# A Secure Architecture of Design for Testability Structures

**K. Swaraja, K. Meenakshi, Padmavathi Kora, Mamatha Samson, G. Karuna, A. Ushasree**

***Abstract*: *The structures of Scan-based Design for Testability are extremely susceptible towards unapproved access of the signals present inside the chip. This paper suggests a protected output based plan which averts the unapproved access without any compromise in the testability. A unique key for each test vector is provided in the proposed secure architecture. These inimitable keys are produced by a multi-polynomial linear feedback shift register (LFSR) in addition they are utilized as test vectors. The dimensions of the multi polynomial LFSR bit is saved bigger than the dimension of key so as to augment the level of security to the key. As the keys are concealed within the test vectors, there is reduction in area overhead. The amount of security is improved predominantly by changing the key for all test vectors, along with the location of the bit in the test vector by choosing a valid combination out of available test vector generated by multi polynomial LFSR.***

***Index Terms*: *Design for Test (DFT), Scan Chain, Multi polynomial LFSR, Testability, Security.***

## I. INTRODUCTION

The rising intricacy of the Integrated Circuits (IC) has proved testing very ambiguous. Thus, there is a need for minimal effort and high proficiency testing techniques [1] as there is a substantial rise in the proportion of testing results to the wide-ranging expense of an IC. This problem can be solved if the structures of test arrangement are concealed into the chips in the design cycle. The extensive and broadly explored area of present-day IC configuration is the emerging techniques that permit choosing and setting up the best test situation and device in the design of IC is Design for Testability (DFT) [2], [3]. It refers to those design techniques with the purpose of making test generation and test application cost-effective. DFT plays a vital role in chip manufacturing. Full scan design turns out to be utmost prevailing structured DFT approaches, because of its treatment to high faults besides decrease in overhead of hardware. In the testing of circuits a scan chain is utilized broadly which are sequential, as it resolves the challenges in controlling and perception of inner nodes of a circuit by providing entry to all components of storage in the design, so as to accomplish test spur and detect the responses to expand the coverage of faults. But security usually requires the opposite. The observability furnished by test structures can be utilized by a mugger to inspect the information being handled within the chip. Likewise, the test structures can uncover the confidential data concerning the design of chip. Scan chains open side channels for interlopers to look at the hidden information stored in cryptographic systems [1] and it has been verified as a safety hazard to the Intellectual Property (IP) of the chip. Thus concerning protection with testability, it is known that they were contradicts to each other. Though, testability itself is a crucial obligation of safety, as the scheme is not protected completely except it is fully testable. Enduring a counterbalance among the two is essential. In any case, DFT can't be kept away from insecure systems, in light of the fact that the IC requires elevated quality of testability necessities and the security might be undermined by some faults [4]. So as to fulfil both security and testability, additional equipment is combined into the ordinary scan chains so as to provide them safety with no arrangement in the testability of the target design. The remaining paper is structured as follows. Summary of the past methodologies is reported under Section II. Section III proposes a secure architecture for DFT structures, further the simulation outcomes are evaluated in section IV. At last, section V concludes the proposed work.

**Revised Manuscript Received on July 9, 2019**

**K. Swaraja**, ECE, GRIET, Hyderabad, India.
**K. Meenakshi**, ECE, GRIET, Hyderabad, India.
**Padmavathi Kora**, ECE, GRIET, Hyderabad, India.
**Mamatha Samson**, ECE, GRIET, Hyderabad, India.
**G. Karuna**, CSE, GRIET, Hyderabad, India.
**A.Ushasree**, ECE, GRIET, Hyderabad, India.

## II. LITERATURE SURVEY

Improving both testability and security is a problematic task and usually a trade-off is upheld among the necessities for testability and security. By monitoring the circuit behavior in the scan mode the attacker can obtain the secret key. Yang et al. in [7] have determined that the conventional scan chains are prone to disclose significant details of advanced encryption standard (AES). In [8], a mirror key register method (MKR) has been presented in which a counterfeit secret key is stacked into the scan chain to shield MKR from unapproved access. To ensure crypto centers, counter to the scan based attacks can be characterized into two procedures of restricting the admission to avert muggers after perceiving the scan data and it is prone to a more overhead in timing and hiding the secret data while giving access to all clients. A power- reset is essential to shift the mode as of secure towards the test [9]. The stream of scan output is amended by [10] through accumulating gates of inverter haphazardly to the scan cells to control the yield data. Yet, the area of inverters can be resolved if appropriate data sources are connected to the scan chain. A minimal cost solution is proposed by adding sham flip-flops in the design of scan chain. If the correct key related to the area of these flip-flops is not entered, haphazard data will be displaced [11]. Configuration for Scan chain using scrambling is presented in [12], which separates the scan chain into littler sub-chains. At whatever point the test mode is secure it works in a predetermined order; else it reorders the sub-chains.

This strategy makes an expansive routing and overhead to system. The lock and key protection method [13] additionally utilizes the sub-chains in its structure also confirms the test key with the assistance of a Test Security Controller (TSC). For an approved key, the chip is transferred to the mode of secure, else it pass into an uncertain mode. The shortcoming of this procedure is that its area overhead is large. One more methodology of adding XORs haphazardly within the scan chains is exhibited by [14]. The Secure Scan architecture with Key Authorized Test Controlling (SSKTC) presented in [19] essentially partitions the scan chain into two Key Checker Flip-Flops (KCFFs) and normal scan flip-flops. The Key Authorization Logic (KAL) uses the keys taken by the KCFFs then regulates the operation mode based on the verification result.

In Secure Scan by utilizing the Test Key Randomization (SSTKR) [15], inimitable validation keys are created by programming off-chip. These keys are confirmed by key verifier with an on-chip LFSR reaction. The inimitable validation keys have the dimension of security and can procure an extra part with the utilization of LFSR. Additionally, this procedure utilizes a key verifier with (2k-1) XOR gates, k being the dimension of the key. This verifier works wonderfully for a key with large dimension, the disadvantage of this method is an additional area overhead by key verifier logic. To rectify this a technique proposed in "A Secure Architecture for the Design for Testability Structures"[16] modifies key verifier logic with NAND and XNOR gates instead of XOR gate. It also results in removing error probability. This method uses an LFSR of size greater than the key, makes an additional layer of security.

In scan-based BIST, usually for every n clock cycles, it generates one pattern, where n is the measurement of the scan chain. The period for test application is decided by the multiplication of the quantity of the test designs and the measurement of the scan chain. In this pseudo-random design generator built by multi-polynomial LFSR[17], which can accomplish practically similar fault coverage with less stages, which implies with the utilization of less number of registers and logic leading to reduction in overhead of hardware and power utilization and thus accomplishes higher fault coverage.

## III. PROPOSED SYSTEM

Security is very important for any circuit. But it can be concluded that high observability and controllability is provided by using the scan chain for better testability, but it may reveal the circuit information. In the proposed approach testability is provided as well as another layer of security is achieved to the system as shown in Fig1.

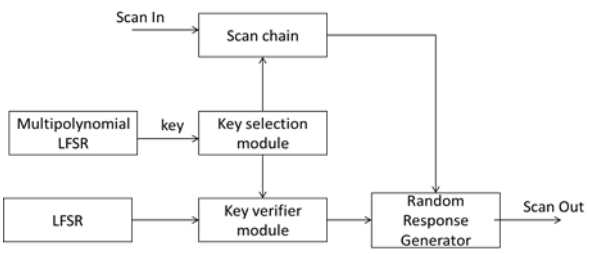


**Fig 1: Proposed secure architecture of DFT structure**

### A. Scan Chain

In the design for testing (DFT), the method utilized is the Scan Chain, to accomplish testing effortlessly by giving a transparent approach to establish and scrutinize all flip-flops within an IC. The testability is improved by including auxiliary logic gates to flip-flops (FF) to construct a shift register or a scan chain [5]. Fig. 2 illustrates the familiar cell of MUX-scan flip-flop structural design. The inclusion of scan chains is achieved via substituting the flip-flops (FFs) by means of scan flip-flops (SFFs). It contains a D Flip-Flop (DFF) besides a multiplexer. The SFFs are then connected in a series. The Circuit Under Test (CUT) is primarily verified functionally further the D flip-flops are altered with the Scan Flip-Flops (SFFs). The subsequent steps are the set of signals so as to control and detect the scan method.

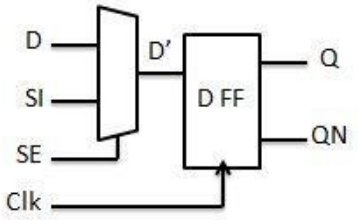


**Fig 2 Scan Flip Flop**

1. Scan_In (SI) and Scan_Out (Q) designate the source and response of a scan chain. Every input in the mode of full scan usually initiates only one chain to observe the scan out.
2. A special signal added in the design is a scan enables (SE) pin. Once this signal is activated, all flip-flops are allied in the design to a lengthy shift register.
3. FFs in the scan chain all through the phase of capture and shift are controlled by CLK.

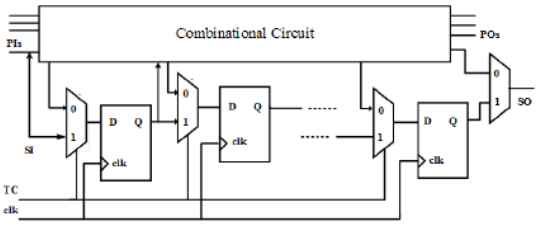


**Fig 3: Scan chain**

Fig 3 presents the example of scan chain design. The DFT based on scan remoulds the circuit which is sequential to facilitate the combination testing as depicted in Fig. 3. The circuit under test (CUT) (i.e., the combinational logic) comprises of inputs which are at current state and primary state (PI), wherein data is saved in the flip-flops (FFs). Likewise, CUT outcomes comprise of next state and primary outputs (PO). The current state inputs and subsequent state outcomes are mentioned as the primary inputs which are pseudo (PPI) and primary outputs which are pseudo (PPO), correspondingly. The Flip Flop's are elements to store which are internal that are neither manageable nor noticeable. Consequently, testing is complicated as there are more number of Flip Flop's in modern VLSI. While designing

based on scan, this issue is resolved through altering the Flip Flop's into scan Flip Flop's (SFFs). The S- Flip Flop's are allied to scan chains so as to shift the state inputs into the scan-chain by means of the pin labelled as scan-in (SI) which is input pin whereas test responses are moved out through the output pin labelled as scan-output (SO).

The two modes that the circuit consists of are functional and test mode. The choice within the scan mode (SE = '1') and the functional mode (SE = '0') is permitted through the Scan Enable (SE) signal which is input to the circuit. In scan mode, the values generated from the Scan Input (SI) are saved in the flip-flop, despite the fact in the functional mode it saves the values engendered from D-flip flop. By monitoring the scan-enable pin, an opponent can take a picture of states of whole S-Flip Flop's in the circuit followed by scanning. In the scan chain, if few of the S-Flip Flop's encompass private details (i.e., private key), at that time the safety of the chip is conceded.

The scan architecture is necessary for testing ICs as well as it can be operated by muggers to allow harmful information into the chips which are secure. Scan chains are prone to several intruders for instance differential power analysis [6], timing analysis, attacks which are faultily inducted.

Actually, the CUT used in the scan chain for the proposed method (S27) needs only 4 test vectors. But to provide security another 2 bits are added, so the Multi-polynomial LFSR is used to generate 6 bits. The test vectors generally have more than required bits which are generated by using multi-polynomial LFSR to provide security. The key selection unit comprises of a multiplexer which opts for a specific amalgamation of 4 bits out of 6 bits which are engendered by the Multi-polynomial LFSR.

### B. Key verifier

A Key verifier is a grouping of XNOR gates to relate the Multi-polynomial LFSR created shape with the one presented in on-chip LFSR. k XNOR gates are utilized for designing the key verifier unit, in which k is dimension of the key, subsequent to this there is amalgamation of (k-1) AND gates. Error is abated in the key verifier unit by exploiting AND gates with XOR gates, later lessens the likelihood towards attack and incurs less area overhead.

### C. Multi Polynomial LFSR

In case of normal LFSR, normally unique pattern is engendered for all n clock cycles, here n is the dimension of the scan chain. Whereas Multi-polynomial LFSR generates at least two characteristic polynomials by generating pseudorandom pattern. With multi-polynomial LFSR, handling of faults by means of less number of stages can be attained, which entails fewer registers and logic ensuing in a reduced amount of overhead in hardware and a smaller amount of power consumption.

LFSR with 4-stage 2- polynomial depicted in Fig. 4 illustrates the simple knowledge of the LFSR with Multi-polynomial. In this model, LFSR with 4-stage 2-polynomial has two characteristic polynomials as given in Eq (1)

$$P1(x) = 1 + x^3 + x^4 \text{ and } P2(x) = 1 + x + x^4 \qquad (1)$$

Compared to general LFSR, Multi-polynomial LFSR generates multiple patterns without any delay in the circuit and almost negligible area overhead.

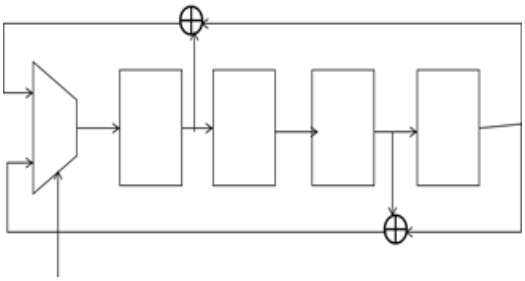

**Fig.4: Multi Polynomial LFSR**

### D. Random Response Generator

With regard to TC, the matched Key Flip Flop is triggered to negative edge. When the CUT changes to normal mode from the mode of test, TC drops and the Flip Flop clocks in the outcome of the key verifier. Depending on Match signal proper deed is taken. The signal that is matched can be activated either to reorganize the scan chain or else to randomize the outcome. If the match fails, then the output will be taken from a random response generator. Otherwise, the scan chain output will be the system output.

## IV. SIMULATION RESULTS

The simulation results for the circuit of S27 benchmark were observed. The circuits in Benchmark are a collection of circuits that are broadly utilized in the FPGA societies while evaluating the solutions with hardware in addition to software. International Symposium on Circuits and Systems (ISCAS) offered a circuit designated as S27 which is sequential in nature. In S27, the letter 'S' signifies the nature of the circuit as sequential whereas the numeral 27 reveals the count of lines that are interrelated amongst the primitives of circuit [9]. The specifics of the circuit for benchmark with label S27 are depicted in Table 1.

In the proposed system code written in Verilog is simulated and synthesized through implementing Xilinx ISE. The simulation outcomes were attained for the device with label XC3S500E, which is a member in the family of the Spartan 3E. Only one scan chain was utilized for the methodology. The circuit for the benchmark with label S27 was practically checked and tried with each and every stuck at faults. The input and output specifics of the circuit with label S27 is depicted in Table1.

**Table 1 Details of Circuit with S27 Benchmark**

| Name of the circuit | Count of primary inputs (PIs) | Count of flip-flops (FFs) | Count of primary outputs (POs) | Count of logic gates |
|---|---|---|---|---|
| S27 | 04 | 03 | 01 | 10 |

**Elements of Security:**

To simulate the attack effectively, the unlicensed client requires to pass the subsequent elements of security. At first, there is a necessity for the unauthorized client to understand that the reaction given at the output is an adjusted outcome. If that is positively completed, the subsequent data is essential

a. The seed for the LFSR is utilized for the creation and approval of key.

b. The chosen polynomial is Multi-polynomial LFSR.

c. The LFSR output bits are in fact utilized for the creation and approval of key.

d. The location of bits related to the key utilized for the purpose of testing in the test vector.

e. The seed related to the LFSR utilized in the response which is randomly generated.

f. The LFSR polynomial utilized in the response which is randomly generated.

g. The count of gates utilized in the response which is randomly generated.

h. The kind of gates utilized in the response which is randomly generated.

i. With regard to many scan chains, the unlicensed client have to decide the arrangement of the decoder/encoder at the input/output of the scan chain [8].

The size of the components utilized in the proposed design is related to the dimension of the key. LFSR needs k Flip Flop's to create a key with dimension k. On the other hand, since the system preserves the dimension of LFSR bit larger than the dimension of key, the required K flip-flops should be more for LFSR. The key verifier unit entails whole (2k-1) gates for the verification of the key. The extra bits expected augments the total area. Likewise, the extra MUX utilized for LFSR makes a negligible area overhead.

So as to additionally boost the security, the dimension of LFSR bit is set greater than the dimension of the key, and by utilizing multi-polynomial LFSR. The XNOR and AND gates devour a smaller amount of power compared to the XOR gates utilized for key validation in the SSTKR system. The security level or the proposed scheme is superior than [6]. The key verifier unit utilized in the methodology eliminates the likelihood of happening error in [6]. The dimension of the bit for the LFSR is greater to boost the security.

The choice of maintaining the dimension of LFSR bit greater than the dimension of key through utilizing multi-polynomial leads in the expansion of the security level. Defining the seed and polynomial of the LFSR is simply not sufficient. The unlicensed client likewise desires to decide the output bits of the multi-polynomial LFSR for the generation and validation of the key to offer greater security to the key. The proposed architecture can be promoted to higher benchmark circuits without any area overhead and delay. The attained outcomes cannot be contrasted simply with the earlier work as there is distinction in the technology, design contemplations, and the scheme utilized among them.

Thus, the outcome will fluctuate in accordance with the design constraints like the count of scan chains, test vectors, lines needed to select in the design of the multiplexer, polynomials in the multi-polynomial LFSR, dimension of key and the dimension of LFSR bit. Later the area overhead might even become negligible by multi-polynomial LFSR when contrasted with the present approaches. The assessment between the proposed work and current works with different key values are shown below by considering the factors such as delay and the number of 4 input Lookup Tables (LUT).

**Table 2: Comparative Analysis**

| Parameter | Key size | [13] | Proposed method |
|---|---|---|---|
| Overhead (no of 4 input LUT's) | 6 | 35 | 33 |
| | 8 | 47 | 46 |
| | 10 | 53 | 50 |
| | 15 | 62 | 71 |
| | 20 | 82 | 81 |
| Delay (nsec) | 6 | 6.709 | 6.709 |
| | 8 | 7.662 | 7.662 |
| | 10 | 7.832 | 7.832 |
| | 15 | 5.056 | 5.056 |
| | 20 | 5.182 | 5.182 |

From Table 2 it can be decided that the area overhead and delay varies with key size. For the key size of 6 bit, the numbers of LUTs required are 35 for [16] and 33 for the proposed method. Thus the proposed method reduces area overhead for lower key sizes and in addition to this increases the area overhead slightly for higher key sizes. The delay increases with respect to key size. The delay is almost the same for [16] and the proposed method.

## V. CONCLUSION

In the design of digital circuit, architecture based on Scan is principally utilized as a design-for-test methodology. Architecture based on Scan is a well-designed essential tool for engineers under testing, correspondingly it is a device in the hands of assaulters to acquire undisclosed data present in the circuit under test. This paper shows another way to deal with ensure the scan architecture using two layers of security. The solution proposed by the paper ensures that the architecture based on scan saves unapproved examiners from gaining access to the attacks in scan chain. To examine the CUT under the test mode, a restructuring Multi-polynomial LFSR is accustomed through generating a key which is dynamic. This substantially prone to reduction in terms of the area overhead. Along these lines, the proposed technique expands security further with the same delay and area overhead compared to the existing method.

## REFERENCES


1. Yier Jin, "Design-for-Security vs. Design-for-Testability: A Case Study on DFT Chain in Cryptographic Circuits," Proc. of IEEE Computer Society Annual Symposium on VLSI, 2014, pp. 19-24.
2. A. Richardson, T. Olbrich, V. Liberali, F. Maloberti, "Designfor- test strategies for analogue and mixed-signal integrated circuits," IEEE 38th Midwest Symposium on Circuits and Systems, vol.2, 1995, pp. 1139-1144
3. C. Hoffmann, "A New Design Flow and Testability Measure for the Generation of a Structural Test and BIST for Analogue and Mixed-Signal Circuits," Proceedings of the 2002 Design, Automation and Test in Europe Conference and Exhibition (DATE'02), 2002, pp. 197-204.

4. J. Da Rolt, A. Das, G. Di Natale, M.-L. Flottes, B. Rouzeyre, and I. Verbauwhede, “Test Versus Security: Past and Present,” IEEE Trans. Emerg. Top. Comput., vol. 2, no. 1, pp. 50–62, 2014.

5. VLSI Test Principles and Architectures: Design for Testability by Laung-Terng Wang Cheng-Wen Wu Xiaoqing Wen.
6. P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Lecture Notes in Computer Science, vol. 1666, pp. 388–397, 1999.
7. B. Yang, K. Wu, and R. Karri, “Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard”, Proc. IEEE Intl Test Conference, 2004, pp. 339-344.
8. B. Yang, K. Wu and R. Karri, “Secure scan: A design-for-test architecture for crypto chips,” IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, vol. 25, no. 10, pp. 2287–2293, Oct. 2006.
9. Y. Shi, T. Nozomu, Y. Masao, and O. Tatsuo, "Robust secure scan design against scan-based differential cryptanalysis," IEEE Transactions on Very Large Scale Integration (VLSI) Systems 20, pp. 176-181, 2012.
10. G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, "Secured flipped scan-chain model for crypto-architecture," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 26, no. pp. 2080-2084, 2007.
11. J. Lee, M. Tebranipoor, and Jim Plusquellic, "A low-cost solution for protecting IPs against scan-based side-channel attacks," In 24th IEEE VLSI Test Symposium, pp. 6-pp, 2006.
12. D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, and N. Berard, “Scan design and secure chip,, 10th IEEE International On-Line Testing Symposium, 2004, pp. 219-224.
13. J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, “Securing Design Against Scan-Based Side-Channel Attacks,” IEEE Trans. on Dependable and Secure Computing, vol. 4, no. 4, Oct.-Dec. 2007, pp. 325-336.
14. H. Agrawal, S. Karmakar, and D. Saha, and D. Mukhopadhyay, "Scan based side channel attacks on stream ciphers and their countermeasures," International Conference on Cryptology in India. Springer Berlin Heidelberg, 2008.
15. M. Razzaq, V. Singh, and A. Singh, “SSKTR: Secure and Testable Scan Design Through Test Key Randomization,” Proc. of Asian Test Symposium, 2011, pp. 60-65.
16. Samta D. Talatule, Pravin Zode, Pradnya Zode, “A Secure Architecture for the Design for Testability Structures” IEEE conference 2015.
17. A Multi-Polynomial LFSR Based BIST Pattern Generator for Pseudorandom Testing Haoqi Ren, Zhenya Xiong

## AUTHORS PROFILE

Dr. K.Swaraja is currently working as Professor at Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India and has obtained her Ph.D. in the area of Digital Image Processing from the auspices JNTU, Hyderabad, A.P, India. She received M.Tech degree in Digital Electronics & Communication systems from the prestigious JNTU, Anantapur, A.P, India and B.Tech degree from JNTU, Anantapur, AP, India in Electronics and Communication Engineering. She has more than 30 publications on an assortment of topics in reputed national & international journals and conferences. Her areas of interest are digital signal, image and video processing besides VLSI, Machine learning and Communication systems.

Dr. Meenakshi K completed her PhD in 2018 and having 15 years of teaching experience. Presently working as a professor in Gokaraju Rangaraju Institute of Engineering and Technology. Published more than 15 articles in international journals/conferences. Her research interests include image and video watermarking, Machine learning and network security.

Dr. Padmavathi Kora completed her PhD in 2016 and having 15 years of teaching experience. Presently working as a professor in Gokaraju Rangaraju Institute of Engineering and Technology. Published more than 36 articles in international journals/conferences. Her research interests include ECG and EEG signal processing, Image processing, Machine learning, Swarm and Evolutionary optimization and Wireless sensor networks.

Dr. Mamatha Samson completed B.E in ECE from Mysore University in 1991. MS from BITS, Pilani. Ph.D from IIITH in 2013. She is working as Professor in Gokaraju Rangaraju Institute of Engineering and Technology. She is a member of ISTE, Institution of Engineers, IEEE. She has published 25 research papers in National and International journals and conferences. Her research interests are VLSI design, Mixed signal circuits and Biomedical circuits.

Dr.G.Karuna is currently working as a Professor in Computer Science and Engineering Department at Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. She has completed her Ph.D. in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. She has thirteen years of experience in teaching for both undergraduate and post graduate students. She is a life member of CSI. She has published 25 research papers in National and International journals and conferences. Her research interests are Image Processing, Computer Networks, Cryptography and Network Security, Big Data Analytics, Machine Learning.

A.Ushasree is currently working as Assistant Professor at Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India and pursuing Ph.D in the area of Antenna Designing from the KL University, Vijayawada, A.P, India. She received M.Tech degree in Embedded Systems from the Annamacharya Institute of Technology & Science, Anantapur, A.P, India and B.Tech degree from Adhiparasakthi college of engineering for Women, Kalavai, Vellore, India in Electronics and Communication Engineering. Her research interests are Antenna Designing, Communication Networks and Image Processing.