International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 02
February 2017

Design End-to-end Encryption based Biometric system for Security

[1]M. Chiranjeevi, [2]V. Ramakrishna Reddy
[1]M.Tech, Balaji Institute of Technology & Science,Telanagana, India
[2]Assistant Professor,Dept. of ECE, Balaji Institute of Technology & Science, Telanagana, India

ABSTRACT: Biometric systems are an integral part of physical access control systems. Biometric systems ensure that an opportunity to use a system or service is done by a valid user. These systems are used in various applications like ATMs, voting system, aadhar card, attendance management system etc. The biometric systems are in operation for a quite long time and their use is increasing. There is a need for low cost, scalable systems with high availability. In this paper a cloud based biometric system architecture is proposed, to make the system efficient and economical for remote enrollment. Authentication node is implemented on a Raspberry Pi, which is a low cost computer running on Linux. The system is capable of capturing multimodal biometric traits such as face and fingerprints and send them to cloud service by end-to–end encryption process.

IndexTerms: Biometric system, encryption, remote transmission, ARM11

I. INTRODUCTION

Security of computer data, information and computer networks has become very important in today's world. A great amount of resources are being invested to build secure systems. Biometric systems are a secure way to authenticate a person and to grant access to services or a system only to legitimate users. [1] In this computer-driven era, identity theft and the loss or disclosure of data and related intellectual property are having upward trend. Users have many accounts and use multiple passwords on an ever-increasing number of computers and Web sites. Preserving and managing access while protecting the user's identity, the data and computer systems has become a difficult task. At the heart of all security systems is the concept of authentication- verifying that the user is who he claims to be. [2] Traditional methods for authentication depend on external things like tokens, passwords, keys which can be easily lost or forgotten. This issue can be solved through biometrics as each person has unique biometric features. Biometric systems are used to secure facilities, counter fraud and protect access to computer networks. Biometric traits are actual characteristics or entities which are used to identify a human. Physiological biometric traits include fingerprint, palm print, hand vein, iris, retina, ear or the DNA information of an individual. The biometric systems are becoming ubiquitous due to the availability of low cost implementations but still the gap is there as the customer are demanding better and cheaper solutions. In the conventional approach the systems are built upon a traditional client server architecture, this limits the scalability, availability, pluggability as well as the cost of implementation is high. In recent years, optimum resource utilization has become a keyword to build the systems and this has given a drive to develop cloud based systems. The cloud based systems offer a low cost, scalable and flexible solutions for next generation computing needs. The bottlenecks faced by the biometric systems can be solved by implementing cloud based solutions.

Raspberry pi is a small, low cost personal computer running on Linux. In this research paper, a low cost architecture of biometric systems is proposed, which is using a low cost wireless enrollment node and the authentication is done by Biometric service hosted on the cloud. The captured biometric traits are sent to the Biometric Software-as-aService (SaaS) by end-to-end encryption process. Raspberry Pi has verified peripherals for capturing fingerprints and face images: Fingerprint Scanner Futronic FS 88 Optical Fingerprint Reader with Live Finger Detection and the PiCamera module. This will capture the biometric traits and send them to a remote PC or to a web service or to a remote procedure or to a cloud service for enrollment or

authentication purposes. Since the biometric traits are transmitted over an unsecured channel to a remote location, it is very important to have a secure transmission. Encryption is one of the effective ways of protecting data which is being transmitted to a remote location. Hence, in the proposed system end-to-end encryption based on AES-256 is used. The Raspberry Pi acts as a remote enrollment and authentication node. This system can be used for remote authentication and enrollment of a multimodal biometric system. The multimodal biometric system overcomes the limitations of the unimodal biometric system, reduces fraudulent access, and also has more accuracy [1], the cloud implementation provides the pluggability and scalability required by real time application of biometric authentication system.

The technological advancement in the field of electronics and telecommunication has brought more and more arrangements in the domestic and industrial environment. Security systems can avoid the unauthorized entry of peoples into the protected area and it stores the details about the authorized peopled entered in the area on the computer through a wireless transmitter. Up gradations in this system can be done easily to improve the efficiency of the system. Security systems are the demands of the day, which helps to avoid theft and avoids unauthorized entry of peoples into the restricted area. Conventional security systems used either knowledge based methods (passwords or PIN), and token-based methods (passport, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. Personal Safes are revolutionary locking storage cases that open with just the touch of your finger. These products are designed as secure storage for medications, jewelry, weapons, documents, and other valuable or potentially harmful items.

These utilize fingerprint recognition technology to allow access to only those whose fingerprints you choose. It contains all the necessary electronics to allow you to store, delete, and verify fingerprints with just the touch of a button. Stored fingerprints are retained even in the event of complete power failure or battery drain. These eliminates the need for keeping track of keys or remembering a combination password, or PIN. It can only be opened when an authorized user is present, since there are no keys or combinations to be copied or stolen, or locks that can be picked. Galton [1] defined a set of features for fingerprint identification, which since then, has been refined to include additional types of fingerprint features. This powerful device uses the latest in fingerprint ID scan technology to make sure only authorized drivers with enrolled fingerprints can enter[6]. This primary (+ secondary) security system uses a combination of an enrolled Fingerprint plus the random number as a key to enable the process. A system is secured here by a password and finger print. A Finger print Scanner is used to store and read a particular Finger Print. Biometric fingerprint security has practical applications which can be used to help protect security or privacy concerns on a personal level. For example, fingerprint scanners and locking systems are designed to prevent unauthorized access to your personal data or information.

RPi has been used for various applications, in [3], the authors have proposed a system which focuses on cost saving and enhancing the quality of service in the field of technologyaided teaching. Raspberry Pi and its web interface stores files that have been sent from remote computers and view these power point files or Portable Document Files (PDF) on the multimedia projector. It targets to substitute laptops with Raspberry Pi, which will not only considerably reduce the cost involved, but also will help achieving quality of service as the system will consume a smaller amount of power. In another

implementation [4] authors proposed an image capturing technique in an embedded system based on Raspberry Pi boards. Most of the recognition systems are based on a PC, the portability of which is limited by its weight, size and the high power consumption.

II. LITERATURE SURVEY

In [5], attendance of the students is taken automatically based biometric traits such as

fingerprint. Here the images are captured by the fingerprint sensors. The hardware components used are Arduino UNO board, Wi-Fi Shield, GSM Shield, Keypad, LCD Display, Adafruit Fingerprint Sensor and Raspberry Pi. This implementation is a client server based implementation. Besides these there are many real time applications of RPi [7] [8] [9].

The security is also part of biometric systems. Kaul and Sheikh [7] have proposed data security for end-to-end transmission, which is achieved by many different symmetric and asymmetric techniques for message confidentiality, message authentication and key exchange using transport layer security. They proposed combination of two symmetric algorithms AES and Blowfish to enhance security. AES is enhanced by modifying the S-boxes, columns, and then combination of enhanced AES and blowfish is used for data confidentiality. Message digest 5 is used for authentication. Key exchange is done using ECDHA, Elliptic Curve DiffeHellman algorithm. Security into proposed architecture is achieved by integrating this approach for end–to-end encryption of biometric traits captured by enrollment node. As far as the cloud implementations are considered

R.Tade has discussed [10] how piracy can be reduced by the combination of embedded system and the cloud computing technology. This research also highlights on the advantages of using cloud computing technology, Linux Operating System, ARM processor and the Raspberry Pi. In [11], the different challenges, opportunities and the transactions in cloud computing are defined. This paper gives a brief introduction on SaaS, IaaS, PaaS and about the types of cloud. This paper also explains how with cloud computing resources can be shared in an effective manner reducing the cost. It shows what challenges are faced by the developers, engineers, administrators etc. Current paper is focusing on how the portability and simplicity of Raspberry Pi can be combined with Cloud and Encryption technique to design an authentication system with high availability, scalability, security , portability and low cost.

III. PROPOSED FRAMEWORK

Following Fig.1 show the system architecture block diagram including the ARM processor based development board, Fingerprint module, and motor controlling Door (motor driving card),LCD and related hardware.

A. Raspberry Pi

The Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZF-S 700 MHz processor, VideoCore IV GPU and was originally shipped with 256 megabytes of RAM, later upgraded (Model B & Model B+) to 512 MB. It does not include a built-in hard disk or solid-state drive, but it uses an SD card for booting and persistent storage, with the Model B+ using a MicroSD. The Foundation provides Debian and Arch Linux ARM distributions for download. Tools are available for Python as the main programming language, with support for BBC BASIC (via the RISC OS image or the Brandy Basic clone for Linux), C, Java and Perl.

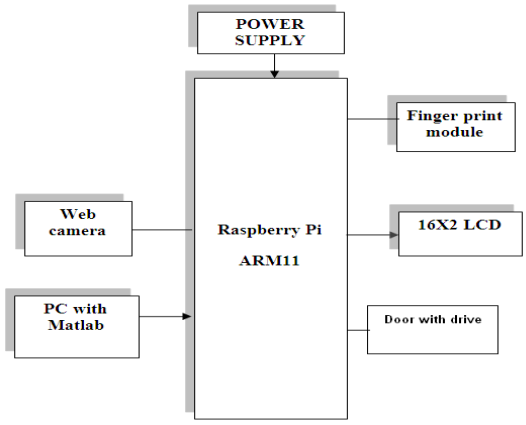

Fig.1 Block diagram of functional unit

B. DC Gear motor

A geared DC Motor has a gear assembly devoted to the motor. The speed of motor is counted in terms of rotations of the shaft per minute and is termed as RPM .The gear assembly helps in increasing the torque and dropping the speed. Using the correct arrangement of gears in a gear motor, its speed can be reduced to any required figure. This concept of reducing the speed with the help of gears and increasing the torque is known as gear reduction. Reducing the speed put out by the motor while increasing the quantity of applied torque is a

important feature of the reduction gear trains found in a gear motor. The decrease in speed is inversely relative to the increase in torque.DC Geared motors with robust metal gear box for heavy duty applications, available in wide RPM range and ideally suited for robotics and industrial applications. Very easy to use and available in standard size. Nut and threads on shaft to easily connect and internal threaded shaft for easily connecting it to wheel.

Specifications:

•100 RPM 12V DC motors with metal Gearbox.
• Same size motor available in various rpm.
•Shaft diameter : 6mm
•weight :122 gm
•Torque : 2 Kg-cm
•No-load current :- 70mA (Max)

MATLAB testing of face detection

As our final aim was hardware implementation , so the Matlab testing is done with the face detection given in computer vision system toolbox. It comes with already trained classifiers. This was to test the required efficiency of face detection. Whenever any human face is detected and recognized and found in database, then ARM 11 board sends commands via RS232, and which drives the DC motor for 15 seconds in clockwise direction i.e. to open the door driven by DC motor , then waits for next 15 seconds and then again drives the DC motor for 15 seconds in anticlockwise direction, i.e. to close the door. The DC motor is driven through through the motor driver IC L293D.

IV. RESULTS AND DISCUSSIONS

The purpose of the enrollment model is to register all the authority users to access control and save the biometrics features in a database. The verification (or authentication) model used for veryify the claimed identify of person.This model consist of two stage : the first one for the fingerprint and the second for the voice ,as expalain below: This systemregisterd the users that consider as authority to access control in the enrollment model as shown in the (Fig.2). Each user in this stage will take the ID number that save in the database.

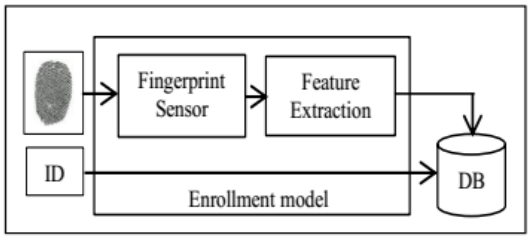

Fig.2 Enrollment model

In (Fig.3) shows the blok daigram of the fingerprint verification model.

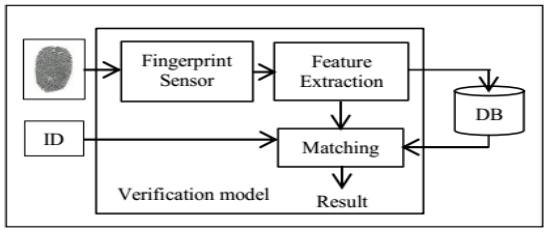

Fig.3 verification model

In fingerprint stage we used two important functions: feature extraction and the matching function. The brief description of these functions as follow:

• Feature Extraction

The feature extraction is responsible for expressing fingerprint's unique characteristics adequately such as directions of the lines, terminals of lines, bifurcation and so on. To ensure the accuracy of comparison, the method of feature extraction must extract useful features as much as possible; meanwhile, filter false features for various reasons. There are two kinds of features in fingerprint images: global feature and local feature. Global feature can reflect overall shaper of fingerprint, which usually applies to fingerprints' classification, the process of extract global feature frequently belongs to procedure of fingerprint classification. The Local feature can reflect minutiae of fingerprint, usually applies to fingerprints' comparison. [16]

Strict feature extraction means local features' extraction. Two fingerprints often have the same global features, but their local features can not be exactly the same. The important information of fingerprints' local feature is following: terminals, bifurcations, branch points, isolated points,

enclosures, short lines and so on. In fact, not all the fingerprints have these two features, it often be used as fingerprints' sub-matches [17].This system uses terminals and bifurcations in feature extraction and matching algorithm.

• Feature Matching

The matching function, features extracted from the input fingerprint is compared against those in a database, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images using correlation-based methods, so that the fingerprint template coincides with the gray scale image. However, most of the fingerprint matching algorithms use features that are extracted from the gray scale image. A large number of approaches to fingerprint matching can be found in previous work [17, 18]. In this proposed work we used the matching algorithm that support the optical fingerprint reader module SFG algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction &tolerance to deformed and poor-quality fingerprint and work with both 1:1 and 1:N.

V. CONCLUSION

In this paper a low cost computer Raspberry Pi is used as a remote enrollment and authentication node. The enrollment part is successfully done and the captured data is sent to the cloud. The Fingerprint & face capturing sensors along with Wi-Fi adapter is successfully interfaced to Raspberry Pi. The captured traits are sent to a Microsoft Azure based biometric service, this service will extract the feature vectors and store it to the feature vector database. Proposed system has application in all the biometric access control systems, which needs portability, scalability and low implementation cost.

REFERENCES

[1] Omar Abdulwahabe Mohamad, Rasha Talal Hameed, Nicolae Tapus, " Access Control Using Biometrics Features with Arduino Galileo", International Journal of Advanced Research in Computer Science and Software Engineering, vol 4, issue 8, Aug 2014.

[2] Biometric Authentication, Available: http://www.computer world.com / article /2556908 /security0 /biometric-authentication .html.

[3] Dhaval Chheda, Divyesh Darde, Shraddha Chitalia: "Smart Projectors using Remote Controlled Raspberry Pi", International Journal of Computer Applications (0975 – 8887) vol. 82 – No 16, Nov 2013.

[4] G.Senthilkumar, K.Gopalakrishnan, V.Sathish Kumar, "Embedded Image Capturing System Using Raspberry Pi System", International Journal of Emerging Trends & Technology in Computer Science, vol 3, issue 2, March – April 2014.

[5] Karthik Vignesh, Shanmuganathan , A.Sumithra, S.Kishore and P.Karthikeyan, "A Foolproof Biometric Attendance Management System" International Journal of Information and Computation Technology, vol 3, Number 5 (2013), pp. 433-438.

[6] Camera Module. Available: http://www.raspberrypi.org/ documentation/ usage/camera/README.md

[7] Shaikh Ammarah P. Vikas Kaul S K Narayankhedkar, "Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie-Hellman Key Exchange", International Journal of Applied Information Systems – Foundation of Computer Science FCS, New York, USA and the International Conference & workshop on Advanced Computing 2014

[8] "Hiding Biometric Data" , IEEE transactions on Pattern Analysis and Machine Intelligence, vol. 25, No.11, November 2003

[9] Rajeeb Lochan Dash, Mrs. A. Ruhan Bevi, "Real-time Transmission of Voice over 802.11 Wireless Networks Using Raspberry Pi", International Journal of Engineering Development and Research, vol 2, issue 1 2014, ISSN: 2321-9939.

[10] Md. Maminul Islam, Md. Sharif Uddin Azad, Md. Asfaqul Alam, Nazmul Hassn, "Raspberry Pi

and image processing based Electronic Voting Machine" , International Journal of Scientific & Engineering Research, vol 5, issue 1, January-2014 1506 ISSN 2229-5518.

[11] Rushikesh Tade, "Embedded Cloud for Antipiracy" International Journal of Scientific & Technology Research, vol 2, issue 6, June 2013 Issn 2277-8616.

[12] Jianjiang Feng, Anil K. Jain,"Fingerprint Reconstruction: From Minutiae to Phase" IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 33, No. 2, Feb 2011

[13] About Raspberry Pi, Available: www.raspberrypi.org

[14] Available: https:// encryptedtbn1.gstatic.com /images?q=tbn: ANd9Gc T4bhmDSBRO A76ZfEXCBJ6FUKkEXHNmBhkRzBpZYfVs4E UfHUm

[15] FS88 FIPS201/PIV Compliant USB2.0 Fingerprint Scanner, Available: http://www.Futronictech.com/product_fs88.html#

[16] Available: http:// www.element14.com /community/servlet/ JiveServlet/showImage/2-104955192660/DSC_2624_33%25 .JPG.4.