ELSEVIER

Biometrics in e-Governance and Academia using Hand-held Fingerprint Terminals

A. Tirupathi Rao[1], N. Pattabhi Ramaiah[1], Ahmed Babu I.A.S[2] and C. Krishna Mohan[1]
[1] Department of Computer Science and Engineering, Indian Institute of Technology Hyderabad
Email: {tirupathi.avula, ramaiah.iith}@gmail.com, ckm@iith.ac.in
[2] Government of India
Email: babuahamedias@gmail.com

Abstract— **Fingerprints are one of the biometrics which play an important role in identifying a person based on some minutia features. These biometrics have several applications in the fields of forensics, e-governance, border security, academia and so on. In this paper, an attempt is made to illustrate two different applications using hand-held terminals in the fields of e-governance and academia. One application is fingerprint authentication approach for public distribution system (PDS) using point of sale (PoS) device. The public distribution system finds the genuine beneficiaries with the help of electronic fingerprint authentication system, and Aadhaar central identification repository (CIDR). Another application is portable time and attendance system for students using hand-held fingerprint readers. In many educational institutions, attendance for students is mandatory to better understand the lessons in an interactive manner. In this paper, a new method is proposed for student's time and attendance system which uses IP-based fingerprint reader.**

Index Terms— **fingerprints, public distribution system, portable time and attendance system, point of sale device, Aadhaar**

I. INTRODUCTION

A fingerprint [1] consists of ridges and valleys on the surface of the finger. The uniqueness of a fingerprint can be determined by the minutiae points. Minutiae points are the local ridge features which are identified by a ridge bifurcation or a ridge ending. The fingerprints are mostly used in civilian applications, due to its uniqueness and reliability. There are several fingerprint-based applications in the fields of forensics, border security, e-governance, academia and so on. This paper presents two different applications using hand-held fingerprint terminals in the fields of e-governance and academia.

One application is fingerprint-based online authentication approach for public distribution system (PDS) [2] using point of sale (PoS) device. After the implementation of India's large-scale Aadhaar project, there is a growing demand for biometrics in public distribution systems (PDS). The goal of Aadhaar project is to provide a Unique Identity (UID) number for all the residents in India. A Unique Identity number assigned for every person would obviate the need for a person to produce multiple documentary proofs of his/her identity

for availing any government service. The unique identity number would remain a permanent identifier right from birth to death of every person in the country. UID would enable government to ensure that benefits under various welfare programs such as PDS reach the intended beneficiaries, prevent cornering of benefits by a few sections of people and minimize frauds. The main objective of the PDS is to find the genuine beneficiaries with the help of electronic fingerprint authentication system.

Another application is portable time and attendance system for students using hand-held fingerprint readers. In many educational institutions, attendance for students is mandatory to better understand the lessons in an interactive manner. In this paper, a novel approach is proposed for student's time and attendance system which uses a portable and hand-held fingerprint reader.

This paper is organized as follows. In Section II, the motivation behind the proposed electronic fingerprint authentication systems is explained. Section III, presents two different types of handheld fingerprint readers which are used in the proposed approaches. Implementation model is presented in Section IV. Program analysis and experimental results are given in Section V. Conclusions are explained in Section VI.

II. MOTIVATION

A. Aadhaar Authentication

Aadhaar project is implemented by UIDAI (Unique Identification Authority of India) [3]. The main objective of Aadhaar project is to provide a unique number based on the person's biometrics such as fingerprints, iris and face. As part of the enrollment phase, 10 fingerprints, 2 irises and one face photograph of each person are collected and stored in a central identification repository (CIDR). This Aadhaar number is the single source of identity verification. By providing a clear proof of identity, Aadhaar will facilitate entry for the residents to avail the welfare schemes and services such as PDS provided by the government. There are few existing public utility systems which are implemented based on smart cards in the countries Austria [4], Germany [6], Taiwan [7], Italy [5] and Mexico [8].

Aadhaar authentication is an on-line process of submitting Aadhaar number along with other attributes, including biometrics to the CIDR. Aadhaar authentication provides several ways in which a resident can authenticate themselves using the system. At a high level, authentication can be demographic authentication and/or biometric authentication. During the authentication transaction, the resident's record is first selected using the Aadhaar number and then the demographic/biometric inputs are matched against the stored data provided by the resident during enrollment/update process. Fingerprints in the input are matched against all stored 10 fingerprints.

B. Students' Attendance in Academia

Now a day there is a growing demand for biometrics in academic institutions for student's attendance. The existing biometric time and attendance system is not convenient to utilize for students' attendance. The issues involved in student time and attendance system are as follows:

1. In general, the fingerprint readers in the time and attendance system are mounted to a wall, which is not flexible for taking students' attendance and also it is a time consuming process.
2. Allotting class timings in device-level is a difficult task because some classes will be at flexible timings.

III. HAND-HELD FINGERPRINT TERMINALS

There are two different types of hand-held fingerprint terminals which are used in the proposed methods of fingerprint authentication or verification. One is the point of sale (PoS) device and the other is IP-based fingerprint reader.

A. Point of Sale device

The point of sale (PoS) device consists of the display module, communication module, biometric module and printer. The communication modules are GPRS modem and Ethernet connection. The PoS device consists of the UID compatible application interface for generating the request which is compatible with UID/Aadhaar authentication. The device will be placed at the fair price shop (FP shop) with the dealer. The device is locked with the particular FP shop dealer to make sure the device is operated by dealer only with his UID authentication. The PoS based on-line authentication systems have lot of advantages over traditional smart card authentication systems [10].

B. IP-based Fingerprint Reader

The proposed implementation of portable time and attendance system uses Suprema BioLiteNet [11] fingerprint reader. This device has the features like LAN connectivity through which data can be transfered from device to server and vice versa. Each device can store up to 3000 persons biometric fingerprint templates of two fingers. The device can store the logs of student attendance is around 60000.

IV. IMPLEMENTATION MODEL

A. PDS fingerprint authentication approach using PoS devices

The fingerprint authentication workflow for the public distribution system is explained as follows:
1. The residents provide Aadhaar number, necessary demographic and biometric details at PoS terminals to an operator.
2. Each device is installed with the Aadhaar authentication-enabled software which packages the input parameters. The package will be encrypted and transmitted to the authentication server using a broadband/mobile network.
3. Authentication server validates the package and adds necessary headers (license key, transaction id, etc.), and passes the request to the central server (UIDAI CIDR).
4. Aadhaar authentication server returns a yes/no based on the match-ability of the input parameters.
5. The operator proceeds with the transaction based on the response at the PoS device.

There are many advantages of using PoS based biometric authentication system.
1. Fast and efficient services are provided to the beneficiaries.
2. The commodities will be allocated to the FP shop based on the real time closing balances.
3. The accountability and transparency is increased at FP-shop level.
4. Eligible beneficiaries can get the commodities without wastage.

The program requires UID number as primary for distribution of commodities. There is a secondary authentication method using mobile numbers for the residents who are not having the aadhhar numbers. The PoS terminal generates a 'one time password' (OTP) and will be verified using the SMS received in the mobile. If the user doesn't have UID as well as mobile number, a government supervisor will authenticate on behalf of the beneficiary.

B. Student Time and Attendance System using portable fingerprint readers

The fingerprint authentication workflow for the student time and attendance system is explained as follows:
1. The details of students, faculty and courses are collected.
2. In the enrollment phase, the biometric fingerprint templates are collected from faculty members and students. Each person is assigned with a biometric id which is unique.
3. Once the enrollments are completed, each faculty is allotted with a BioLiteNet fingerprint device. For example a faculty member deals with three courses in a semester, the two fingerprints (left index and right index) of students who are registered for those courses are stored in that particular device. For the entire semester, the device is dedicated to that faculty member.
4. Each course is assigned with a biometric id and assign the authorized people's biometrics for that course. Only the authorized people can verify the course based on course-biometric id. Authorized people may be faculty members or teaching assistants of that particular course.
5. As and when the faculty member takes a class, he/his teaching assistants need to carry the device. Before the class starts, faculty member or his teaching assistant needs to authenticate the course by entering the course-biometric id and his fingerprint. This is a mandatory task which will be used to track the course-wise attendance easily from the device at a later point of time.
6. Once course authentication is over, the device will be passed on to each student for their finger authentication, which stores the attendance status of each student for that particular course.
7. At regular intervals of time (may be weekly or monthly), the faculty or teaching assistants should be responsible for syncing the data to the server from anywhere in the institution's LAN network.
8. At the server side, all these details will be segregated based on course-registration details.

V. PROGRAM ANALYSIS AND EXPERIMENTAL RESULTS

A. PDS Fingerprint Authentication and its Proof of Concept

The proof of concept was implemented in 100 fair price (FP) shops in Andhra Pradesh, India [9]. As part of this analysis, rural, urban and hamlet areas are chosen. Nearly 85 percent of the beneficiaries have the UID numbers and remaining 15 percent beneficiaries have EID (Enrollment Id) numbers. The beneficiaries who have UID numbers are authenticated using fingerprints captured from PoS terminal. The beneficiaries with EID numbers are authenticated using (one time password) OTP or authorized village servants' UID on behalf of the beneficiary. Initially, in the first month of implementation, 97 percent of the beneficiaries are authenticated with their fingerprints and the remaining 3 percent of the beneficiaries who are not mapped their UIDs at the central server. The unmapped UIDs are corrected. In the second month, 99 percent of the beneficiaries are authenticated with their fingerprints and rests of the beneficiaries were not able to authenticate due to the bad quality fingerprints. The authentication accuracy is improved by fusing the matching scores of two fingerprints.

Initially, the average number of authentications for each person was around two attempts. Later it is reduced to 1.3 attempts using the method of 'best finger detection'. The 'best finger detection' method captures the ten fingerprints of the beneficiary and sends the data in the form of UID compliant packet to the central server. It processes the request and gives the response of best fingers of the beneficiary on the rank scale of 1 to 10. If the fingerprints are not matched with the existing fingerprint data in the central server, the 'best finger detection' method prompt the message 'recapture fingerprints again'.

The implementation weeded out nearly 5 percent of the bogus cards and showed nearly 20 percent of savings to government. The tests have been conducted on nearly 70000 families. Each family consists of approximately 4 persons. 85 percent of these families are having valid UID numbers.

The transaction trend is as shown Figure 1, for 9 months starting from September - 2012 to May - 2013. First two months, this program is implemented in 47 FP shops and from November onwards, FP shops are increased to 100. Total ration cards in the FP shop is around 66000. On an average each FP shop consists of 600 below poverty line (BPL) families.
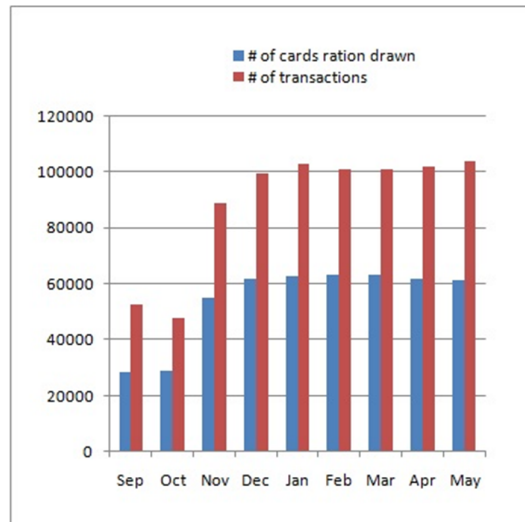

Figure 1. Transaction trend

The authentication percentage with respect to the number of cards in all the FP shops are illustrated in Figure 2.
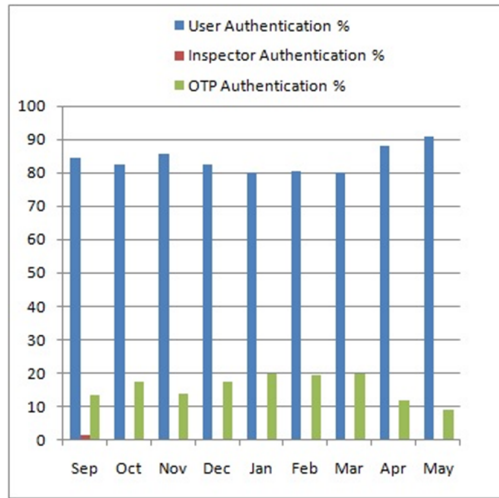
Figure 2. Authentication percentages

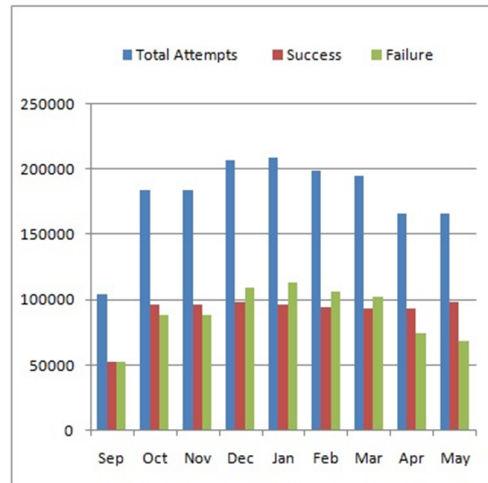Figure 3, shows the number of authentication attempts , success and failure.

Figure 3. Authentication attempts

It is observed that the failure-to-capture rate exists for the people who work hard, old aged, people with leprosy, very dry fingers, very wet fingers, people with shivering hands. Nearly 60% of the people are able to authenticate with in the first attempt. 30 to 35 % people are able to authenticate within 2-3 attempts. Observed very less percentage of people with 0.5% are not able to authenticate, mainly due to old age or leprosy. Each Fair Price shop will consists on an average of 600 cards, nearly 2 to 3 people are not able to authenticate with their fingers. These people were authenticated throw Mandal Revenue Officer (MRO) to do transaction without fingerprint authentication.

B. Students' Time and Attendance System and its Proof of Concept

As part of the student's time and attendance system proof of concept, five courses (C1, C2, C3, C4 and C5) are considered for 160 students. The faculty members allotted for courses C1 and C4 are one, for course C2 are two, for course C3 are three and for course C5 are 10. The proof of concept is conducted for one semester and the attendance percentage for every student is plotted as shown in the figure 4. Based on the observations made in real-time, the proposed approach is proved as a fool-proof concept.
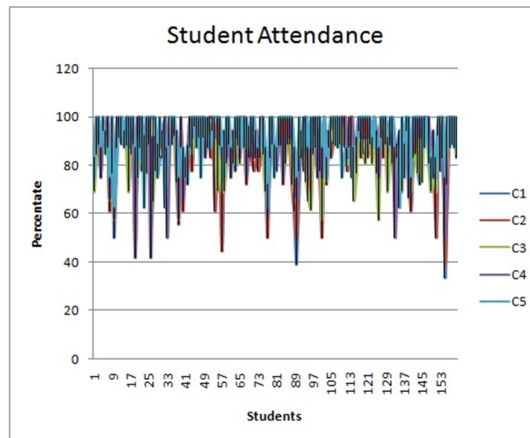
Figure 4. Student Attendance for five courses

VI. CONCLUSIONS

In this paper, two different fingerprint-based authentication approaches are proposed for the applications in the fields of e-governance and academia. The fingerprint based Aadhaar authentication has been implemented in the 100 fp-shops in Andhra Pradesh, India. It is observed that the process is faster than the traditional method of smart-card based authentication. In e-governance this is an first application which issues subsidy through online authentication in India. The program showed the loopholes in the PDS system how much leakage is happening. It is observed that nearly 25% savings in urban areas, 15-20% in rural areas and nearly 30% savings in tribal areas. Advantages of this system are people will know the stock arrival through SMS; nobody can take one person benefits on behalf of others. It provides lot of transparency in the system through online public portal. A lot of attention takes place for portable time and attendance system from the academic institutions. These time and attendance systems will be easy for the instructor to calculate the overall attendance of the student for particular subject. The system showed better results over the traditional paper based attendance.

REFERENCES

[1] FBI, "The science of fingerprints," Washington, DC: U.S. Department of Justice, 1984.

[2] Ahmed Tritah, "The public distribution system in India: counting the poor from making the poor count," France: Toulouse July 7, 2003.

[3] The Unique Identification Authority of India website. [*Online*]. Available: http://uidai.gov.in/

[4] Marcus Kind, Austria introduces an electronic social insurance card. Giesecke and Devreint, Smart Issure 02/2004. [Online]. pp. 1-2. Available: http://www.scc.rhul.ac.uk/ public/ smart2 final.pdf, Feb. 2004.

[5] M.E.Baumgartner, EMV in Italy. Giesecke and Devreint, Smart Issure [Online]. pp. 5. Available: http://www.scc.rhul.ac.uk/public/smart2 final.pdf, Feb. 2004.

[6] Oliver Pannke, On the contactless cards at the Munich Oktoberfest. Giesecke and Devreint, Smart ! Issure 02/2004. [Online]. pp. 7. Available: http://www.scc.rhul.ac.uk/ public/smart2 final.pdf, Feb. 2004.

[7] Michael Gollner, On the electronic smart card system in Taiwan. Giesecke and Devreint, Smart ! Issure 02/2004. [Online]. pp. 14. Available: http://www.scc.rhul.ac.uk/ public/smart2 final.pdf, Feb. 2004.

[8] Gemalto, eHealthcare Solutions-Sergio Popular, [Online]. Available: http://www.gemalto.com/brochures/download/ mexico.pdf Feb. 2004.

[9] Details of ration cards, Scale of Issue & Retail Issue Prices. [Online]. Available: http://icfs2.ap.gov.in:8080/eposmis/welcome.do

[10] Amit Krishnan, Kaushik Raju , Abhishek Vedamoorthy, "Unique IDentification (UID) based model for the Indian Public Distribution System (PDS) implemented in Windows Embedded CE," *IEEE* conference ICACT 2011.

[11] Suprema Time and Attendance products, Available: http://www.supremainc.com/eng/product/fs_00.php?mark=1