IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-9 E-ISSN: 2347-2693

A Fingerprint and RFID Tag Based Authentication System for Driving

Kadali Sridhar[1], K. Naga Divya [2] and D. Sree Lakshmi [3]*

[1,2,3] Department of CSE, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, India*

www.ijcseonline.org

Received: Aug/26/2015 Revised: Sep/03/2015 Accepted: Sep/19/2015 Published: Sep/30/2015

Abstract— A vehicle theft is becoming very common nowadays, which is one of the main issues for a person having car or bike. In this technical paper work; the design of a fingerprint and RFID tag based authentication for a vehicle is explained. Fingerprint identification gives the biometric based authentication and RFID tag gives a keyless authentication for a vehicle. So inorder to avoid vehicle theft the proposed system is designing a keyless authentication system for a vehicle instead of going with key based authentication system; it also provides a biometric based authentication which is a fingerprint of a person. A person, who wishes to drive the vehicle, first step is to verify with their fingerprint whether the person who wish to Drive the vehicle is allowed to drive or not; by checking the data base, once verification done then ignition unit of vehicle will starts automatically. If the person is not valid in the Fingerprint Module data base then the vehicle will not get started.

Keywords— Fingerprint, RFID tag, Vehicle Security, Biometric, Ignition System, ARM-7

I. INTRODUCTION

Biometrics refers to the identification or verification of a person based on his/her physiological or behavioral characteristics. The paper presents the designing of fingerprint identification [1] in vehicles which is a biometric authentication, to avoid theft which includes the RFID tag [2] for keyless authentication of a vehicle. Fingerprint identification is one of the most honest and dependable personal biometric identification [3] methods. The proposed system was designed on keyless vehicle authentication instead of going with key based authentication system; it is providing a system based on biometric authentication. A person, who chose to drive the vehicle, first step is to verify with their fingerprint and then second step is to check whether the person is having RFID tag or not, once the verification is cleared then ignition unit of vehicle is started automatically. If the person is not valid on the Fingerprint Module then the vehicle will not get started, hence RFID tag verification is not needed to show.

For this purpose security it requires an "RFID" tag and a "fingerprint" scanner, the following shows the required configuration of the system. An inbuilt system in an automobile which prevents such cases has therefore become vital. This paper aims to introduce a hardware architecture which detects the fingerprint as well as the validity of the keyless authentication of the driver and takes a robust decision to turn on or off the ignition system based on the validity. Firstly it describes about the fingerprint matching algorithm followed by RFID tag authentication and in last it describes about the system architecture.

The rest of the paper is organized in the following manner. In section 2, we review Block Diagram and System Description, along with building the prototype system in section 3 and System operation work flow in section 4; in section 5 the biometric study of the proposed system. Finally the conclusion of the paper is presented in section 6.

II. BLOCK DIAGRAM AND SYSTEM DESCRIPTION

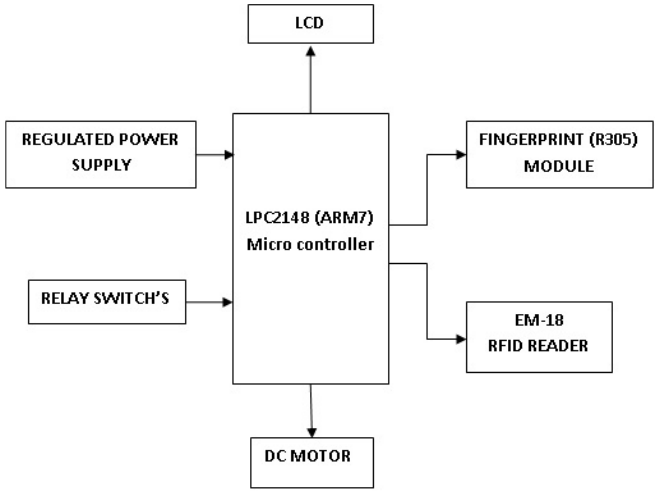

Figure 1: Block Diagram of the paper

A. Analysis of Hardware Structure

1) Fingerprint Module (R30X):

A Fingerprint Sensor is an electronic device, which are used to apprehend a digitalized image of the fingerprint pattern. The apprehend image is called as a live scan. The following figure 2 shows the image of the fingerprint module R305 model. This live scan finger is followed by digital processing to create a biometric template (a stockpile of

deduced features) which is stored and used for matching purpose.

Figure 2: Fingerprint Module (R305)

This module can also work with different devices based on UAWRT such as PC, SCM and so on. Instead on going on complex circuits only easy circuits and fingerprint module can enhance the paper into fingerprint authentication power. It is universally used in different areas like electronics business, information security, access control, identity authentication and other security industry.

This module has some properties of communication or connections for the fingerprint authentication of the paper which are as follows:

- Hardware connection

Via serial interface, the fingerprint module may communicate with MCU of 3.3V or 5V power: TD (transmitter pin 3 of P1) connects with RXD (receiving pin of MCU), RD (receiver pin 4 of P1) connects with TXD (transferring pin of MCU). This connection with PC is being in RS-232 mode, but to connect MAX232 is added for level converting circuit, between the Module and PC.

- Serial communication protocol

This mode is a semiduplex asychronism serial communication, and it has some default baud rate of 57600bps. The baud rate can be rooted in 9600~115200bps. Transferring frame format is 10 bit: the low-level starting bit, 8-bit data with the LSB first and an ending bit, and there is no check bit.

2) RFID Reader Module (EM-18):

Radio-frequency identification (RFID) is a wireless identification method, confide on storing and remotely retrieving data using wireless device called RFID tags or transponders [10]. The figure 3 shows the RFID tag module of the system. An RFID tag is an object that can be implemented to or assimilated into a product, animal, or person for the cause of identification using radio waves. Some tags are read from several distinct meters distance away and beyond the field of view of the RFID tag reader.

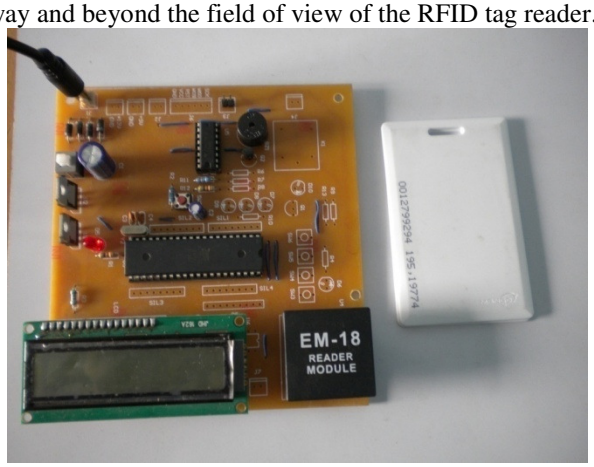

Figure 3: RFID tag

RFID tags contain at least two parts:

- One is an integrated circuit for storing and processing the information of identification, modulating the signal and demodulating the radio frequency signals, and other specialized functions.
- The second one is an antenna for receiving and transmitting of the signal.

Radio Frequency Identification (RFID) involves a contactless reading and writing of data into an RFID tag's nonvolatile memory through an RF signal unlike barcodes which are printed on product and read by the laser scanner which is a high cost process. An RFID system consists of an RFID reader and an RFID tag. The reader emits an RF signal and data is exchanged when the tag comes in the range of the reader signal. The RFID tag derives its power from the RF reader signal and does not require a battery or external power source.

The TK5530 is a complete transponder, which implements all important functions for immobilizer and identification of the systems.

The RFID contains antenna which consists of a coil and a capacitor for tuning the circuit to the nominal carrier frequency of 125 kHz. The coil has a ferrite-core for improving the readout distance.

3) Microcontroller Module:

ARM architecture is based on RISC principles. The RISC a Reduced Instruction Set Computer, and related decode mechanism are much simpler than those of CISC design which is a Complex Instruction Set Computer. This simplicity gives:

- High instruction throughput
- Excellent real- time interrupt response
- Also small, cost- effective, processor macro cell.

Microcontroller: A Micro controller module is a powerful Central Processing Unit (CPU) which is incorporated with the memory (RAM, ROM or EPROM), various I/O features like Serial ports, Parallel ports, Timer/Counters, Interrupt Controller (ADC), Digital to Analog Converter (DAC), everything integrated onto a single Silicon Chip.

B. Software Used for the programming

1) Keil µVision IDE

Keil Micro Vision is free software which can solve many problems of the pain points for an embedded programming for the developer. This software is an integrated development environment (IDE), which integrates a text editor to write programs for devices, a compiler environment and it converts the source code of the logic into hex files too.

Here are the simple steps to start working with Keil uVision environment which can be used for

- Writing programs in C/C++ or Assembly language
- Compiling and Assembling Programs
- Debugging program
- Creating Hex and Axf file
- Testing developers program without Available real Hardware (Simulator Mode)

The µVision IDE environment from Keil, combines properties like project management, make facilities, source code editing, program debugging, and complete simulation in a single powerful environment to generate efficient program. The µVision development platform contains features like easy-to-use and helping the item to quickly create embedded programs that works for that particular device. The µVision editor and debugger are confederated in a single application that provides an absolute embedded project development environmental tool.

The µVision IDE is the easiest way for most program developers to create embedded applications using the Keil software development tools. The µVision Debugger from Keil helps the simulation using only the PC or laptop, and debugging program using the target system and a debugger interface for the programmer. The µVision has also features like simple and complex breakpoints, watch windows, and execution control other than these; it has sophisticated features like trace capture, execution profiler, code coverage, and logic analyzer. A Project is the collection of all the source files as well as the compiler, assembler, and linker settings required to compile and link a program. It also includes several robust features that make project management easy.

2) Embedded C

Embedded C is a set of language which is an extension for the C Programming language by the C Standards committee to address common issues that are existed between C extensions for different embedded systems. Basically, embedded C programming requires nonstandard extensions features to the C language in order to support extra properties such as fixed-point arithmetic, multiple distinct memory banks, and basic I/O operations.

In early times, the C Standards Committee extended the C programming language for addressing these issues by providing common standards for all the implementations to cling to its commonality. In embedded C language it has a more number of features that are not available in normal C language, such as, fixed-point arithmetic, named address spaces, and basic I/O hardware addressing.

Embedded C follows the most basic syntax and semantics of standard C language, e.g., main () function, variable definition, data type declaration, conditional statements (if, switch, case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros, etc.

In the time of beginning years of microprocessor based systems, programs are used to develop in the assemblers and agglutinated into the EPROMs. There are no mechanisms which are used to find what exactly the program was doing because there are no displays to read. Instead they use LEDs, switches, and etc. to check for correct execution of the program within a device. Some 'very fortunate' developers had simulators like In-circuit Simulators (ICEs), but they are way too costly to purchase and also not quite reliable for the outcomes. As time progressed, the use of microprocessor-specific assembly left behind, and only the programming language of embedded systems slowly skimmed onto C as the embedded programming language as an option. Afterwards C is the most universally used programming language for embedded processors/controllers. Assembly is also used but it is implemented when the portion of the code requires very high timing accuracy, code size efficiency, etc. for the ultimate requirements.

As assembly language programs are specific to a processor, assembly language didn't offer any portability across the systems. To overcome this drawback, several high level languages, including C, came up. Some other languages like PLM, Modula-2, Pascal, etc. also came into existence but couldn't find any wide acceptance. Amongst those, C language got the full-fledged acceptance for not only embedded systems, but also for desktop applications. Even though C language might have lost its gleam as mainstream language for general purpose applications, it is still having a strong-hold in embedded programming language.

Due to the wide acceptance of C language in the embedded systems, various kinds of supporting tools like compilers & cross-compilers, ICE, etc. become highlighted and all this facilitated development of embedded systems using C

language. Assembly language later seems to be an obvious alternative for programming into embedded devices. However, use of assembly language is confined for developing an efficient code in terms of size, speed and accuracy. Also, assembly codes become costly software development tool to purchase and code portability is not there. Developing small codes is not exactly the main problem, but to make large programs/projects have become increasingly arduous to maintain in assembly language. Finding good assembly program developer is also becoming big issue nowadays. Hence high level languages for device are preferred for embedded systems programming.

III. BUILDING THE PROTOTYPE SYSTEM

Foremost aim of the paper is to enroll the users' fingerprints and RFID tag of a single vehicle that will be store in a data base [9]. Figure 1 shows the block diagram of the paper.

STEP 1: A Person who wishes to drive a vehicle or buy a new vehicle, foremost thing is to place the finger on the fingerprint scanner i.e.; fingerprint module. If the placed finger matches with the data base then it goes to step 2. Otherwise it will show an error message display like please place valid fingerprint and again displays please enter a valid fingerprint. In case the fingerprint accessing process is failed for more than three times than process for fingerprint will go to the initial condition i.e.; place a valid fingerprint.

STEP 2: In this step the user has to show a valid RFID tag of that particular vehicle, if it is not a valid identification then it will display an error message like it is an invalid RFID tag please show a valid RFID and again it displays like waiting for valid RFID to show. In this process if the RFID tag shown fails for more than three times, then as in the step1 after the process of fingerprint the RFID tag process will move to the initial condition i.e.; fingerprint placing step. If a valid RFID tag is shown it will forward to the next step.

STEP 3: In this step a person who wishes to drive a vehicle then step1 is processed and after the validation of step1 it will proceed to step 2. After step 2 validation finally the last step which is after fingerprint scan and RFID tag verification, the kit is proceeding for the ignition of the system [4]. If all of the process fails to do this process then the ignition system will not work.

STEP 4: In this step if any person other than the user wishes to drive a vehicle, then that person's fingerprint is infiltrated to the data base with the help of first persons fingerprint before accepting the new user and this whole process is done in the software environment with the help of Keil IDE environment. If the fingerprint matches and the RFID of the vehicle is verified then the ignition system will start and the user can drive the vehicle and the process goes on. If the fingerprint does not matched with the first taken fingerprint then the controller gives an error message to process the verification and set back to its initial step 1 [6]. Figure 4 shows the complete system operation flow.

To keep the paper straightforward and more software based, we are going for basic hardware usage as an interfacing device to scan the data from the fingerprint and read the data from the card and store it on application's database. The task of the fingerprint scanner is to read the finger placed on it and for card reader is to read a ten digit unique RFID tag and feed it to any display device or visible fields on the screen. So each fingerprint scanned has unique template identification for single user and a RFID tag card has a film with a 10 digit unique RFID and the number is printed on the card itself for recognition purpose.

IV. SYSTEM OPERATION WORK FLOW

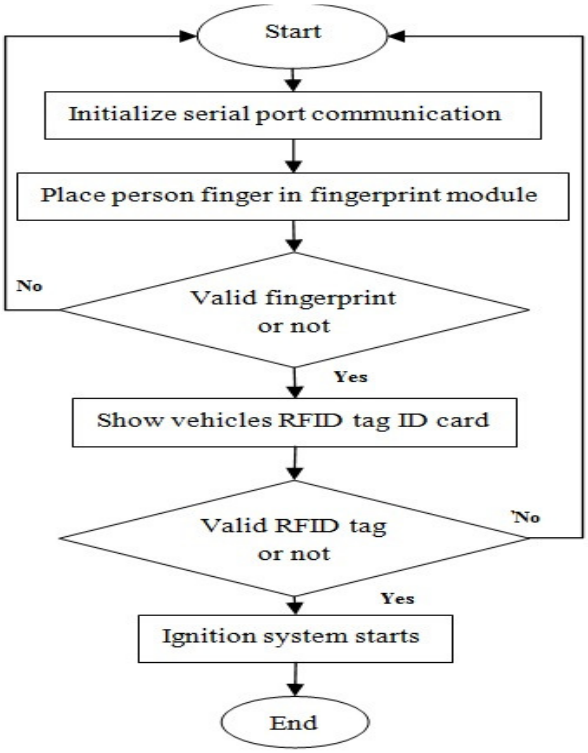

Figure 4: The System Operation Flow

When kit is switched on, first it displays "VEHICLE SECURITY BIOMETRIC AND RFID" in LCD. After some delay it displays "ENTER AN OPTION S1 S2 S3" in LCD display. Here S1 is an option for the user to erase the database in the ARM Processor module and when pressed S1 option it displays "CONTENTS IN THE DATA BASE ARE ERASED" in the LCD, S2 is an option for the user to enroll a new person to drive the vehicle and when pressed S2 it displays "FINGER IS NOT DETECTED PLEASE PLACE A FINGER TO SCAN" after placing a finger in the fingerprint module it scans the live finger two times and storage it in the database and generates a unique template for a finger of person; it displays "YOUR TEMPLATE ID

IS: 000 OR 001" in LCD, and S3 is an option to search a live scan fingerprint in the data base, when pressed S3 the LCD displays " NO FINGER IS DETECTED PLACE A FINGER TO SCAN" and when finger is placed then it checks the database for the validity of the person . The users have to place their fingerprint on the fingerprint module. If the placed finger is invalid then it will displays "PLACE A VALID FINGER" in LCD display. If the placed finger is valid then it will display "VALID PERSON" in LCD display. After some delay it displays "WAITING FOR RFID TO VERIFY" in LCD display, through the keyless authentication user shows the RFID tag at the RFID tag reader module. If the user shows the wrong RFID tag then it displays "INVALID RFID PLEASE SHOW VALID RFID" in LCD display but if it is valid RFID tag then it displays "RFID ID NO:180xxxxxx0" and then the finally the DC motor will be started as an ignition system unit. Figure 5 shows the practical implementation on AMR-7 kit.

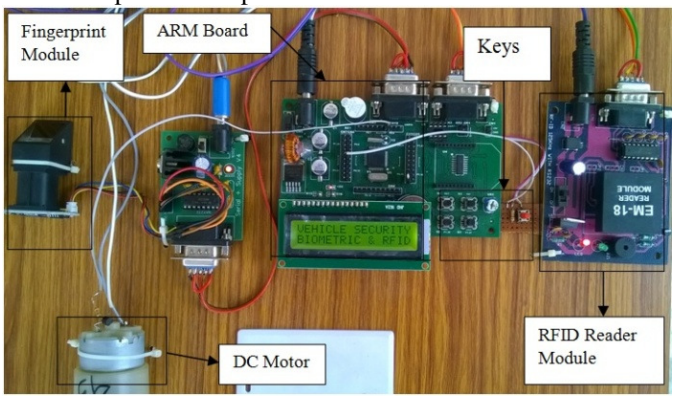

Figure 5: Practical implementation on kit

V. BIOMETRIC

Biometric is a technology which uses physiological or behavioral characteristics to identify or verify a person [5]. Typical characteristics used for authentication include fingerprint, iris, and mouth and face [7]. A conventional biometric authentication system consists of the processing of two parts: fingerprint enrollment and fingerprint matching (Figure 5).

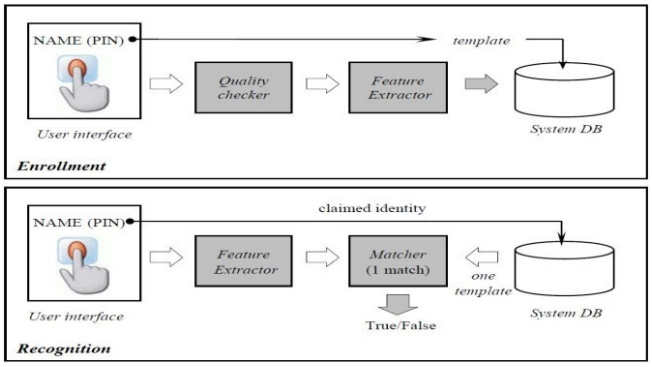

Figure 5: Conventional biometric authentication

The matching ration of the fingerprint can be 1:1 or 1: N ratio. When enrolling, user needs to enter the fingerprint two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical fingerprint sensor and system will generate a template of the finger and compare it with templates of the fingerprint library.

For 1:1 matching, system will compare the live finger with the stored template designated in the Module; for 1: N matching, or searching, system will search the whole fingerprint library for the matching finger. In both cases the system will return the matching percentage, with success rate or failure rate.

VI. CONCLUSION

Secured Approach for Authentication or identification of the System by using Fingerprint and RFID tag proves to be very effective in providing security.

A newfangled approach in designing the Authentication System were implemented using Fingerprint and RFID tag gives security to the users' vehicle system and provides safety for the ignition system using a finger print scanner and RFID tag for the authentication of the ignition system. The result obtained in providing the security gives quite reliable in all the different modes of the paper.

The system has successfully gain mastery over some of the aspects existing with the present technologies, by the use of finger print Biometric and RFID tag identification as the authentication Technology.

ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Science & Engineering of Prasad V. Potluri Siddhartha Institute of technology (Autonomous), Vijayawada, Andhra Pradesh, India, for allowing us to explore this interesting area.

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] Ahmed Saeed Alzahrani, "*Security analysis of RFID based devices in educative environments*," Life Science journal **2014**.

[3] http://www.biometricinfo.org/fingerprintrecognition.htm"Biometrics Information Resource"

[4] Omidiora E. O., Fakolujo O. A., Arulogun O. T., Aborisade D. O., (2011), A Prototype of a Fingerprint Based Ignition Systems in Vehicles, European Journal of

Scientific Research, ISSN 1450-216X Vol.62 No.2 (**2011**), pp. 164-171.
[5] K. Karu, A.K. Jain, "Fingerprint classification, Pattern Recognition", **1996**.
[6] http://auto.howstuffworks.com/ignitionsystem.htm, "How Automobile Ignition Systems Work"
[7] Anil K. Jain, Lin Hong, Sharat Pankanti, and Ruud Bolle, "An identity authentication system using fingerprints,"
[8] Emma Newham, "The biometric report," *SJB Services*, **1995**.
[9] Ahson, S. A., & Ilyas, M., (**2008**). RFID Handbook, Applications, Technology, Security, and Privacy, CRC Press, FL, USA, ISBN: 978-1- 4200-5499 6.
[10] Nordby, K. (**2010**). Conceptual Designing and Technology: Short-Range RFID as Design Material. The Oslo School of Architecture and Design, Oslo, Norway: International Journal of Design Vol.4 No.1, pp. 29-44.

AUTHOR PROFILE

Mr. K. Sridhar Received his B.Tech degree in Computer Science & Engineering from Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. And he is currently pursuing M.Tech Degree in Computer Science & Engineering in Prasad V. Potluri Siddhartha Institute of Technology (Autonomous) Vijayawada, Andhra Pradesh, India and is affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. His area of research includes Embedded System.

Mrs. K. Naga Divya been working as Assistant Professor in the Department of Computer Science and Engineering Prasad V. Potluri Siddhartha Institute of Technology(Autonomous) Vijayawada, Andhra Pradesh and is affiliated to JNTU-K, Kakinada,. She obtained M.Tech, and she is currently pursuing Ph.D. She had more than 4 Years 4 months of teaching experience. Her areas of interests are Computer Networks, Embedded System. She is a life member of ISTE and Acted as peer Reviewer for Springer Journal. Ph.No:8885561230

Mrs. D. Sree Lakshmi been working as Assistant Professor in the Department of Computer Science and Engineering Prasad V. Potluri Siddhartha Institute of Technology(Autonomous) Vijayawada, Andhra Pradesh and is affiliated to JNTU-K, Kakinada,. She obtained M.Tech. She had more than 5 Years 8 months of teaching experience. Her areas of interests are Computer Network, Embedded System. She is a life member of ISTE. Ph.No: 9948723569