Volume 3, Issue 9, September 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Effective Approach Using Combination of Electronic Identity Card (EIC) Systems and Fingerprint Authentication for Automated Student's Attendance Program

Mr. Bhargav B. Patel *
Assistant Professor, EC Department, MBICT College, New V.V. Nagar, Gujarat, India.

Mrs. Suchita B. Patel
Assistant Professor, M.Sc. (IT) Department, ISTAR College, V.V. Nagar, Gujarat, India.

Abstract: ***Electronic Identity Card (EIC) and Mobile fingerprint authentication Systems is one of the most successful applications of Computer science and technology. The main purpose of switching EIC in place of normal Identity card is it avoids maintenance of attendance register and computer attendance entry. Authentication is a significant issue in computer based communication. Human identity recognition is an important role and widely used in many applications, such as any monitoring system, human-computer interaction, online and offline applications like shopping, open bank accounts check into hotels etc. This paper describes a method for Student's Attendance Program which will integrate with EIC technology and Mobile based fingerprint authentication using different algorithms. To automate the whole process of taking attendance manually which is a laborious and troublesome work and waste a lot of time, with its managing and maintaining the records for a period of time is also a burdensome task. The proposed system will overcome drawbacks of all manual systems as well as handles issue new or update EIC cards procedure, student fingerprint authentication procedure using mobile device, record the attendance of students in system database automatically and it will provide the facilities to the faculty to access the information of the students easily by maintaining a database log files.***

Keywords — EIC (Electronic Identity Card), NIC(National Identification Card, FP (Fingerprint) , authentication, Program card.

I. Introduction

EIC is same as National Identification Card (NIC), driving license and passport or other identity cards. In the IT world, which is moving towards the online based services in public or private sectors, a person can identify or get access rights by EIC card system. In this paper we are going to develop EIC for (student's identity purpose) and Fingerprint authentication (student verification purpose) embedded in mobile device for automated student attendance program.

I.I EIC DESIGN AND DEVELOPMENT

The proposed system developing the solution for automating procedure of Student Identification which is having processes like Issue New EIC, Update EIC, Program EIC and Clear EIC memory related procedures. This card create individual identity which display front side details like College name, Unique Student ID, Student Name, Department Name, Contact Number, Valid From, Valid To, Student Photograph and Signature. On the other hand for identity purpose proposed system stores data in back side like student unique id is stored in magnetic strip on EIC.

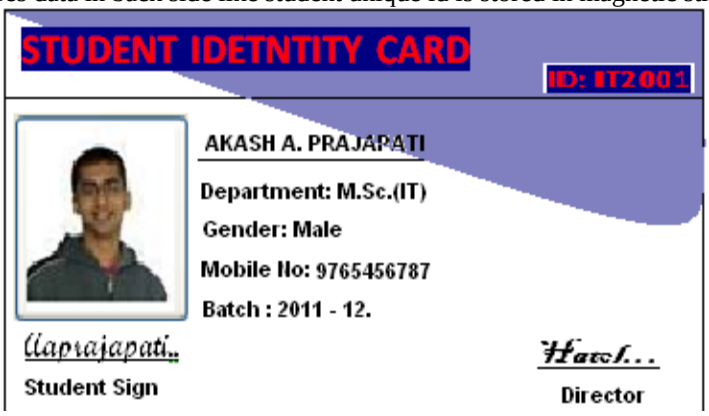


Fig. 1: Design of Proposed EIC

Major Components of EIC Data are identified as follows:

Physical Card: This is to build a physical card which could be of a plastic enclosed an electronic device of regular ID card size

Data in the Card: There can be different types of data that can be stores inside the card in the digital format and some basic data can be printed on the EIC Front Face (shown in Figure 1). Here Student ID store in chip.

Interface: The EIC will be able to interface to any mobile device or tablet via mobile scanner software, thus making it easily usable for automatic student presence.

I.II Comparision Between Nic And Eic

The needs for an EIC could be easily understood when the differences between conventional identity card and an EIC are identified. The following comparison gives brief between national identity card and an EIC:

Table 1: Different criteria wise comparison between NIC and EIC

Criteria	NIC	EIC
Uses	Identity prove	Multi- Purposed
Issue/Update Time	More than one day (at least)	Less than one hour.
Built by	Papers	Plastic and Electronic
Storage Capacity	Card face data	Card face data, Internal memory chip and / or magnetic strip.
Security related data	Hidden image based feature to validate Id	Encrypted PIN number, Digital certificate.
Possession of card readers to access	Any one	Any one, But depend on access level and type, providing data will differ.
Database Access	File and papers in registration	Online Central database access.

I.III Key Benefits Of EIC

The EIC will be more reliable than a paper based ID as it provides more data security and real identification with privacy features [5]. The use of digital signature make it harder or even impossible to make a forged ID as the duplicate ones would invalidate the digital signatures with which the data stored inside the card would be digitally signed. One of the unique features of EIC is its ability to authenticate the right person. The data that are saved in the EIC could be easily and quickly updated by proposed system.

II. Introduction to Fingerprint Authenticate Techniques

Biometric recognition refers to the use of distinctive physiological (e.g., fingerprints, face, retina, iris) and behavioral (e.g., gait, signature) characteristics, called biometric identifiers (or simply biometrics) for automatically recognizing individuals [1].

Among all the biometric techniques, fingerprint-based identification and verification is the oldest method which has been successfully used in numerous applications, because of their uniqueness and reliability. In this system, the fingerprint image data captured during student enrolment is stored / transmitted for 1:1(verification). Based on the mode of acquisition, a fingerprint image is classified as

- Off line image
- Live-scan image

There are a number of live-scan sensing mechanisms that can detect the ridges and valleys present in the fingertip. Examples are

- Optical FTIR
- Capacitive
- Pressure-based
- Ultrasound

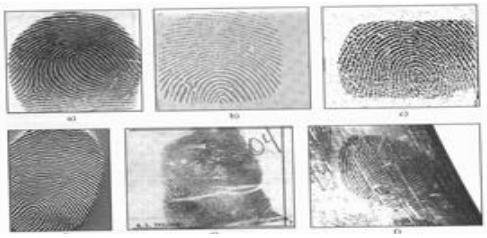


Fig. 2: Visualizations of Live scan fingertips.

There are some applications which are using fingerprint for authentications. They are as follow:

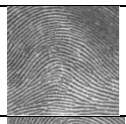
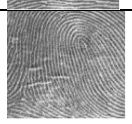
Table 2: List of Government applications for commercial use.

Government	Commercial
National ID Card	Mobile Login
Driver's License	Internet Access
Border Control	Personal Digital Assistance
Parenthood Determination	ATM, Credit Card

In our proposed system we are using fingerprint for authentication of students in automated attendance program via Mobile device. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between human fingerprint and database stored fingerprint.

II.I Fingerprint Patterns

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

arch:	The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger	
loop:	The ridges enter from one side of a finger, form a curve, and then exit on that same side.	
whorl:	Ridges form circularly around a central point on the finger.	

II.II What Is Minutiae?

Minutiae are major features of a fingerprint, using which comparisons of one print with another can be made. Minutiae are formed as ridges separate and create space for forming new ridges due to the growth of the finger surface.
Minutiae include:
Ridge ending – the abrupt end of a ridge
Ridge bifurcation – a single ridge that divides into two ridges
Short ridge, or independent ridge – a ridge that commences, travels a short distance and then ends
Island – a single small ridge inside a short ridge or ridge ending that is not connected to all other ridges
Ridge enclosure – a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
Spur – a bifurcation with a short ridge branching off a longer ridge
Crossover or bridge – a short ridge that runs between two parallel ridges
Delta – a Y-shaped ridge meeting
Core – a U-turn in the ridge pattern

II.II.I Minutia Features

The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot) [6]. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

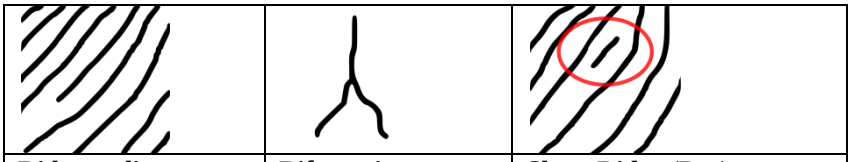


Fig. 3: Representation of Minutiae and Patterns.

II.III Fingerprint Authentication Procedure

In this system we are going to refer Verifier Embedded fingerprint identification technology designed for mobile biometric systems developers [3]. The technology assures fast fingerprint capture and fingerprint matching in 1-to-1 and 1-to-many modes. But for single student verification we will follow 1-to-1 modes. Below figure represents whole process of fingerprint matching which is followed by different fingerprint matching algorithms.

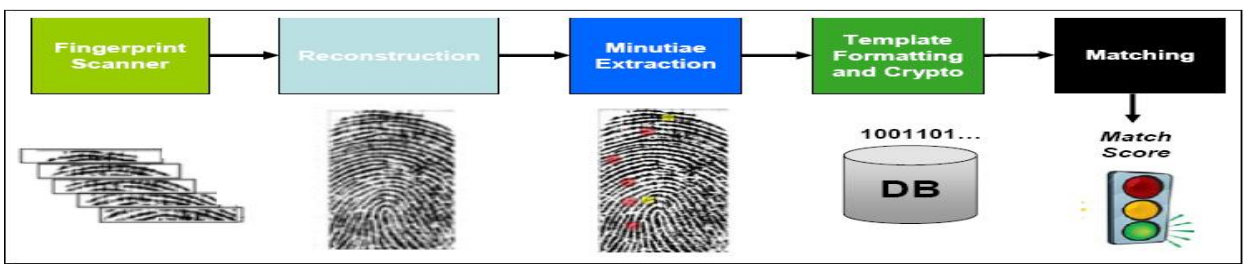


Fig. 4: Fingerprint Authentication Procedure.

In Order to perform Automatic Fingerprint Identification System (AFIS) several techniques have been applied [6], different authors propose many different algorithms but the steps followed for fingerprint identification are similar as follows:

1. Capture of the fingerprint.

2. Pre-processing, to eliminate the redundant information and to adopt the sample to next block requirements.

3. Feature Extraction, where minutiae pores or any information related with the justness of the fingerprint is obtained.

4. Matching of the features obtained with the template previously computed in the enrollment phase.

This matching will provide percentage of similarity that will be used to determine whether the user is same as enrolled user.

III. System Architecture and Its Implimentation

The system works in number of ways for various applications but here we identify the three basic levels which are listed as: detection level, searching level, monitoring level and security level

Detection Level: In this level the individual student's identity is manually verified against his/her photograph obtained from the EIC card by manual. This mode is efficient to use at places where the security requirement is not very high.

Searching Level: Here, a specific student in the sphere of the range is searched. In this level mobile device application can search for student card depending on all or any one of the entered fields like enroll number, name, pin code, blood group and student exam ID card number.

Monitoring Level: Monitoring level is used in high security areas to allow or restrict a student to enter or leave the premises by verifying his/her identity information obtained from the EIC card with the stored database records in the database Server. This is very pertinent in restricted places like director office, administrator office, laboratory buildings, etc.

Security Level: This level is applicable for authenticate right student for attendance for avoiding proxy entries. Besides monitoring, this level also maintains a database of all the student register attendance or reporting late. we divide the information carried by the EID card into three modes viz. NORMAL, SECURITY mode 1 and SECURITY mode 2 that define the access privileges of the application (refer figure) at the mobile application side. Depending on the mode, only the information of the allowed fields is available to the device.

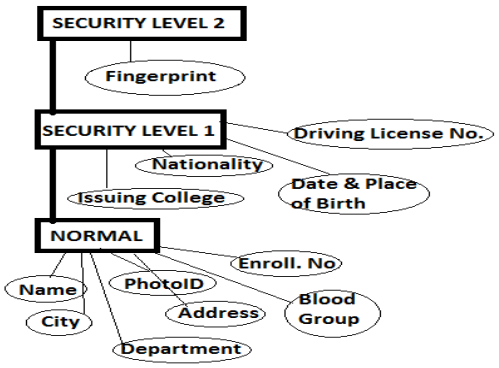


Fig. 5: Security modes available in Security level.

The fields lying in normal mode is termed as general information that is available on front-side of card. By using this general information we can identify right student. So, the user knows when his/her critical information is being accessed and by whom. At mode-2 we can store detail personal student information such as enrollment number, driving license, date and time of birth, nationality and issuing college name. RSA encryption has also been provided to ensure data security so we are using encryption by public and private numerical "keys" based on large prime number s to convert text into a scrambled format. The resulting unreadable "cipher code" cannot be understood without the correct access key. When data is stored on EIC card, it is encrypted using the public key. Only mobile application possesses the private key capable of decrypting the information and made auto entry in attendance application.

III.I Components of the Secure Attendance System

Mobile Equipment: Inside the secure attendance system mobile equipment can be used either by the student or the staff members. The Mobile Equipment should have the student attendance application installed on it. The professor uses the mobile equipment for taking attendance, editing mark. The students' electronic card equipment to register their presence in mobile device.

Electronic Identity Card: Program card module read or writes student details on card memory. Student details and lecture details are stored by application installed in smart mobile devices. Student can easily register their presence by EIC card. Server stores details regarding student information, professor's lecture date-time information, student day-to-day attendance entry and related report information.

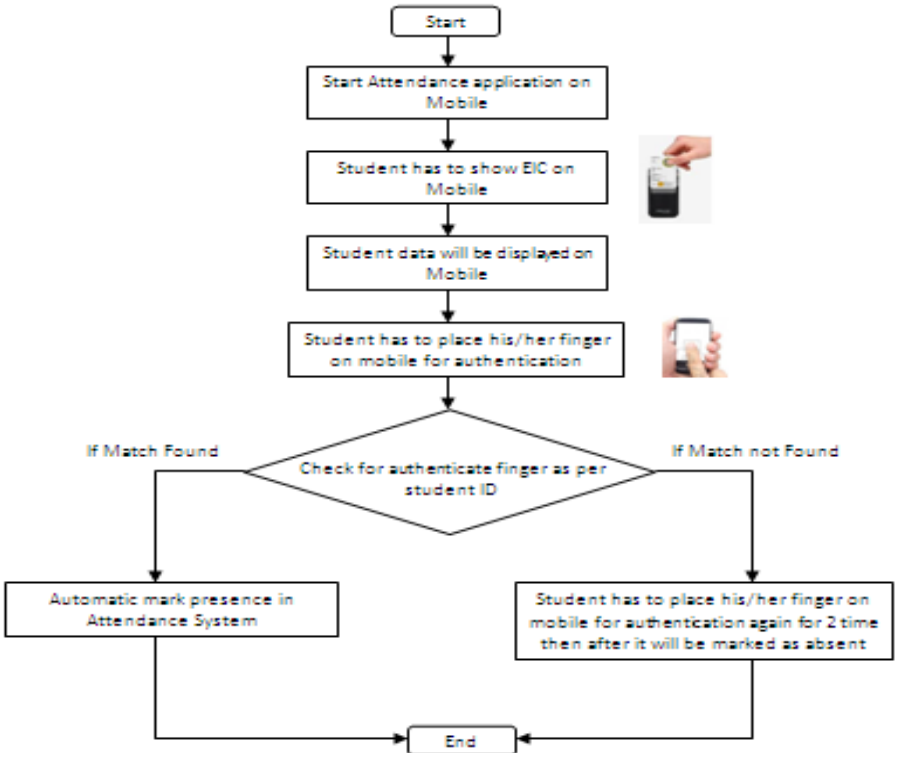


Fig. 6: Represents system flow diagram

III.II Authentication Procedure

The process to authenticate student with EIC and fingerprint using mobile client reader software is as follows.

Step 1: Identification Request: the client software requests student ID data from EIC.

Step 2: Display Identity: Client Software receives identity information from the database server about student regarding given EIC data and displays it on mobile.

Step 3: Authenticate Request: Client software request for fingerprint of student using mobile.

Step 4: Authentication response: Client reader software displays presence or absent of student.

Server software matches the fingerprint data with database server and if it matches then it will manage student attendance else if fingerprint doesn't matches to database data then system only allows encounter 3 times within one lecture time for authentication. The database server forwards the received EIC data to the request client software.

IV. Design and Experiment Result

Design procedure for this system is done as a two modules. First is Program Card and another is Student Authentication. These modules are explained as follows with screen designs. In Program Card module all the required student registration details are written on card as well as on server machine. And in Authentication module consists two separate functions are developed as for now; they are mobile attendance and mobile mark editor. This two let to ease the work of staff member. From mobile attendance they can take attendance and can be update to sever at the moment. It avoids the malfunction like proxy in attendance system. Mobile Mark Editor also has the same function as mobile attendance. It saves the mark details of the student and saved in server.

Fig. 7: Shows screen shots for student Authentication Procedure.

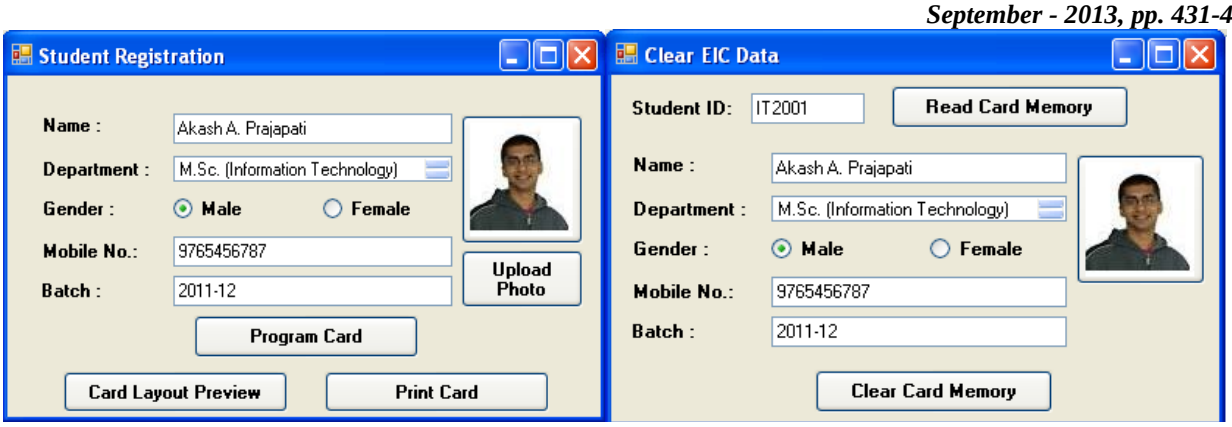


Fig. 8: Represents screenshots for student registration and re-register program on electronic Card.

V. Conclusion

From our previous experiences in the secure attendance application, we would like to offer new choice for academic professors and to ease their work. And we found that Google android is a suitable tool for the attendance application use. In this way, we extended the android platform mainly based on the requirements from previous works. Further, we have included mobile based curriculum activity to increase the usage of the application. This academic attendance system can be further extended by adding feature like NFC.

References

[1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, pp. 2021– 2040, Dec. 2003.

[2] Arulogun O.T, Omidiora, O., M. Olaniyi, andA.A. Ipadeola (2008), "Development of Security System Using Facial Recognition", Pacific Journal of Science and Technology, 9(2):377-386.

[3] Henry. S, S. Arivazhagan and L. Ganesan, (2003),"Fingerprint Verification Using Wavelet Transform",International Conference on Computational Intelligenceand Multimedia Applications, 2003.

[4] Chitresh, S and Amit K (2010),"An efficient Automatic Attendance Using Fingerprint Verification Technique ",International Journal on Computer Science and Engineering (IJCSE),Vol. 2 No. 2,pp 264-269.

[5] Longe O.O.(2009),"Implementation of Student Attendance System using RFID Technology", B. Tech Project Report, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[6] Maltoni D, D. Maio, A. K. Jain, S. Prabhaker (2003), "Handbook of Fingerprint Recognition", Springer, New York,Pp 13-20.

