International Journal of Engineering &Technology, 7 (3.12) (2018) 516-520

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Centralized Authentication Smart Locking System using RFID, Fingerprint, Password and GSM

M. Sai Divya[1], M.NagabhushanaRao[2]

[1]M.Tech Scholar, [2]Professor, [1,2]Department of Computer Science &Engineering,
Koneru Lakshmaiah Education Foundation, vaddeswaram, Guntur, A.P, India
**Corresponding Author Email: mnraosir@gmail.com, saidivya293@gmail.com*

Abstract

The primary aim of implemented project is design of the RFID based high security building locking system, fingerprint, GSM technology, and password. In the implemented system, only authorized person can be enter from the building door locking by scanning his card. The implemented building locking system works based on the RFID, Password, GSM and Fingerprint. The Door locking system can be activated for authorized and valid user by scanning his card and unauthorized user enters in the building a Gsm module sent a message to authority unauthorized user entering in the building.

Keywords: *GSM, Keyboard, Microcontroller, RFID, FINGERPRINT, locking of system*

I. Introduction

Verification of the Fingerprint is one of the real time system security systems. The Fingerprint which can be detected can be sent to the microcontroller for authentication purpose. [1-5] It is implemented with two algorithms and 4 sensors such as optical, ultrasonic, passive and active capacitances. The fingerprint and RFID technology is used widely for security purpose. Here also we used these two algorithms. The system of automatic fingerprint identification having collection of image, pretreatment, extraction of feature as well as matching feature and on many parts. To verify a person, the fingerprints are one of the best identities. The primary advantage of the RFID, Finger Print, GSM and RFID is efficient security. The RFID can detect any type of object by using radio transmission frequency. RFID can be an electronic system which can transmit and receive data over radio waves. It can be useful for tracking, detecting and sorting the different objects. The implemented system having the RFID reader, Modem i.e GSM, finger print scanner keyboard as well as LCD. In this the reader of the RFID reads the Id number of the person. If is valid then only the access can be given. If it is not valid then the entire process can be stopped. When the Finger print is valid the password can be sent to the valid user mobile number through microcontroller. Our implemented system needs 2 passwords to open the home locking. When the user entered the two passwords then the home locking will be opened if those are matched. Otherwise the locker cannot open and a text message will be sent to the authorized user as an alert. RFID means Radio Frequency Identification. It can detect the person useful in banks, offices as well as in homes.

2. Related Works

In this section, the released works regarding this system is described below. The primary aim of this system is provide security to the ATM machines. If the bank card of the user is lost then the password is easily stolen by others. [6-10]The unauthorized persons easily stole your money by drawing it through ATM with the help of your card and password with in less time. So you may face several financial problem, to avoid such type of issued we implemented this secure home locking system. [11-15] The LPC 2148 is used as microprocessor, acts as core in ARM 7 which can be useful for advanced algorithm for providing the security with fingerprint technology. It will increase the security to the user in ATM machine. Here, I proposed the Finger print verification in ATM machines with the help of Biometric. [16-20] this technique has been chosen based on its security, reliability and etc. The working of this machine can be done when the valid fingerprint received only. [21-25] If the ATM receives valid fingerprints then only it works otherwise the process has been stopped. And it may send a message to the registered user regarding the suspicious activity as an alert. Like this we can secure the user money in ATMS even when the card lost.

3. Proposed Method

Here, The fingerprint reader the reads the prints of finger of an user and send it to the Microcontroller, If the id is valid then the microcontroller give access to the user otherwise the entire process can be stopped in the machine and immediately it sent the alert to the authorized user regarding the suspicious activity. Then that person may take necessary steps to stop such type of activity through her/his card locking. When the Fingerprint of the user matched with id then it sent the password to the register user mobile or email. Then that person can type those password he or she can access the machine. If those are matched then building locking will be opened. Otherwise it will be in same conditions and alerts will be sent to the specified person mobile number.

4. RFID Fundamentals

The RFID means automatic identification technology to the various objects. The primary operation of the RFID is it can able to track the tagged time location. According the source of the power, the tags of the RFID may differentiate as 3 types of categories. Those are

- Active tags
- Passive tags
- Semi-passive or semi-active tags

The tag which is active having the transceiver of the radio and battery which is useful for the power to the transceiver.

Active tag is much powerful compared to the passive and semi active or semi passive tags.

Again the Tags of the RFID can be classified into read/write memory as well as read-only memory. The read/write memory tags are costlier then read-only memory tags.

RFID tags can be operated in 3ranges of the frequencies:

- Low frequency (LF,30–500kHz)
- High frequency (HF, 10–15MHz)
- Ultra high frequency (UHF, 850–950MHz, 2.4–2.5GHz, 5.8GHz).

20 Low Frequency tags can be less affected with the fluids as well as metals presence metals among the tags of the higher frequency.

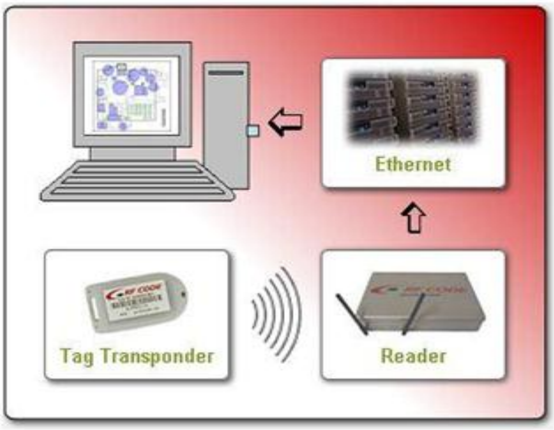


Fig. 1: RFID reader

The Reader of RFID represented in the figure 1. The Smart cards operated on 13.56Mega Hz, may be the usual group member. Moreover, the tags of the UHF affected with the fluids as well as metals. The tags of UHF expensive compared to the other ones. The classic UHF tags frequency is 868 Mega Hz (Europe), 915 Mega Hz (USA), 950Mega Hz (Japan), and 2.45Geha Hz. The tag which is active that can be enabled the higher signal strength as well as extended the range of communication till 100 to 200meters.

5. GSM

The Global System for Mobile communications is one of the technologies that work on all mobile phone networks. GSM can be an open as well as the digital cellular technology utilized to transmit the mobile voice as well as data services.

Fig2. GSM Modem

Features

- Single 3.2 volts to 4.5 Volts supply voltage
- Consumption of the power in the mode of SLEEP is 2.5mA in SIM300 tri-band
- Computable to the MT, CB, MO text as well as mode of the PDU
- Storage of the SMS will be in SIM card
- 1.8Volts and 3Volts Supported SIM Card

6. Fingerprint

It is the widely used techniques for security. It provides high security compared to the others. These are helpful to identify a person. Ithas 3basic patterns. Those arch, whorl as well as loop.

These are helpful for security purpose. If the fingerprint of the person matched then the microcontroller can allowed the user to enter into the building. Otherwise a sms will be sent to authorize user as an alert.

Arch: The ridges started from finger one side and rise in finger center form the arc, as well as after that exit at another side.

Loop: The ridges started from finger one side, like a curve after that exited on the same side.

Whorl: The Finger Ridges forms circularly around finger central point.

7. Block Diagram

The Figure 3 represents the Block Diagram of the smart building locking System with RFID, PASSWORD, GSM technology and FINGERPRINT. Here, the reader of the RFID reads the fingerprints via passive tag and sent to the Microcontroller. If the id is valid then the microcontroller give access to the user otherwise the entire process can be stopped in the machine and immediately it sent the alert to the authorized user regarding the suspicious activity. If it is valid it sent two passwords to the user mobile number. She or he has to enter the passwords and then he or she can access the building locking.

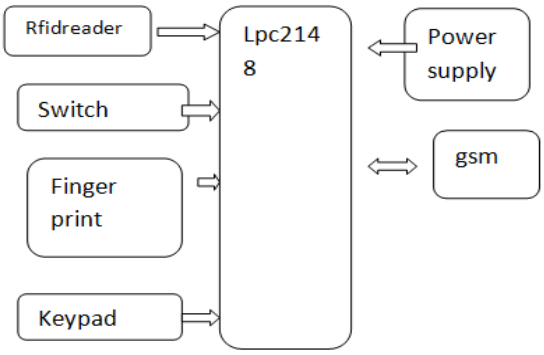


Fig. 3: Block Diagram

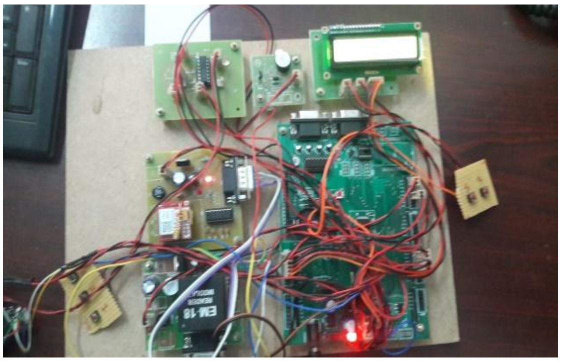
8. Software

The entire code is in C /in assembly language. It is compiled with keil software. The Hex code generated after compiler operation and it can be stored in Computer. It can be embedded into LPC.

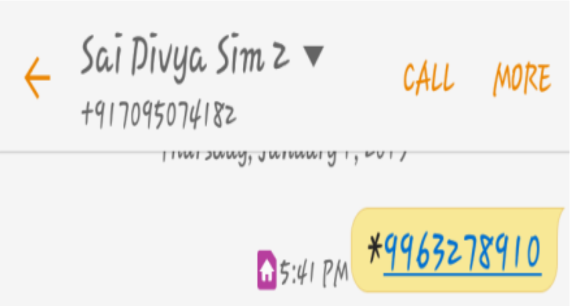
9. Implementation

First we switch on the power and we have two modules of arm 7 is GSM module and RFID module .we want to insert the sim in GSM module we set the GSM mode and we enter the user mobile number and it is successfully entered into the database and we got sms as modem initialized . an LCD will be on and if the signals are in fast then light blink fast and if signals are not fast then light blink slow then we set the RFID mode and the person scan his authorized card and a sms came to mobile as authorized card and then the person give finger print and then the GSM module will check his fingerprint is enrolled or not and if enrolled it will identify in database and door will open then buzzer sound will come it indicates door is opened. If the person scan his card and card is unauthorized card an sms will came to mobile as unauthorized card and person give fingerprint and it does not enrolled and not identify in database for the person the door will not open .if the new person or unknown person enters then the person does not have authorized card then the person has OTP option as alternative if click on OTP then an OTP will be send to mobile then user mobile will tell the OTP to new person then new person enters OTP and person gets permission to enter building and door will open to enter .

10. Results



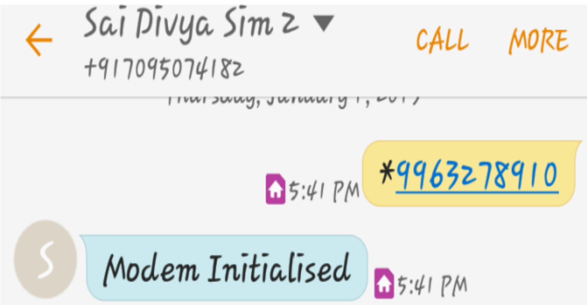
First power switch is on and keep GSM mode to place sim in the GSM module



Sai Divya Sim 2 ▾
+917095074182

*9963278910 5:41 PM

Entering the sim number placed in the kit into database to send sms to user mobile



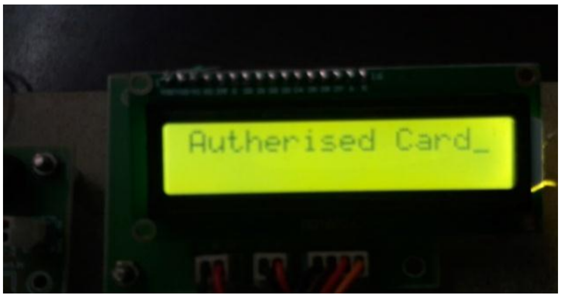
Sai Divya Sim 2 ▾
+917095074182

*9963278910 5:41 PM

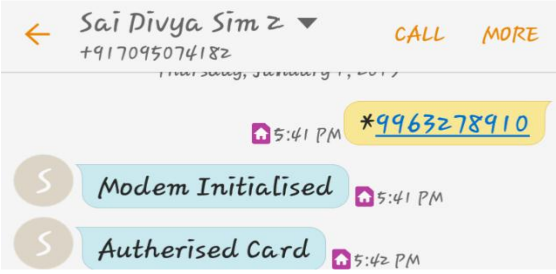
Modem Initialised 5:41 PM

Sim number is entered into database and Database send sms to mobile as modem initialized and LCD will on

Person who enters into building swipe his authorized card



Person swipe card and database shows entered card is authorized card



Sai Divya Sim 2 ▾
+917095074182

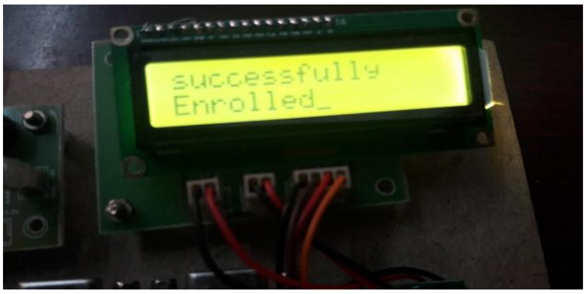
*9963278910 5:41 PM

Modem Initialised 5:41 PM

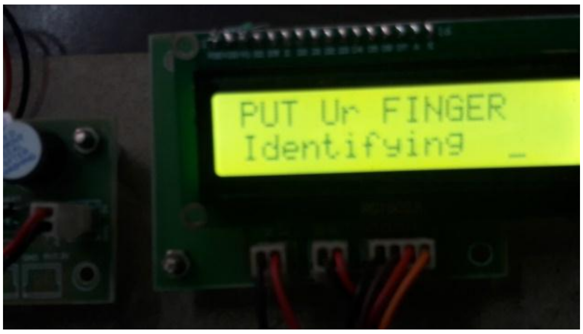
Autherised Card 5:42 PM

Person swipe card and database shows authorized card and GSM sends mobile as authorized card

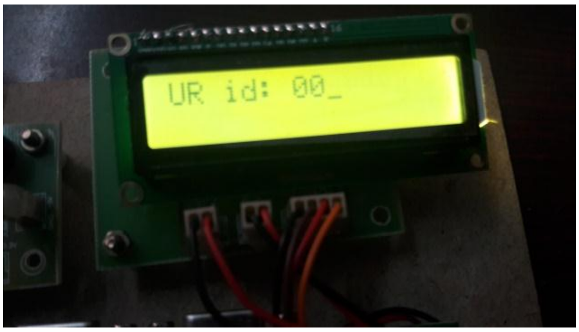
After swiping card person gives fingerprint and the person does not have enrolled his fingerprint in database then enrolls his Finger for fingerprint



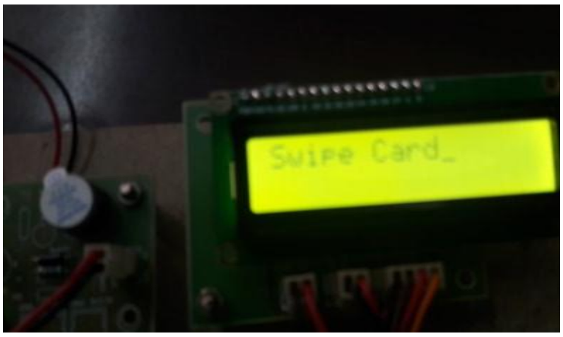
Person Finger enrolled successfully for fingerprint



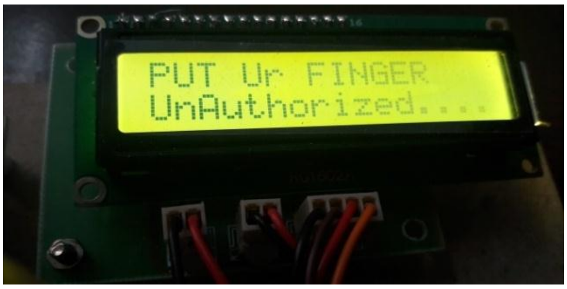
Person enrolls finger for fingerprint and enrolled successfully and database identifies his fingerprint



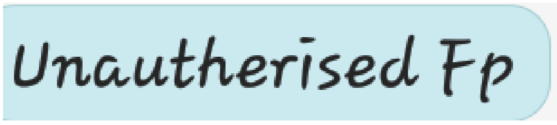
Finger print is identified and database provide ID number



Person swipe the authorized card to enter into building

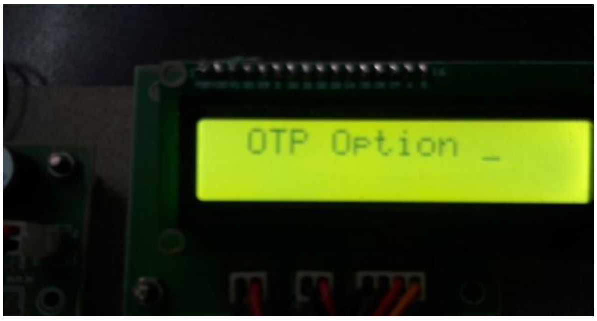


Person swipe card it shows authorized card and GSM sends sms to user mobile authorized card then person give fingerprint and database shows unauthorized fingerprint because his fingerprint is enrolled in database

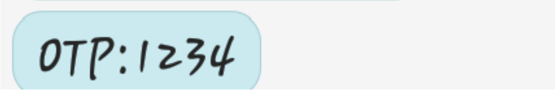


Unautherised Fp

Gsm sends sms to mobile entered fingerprint is unauthorized

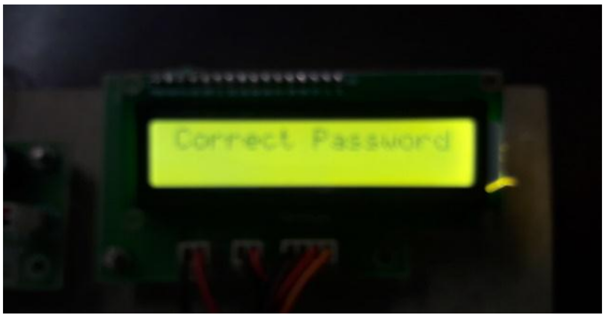


For new person OTP option is there person click OTP and database sends sms OTP to users mobile



OTP:1234

Gsm sends OTP to user mobile and user of mobile tells OTP to new person



The person Enters OTP and database shows entered OTP is correct password and the person can enter into building

11. Conclusion

The implemented building locking security system with the PASSWORD, RFID, GSM, and FINGERPRIENT can be low cost and have low power consumption. It can be in compact size. Here the comparison can be done in micro controller when the password entered by the user. If both passwords are same then the building locking can be opened otherwise an alert will be sent to the authorized mobile number.

References

[1] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", InternationalJournal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[2] Hugh Wimberly, Lorie M. Liebrock, "Using Fingerprint Authentication to Reduce SystemSecurity: An Empirical Study", 2011 IEEE Symposium on Security and Privacy.

[3] Gangi.Raghu Ram, N.Rajesh Babu, " Tracking objects using RFID and Wireless Sensor Networks" [ijesat] International Journal Of Engineering science & Advanced technology Volume-2, Issue-3

[4] [Zhang Jinhai, Liu Xinjian, Chen Bo, "The design and implementation of ID Authentication System Based on Fingerprint Identification", 2011 Fourth International Conference on Intelligent Computation Technology and Automation.

[5] Pramila D. Kamble, Dr.Bharti, W. Gawali, "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization", International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

[6] V.Ramya1, B. Palaniappan, V.Sumathi, “Gsm Based Embedded System For Remote Laboratory Safety Monitoring And Alerting”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.6, November 2012.

[7] Art Conklin1, Glenn Dietrich2, Diane Walz3, “Password-Based Authentication: A System Perspective”, Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[8] D. Vinod kumar, Prof.M R K Murthy, “Fingerprint Based ATM Security by using ARM7”, IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN: 2278-2834 Volume 2, Issue 5 (Sep-Oct 2012).

[9] F. Yen, Y. Xie, F. Yu, R. P. Yu, and M. Abadi, ―Host Fingerprinting and Tracking on the Web: Privacy and Security Implications*”, Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, 5th February – 8th February 2012.

[10] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting", *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, 2013.

[11] K. Mowery, D. Bogenreif, S. Yilek, and H. Shacham, ―Fingerprinting information in JavaScript implementations‖, *Proceedings of W2SP 2011*, H. Wang, Ed. IEEE Computer Society, May 2011.

[12] T. Kohno, A. Broido, and K. Claffy, ―Remote physical devicefingerprinting‖, *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, April-June 2005, pp. 93–108.

[13] G. Nakibly, G. Shelef, S. Yudilevich, "Hardware Fingerprinting Using HTML5", Cornell University Library (CoRR), abs/1503.01408, Mar. 2015.

[14] K. Mowery and H. Shacham-Pixel perfect Fingerprinting canvas in HTML5‖, *Proceedings of W2SP 2012*, M. Fredrikson, Ed. IEEE Computer Society, May 2012.

[15] Y. Shu et al., "Gradient-based fingerprinting for indoor localization and tracking", *IEEE Trans. Ind. Electron.* 63, no. 4, pp. 2424-2433, Apr. 2016.

[16] S.Sivaranjani,S.Sumathi,"Implementation of Fingerprint and Newborn Footprint Feature Extraction on Raspberry Pi", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS’ 15.

[17] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, USA, NY, New York:Springer-Verlag, 2003.

[18] Q. Zhao, D. Zhang, L. Zhang, N. Luo, "Adaptive fingerprint pore modeling and extraction", Pattern Recognition., vol. 43, no. 8, pp. 2833-2844, Aug. 2010.

[19] L. Zhang, L. Zhang, D. Zhang, H. Zhu, "Online finger-knuckle-print verification for personal authentication", Pattern Recognit., vol. 43, no. 7, pp. 2560-2571, Jul. 2010.

[20] L. Zhang, L. Zhang, D. Zhang, "Finger-knuckle-print verification based on band-limited phase-only correlation", Proc. Int. Conf. Comput. Anal. Images Patterns, pp. 141-148, 2009-Sep.

[21] [Kolla Bhanu Prakash (2015), "Mining issues in traditional indian web documents", Indian Journal of Science and Technology, 8(32).

[22] Kolla Bhanu Prakash, Dorai Rangaswamy M.A. and Ananthan T.V. (2014), “Feature extraction studies in a heterogeneous web world”, International Journal of Applied Engineering Research, Research India Publications,Vol.9,No. 22, pp- 16571-79.

[23] Kolla Bhanu Prakash, Dorai Rangaswamy M.A. and Arun Raja Raman (2012), “ANN for Multi-lingual Regional Web Communication”, Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, LNCS 7667, pp. 473-478.

[24] Kolla Bhanu Prakash, Dorai Rangaswamy M.A. and Arun Raja Raman (2012), “Statistical Interpretation for Mining Hybrid Regional Web Documents”, Communications in Computer and Information Science’, Springer-Verlag,Berlin-Heidelberg, CCIS 292, pp. 503- 512.

[25] Kolla Bhanu Prakash and Dorai Rangaswamy M.A. (2016), “Content Extraction of Biological Datasets Using Soft Computing Techniques”, Journal of Medical Imaging and Health Informatics, American Scientific Publishers, Vol. 6, 932- 936.

[26] A Murali, K. Hari Kishore, “Efficient and High Speed Key Independent AES Based Authenticated Encryption Architecture using FPGAs “International Journal of Engineering and Technology(UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 1.5, Page No: 230-233, January 2018.

[27] P Ramakrishna, K. Hari Kishore, “Design of Low Power 10GS/s 6-Bit DAC using CMOS Technology “International Journal of Engineering and Technology(UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 1.5, Page No: 226-229, January 2018.

[28] G.S.Spandana, K Hari Kishore “A Contemporary Approach For Fault Diagnosis In Testable Reversible Circuits By Employing The CNT Gate Library” International Journal of Pure and Applied Mathematics, ISSN No: 1314-3395, Vol No: 115, Issue No: 7, Page No: 537-542, September 2017.

[29] K Hari Kishore, CVRN Aswin Kumar, T Vijay Srinivas, GV Govardhan, Ch Naga Pavan Kumar, R Venkatesh “Design and Analysis of High Efficient UART on Spartran-6 and Virtex-7 Devices”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 09 , pp. 23043-23052, June 2015.

[30] K Bindu Bhargavi, K Hari Kishore “Low Power BIST on Memory Interface Logic”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 08 , pp. 21079-21090, May 2015.

[31] Korraprolu Brahma Reddy, K Hari Kishore, “A Mixed Approach for Power Dissipation Reduction in Nanometer CMOS VLSI circuits”, International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 9, Number 18 , pp. 5141-5148, July 2014.