video processing, fuzzy logic and neural networks. He has published 22 papers in international journals.

B.Lakshmi Prasanna currently working as Assistant Professor at Institute of Aeronautical Engineering Hyderabad in department of Electronics and communication engineering. She completed her bachelor's in ECE and M.Tech in Embedded Systems from JNTU Ananthapur. Her current research includes Embedded systems, internet of things and communication systems.

M Pala Prasad Reddy is currently working as Associate Professor in the department of Electrical and Electronics Engineering. He received B.Tech degree from Jawaharlal Nehru Technological University, Hyderabad in the year 2007. He obtained his M.Tech degree with specialization Instrumentation & Control and awarded with Ph.D in Control systems from National Institute of Technology Calicut, Kerala in 2009 and 2019 respectively. He has 10 years of teaching and research experience and published 10 articles in international journals. He is also a member of IEEE and IAENG. His areas of interest include linear and non-linear control systems, soft computing techniques, signal processing and bio-medical instrumentation.