Hardware-Based Physical Layer Security Solutions and Algorithms for Iot Devices on FPGA Platform

Bharathi R, N. Parvatham

Abstract*: The Physical Layer Security mechanism has emerged as a powerful concept that can provide high-level security and can even replace encryption oriented schemes, which necessitate various difficulties and practical challenges for future communication systems (e.g., IoT). Therefore, the critical goal of this work is to enhance the security performance at IoT and prevent the network from various eavesdropping attacks. In this Manuscript, analyze the hardware-based Physical Layer Security solutions and suitable cryptographic Algorithms for IoT applications. The Cryptographical Algorithms include AES, DES, Light Encryption Devices (LED), PRESENT, Extended Tiny Encryption Device (XTEA) are analyzed on the Hardware platform. The Hardware constraints like Area, Frequency, Latency Throughput, and efficiency are evaluated on FPGA devices.

***Keywords* : Cryptography, Internet of Things (IoT), Physical Layer Security, FPGA, Lightweight algorithms.**

I. INTRODUCTION

In the year 1999, IoT initially came into the picture, which changes everything. It means to realize internetworking and information transmission between the devices. At present, it behaves like a critical enabler for intelligent vehicular systems, smart cities, healthcare systems, and smart grids [1-2]. There is envisioning that thousands of real things are interconnected with a different sensor, actuators, and internet through heterogeneous access networks [3]. The intention behind IoT is the deployment of a machine to machine communication that performs smart/automatic tasks without human collaboration [4].

Furthermore, the evolution of 5G cellular communication technology [5] [6], along with high data rate and delay performance, will guide in IoT ubiquitous computing, create new diverse IoT applications and business models [7]. Day by day, there are large increments in IoT devices, making humans life more comfortable and performing better than humans. It has been surveyed that, in 2019, the adoption of IoT devices will have greater than thrice from 2012, and it will be fifty billion IoT devices that work on the internet [8]. The following figure-1 represents the increasing rate of IoT devices from 2012 to 2020. The large scale deployment of IoT applications makes information security newly significant [9]. The network security solutions are very crucial, which not only handles the multiple operations even also realizing the secure service delivery over the networks. However, security and privacy are the two crucial challenges facing the deployment of IoT.

Generally, all IoT devices will operate via an internet connection so that there is a chance that the attackers can steal confidential information. Hence, security should be ensured by preventing unauthorized access. The security attacks can occur on any layer and affect the IoT applications is discussing in section IV. The traditional security protocols heavily rely on cryptography technology at ISO protocol stack. Though the cryptographic technique is a significant and practical approach that is widely utilized for wired as well as wireless networks example, computer networks and cellular networks respectively, it is not well suited for future IoT applications. For example; As per 3GPP-TR 45.82 functional specification, futuristic IoT applications provision to accommodate a massive number of IoT devices inside the single cellular device [10].Typically, all IoT devices are embedded with many low-cost devices that have minimal storage and restricted powered batteries, which yield minimal computing and communication capabilities. In IoT, the whole network should satisfy large-scale coverage requirements, which senses the local data that should send to the remote control center for further processing. The transmission protocol has to incorporate with new features, i.e., multi-hop routing, dynamic access, and cooperative relaying, which makes IoT heterogeneous and dynamic nature to meet such requirements.

The conventional cryptographic protocols require key distribution or essential management methods, which could be challenging to the deployment of IoT systems with a large scale of MTC devices. As a result, arobust physical layer security protocols can provide lightweight cryptography protocols [11] [12] are suitable solutions for IoT implementation. Unlike classical cryptographic methods, physical layer security (PHYLS) takes advantage of intrinsic features of wireless networks, like; interference, fading, and noise to boost the signals at authentic receiver and lower the signal quality at snooper and it will realize the keyless transmission through signal processing [13].

Revised Manuscript Received on January 06, 2020.

***** Correspondence Author

Bharathi R., Research Scholar, PRIST University, Thanavur, Tamilnadu, India. Email: bharathiresearch2019@gmail.com

N. Parvatham, Associate Professor, PRIST University, Thanjavur, Tamilnadu, India

Fig.1 Growth rate of connected IoT devices from 2012 to 2020

Physical Layer Security schemes have many advantages when compared with cryptographic methods. It doesn't depend on encryption or decryption operations. It can use wireless channel characteristics to realize adaptive signal design as well as resource allocation. Also, provide flexible, secure configurations and quality of services guarantee. It requires simple signal processing algorithms that incur minimum overhead comparing to an encryption scheme. It uses unique characteristics of the channel among intended communicants and provides an intended receiver with a benefit over eavesdroppers. The remainder of this work is structured as; Section II discusses different Physical Layer Security solutions followed by symmetric cryptographic algorithms in IoT security on hardware platforms in section iii. In section IV, the results and analysis of cryptographic algorithms are discussed. In section V, have presented a conclusion and future direction in IoT based Physical Layer Security solutions.

II. PHYSICAL LAYER SECURITY SOLUTION IN IOT

IoT system security is a crucial issue; without security, we cannot exploit the IoT devices properly as well as not able to get all the advantages that are delivered by IoT [14]. In this section, discussing some prominent solutions of physical layer security utilized to secure the IoT infrastructure from the attackers. Additionally, the following figure-2 highlights the Physical Layer security solutions.

A.Hash-based and Encryption method

In IoT application deployment, the internet plays a vital role where information transmits via the internet where intruders also exist. Hence, the user's information is insecure over the network. It is essential for security mechanisms to secure the user's information from malicious threats. For the user's data security perspective, researchers introduced encryption and a hash-based security scheme. During encryption, information is converted into a ciphertext format. When sender forward than that, it converts into another format using a secret key that can't be analyzed or utilized by anyone except authorized user. The same secret key is forwarded to the receiver end, and the receiver has the authority to convert that ciphertext into original content using the key [15]. The encryption mechanism is constructive to secure the user information, but owing to the advancement in communication technology, it can be possible to modify the user's content for hackers. In that context, researchers proposed a hash-based security scheme that can recover the content which has been modified by the hacker. Additionally, digital fingerprinting and watermarking are the significant methods that ensure that the user's information can't be altered or changed by the attackers or virus.

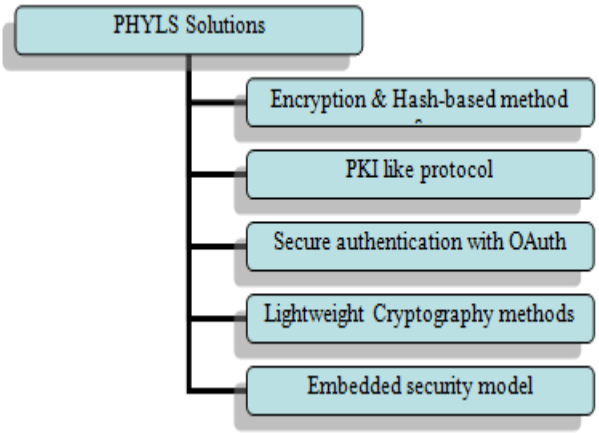

Figure 5 Existing PHYLS Solutions to secure the IoT system

B. Public-Key Infrastructure (PKI) Protocol

Public-Key Infrastructure protocol performed at the recognition-layer of the IoT system. It is responsible for offering high security without allowing anyone to forward the content. This protocol works where nodes are arranged in tree format network topology where the root node behaves like a base station (BS) of the network. It exploits the RSA algorithm where public-key is stored at BS while private-key is distributed to each node via BS [16]. During message transmission from the sender node to the receiver node, the message is transmitted over the child node of the receiver. Further, the child node forwards the message packet to the next child node. This process persists until the message reaches the receiver end. The farmer node to verify the other node authenticity before forwarding the message to the next node. Once the receiver node found, then the message will be transmitted directly, or else the message reverts to the BS.

C.Secure authentication with Open authorization

Generally, there are two terms comes under authorization mechanism including; Role-based and attribute-based access control mechanism where the first one permits the right user who has authority, while attribute-based mechanism permits the particular attributes which are assigned to the authorized user. However, there are different methods where user information can be easily accessed like example; an attacker can access the user's data by entering duplicate information or showing itself as an actual user. The Open-Authorization mechanism is introduced to overcome these problems [17]. It contains four significant characters (owner, service provider, client, and authorized server) by which collaboration among the users and service provider become possible.

D.Lightweight Cryptography mechanism

Lightweight cryptographic is the standard mechanism specifically utilized to meet the privacy and security provisions over the network. Particularly for PHLS, there are three kinds of cryptographic algorithms

(i.e., symmetric key, public-key algorithm, and hash function) are discussing in the following section-IV in detail.

E. Embedded security model

There are various types of intruders and attacks, which not only affect system performance, evenly gain the user's information. Attacks at PHYL directly affect the system's physical components and perform different functions, e.g., stealing information, eliminate sensitive data, and monitor the user's activities without their authorization. However, there are typical PHYL security requirements in the IoT to protect from different attacks [18] such as;

- ***User identification*:** It is a process of user authentications; only authorized users can access or exploit the system resources by doing password entry or pre-shared key validation scheme.
- ***Identity management*:** It deals with recognizing each device in the system and controls their access by associating the user's authorizations.
- ***Secure communication during data transmission*:** It demands secure communication among the devices, and ensures integrity and confidentiality of data communication as well as securing the communication entities.
- ***Storage security*:** The system has the responsibility to protect and preserves the user's data from intruders and attackers. Hence, it is mandatory for the confidentiality and reliability of confidential data stored in the system.
- ***Software execution with a secure environment*:** It responsible for preventing, manage code and design a secure runtime environment that should be protected from unexpected software applications, e.g., viruses.

III. SECURITY ALGORITHMS FOR PHYSICAL LAYER

The cryptographic mechanism provides a set of the necessary tool which provides multiple security features like i) authentication, ii) integrity, iii) confidentiality, and iv) non-repudiation. In other words, it secures users' data, security transmission, as well as maintains the user's privacy. The complex problems is that, to understand the suitable cryptographic algorithm for the particular feature because there are various security or cryptography algorithms are used for physical layer security to ensure security for different IoT applications. Some standard cryptographic algorithms are discussing as follows;

Lightweight Symmetric-Key Cryptography Algorithms facilitate encryption in which both the sender and receiver contain a single symmetric key utilized for the message distribution process. The purpose behind this is to convert the shared message into a ciphertext format, and the same key is utilized to convert the ciphertext into the original message at the receiver end. Therefore, the message can be understood only by a real person (i.e., authentic person). There are many symmetric-key cryptographic algorithms introduced by many researchers, for example, AES (Advanced encryption standard), DES/triple-DES (Data encryption standard), Blowfish algorithm, and many more. But out of these algorithms, AES is most widely utilized and considered as a significant and efficient algorithm that provides security along with improving the performance efficiency for several IoT applications [19]. In the study of King et al. [20], have designed a distributed framework to maintain secure data communication over the network. Usually, the communication performs into two stages, i.e., PHY devices to the IoT gateway & IoT gateway to the Internet. The security level of these communication stages can be maintained by applying a symmetric-key cryptography algorithm (i.e., AES). The one drawback of this algorithmic approach is that both senders, as well as the receiver, needs to share the symmetric-key for data encryption before and then they can move for decryption. The symmetric key cryptographic algorithms [21-22] like AES, DES, LED, XTEA, and PRESENT are discussed in this section briefly.

The **AES** encryption and decryption architectures are represented in Figures 3 and 4, respectively. The AES model uses 128-bit data and key with 10 rounds of operation for both encryption and decryption (ED).

Each ED has four rounds of transformation, namely, SubBytes (SB), ShiftRows (SR), mixed columns (MC), and Add round key (ARK). Initially, the 128-bit plain text is XOR with a primary 128-bit key for round '0', Then perform 9 rounds of operation using 4 transformations, and in the last round, MC is considered for the generation of 128-bit ciphertext. The decryption is the inverse process of encryption and represented in figure 4. The 128-bit is input to the decryption process. The order of the four transformations is changed, and round key operation starts from ten to zero for the generation of 128-bit plain text.

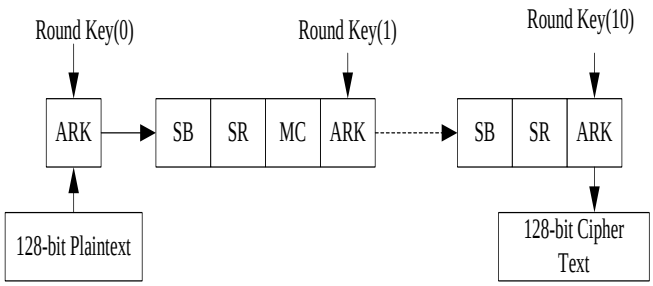

Fig.3 AES-128 Encryption Architecture

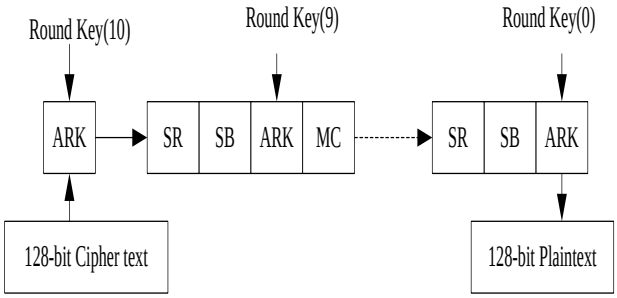

Fig.4 AES-128 Decryption Architecture

The **Data encryption system (DES)** uses a 64-bit data ad key and has a Feistel structure for the ED process. TheEncryption process contains the Initial permutation block followed by the function of round inputs and key computation unit. The round updation and key computation process parallel for the next 16 rounds and last perform inverse permutation operation to generate the 64-bit ciphertext. The decryption process is the inverse operation of the encryption process for the generation of the 64-bit original text.

The **Light encryption device (LED)** is similar to the AES algorithm with a few modifications. The LED modulehas 64-bit plaintext and 128-bit key for the ED process. The LED uses 48 rounds of operation for the ED process. The 128-bit key is divided into 64-bit K1 and K2 keys. The encryption mainly contains XOR, the plain text with K1 followed by fours of operations the XOR with K2, and the process continues till 48 rounds. Then ciphertext is generated for the LED module. The 4-round includes adding constants, substitute cells, shift rows (SR), and MC serial.

The lightweight **Extended Tiny encryption algorithm (XTEA)** uses 64-bit plaintext and 128-bit key for the ED process. The ED process mainly uses two Feistel structures parallel for the next 32-times for round updation. The key scheduling also operates parallel with ED by using basic Arthematic and logic operations.

The **PRESENT** is a lightweight block cipher algorithm that contains 64-bit plain text and 128-bit key for encryption and decryption (ED) process, and it is represented in figure 5.

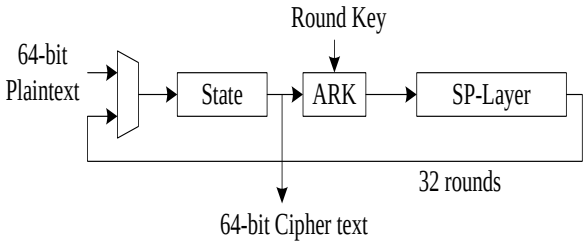

Fig.5 Present Architecture

The PRESENT cipher mainly contains state register for 32-rounds updation, followed by ARK with Key updation module and perform the Substitution –permutation (SP) modules and generated output are a loop back to the multiplexer. The decryption modules use the Inverse SP layer for the generation of the 64-bit original text.

IV. RESULTS AND ANALYSIS

The physical layer cryptographic algorithms are designed and analyzed on the Artix-7 FPGA platform for IoT applications. The security algorithms like AES, DES, LED, XTEA, and PRESENT are designed, and hardware constraints are tabulated in table 1, and its graphical representation is shown in figure 6. The Hardware constraints like Slices (Chip Area), Frequency (MHz), Latency (clock cycles), Throughput (Mbps), and Efficiency (Mbps/slice) are evaluated. The AES module uses 128-bit key and data for encryption and utilizes 42 clock cycles with a throughput of 889 Mbps, and the efficiency of the chip is 0.89 Mbps/ slice. The DES module uses 64-bit data and key for encryption and utilizes 34 clock cycles with a throughput of 590 Mbps, and the efficiency of the chip is 2.25 Mbps/ slice. The LED module uses 64-bit data and 128-bit key for encryption and utilizes 48 clock cycles with a throughput of 478 Mbps, and the efficiency of the chip is 1.2 Mbps/ slice.

Table 1 Comparative analysis of Physical Layer Cryptographic algorithms-Encryption process for IoT

Designs	Data	Key	Slices	Frequency (MHz)	Latency (Clock cycles)	Throughput (Mbps)	Efficiency (Mbps/Slice)
AES	128	128	989	292	42	889	0.89
DES	64	64	262	313	34	590	2.25
LED	64	128	404	358	48	478	1.2
XTEA	64	128	238	264	64	264	1.1
PRESENT	64	128	231	411	32	822	3.55

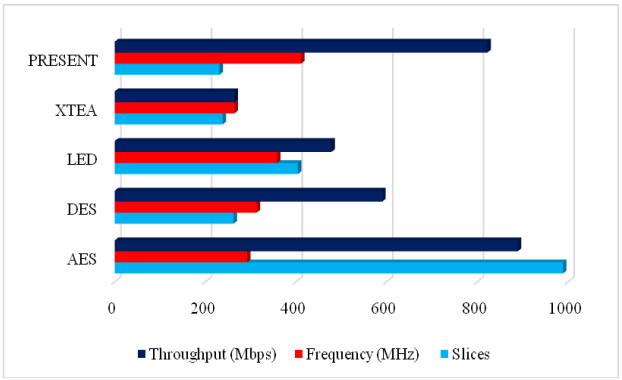

Fig.6 Graphical representation of Physical Layer Cryptographic algorithms-Resources Utilization

The Lightweight cipher module XTEA module uses 64-bit data and 128 bit key for encryption and utilizes 64 clock cycles with a throughput of 264 Mbps, and the efficiency of the chip is 1.1 Mbps/ slice. Similarly, the PRESENT module uses 64-bit data and 128 bit key for encryption and utilizes 32 clock cycles with a throughput of 822 Mbps, and the efficiency of the chip is 3.55 Mbps/ slice. The AES operates with high throughput and the chip area and efficiency are not suitable for IoT. The LED works at low latency and efficiency are moderate. The PRESENT cipher works at low latency, high throughput, and provides excellent efficiency.

V. CONCLUSION AND FUTURE WORK

The hardware-based physical layer security solutions and related cryptographic algorithms are discussed and implemented on Artic-7 FPGA. The physical layer security solutions are highlighted for future usage in IoT environments for real-time applications. The physical layer security based cryptographic symmetric key algorithms like AES, DES, LED, XTEA, and PRESENT are designed and analyzes the performance metrics on the hardware platform.

The AES design work at 889 Mbps and the efficiency of the design is 0.89 Mbps/slice, and it is complicated for IoT applications. The PRESENT cipher works at 822 Mbps, and the efficiency of the design is 3.55 Mbps/slice, and it is quite useful for IoT environments and suitable real-time scenarios. In the future analyzes the better hardware constrained cryptographic algorithms for IoT devices and better authentication from the attacks.

REFERENCES

1. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. IEEE InternetThings J. 2014, 1, 22–32. [CrossRef]
2. Jin, J.; Gubbi, J.; Marusic, S.; Palaniswami, M. An information framework for creating a smart city throughthe internet of things. IEEE Internet Things J. 2014, 1, 112–121.
3. Ericsson, ‘‘Ericsson mobility report on the pulse of the networked society,’’ Jun. 2015. [Online]. Available: www. ericsson.com.
4. I. Stojmenovic, "Machine-to-machine communications with in-network data aggregation, processing, and actuation for large scale cyber-physical systems," IEEE Internet Things J., vol. 1, no. 2, pp. 122–128, Apr. 2014.
5. Gupta, A.; Jha, R.K. A survey of 5G network: Architecture and emerging technologies. IEEE Access, 2015, 3,1206–1232.
6. Zhang, R.; Wang, J.; Zhong, Z.; Li, X.; Guizani, M. Energy-efficient beamforming for 3.5 GHz 5G cellularnetworks based on 3D spatial channel characteristics. Comput. Commun. 2018, 121, 59–70. [CrossRef]
7. Zhang, R.; Jiang, X.; Taleb, T.; Li, B.; Qin, H.; Zhong, Z.; Zhan, X. Connecting a city by wireless backhaul:3D spatial channel characterization and modeling perspectives. IEEE Commun. Mag. 2017, 55, 62–69.
8. Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A survey on 5G networks for the internet of things: Communication technologies and challenges. IEEE Access, 2018, 6, 3619–3647.
9. D. Naccache, D. Sauveron, "Information Security Theory and Practice. Securing the Internet of Things: 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014, Proceedings", Springer, pp. 201, 2014
10. 3GPP. Cellular System Support for Ultra-Low Complexity and Low Throughput Internet of Things. TR 45.820. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2719 (accessed on 23 September 2018.
11. A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, ‘‘A decentralized approach for security and privacy challenges in the Internet of Things,’’ in Proc. IEEE World Forum Internet Things, Mar. 2014, pp. 67–72.
12. K. Zhang, X. Liang, R. Lu, and X. Shen, ‘‘Sybil attacks and their defenses in the Internet of Things,’’ IEEE Internet Things J., vol. 1, no. 5, pp. 372–383, Oct. 2014.
13. Sun, L.; Du, Q. Physical layer security with its applications in 5G networks: A review. China Commun. 2017, 14, 1–14.
14. Kumar, S.A.; Vealey, T.; Srivastava, H. Security in the Internet of things: Challenges, solutions, and future directions. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5772–5781.
15. Sundaram, B.V.; Ramnath, M.; Prasanth, M.; Sundaram, V. Encryption and hash-based security in the Internet of things. In Proceedings of the 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 26–28 March 2015; pp. 1–6.
16. Li, Z.; Yin, X.; Geng, Z.; Zhang, H.; Li, P.; Sun, Y.; Zhang, H.; Li, L. Research on PKI-like Protocol for the Internet of Things. In Proceedings of the 5th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Hong Kong, China, 16–17 January 2013; pp. 915–918.
17. The OAuth 1.0 Protocol. Available online: http://tools.ietf.org/html/rfc5849 (accessed on 6 January 2018).
18. Ravi, S.; Raghunathan, A.; Kocher, P.; Hattangady, S. Security in embedded systems: Design challenges. ACM Trans. Embedded Comput. Syst. (TECS) 2004, 3, 461–491.
19. Fathy, A.; Tarrad, I.F.; Hamed, H.F.; Awad, A.I. Advanced encryption standard algorithm: Issues and implementation aspects. In Proceedings of the International Conference on Advanced Machine Learning Technologies and Applications, Cairo, Egypt, 8–10 December 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 516–523.
20. King, J.; Awad, A.I. A distributed security mechanism for resource-constrained IoT devices. Informatica, 2016, 40, 133–143.
21. Guruprasad, S. P., and B. S. Chandrasekar. "An evaluation framework for security algorithms performance realization on FPGA." In 2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), pp. 1-6. IEEE, 2018.
22. Anusha, R., and V. Veena Devi Shastrimath. "LCBC-XTEA: High Throughput Lightweight Cryptographic Block Cipher Model for Low-Cost RFID Systems." In Computer Science On-line Conference, pp. 185-196. Springer, Cham, 2019.

AUTHORS PROFILE

Mrs Bharathi R has got her B E degree from DSCE, B’luru ,M. Tech., degree in VLSI and Embedded Systems from SJCE , Mysore, Perusing PhD in PRIST university, Thanjavur, Tamilnadu. Presently working as an Associate Professor in the Department of Computer Science and Engineering in BMSIT &M, Bengaluru. Her fields of interest are Computer Networks, Cryptography, Microprocessor and Microcontroller, DAA. She has got 18 years of rich experience in teaching and 4 years of research experience. She has guided final year BE students and M.tech students in her carrier. She has published 20 research papers in both national and international journals and conferences.

Parvatham Vijay is currently working as a Professor in PRIST deemed to be University, Vallam, Thanjavur. She received B.E. degree in Electronics and Communication Engineering fromBharathidasan University, Tiruchirappalli. M.E. and Ph.Ddegreesreceived from Anna University, Chennai in 2006 and 2017 respectively. Her research work is carried out in the field of Image processing, VLSI Design Algorithms and Architectures, SoC design, fractal image analysis.