An Android Based Secure Access Control Using ARM and Cloud Computing

K. Srividhya
PG Scholar
Dept. of Electronics &Communication Engineering
Dr.Paul's Engineering College, Villupuram.
sri_srividhya25@yahoo.com

Mr. S.V.Manikanthan,M.E
Assistant Professor
Dept. of Electronics &Communication Engineering
Dr.Paul's Engineering College, Villupuram.
manikanth77@hotmail.com

Abstract- **Biometrics in the cloud infrastructure improves the security of the system. The physical characters in biometrics are finger print, facial structure, iris pattern, voice, etc. Any of these characters are given to identify the persons and authenticate them. This paper describes the enrollment and identification for the system which allows the accessing of person's well known by the higher officials. The physical behaviors are scanned by using android mobile phone. The enroll and recognize operation are achieved with the help of cloud computing. LPC2148 is ARM processor used for controlling the overall system. The primary goal is to achieve the best security to the system and reliable. In this system, there is no need for password.**

Keywords: authentication, cloud computing, enrollment and identification

I. INTRODUCTION

Cloud computing is the emerging technology of delivering many kinds of resources as services, mainly over the Internet. Biometrics in the Cloud means that the entire biometrics infrastructure of a business is placed in the hands of the hosting provider, and is available on demand. This includes the servers which contain the biometric template database, the network connectivity to the business, and all of the processing which occurs in order to conduct the necessary verification and identification transactions. This system prevents the biggest problem with authentication, (i) for-getting the passwords, (ii) misuse of password, (iii) using same username and password to multiple sites.

Biometrics are said to be the best way of authentication made using physical and behavioral traits such as facial, fingerprint, iris, voice, tongue etc. while using passwords for authentication may occurs several problems as discussed above. By this technique, user himself/herself only can access their system. So, No way of illegal authentication can be possible. The systems are used to allow access based on the biometric identification. This improves the level of the security in the system than the usage of passwords.

The most important characteristics of cloud computing are:

- On demand self-service: cloud services can be accessed automatically, anytime and anywhere in the world.
- Broad-based network access: all cloud-based services are available via any type of network connection, and can be accessed by any kind of device.
- Resource pooling: at the hosting provider, all IT and network resources are pooled together, which is what gives the cloud its economies of scale, resulting in fixed and predicable costs for a business.
- Rapid elasticity: the cloud resources can be released to the business within seconds, in proportion with the particular level of demand.

This paper describes the implementation of fingerprint using ARM processor into secure access system. The enrollment and identification are takes place in the cloud infrastructure. The section 1 describes the brief introduction about the cloud computing with fingerprint authentication. Section II discusses the literature survey of the paper. Section III explains about the system working and its hardware specification. Section IV deals about the experimental results of the authentication system using fingerprints. Finally, the paper is concluded with some discussion about the implementation.

II. RELATED WORK

The biometrics in cloud infrastructure is a highly secured way of authentication for accessing a system. The cloud uses any of the services (i.e., IaaS, PaaS and SaaS). These services are not possible for all the time in the system.

When the finger print detector detects any finger on its screen its scans it, and checks for the user id of the fingerprint if already present in its database. If the fingerprint is detected then prints the user id on the LCD screen, authenticating the person is valid [8]. A biometric access control system which supports various authentication media and different security combination: Fingerprint password & RF cards [1]. The lack of a direct matching process in our model enforces its security and makes it better conditioned for law compliance [4]. The conventional knowledge-

based and token-based methods do not really provide positive personal recognition because they rely on surrogate representations of the person's identity (e.g., exclusive knowledge or possession). It is thus obvious that any system assuring reliable personal recognition must necessarily involve a biometric component [3]. When designing cloud-based on biometric services and a case study, where a cloud fingerprint service was developed and integrated with the e-learning framework Moodle [2]. The data has to be stored in encrypted format using cryptography on biometric for the security reasons .A blind protocol in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa [5].

III. WORKING SCHEME

In this paper, the fingerprint authentication is consisting of two parts: enrollment and verification/recognition [2]. These two processes are takes place in the cloud infrastructure. Firstly, the database is created with the enrollment session.

Secondly, the database is verified by checking whether the live fingerprints gets match with the stored database or not. The fingerprint are get captured by using android mobile phone. The captured fingerprint are get passed to LPC2148 through Bluetooth module. The purpose of ARM processor is to pass the fingerprint to cloud infrastructure from mobile phone. Figure 1 refers the overall authentication system block diagram.

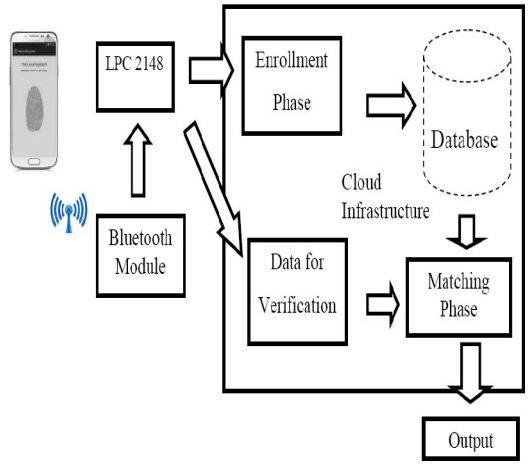

Figure .1.Block diagram of the overall authentication system

A. Fingerprint scanning

The fingerprint are get scanned by using an Android mobile phone. The fingerprint scanning takes with optical sensor. An optical fingerprint scanner is the same charge couple device used in digital cameras. A charge couple device is a light sensor system that consists of light sensitive diodes called photo sites, which are responsible for generating electrical signals when they detect light.

Different levels of light produce different levels of charge in each photo site, and each photo site diode is a single pixel of the completed image.

The number of these little photo sites on the sensor will determine the resolution of the image generated, which in turn determines how accurately the scanner can differentiate between fingerprints. In other words, the higher the PPI sensor the higher the level of security.

If a scanned fingerprint matches several of these minutiae then it will be considered a match. This helps reduce the amount of processing power required to identify each fingerprint, helps avoid errors if the scanned fingerprint is smudged, and also allows the finger to placed off-centre or be identified with only a partial print.

The merits of scanning using android mobile phones are more than using biometric scanner. In biometric scanner, there are some advantages which discussed above; there are also some notable disadvantages. The fingerprint database using biometric scanner can be hacked easily. Therefore, the security of the database is very poor. While using Android phones for scanning, the database are able to hack by any of the intruders.

B. Bluetooth module

Bluetooth technology handles the wireless part of the communication channel; it transmits and receives data wirelessly between these devices. It delivers the received data and receives the data to be transmitted to and from a host system through a host controller interface (HCI). The most popular host controller interface today is either a UART or a USB. Figure 2 describes the LPC2148 connection with Bluetooth.

To transmit & receive the data from host system to LPC2148 by using Bluetooth module through UART0. The serial data is taken from or sent to the host system by using Bluetooth module through MAX232 into the SBUF register of LPC2148 microcontroller. The serial data from the host device is taken by using the Serial Interrupt of the LPC2148 controller. The UART0 pin lines are used to transmit & receive operations in LPC2148.

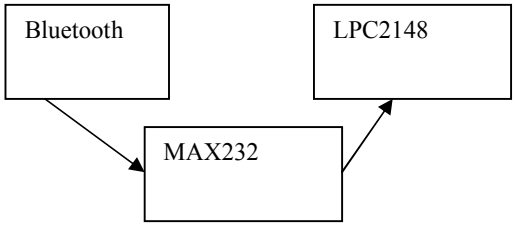

Figure2.bluetooth interfaced with LPC 2148

C. LPC 2148

The LPC2148 microcontrollers are based on a 16-bit/32-bit ARM7TDMI-S. CPU with real-time emulation and embedded trace support that combine the microcontroller with embedded high-speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty. Due to their tiny size and low power consumption, LPC2148 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale.

D. cloud infrastructure

Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities.

Platform as a service (PaaS) is a category of cloud computing services that provides a computing platform and a solution stack as a service. This automates the configuration, deployment and ongoing management of applications in the cloud. The cloud provider manages and delivers programming languages, frameworks, libraries, services and tools for you to create and deploy applications. The service provider also manages and controls the infrastructure, including network, servers, operating systems and storage.

E. Android

Fingerprint Scanning using Android is perfectly suitable for Government / Semi Government / Banking Projects related to Identity management and National ID. Fingerprint is read by using Android mobile phone is very safe and convenient for fingerprint data collection for wide range of Identity projects. This improves the length of the database and stores more number of data than the ordinary fingerprint scanner.

IV. EXPERIMENTAL RESULTS

The fingerprint authentication is chosen because when compared to other behavior it is quite easier and contains more stability. Table I explains the various biometric behavior comparison in terms accuracy, cost and acceptance.

Based on the above table I, the fingerprint has accuracy of high than the facial and hand geometry. It also contains low cost when compared to the other physical behavior system. This system used to authenticate the persons with their ridges and valleys. Because the ridges values will be same for a long time.

TABLE I Comparison of biometric behaviors

Physical Behaviors	Accuracy	Cost	Acceptance
Iris Recognition	High	High	Medium
Retinal Behavior	High	High	Low
Facial Recognition	Low	Medium	High
Fingerprint Recognition	High	Medium	Medium
Hand Geometry	Low	Low	High

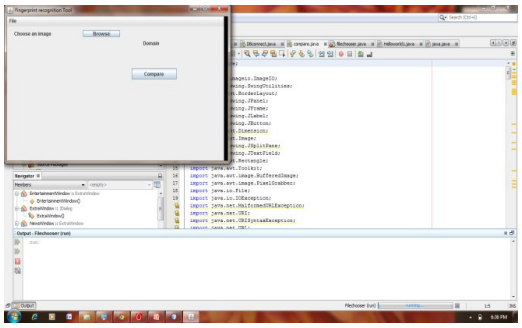

Figure.3 Fingerprint Matching Applet

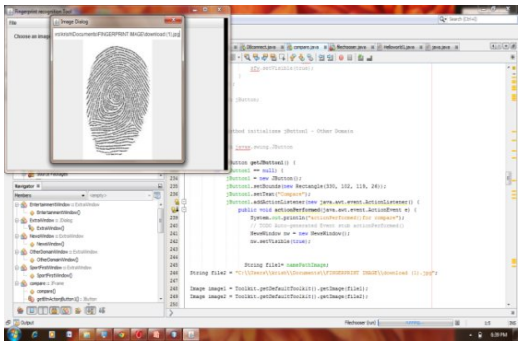

Figure 4 Browsing A Input Image

The enrollment and verification session are takes place in the cloud. The database is created with fingerprints. The enrollment phase is used to store fingerprint in the database. The verification phase is used get live fingerprint from an android through LPC2148. Figure 3 refers The fingerprint recognition

applet. Figure 4 refers giving an input image which is compared with the database. Figure 5 refers the fingerprint matching form. This used to compare the live fingerprint and store fingerprint. LPC 2148 is connected with Bluetooth module and the templates are get stored not the database.

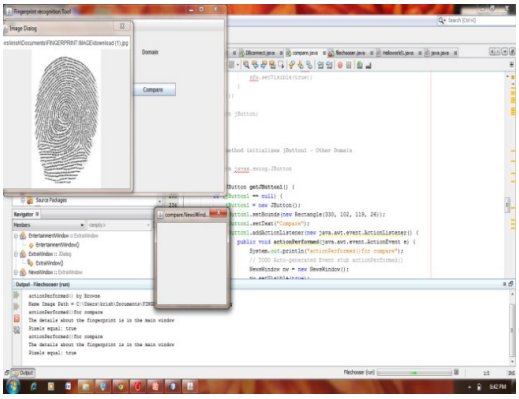

Figure 5. Fingerprint Matching form

V DISCUSSION

When using ARM Cortex processor, the system used to store 4700 templates where each contains 1-master and 1-slave because it contains 215kB of data capacity. Here, ARM LPC2148 is used which increases the data capacity than the cortex. So, the system can store more than 6000 templates as it has a data capacity of 512KB. In the fingerprint scanner, the fingerprint data's are easily hacked by the intruders. But In case of android mobile phone fingerprint scanning, the data's cannot be steal by any other person. Therefore, this system is unique and reliable. The accuracy and security are getting improved.

V CONCLUSION

This paper presents fingerprint authentication into the access system which support the system to be more secured and protect from intrusion. The LPC 2148 is used to communicate faster with the Bluetooth module than the other LPC 21XX. Therefore, the data transfer becomes very easier as well as faster. The scanning of fingerprint is also simple through the android phones. The privacy concerns are getting increased through this system. Unauthorized person cannot able to enter into system and get accessed.

REFERENCES

[1] Akansha Bhargava and Dr. (Mrs) R. S. Ochawar," Biometric Access Control Implementation using 32 bit Arm cortex processor", International Conference on Electronic Systems, Signal Processing and Computing Technologies ,2014, pp 40-46.

[2] Peter Peer and Jernej Bule, Jerneja Žganec Gros and Vitomir Štruc, "Building Cloud-based Biometric Services", Informatica 37,2013, pp.115-122.

[3] A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," Trans-actions on Circuits and Video Technology, vol. 14, no. 1, pp. 4-20, 2004.

[4] D. Gonzales Martinez, F.J. Gonzels Castano, E. Argones Rua, J.L. Ala Castro, D.A. Rodriguez Silva, "Secure Crypto-Biometric System for Cloud Computing," in: International Workshop on Securing Services on the Cloud, pp. 38-45, 2011.

[5] R.V.Sathyanarayana, Himabindu Vallabhu,"Bio-metric Authentication as a service on cloud: a novel solution", IJSCE, Vol-2, 2012 ,pp163-165.

[6] N.K. Ratha, J.H. Connell, and R. Bolle, Enhancing Security and Privacy of Biometric-Based Authentication Systems, IBM Systems Journal, 40(3): 614–634, 2001

[7] M. Tovšak, J. Bule, P. Peer, "Upgrading a system for verification based on fingerprints," in: Electrotechnical and Computer Science Conference (ERK), vol. B, pp. 135-138, 2011.

[8] V.Sridhar, M.Rajendra Prasad,Prof. D.Krishna Reddy, Sai Shiva Neethi Reddy, B.Srikanth ," Arm-7 Based Finger Print Authentication System, Volume 2, Issue 4, April 2013,Pp. 149-154.

[9] Vishal P. Patil, Dr. K.B. Khanchandani "Design and Implementation of Automotive Security System using ARM Processor ",International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013.

[10] Adeoye Temitope Onaolamipo,"Development of A Computerized Biometric Control Examination Screening And Attendance Monitoring System With Fees Management ", ISSN: 2221-0741 Vol. 4, No. 6, 76-81, 2014

[11] Dhiraj Sunehra," Fingerprint Based Biometric ATM Authentication System", International Journal of Engineering Inventions, Volume 3, Issue 11 (June 2014) PP: 22-28.

[12] Iswarya G, M. Baranidharan, Bagavathi Shivakumar. C, R. Rajaprabha," Advanced Biometric Authentication System in Two Wheeler", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 1, January 2014.