International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences
(NCDATES- 09th & 10th January 2015)

RESEARCH ARTICLE OPEN ACCESS

A Secured Approach for ID Authentication System using RFID and Fingerprint Technology

M.Hima Bindu, T.Jayanthi, P.Chethana
(1), M.Tech(ECE), Assistant Professor, DVR College of Engineering and Technology, Medak,Telangana.
(2), M.Tech(ECE), Assistant Professor, DVR College of Engineering and Technology, Medak,Telangana.
(3), M.Tech(ECE), Assistant Professor, DVR College of Engineering and Technology, Medak,Telangana.

Abstract-
Authentication is a fundamental issue to any trustoriented computing system and also a critical part in many security protocols. In addition, authentication also serves as the first step for many other security purposes, such as key management and secure group communication [5].Passwords or smartcards have been the most widely used authentication methods due to easy implementation and replacement; however, memorizing a password or carrying a smartcard, or managing multiple passwords/smartcards for different systems (one for each system),is a significant overhead to users. In addition, they are artificially associated with users and cannot truly identify individuals Performing authentication is notoriously difficult. Biometrics has been widely used and adopted as a promising authentication [8] method due to its advantages over some existing methods, particularly, its resistance to losses incurred by theft of passwords and smart cards. However, biometrics introduces its own challenges, Such as being irreplaceable once compromised. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, workstations, and computer networks. It can be used during transactions conducted via telephone and internet (electronic commerce and electronic banking).
Keywords: ARM7 (LPC2148), RFID, Fingerprint module,keypad, buzzer, DC motor

I. INTRODUCTION

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioural characteristics. This method of identification [1] is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-of identification; identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access [8] to or fraudulent use of ATMs, cellular phones, smart cards, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest. Various types of biometric systems [1] are being used for realtime identification; the most popular are based on fingerprint matching. A biometric system is essentially a pattern recognition [4] system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristics possessed by the user. Depending on the context, a biometric system can be either a verification (authentication) [8] system or an identification system. The current security model for verification of identity, protection of information and authentication to access data or services is based on using a token or password, tied to and thereby representing an individual to either authenticate identity or allow access to information [Annet al, 2007]. This token may be password or shared secret (something you know), an identity card (something you have) or biometric (something you are). In all this cases, the details of the token are held by a third party whose functions is to authorizes and at times allow the
transaction to proceed if the details of an individual's token match those stored in a database. By using biometrics it is possible to establish an identity
based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.

1.1 EXISTING SYSTEM

Present in existing system the person who ever want to access his things or take his amount from Bank Lockers first of all he wants to show his id card

in front of the card accessing machine. If the card is valid then he wants to enter the password in a particular machine. If the password is correct then only the locker system will be opened otherwise it will not be opened. So likewise the person can access his things from bank lockers.

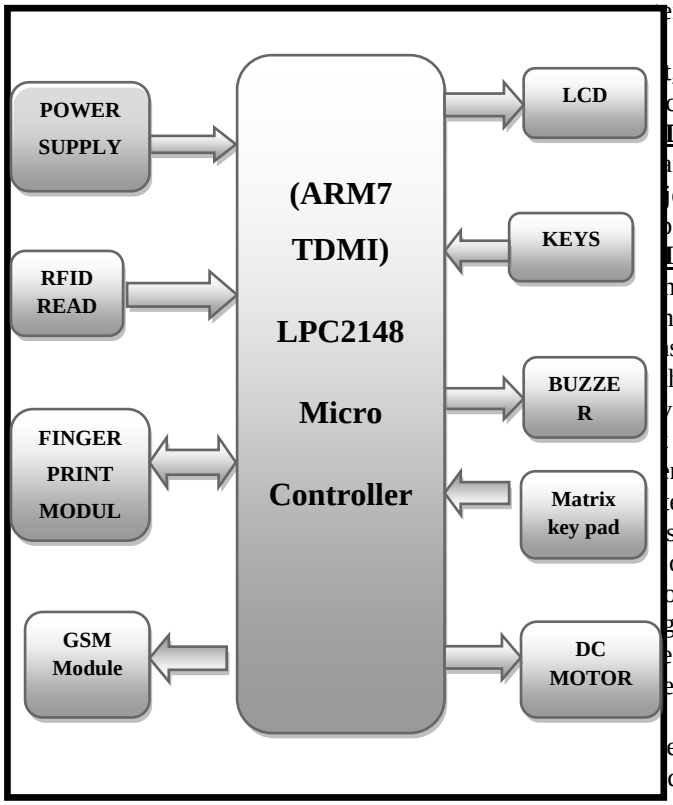
Not only in banking systems for suppose in military areas also only authorized persons have to enter in that secure area that means the area will be restricted. The authorized persons those who wants enter in that restricted area first of all he wants to show his id card in front of the card accessing machine, if it is valid card then the person will have to enter the password, if it is valid password then only the door will be opened otherwise it will not be opened

DISADVANTAGES OF EXISTING SYSTEM

- The main disadvantage of this existing system is person ID card is stolen by his colleagues or family members and they know the password also what happens in that case?
- By using authorized persons identity card some other person will enter in that particular restricted area in military what happens in that situation?

II. PROPOSED SYSTEM STRUCTURE AND PROTOTYPE DESIGN

Figure.



A. Analysis of hardware Structure

ARM7TDMI: The ARM7TDMI-S processor is a member of the ARM family of general-purpose 32-bit microprocessors. The ARM family offers high performance for very low-power Consumption and gate count.

The ARM architecture is based on Reduced Instruction Set Computer (RISC) Principles. The RISC instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs. This simplicity gives:

- A high instruction throughput
- An excellent real-time interrupt response
- A small, cost-effective, processor macro cell.

Microcontroller: A Micro controller consists of a powerful CPU tightly coupled with memory RAM, ROM or EPROM), various I / O features such as Serial ports, Parallel Ports, Timer/Counters, Interrupt Controller, Data Acquisition interfaces-Analog to Digital Converter (ADC), Digital to Analog Converter (ADC), everything integrated onto a single Silicon Chip.

It does not mean that any micro controller should have all the above said features on chip, Depending on the need and area of application for which it is designed, The ON-CHIP features present in it may or may not include all the individual section said above.

Any microcomputer system requires memory to store a sequence of instructions making up a program, parallel port or serial port for communicating with an ernal system, timer / counter for control purposes generating time delays, Baud rate for the serial , apart from the controlling unit called the Central cessing Unit.

D Display Section: This section is basically ant to show up the status of the project. This ject makes use of Liquid Crystal Display to lay / prompt for necessary information.

ID: RFID is an acronym for Radio Frequency ntification. In general terms, RFID is a means of ntifying a person or object using a radio frequency smission. In other words RFID is an electronic hod of exchanging data over radio frequency ves. The technology can be used to identify, track, or detect a wide variety of objects.

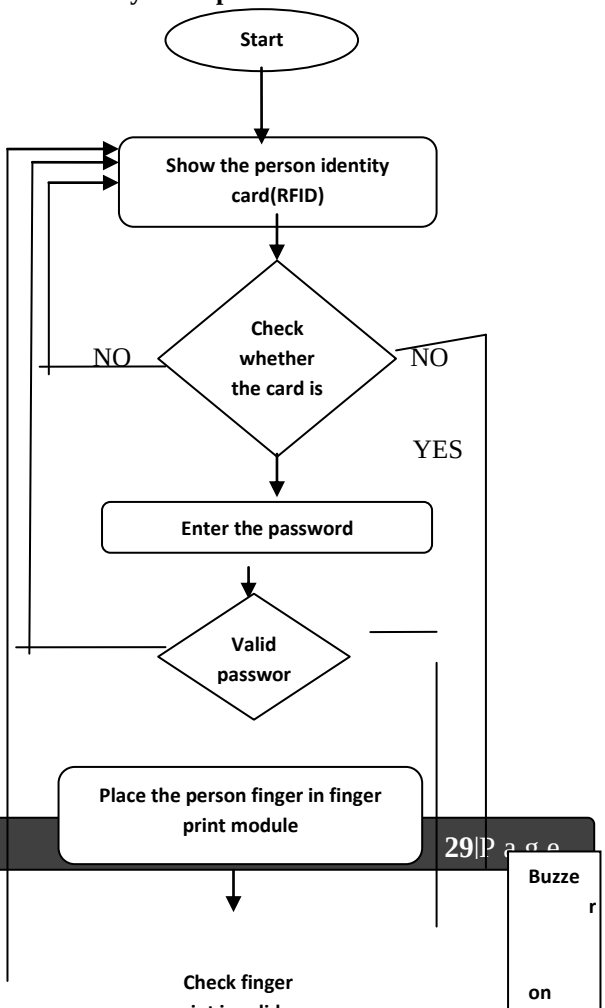
re are three major components of an RFID tem: the reader, the antenna, and the tags. Each tag ssociated with a unique number. When a tag is in detection range of the reader, the number is read. o types of tags can be found: active tags with a ger detection range and passive tags with a shorter ction range. An RFID tag is usually attached to an ct and the information of the object along with RFID number are recorded in the database. enever the RFID tag is sensed, the object can thus dentified.

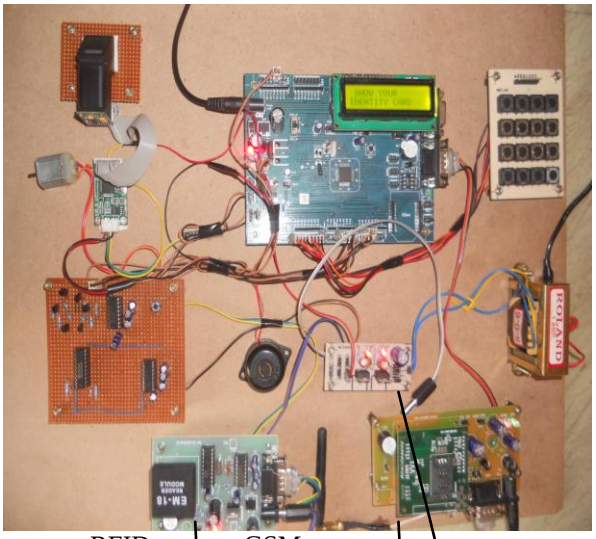
Finger Print Scanner: A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.
It supports wide range of fingerprint sensor interoperability giving you a freedom to select suitable sensor that most fits to your application. Furthermore, the fingerprint data for enrollment and verification are compatible among different sensors, even if they are based on different technologies. This feature of unification presents application manufacturers and system integrators with much more flexibility than ever before.
Keys Section: With the help of these keys the users can enroll their Finger prints and deleting their figure prints.
MAX- 232: To allow compatibility among data communication equipment made by various manufactures, an interfacing standard called RS232 was set by the Electronic Industries Association (EIA).This RS-232 standard is used in PCs and numerous types of equipment .However, since the standard was set long before the advent of the TTL logic family, its input and output voltage levels are not TTL compatible. In RS-232 ,a 1 is represented by -3 to -25V,while a 0 bit is +3 to +25V,making -3 to +3 undefined. For this reason, to connect any RS-232 to a microcontroller system we must use voltage converters such as MAX232 to convert the TTL logic levels to the RS-232 voltage levels and vice versa.
So here we are using this MAX-232 to have compatibility between the Finger Print Scanner and microcontroller.
GSM Module: This module is mainly used to send the message for the authorized person.
Buzzer: This is the output device which we are using to indicate the unauthorized person.
Locker system(DC motor): Here we are demonstrating a DC motor as the Locker for the authorized persons in the Locker system mode.

B. Building the Prototype System

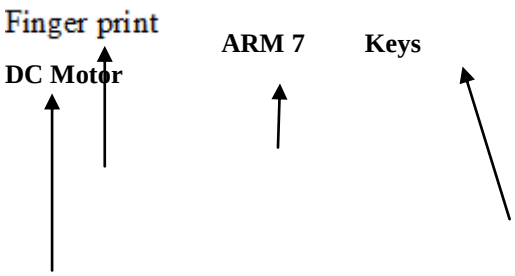
In this project initially the users will enroll their figure prints that will be save in the data base.
step1: In this project initially the user is made to show a RFID tag to the reader. If it is a valid one then it goes to second step. Otherwise it gives the error message display like invalid person again it displays to show your RFID card.
step2: In this step the user have to enter the correct password, if the user will entered the wrong password it will not moves the next step and the buzzer will be on, if the password accessing is continuously failed for three times means then process will move to the initial condition i.e. RFID tag showing step. If the user will entered the correct password then controller asks for a fingerprint access and message is sent to authorized person through GSM,
Step3: In this step the controller asks for a figure print access, if the finger print accessing is failed then buzzer will be on and the process will move to the first step i.e. RFID tag showing step. If fingerprint access is matched with stored fingerprint or authorized person finger print then it moves to fourth step. If it matches then he or she can open the locker and message is sent to authorized person through GSM.

C. System operation flow





When kit is switched on, first it displays "WELCOME TO THE PROJECT" in lcd. After some delay it displays "SHOW YOUR IDENTITY CARD" in lcd display. The user show their RFID tag in front of the RFID reader. If the tag is invalid Buzzer will be on at the same time it displays "INVALID PERSON" in lcd display. If the tag is valid one it displays "VALID PERSON" in lcd display. After that it displays "ENTER CODE FOR VERIFY" in lcd, through the keys user have to enter the password. If the user wrong password Buzzer will be on and at the same time it displays "WRONG PASSWORD REENTER CODE VERIFY". If we entered the correct password it displays "PASSWORD ENTERED CORRECT". After some delay it displays "CHECKING FOR FINGER PRINT" "PLACE YOUR FINGER IN FINGERPRINT MODULE showing this display user have to place his print module. If the fingerprint image is not valid buzzer will be on and displays "INVALID PERSON" but if it is valid image it displays "IMAGE IDENTIFIED" "VALID PERSON IMAGE" then the DC motor will be opened and closed. the practical implementation on kit.



III. BIOMETRICS

Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person Typical characteristics used for authentication include fingerprint, iris and face. A conventional biometric authentication system consists of two phases: verification (below Figure).

During the enrolment phase, a biometric feature set is extracted from user's biometric data and a template is created and stored. During the verification phase, the same feature extraction algorithm is applied to query biometric data, and the resulting query feature set is used to construct a query template. The query template is matched against the stored template(s) for authentication. Compared to password/smartcard approaches, biometrics-based solutions have many desired features [5] such as being resistant to losses of passwords and smartcards, as well as Biometrics bears a user's identity and it is hard to be forged. Unfortunately, brings its own complications:

• Security concern: conventional system record *biometric templates* Entity's (CA's) database. The stored templates, which correlate to users' biometric data, become potential targets to be attacked. Some literature [1], (8)vulnerabilities caused by the compromise of stored templates [1]. enrolment and smartcard-based authentication incurred by theft user-friendliness. biometric authentication

in a Central Authentication tacked. 8] has identified the • Privacy concern: Biometrics identifies individuals. To the best of our knowledge, conventional biometric authentication system is primarily built upon a fully-trusted model; that is, the central authentication entity (CA) is trusted to take full control of users' biometric information and is assumed to not misuse the information. This

assumption of trustworthiness about the CA is not sufficient in the current malicious environments, since handing over one's biometric information to other parties or loss/compromise of one's biometric template will cause serious user privacy [5] concern.

• Irreplaceability: biometric data is permanently bound to a user, and it is almost impossible to generate a new set of biometric features for a legitimate user. Thus compromised biometrics is not replaceable. Many approaches [5], [8] addressing the security and privacy issues of biometrics have been proposed in the literature. These approaches avoid storage of plain biometric templates by recording them in a "distorted" way.

A. Biometric Recognition System

The Biometric Recognition Systems are used to identify the person based on the feature vectors of any one of the biometric that the person possesses [8]. These systems are person authorized systems hence offer more secure and convenient process of identification compared to alternative methods of identification. Each person has to establish the identity ranging from drivers' license to gaining entry into a country to the passport. The biometric system uses the individual's physical characteristics like fingerprint, hand geometry, face, voice or iris. A simple biometric system consists of four modules: Image acquisition, Pre-processing, Feature extraction and Recognition.

i) Image Acquisition Module

This is the first module to acquire the biometric input. The input can be image according to the selection of biometrics. The sensors like high resolution CCD camera or recorder can be used to capture the biometric image. The distance between the sensor and human should be constant, the lighting system as well as physical capture system should be constant to acquire standard biometric input.

ii) Pre-processing Module

Once the input is captured, the original input image or voice signal is processed to remove the noise and blurring effect. The image is localized to extract the region of interest. The voice signal is framed to extract the desired signal. Then this processed input is given to feature extraction module.

iii) Feature Extraction Module

In the feature extraction module, the pre-processed image is used to extract the features. The feature extraction algorithms are applied to get feature vector of the biometric image. There are various feature extraction techniques like Independent Component Analysis, Linear discriminate component, principal component analysis, wavelet transform, LPC, MFCC, etc. According to the biometrics selected and its application the feature extraction technique can be applied.

iv) Recognition Module

The feature vectors, generated in the Feature Extraction Module are used in this module to classify the biometric data. There are the classifiers like hamming distance, Euclidian distance, and Support vector machine classifier. The rules are defined for recognition of a person with his /her biometrics [5]. According to the biometric applications, the suitable classifiers can be used to get better performance of the system. The feature vectors are used to write the decision making rules. In this module user's identity is established or a claimed identity is accepted or rejected.

B. FINGER PRINT

Among all the biometric techniques, fingerprint-based identification [4] is the oldest method which has been successfully used in numerous applications. Figure5 shows fingerprint images. The finger prints of a person have been used as person identification from long time. The finger prints of the identical twins are different. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points [3]. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching techniques can be placed into two categories: minutiae based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures cannot be completely characterized by minutiae. Efforts are being on to try an alternate representation of fingerprints, which will capture more local information and yield a fixed length code for the fingerprint. The matching [12] will then hopefully become a relatively simple task of calculating the Euclidean distance will between the two codes.

Finger Print Classification*:*

Fingerprint classification [4] is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature, which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse

level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. Different algorithms [13] are developed to classify fingerprints into five classes, namely, whorl, right loop, left loop, arch, and tented arch. The algorithm separates the number of ridges present in four directions (0 degree, 45degree, 90 degree, and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters. This information is quantized to generate a Finger Code which is used for classification. This classification is based on a two stage classifier which uses a K-nearest neighbor the first stage and a set of neural networks in the second stage.

VI. CONCLUSION

Secured Approach for ID Authentication System by using RFID and Fingerprint proves to be very effective in providing security.

A step by step approach in designing the Approach for Authentication System by using Fingerprint giving security to the users banking system and providing the security for the locker system using a finger print scanner has been followed. The result obtained in providing the security is quite reliable in all the three modes.

The system has successfully overcome some of the aspects existing with the present technologies, by the use of finger print Biometric Biometric as the authentication Technology

Future Applications:

- ATM machine use: Most of the leading banks have been experimenting with biometrics for ATM machine use and as a general means of combating card fraud.
- Workstation and network access: Many are viewing this as the application, which will provide critical mass for the biometric industry and create the transition between sci-fi device to regular systems component, thus raising public awareness and lowering resistance to the use of biometrics in general.
- Travel and tourism: There are multi application cards for travelers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc.
- Telephone transactions: Many telesales and call center managers have pondered the use of biometrics.

Benefits:

_ No more forgotten passwords, lost cards or stolen pins.
You are your own password.
_ Positive Identification-It identifies you and not what you have or what you carry.
_ Highest level of security.
_ Offers mobility.
_ Impossible to forget.

REFERENCES

[1] Kresimir Delac, Mislav Gregic, "A Survey of Biometric Recognition Methods", 46thInternational Symposium Electronic in Marine, ELMAR-2004, 16-18June 2004,Zadar, Croatia.
[2] Li Ma , Tieniu Tan , Yunhong Wang , Dexin Zhang , "Personal Identification Based on Iris Texture analysis" , IEEE Transactions on pattern Analysis and Machine Intelligence , Vol. 25 No. 12, December 2003.
[3] A.K. Jain, L. Hong, R. Bolle, "On-line Fingerprint verification" , IEEE Trans. Pattern Anal. Mach. Intel. 1997.
[4] K. Karu, A.K. Jain, "Fingerprint classification, Pattern Recognition", 1996.
[5] Anil K. Jain, Arun Ross, Sharath Pankanti "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Vol 1,No. 2, June2006.
[6] Sulochana Sonkamble, Dr. R.C. Thool, Balwant Sonkamble,"An Effective Machine-Vision System for Information Security and Privacy using Iris Biometrics", in The 12th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2008 at Orlando, Florida, USA during June 29th - July 2nd , 2008.
[7] John Daugman, Cathryn Downing, "Effect of Severe Image Compression on Iris Recognition Performance", IEEE Transactions on information Forensics and Security, Vol. 3, No. 1, March 2008.
[8] Joseph Lewis, University of Maryland, Bowie State University," Biometrics for secure Identity Verification: Trends and Developers" January 2002.
[9] Lia Ma, Yunhong Wang, Tieniu Tan, "Iris Recognition Based on Multichannel GaborFiltering", ACCV2002: The 5th Asian Conference on Computer Vision,23-25 January 2002, Melbounce, Australia.
[10] Daugman J: How iris recognition works. *The Computer Laboratory, University of Cambridge.* [Acessed 2003 Jan23at

http://www.CL.cam.ac.uk/users/jgd1000 *webcite*]

[11] http://fingerprint.nist.gov/latent/elft07/ phase1_aggregat.p df.

[12] J. Feng. Combining minutiae descriptors for fingerprint matching. Pattern Recognition, 41(1):342–352, 2008.

[13] Evaluation of latent fingerprint technologies 2007. http://fingerprint.nist.gov/latent/elft07/.

[14] Conclusion of circuit court judge Susan Souder – grants motion to exclude testimony of forensic fingerprint examiner capital murder case: State of Maryland v. Bryan Rose, October 2007.http://www.clpex.com/Information/STATEOFMARYLAN D-v-BryanRose.doc.

Miss. P. Chethana is presently working as an Assistant Professor of Electronics and Communication Engineering in DVR Engineering College Hyderabad, India has done M.Tech from JNTU Hyderabad

Mrs. N.Hima Bindu is presently working as an Assistant Professor of Electronics and Communication Engineering in DVR Engineering College Hyderabad, India has done M.Tech from JNTU Hyderabad

Mrs. T Jayanthi is presently working as an Assistant Professor of Electronics and Communication Engineering in DVR Engineering College Hyderabad, India has done M.Tech from JNTU Hyderabad.