World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:3, 2015

Student Records Management System Using Smart Cards and Biometric Technology for Educational Institutions

Patrick O. Bobbie, Prince S. Attrams

***Abstract*—**In recent times, the rapid change in new technologies has spurred up the way and manner records are handled in educational institutions. Also, there is a need for reliable access and ease-of use to these records, resulting in increased productivity in organizations. In academic institutions, such benefits help in quality assessments, institutional performance, and assessments of teaching and evaluation methods. Students in educational institutions benefit the most when advanced technologies are deployed in accessing records. This research paper discusses the use of biometric technologies coupled with smartcard technologies to provide a unique way of identifying students and matching their data to financial records to grant them access to restricted areas such as examination halls. The system developed in this paper, has an identity verification component as part of its main functionalities. A systematic software development cycle of analysis, design, coding, testing and support was used. The system provides a secured way of verifying student's identity and real time verification of financial records. An advanced prototype version of the system has been developed for testing purposes.

***Keywords*—**Biometrics, fingerprints, identity-verification, smartcards.

I. Introduction and Background

RECORDS are vital to every organization. Maintaining records helps in keeping track of the roles and information of every person belonging to an organization. Such records often include operational, policy, and other pertinent data. In educational institutions, the case is obviously no different from other organizations. Basically, the two types of records which are critical and vital in every educational institution are staff records and student records. Kemoni and Wamukoya [1] are of the view that effective record management systems provide information required for the proper functioning of organizations, including educational institutions such as universities. On the other hand, poor record management can be risky to organizations.

Most importantly, since the main function of educational institutions is to provide service in line with its core mandate, which includes teaching, training, learning, research and development to students, it is important that student records are handled very well. It should be easy to retrieve records at any point in time and be reliable at all times.

There are many forms of record management schemes employed in various institutions ranging from record bookkeeping systems which are largely manual to some form of electronic management system. In both manual and electronic record keeping systems, mechanisms and procedures for secured access to the records are fundamental and a requirement.

In recent years, it is common for most educational institutions to offer some sort of identification for students by issuing student identity cards and identity numbers to gain access to use, view, or manage the records. Yet identity fraud and impersonation schemes compromise this approach affecting the efficiency of the core service of educational institutions using ID solutions. This research seeks to enhance existing student record management systems with a more reliable approach using smart cards and biometric technology to improve upon identification and verification of student credentials.

Biometric technology is a widely known technology which measures and analyzes human biological data. The biological data often include DNA, fingerprints, eye retinas and irises, and voice patterns recognition. Storing of biometric data is increasingly becoming a trend for verification and identification processes in recent developments. Storing biometric data on cards has also made it possible to effectively retrieve user identification details electronically.

Magnetic strip cards and some sophisticated smart cards can hold this information over long periods of time and they have been applied in various fields such as financial institutions and some transport agencies such as banks and driver's license authorities, respectively [2]. Its associated readers are designed to collect the stored information in a matter of seconds and this creates an expedited way of data acquisition.

Student records management is imperative to the productivity of every educational institution. The credentials of students provide the security access to records such as financial records, examination records and class attendance records that permit the provision of quality service, monitoring of student academic progress, and performance data.

Often, granting student privileges and accessibility to certain restricted areas depend on the aforementioned records.

P. O. Bobbie is with the Dept. of CS, Southern Poly State University, Marietta, GA, 30060, USA (phone: +678.915.4284, fax: 678.915.1511; e-mail: pbobbie@spsu.edu. He worked in collaboration with Faculty of Engineering Ghana Technology University College, Tesano-Accra, while in Ghana.

P. S. Attrams graduated with B. Telecom Eng (Hons), First Class, in 2013 from the Faculty of Engineering, Ghana Technology University, College, Tesano-Accra, Ghana (e-mail: attrams2000gh@yahoo.com).

As such, educational institutions require reliable and rapid techniques to enhance the rendering of service to students who have satisfied all necessary requirements. These reliable techniques will help lessen the bane of possible impersonation and identity fraud in educational institutions.

A. Problem Statement

The current methods for record management in most educational institutions around the world use a considerable amount of manual or electronic procedures in storing and retrieving student records. Inefficient record management systems often create difficulties in managing the records of students, because the techniques used in the record management systems create difficulties in identifying and verifying students by matching them to their records

In the academia, student financial obligation often determines the level of accessibility and privileges to certain restricted physical areas or spaces on a computer. This may be access to an examination hall, or an electronic system such as the login interface to a library's resource system.

Also in most cases students may be required to seek authorization to attend lectures or take an examination. The reliability of this security information is critical for individual students and is also significant for the effective and quality operations of the educational institution and the student.

This research is motivated by the need to enhance and create a student's management system capable of delivering reliable verification and identification of student records using biometric and smart card technology.

II. Related Research

A. Smart Card Technology

Smart card technology is a widely used technology in various industries for many applications. They are preferred over magnetic strip card technology due to security concerns. Smart cards are embedded with microprocessors that allow a comparative advantage over its magnetic strip counterpart because of its larger storage size, support for strong authentication techniques, and digital signatures. Since this research is focused on adding biometric technology to smart cards technology, security is a major functionality of the system. The system also comprises an identification and verification modules for reliably storing of information and protecting of the student's biometric details. Authentication issues require that the cards be checked using digital signatures to aid in determining if the card was issued by a valid educational institution.

B. Biometric Technology

Smart Card Alliance defines biometrics as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics [3]. It is of great importance that one or more, unique physiological human characteristics is chosen, and well defined in order to select the right biometric technology for the system. Selection of the right biometric technology will depend on the application of the system and factors that may affect the system including the environment in which the system will be used, requirements for verification, accuracy, cost and cultural issues are critical metrics for the overall system performance. Fig. 1 below depicts a comparative analysis of different biometric technologies and some human characteristics.

Using one of these human biological characteristics in the design of a system is commonly referred to as a "unimodal biometric system" whereas the combination of two or more of these biological data in a system is known as a "multimodal biometric system". This research deals with the scanning of fingerprints of students. The system can conveniently be described as a unimodal biometric system. Fingerprints scanning technology is the most commonly deployed biometric technology, used in a wide range of physical access and logical access applications [4]. It was also chosen for this research due to its long-term stability, ease of use and average user acceptance.

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds
Accuracy	High	High	Very High	Very High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

Fig. 1 A Practical Guide to Biometric Security Technology [6]

C. Identification and Verification Systems

The primary function of identification systems is to use some form of information to differentiate between individual members in a group of identical data. The data is usually stored in a central database and the identification system intelligently performs matching with biometric data stored in

the database. This is otherwise known as one-to many matching. In most systems, the identification system is used at the enrollment stage where data needs to be stored [3].

Generally, identification systems perform some form of verification as well. The system uses something that the user knows or has in possession in order to perform identity verification functions. For example, ATM machines require PIN numbers which the user knows, and are needed for the system to identify the user. Some concerns raised with this approach is that, many may forget or lose their PIN numbers [5]. But the use of biometrics solves all these challenges to some considerable extent. When the scanned biometric capture is received by the system, it compares it with a stored template. They are both matched to verify the identity of the user. Usually, a threshold is set normally known as the matching score to measure the level of accuracy of both templates. A systematic procedure, logical flow is for processing or performing biometric matching, is shown in Fig. 2.

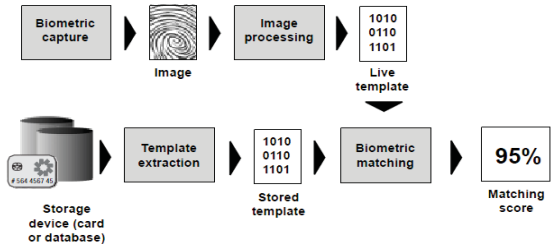

Fig. 2 Identification System Process Courtesy Smart Card Alliance

D. Security Features in Biometric Systems

To protect the data of users, biometric systems need to ensure that the biometric information of each user is secure. A lot of schemes are used to ensure the safety of this vital information especially due to privacy concerns. Hao et.al posit that many users may be reluctant to have biometric data stored on central databases. They continue by saying that there may be less resistance to biometric technology if users can be credibly assured that their data are not stored centrally [7]. It shows the reason why the security schemes used should be as efficient as possible.

Using smart cards significantly enhances privacy in biometric systems. The smart card provides the user with a personal database and it secures personal information on the card which allows the individual to control access to that information and it removes the need for central database access during identity verification [3]. Physical authentication techniques are also used in the printing of the smart cards that enhances physical inspection of the cards to ensure that it was issued by the right issuing authority.

E. RFID (Radio Frequency Identification)

Radio frequency identification (RFID) is a technology that uses tags and readers to capture information automatically. It can be viewed as a form of Automatic Identification Capture. The tags normally contain electronically stored information and the stored information is read by the readers normally within the frequency range of the reader. The readers collect the data to a backend application system for user manipulation purposes. The RFID tags come in two forms; the powered tags (active tags) and the unpowered tags (passive tags). The Active RFID tags normally contain batteries that allow them to be self-powered whereas the Passive RFID tags do not contain batteries but power is supplied from the RFID readers.

Once the RFID reader is on, it emits a signal at a selected frequency which allows every corresponding RFID tag within the range of the reader to detect and send information. The tag decodes the signal from the reader and ensures its validity before it replies with the required information. Some applications use an RFID middleware which handles operations such as filtering, data coordination and processing. Many applications also use a host computer which provides an interface between the RFID hardware (Tags and Readers) and an application based system. The computer is used to network multiple RFID interrogators together and to centrally process information. [8] There are numerous advantages that come with RFID which makes it useful in systems that may require automatic identification.

F. RFID Based Student Database Management System

In this research, student database management system stores student's records in a database and identifies students with a valid contactless RFID tag. Student data stored includes their student ID number, academic details, hall of affiliation, and institutional details. The system comprises a reader connected to a PC through a RS232 to USB converter a simple connection or configuration that allows easy access to the computer. The system components include a front-end GUI implemented using C# language with the support of Microsoft Access database as the back-end. The GUI allows users to enroll data into the system and it also displays the identity of the user once the tags fall within the range of the reader.

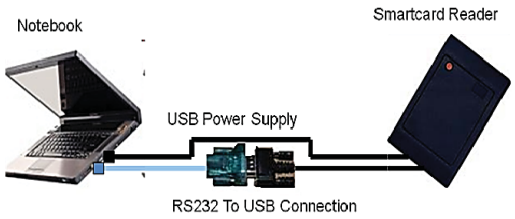

Fig. 3 RFID reader to PC connection [9]

Fig. 3 depicts how identification of students can be achieved through a means of contactless communication. Tudu and Ramachandra proposed a system that could be used in colleges or institutions for tracking attendance where each and every student would have an RFID tag attached to their identity cards. They proposed that the readers can be installed in classrooms or anywhere the tracking of students would be needed. However, this system may not reliably verify the identity of students since an impostor may use the same card within the range of the RFID reader.

III. Methodology and System Design

System development methodologies are used to control and manage software design process as well structuring and simplifying the entire system development process. It also helps in standardizing the development process and production by indicating the activities to be done and the techniques to be used. In this research, the process model used was the Linear Sequential Model also known as the classic life cycle or the Waterfall model. The LSM is a systematic approach to software development that begins at the system level and advancements through analysis, design, coding, testing and support.

A. Functional Requirement of Record Management System

The functional requirements define the function of the software system or its components. A function is described as a set of inputs, the behavior outputs and how the system is able to evolve to meet the changing environment. It describes the details of what the system is supposed to provide as well. Since this research was developed in the context of educational institutions, student records were used as the primary test data.

B. Smart Card Reader/Writer

The smart card reader/writer reads/writes the stored information on the smart card. The type of smart card reader/writer used for this research was based on the ISO 14443 and ISO 15693 standards. It was selected due to its close range contactless property which operates at 10cm and its capability of writing different types of data including additional authentication factors such as biometric templates.

C. Fingerprint Scanner

The fingerprint scanner takes the fingerprint inputs of the students and compares them with the template stored on the Smart Card. The scanner is used along with the Smart Card reader, the student registration module and the identity verification module to take fingerprint inputs from the students during the registration process, and, furthermore, to authenticate the identity of the students. The type of fingerprint scanner used in this research was an optical fingerprint scanner. It was chosen because of its small size and its ability to capture high quality images. It supports DES/3DES encryption algorithm, which executes at a high speed at the hardware-level.

D. Smart Card

The smart card stores the identity information of students including the fingerprint templates captured during the student registration process. Its contactless nature communicates with the reader through an induction technology similar to that of an RFID. Like smart cards with contacts, contactless cards don't have batteries. However, they use a built-in inductor to capture some of the incident electromagnetic signal to power the card's electronics. The smart card's microcontroller processing ability and writeable memory allows flexible data storage and upgrade without changing the card itself. The biographic information, along with the student's registration number, is printed on the cards.

E. The Student Record Registration Module

The student registration module is used to receive input data from the students, which is uploaded to the centralized database and to the smart card. The fingerprint scanner and the biometric reader/writer are the main components used in the registration process. The fingerprint scanner and the biometric reader/writer are linked to the host computer via a USB cable. This module also allows an authorized user to update the records of students. One of the main entry fields for the purpose of this research is the financial record field. This record field is used as a basis for identification in the record management system.

F. Centralized Database

The centralized database stores all information recorded during the registration period. It utilizes the Internet in receiving information as entered by the user via the student record registration module. It comprises two major categories: the processed financial category and the unprocessed financial category. The database was developed using the Oracle Database, and with Java Server Faces as the framework. All interfaces were developed using the Java programming language as well.

G. The Record Identification and Verification Module

The record identification and verification module is responsible for the authentication of the identity of students. This module is also used along with the fingerprint scanner and the biometric reader/writer. This module has two phases.

The first phase is where the stored template from the smart card is matched to the live template taken from the fingerprint scanner. The matched result verifies the identity of the smart card bearer. This phase of the record identification and verification module does not rely on the central database but takes all information from the smartcard, which ensures rapid one-to-one matching results.

The second phase is where the stored template from the smart card is matched to the record information stored in the processed financial record category of the centralized database. This phase depends on the central database but ensures that the searching is done in one category of the database which promotes rapid results as well.

H. The User Login Module

This module authenticates the user before accessing the centralized database and any of the modules. The login module grants access to only authenticated and authorized users depending on their access rights and restrictions.

IV. Use Case Diagram

The use case diagram describes the sequence of logical steps for user interactions with the system. There are three users designated to have access to the system, and they are categorized as the first degree administrator, the second degree

administrator and the normal user. All three users have specific privileges and restrictions. All users require a unique username and password to gain access rights. Fig. 4 depicts the privileges and access rights of each user category.

A. The System Design

The system design phase focuses on the various modules of the system. The activities of the design phase ensure that all components exhibit cohesive and coherent properties, that is, they work independently and interdependently at the same time, with well-designed interfaces. Fig. 5 depicts the system architecture that was developed from this research.

The logical flow in the system architecture shows an interconnection of the system components and the Internet. It shows the centralized database, and the backend system which has the server application installed on it. Other devices, such as were laptops, are connected to the database via the Internet. The laptops act as clients, or end systems, for accessing all the system modules/interfaces depending on their access rights. The smart card readers and fingerprint scanners are also connected to the backend system, and the clients through USB connections.

When a new student is due for enrollment, the *first degree administrator* (a staff at the office of admissions) enrolls the student and stores all necessary information into the database. The fingerprint scanner and biometric smart card reader/writer aids in collecting and storing fingerprint templates respectively. The *second degree administrator* (a staff at the office of finance) enters/updates the student's financial record, which is also stored in the database.

The identification and verification process is effectively utilized in checking the financial record of the student at the entry point of the examination hall. The actual verification step is complete when the student hovers the smart card over the reader at a close range.

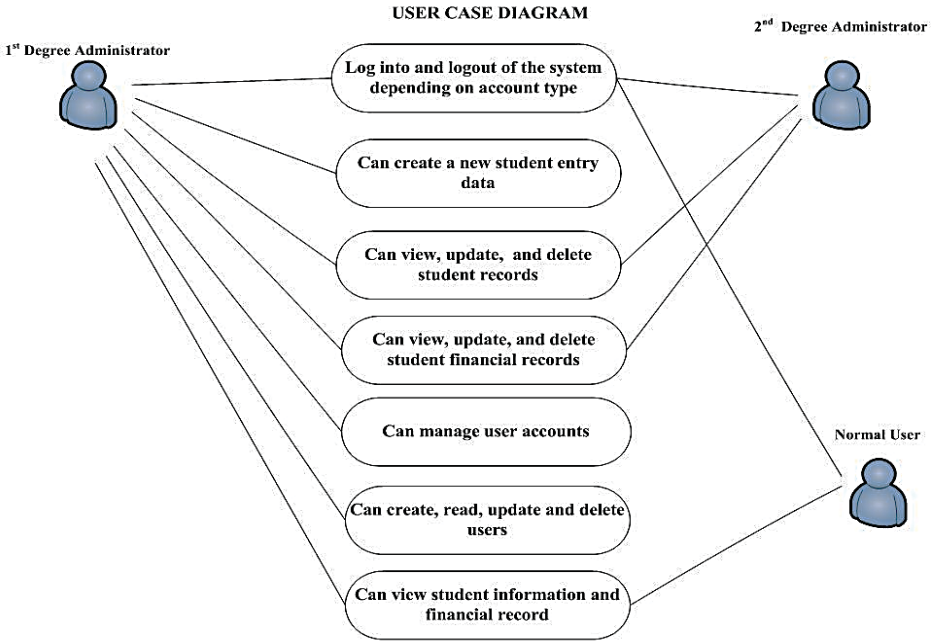

Fig. 4 Use Case Diagram for Student Records Management System

A *normal user* (e. g., a security guard) may log into the system to view the financial record of the student before permitting entry. At the end of the exam, the verification of the student's identity is achieved by hovering the smartcard over the reader while the student is scanning his/her finger from the fingerprint scanner. The matched results are displayed on a screen of an assigned staff (e. g., the chief examiner).

B. Security

Security within the system is essential to ensuring the safety of sensitive data during transmission via the Internet. The main security features adopted in this research were encryption and physical security features using unique features like the emblem of the educational institution.

The RSA public key algorithm was used to generate the key, encrypt and decrypt data. Also encrypting the data on the smart cards was imperative. This was to keep the data stored on the cards confidential. Also the physical security technique used was to aid in the rapid physical inspection of the smart cards to ensure that it was issued by the authorized institution.

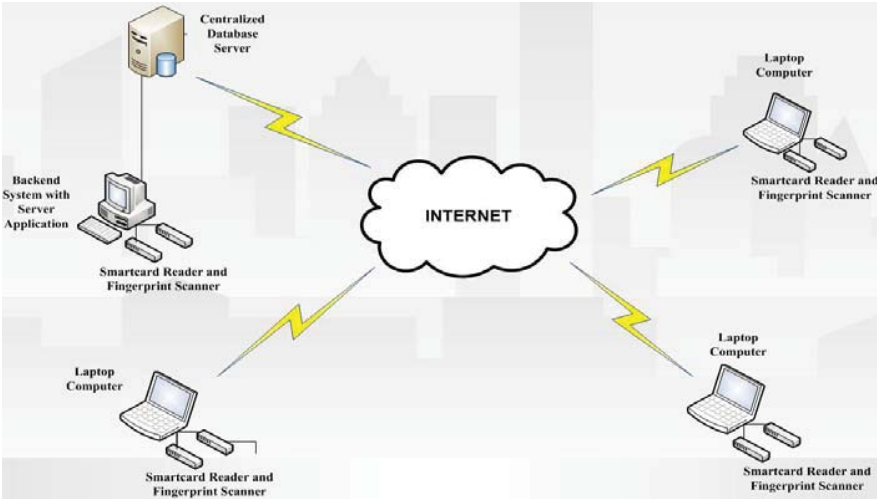

Fig. 5 System Architecture for Student Records Management System

V. System Development and Regression Testing

Once system modules are developed, regression testing ensures that individually tested modules coherently conform to the overall system behavior, or functionalities. Regression testing further reveals improper interfacing of the system modules and non-compliance to its functional requirements.

A. Implementation

The entire system of this research comprises a fingerprint scanner, a smart card reader/writer, a backend database that stores the records of students including biometric data (fingerprints), and an interface that allows users to register student details, view student details and verify the identity of students. The system depends on the database for verifying student's financial records and the data stored on the smart cards for identity verification. The user interface and the database interact in real-time when verifying the student's financial records but the identity verification is done offline without any interaction with the database.

B. User Login Screen

The user login page shown in Fig. 6 allows a user to enter a username and a password to allow access into the system. The privileges the user has depends on the login details of the user.

C. Student Registration Page

As depicted in Fig. 7, the student registration page provides all the necessary fields for registering a new student. It also has a fingerprint template field that stores the image of the fingerprint template received from the fingerprint scanner and a picture field that stores the picture of the student. After inserting the correct details and all necessary data into the fields, the student registration page has the *submit* and *reset* features, which allow the user (first degree administrator) to either send the student's data to the database for storage or cancel the entire process respectively.

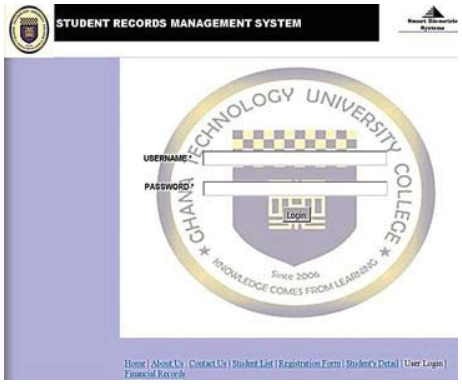

Fig. 6 User Login Page

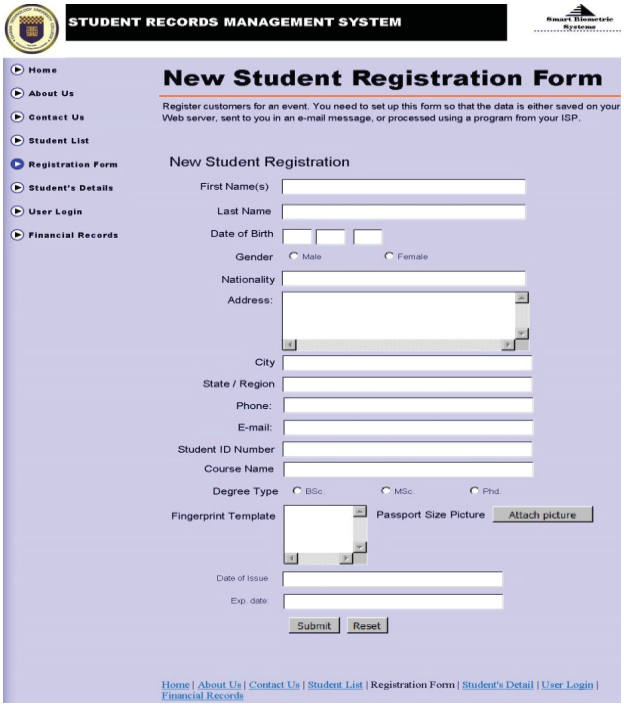

Fig. 7 Student Registration Page

Fig. 8 also depicts the student details page. This page gives a summary of the student's identity details and allows the user to print the student's identity details on the smart card. Fig. 9 depicts a sample smart card with the details of the student printed on it.

Fig. 8 Summary Student's Details Page

Fig. 9 Sample Student Identity Details (printed on a smart card)

D. Student's Identity Verification Page

The Identity verification page allows the user to verify the identity of the student using the biometric data stored on the card and a live fingerprint template. The page is usually blank at first. However, upon hovering the smart card over the smart card reader the data on the card is read and displayed on the page. Fig. 10 depicts the page shown after the data is read from the card. The page prompts the student to take a fingerprint scan using the fingerprint scanner. After a successful match of the live template with the template stored on the card, the student is successfully verified as depicted in Fig. 11. However, if the live template is different from the template stored on the smart card, the page depicted in Fig. 12. The page indicates a rejected identification outcome.

Integrated and system testing ensures that the entire interconnected system works according to specification. This process also ensures that the hardware devices connected to the system work in harmony with the interfaces and the backend system. The student registration form was filled with data to check if the database could store the data. A sample card was printed to test the financial records identification and the identity verification functionalities of the system.

Fig. 10 Student Identity Verification Page after data is read from smart card

Fig. 11 Student Identity Verification Page after successful match of fingerprint templates

Fig. 12 Student Identity Verification Page after unsuccessful match of fingerprint templates

E. Integrated and System Testing

These processes confirmed the desired operation of the system modules. During the system implementation phase, one of the main challenges was finding the right tune to support the system security requirements. Since the highest security was needed during identity verification, it was revealed that the system was able to achieve a low FAR (False

Acceptance Rate) and tolerated a relatively high FRR (False Rejection Rate).

VI. Conclusion and Recommendation

With advances in technology and the constant improvement of existing products and software / system implementations, the deployment of state-of-the-practice methods and devices in handling records in educational institutions will ensure productivity and effective assessments of students. This research outcome presents a verification system (tool) for educational institutions or organizations who are currently facing challenges in managing secured records, that require authentication. This is particularly the case where access to restricted areas or where serious examination malpractices such as impersonation are prevalent in academic institutions.

The system is easy to use and requires little training for first-time users. The system handles security concerns such that the secure storage on the smart card allows students to control access to the information stored on the card. The system also removes the need for the central database during identity verification.

New features and upgrades are necessary to enhance the performance (improved response times) of the system and also scalable (for large datasets). Also, additional functionalities such as an identity verification log can be added to the system to store the verified details of students after taking an examination. The identity log would be useful in record management procedures found in educational institutions. It may also be very useful in class attendance monitoring and evaluation, and minimization of identity theft cases.

References

[1] Kemoni, H. and Wamukoya, J. "Preparing for the management of electronic records at Moi University, Kenya: A case study," African Journal of Library, Archives and Information Science, vol 10, no.2, February 2000, pp 125-138.

[2] Dandis A.T and Hamoury T (2012, September 6) *Smart Card Technology: Evaluation Approach* [Online]. Available: http://www.docstoc.com/docs/128383947/Smart-Card-Technology-Evaluation-Approach

[3] Smart Card Aliance, May 2002, Smart Cards and Biometrics in Privacy-sensitive secure personal identification systems. pp.8

[4] Samir Nanvati, "Biometrics: Identity Verification in a Networked World", New York: Wiley and Sons Inc, 2002, pp.12.

[5] Anul et. al. "Biometrics Personal Indentification on Networked Society", New York: Kluwer Academic Publishers 2002, pp. 21-22.

[6] Liu, Simon; Silverman, M., "A practical guide to biometric security technology," *IT Professional*, vol.3, no.1, Jan/Feb 2001, pp.27-32.

[7] Hao et.al. "Combining Crypto with Biometrics Effectively, IEEE Transaction on Computers, vol.55, No.9 September 2006. pp. 2.

[8] Daniel Hunt, V. Puglia, A., Puglia, M. RFID-A Guide to Radio Frequency Identification, Wiley-Interscience, 2007, pp. 7.

[9] D.K. Tudu and S. Ramachandra, "RFID Based Students Management System", M.S. thesis, Dept. Elect. and Comm. Eng. National Institute of Rourkela, India, 2010/2.