Biometric Secured Result Processing Software For Nigerian Tertiary Institutions

Oladipo Oluwasegun, Akomolafe, O.T., Oyedeji A.I

Abstract: One of the challenges facing result processing in Nigerian tertiary institutions is the problem of insecurity. Untraceable changes are made to students' result and this result to various disasters such as innocent people losing their jobs since their innocence cannot be proven. Biometric based systems operate on behavioral and physiological biometric data to identify a person and grant required access to a user. Physiological characteristics such as fingerprint remains unchanged throughout an individual's life time and thus, it can serve as a viable means of identifying and authenticating users who are to access a system. In this study fingerprint biometric based result processing software is developed to ensure that users are well authenticated and are made to see only what they are pre-configured to see and work with. The fingerprint authentication system was developed using visual basic.net. Staff fingerprints were enrolled into the system to form a biometric template which the system validates against at every login attempt on the result processing software. The digital personal one touch ID sdk and other libraries were used in developing the authentication system. The result processing software also ensures that all write transactions to the database are confirmed and identified by forcing another biometric authentication at the point of making a write request to the web server and associated database. This ensures that the exact person initiating the transaction was the same user who logged in to the application. The users identified at login and various confirmation milestones set for write transactions are logged into a table for future reference and audit trail. Conclusively, the developed system has helped to eradicate the problem of user impersonation by ensuring only authorized users are made to access the software and in-turn participate in result processing activities.

Index Terms: Biometric, Nigeria, Result processing, software, Tertiary Institutions,

1 INTRODUCTION

The computation and processing of examination results in tertiary institutions is quite awesome and demanding. Being that, it involves sensitive information processing of students most important data, the process must be characterized by the most efficient security techniques. In every tertiary institution it is imperative that proper measures are put in place to ensure that the right people have access to the result processing process and it's important that they can only perform write operations within the limit to which they are authenticated. Traditional methods of user authentication unfortunately do not authenticate users as such. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier [1]. Typically, authorized person checking is done either by entering some password, using some (smart) cards or drawing patterns [1]. But, there is high risk of intrusion which might be from stolen cards or exposed password. This places data in an online environment open to alteration by unauthorized personnel. This could be more disastrous when accesses cannot be traced.

The study recognizes the importance of identifying and authenticating any given user in a result processing environment and the increasing demand of enhanced security systems has led to an unprecedented interest in biometric based person authentication system. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. It is an automated method of recognizing an individual based on physiological or behavioral characteristics such as fingerprints, distinctiveness in terms of characteristics, persistence characteristics, collectability characteristics, and the ability of the method to deliver accurate results under varied environmental circumstances, acceptability, and circumvention [2]. The advent of biometrics has introduced a secure and efficient alternative to traditional authentication schemes. The aim of this study is to implement a layer of biometric security using Visual Basic.Net (Vb.net) on multimodal result processing software. To achieve this all valid users were enrolled into a central database for proper identification before accessing the result processing software. An identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity [7].

2 REVIEW OF EXISTING LITERATURE

Establishing the identity of an individual is of paramount importance in several applications where errors in recognition can undermine the integrity of the system. Traditionally, a combination of ID cards (token-based security) and PINs/passwords (knowledge-based security) has been used to validate the identity of an individual [6]. These methods are, however, vulnerable to the wiles of an impostor and cannot be reliably used in large-scale applications such as border control, where the throughput is required to be in the order of thousands of users per day. A typical biometric system comprises of several modules. The *sensor module* acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. The *feature extraction*

- *Oladipo Oluwasegun is currently a lead programmer at yabatech and pursuing a PhD degree program in Computer Science at Covenant University, Nigeria, 08065732380. E-mail: cscwonder@gmail.com*
- *Akomolafe, O.T is currently a program analyst at the Center for Information Technology and Management, Yaba College of Technology Yaba, Nigeria, 08035246387. E-mail: olumidetunde@gmail.com*
- *Oyedeji A.I is currently a lecturer in Computer Engineering Department of the Ogun State Institute of Technology, Igbesa, Nigeria, 08030605961.*
  E-mail: ayooyee@yahoo.com

module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a *template*. The *matching module* compares the feature set extracted during authentication with the enrolled template(s) and generates match scores. The *decision module* processes these match scores in order to either determine or verify the identity of an individual. Thus, a biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into one of several identities (viz., identification) or into one of two classes - genuine and impostor users (viz., verification) [4]. Popular behavioral characteristics include gait, speech, signature and keystroke, but unfortunately, these parameters are bound to change with time, age and environment. Whereas, physiological characteristics such as finger print, palm print and iris remains unchanged throughout the lifetime of a person. The biometric system operates as verification mode or identification mode depending on the requirement of an application. The verification mode validates a person's identity by comparing captured biometric data with readymade template. The identification mode recognizes a person's identity by performing matches against multiple fingerprint biometric templates [3]. In conjunction with traditional authentication schemes, biometrics is a potent tool for establishing identity [5]. A number of biometric identifiers are in use in various applications. Each biometric has its strengths and weaknesses and the choice typically depends on the application. No single biometric is expected to effectively meet the requirements of all the applications[4]. For any human physiological and/or characteristics can be used as a biometric identifier, it must satisfy the requirements such as Universality, which means that each person should have the biometric. Distinctiveness: indicates that any two persons should be sufficiently different. Permanence - This means that it should be invariant over a period of time and Collectability: which indicates that it can be measured quantitatively. In this study fingerprint biometric identifier is being used in authenticating users prior to accessing the centralized result processing software. The most widely used method for representing a fingerprint is minutiae pattern [7]. Fingerprint Identification is the method of identification using the impressions made by the minute ridge formations or patterns found on the fingertips. No two persons have exactly the same arrangement of ridge patterns, and the patterns of any one individual remain unchanged throughout life. Fingerprints offer an infallible means of personal identification. Other personal characteristics may change, but fingerprints do not.

3 SYSTEM DESIGN AND METHODOLOGY

The biometric security layer developed on the result processing software is a windows application implemented using visual basic.net (VB.net). Digital person finger print library component and the digital personal SDK were used for the fingerprint identification framework. The digitalperson is equipped with dlls and components that convert scanned fingerprints into features and fingerprint template which can be stored in a binary field of a database table. It also has facility to compare test sample features with stored template for identification purposes.

3.1 Simulation tools

The following software applications and SDK were used in the development of the biometric authentication part of the biometric secured result processing software.

- Visual studio 2010
- Digitalpersona one touch SDK
- Microsoft SQL server database 2008

3.2 System development stages

The system development can be divided into three basic parts namely

1. The enrollment module
2. The verification module
3. The handshake mechanism

Enrollment module

The enrollment module is a window application installed on designated systems to acquire staff fingerprint. During enrollment process four of the ten fingers were enrolled into the system and stored in the users table on the result server. it should be noted that enrollment was done prior to the deployment of the biometric secured result processing software to ensure that all the fingerprint template are loaded during verification. The enrollment application has the ability to re-enroll an individual several times this is to ensure that a user can come and re-enroll in-cases of wrong or incorrect recognition. The fingerprint is stored into a binary field in the database after the features are cumulated and converted to digitalpesona fingerprint template using the digital personal library files that comes with the one touch SDK. The flow chart in Figure 1 shows a representation of the enrollment system design.

The Verification module

The verification module is a windows application installed on all valid users' system. To successfully launch the result processing application is only possible via the verification module has it redirect users to their designated page (each user has a privileged level that characterizes the data available to work with). The normal login page of the result processing software is made in-accessible by typing the url only. The verification module generates an encrypted code which is a combination of the username and a secret key. The secret key is changed periodically by a programmed job from the Microsoft sql server database. The secret key is a collection of five characters to make a string. The collection of characters is to ensure that it remain highly unpredictable by a simple guess. The encrypted code generated is sent to the Browser to open the result portal for use. Figure 2 describes the system design for the verification module using a flow chart.

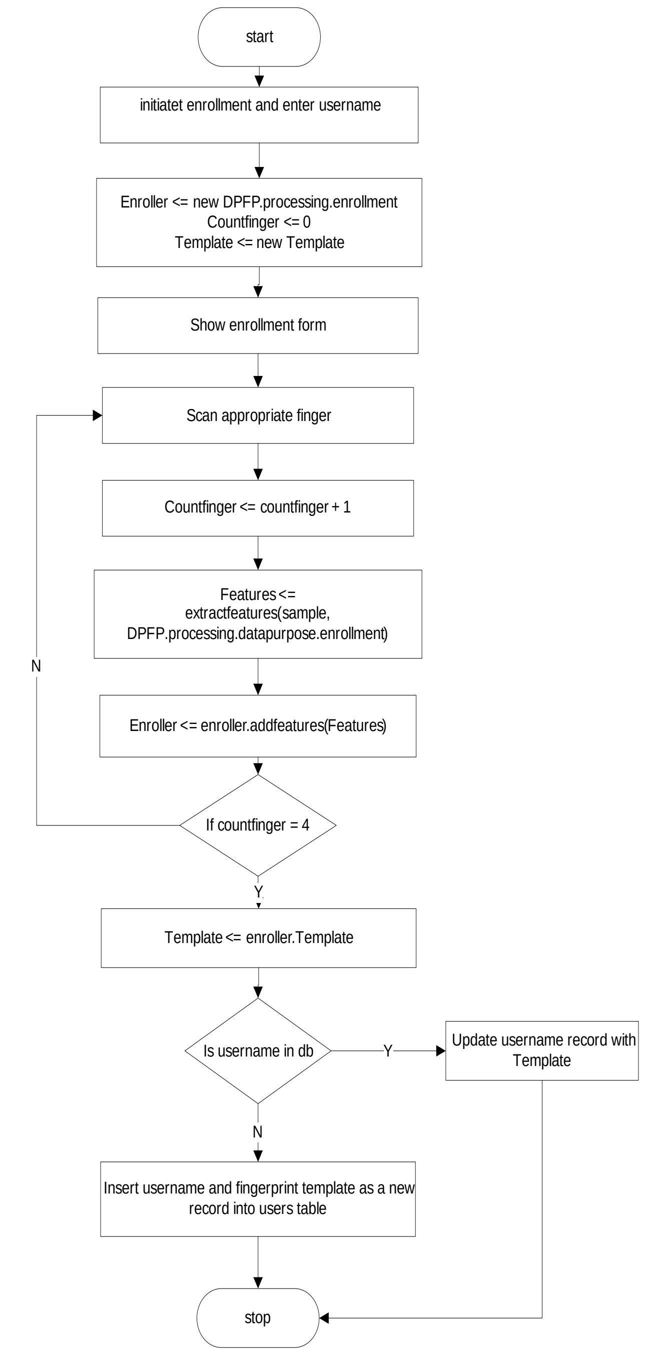

start
initiatet enrollment and enter username
Enroller <= new DPFP.processing.enrollment
Countfinger <= 0
Template <= new Template
Show enrollment form
Scan appropriate finger
Countfinger <= countfinger + 1
Features <=
extractfeatures(sample,
DPFP.processing.datapurpose.enrollment)
Enroller <= enroller.addfeatures(Features)
If countfinger = 4
N
Y
Template <= enroller.Template
Is username in db
Y
Update username record with Template
N
Insert username and fingerprint template as a new record into users table
stop

Fig. 1: Flowchart for enrollment system

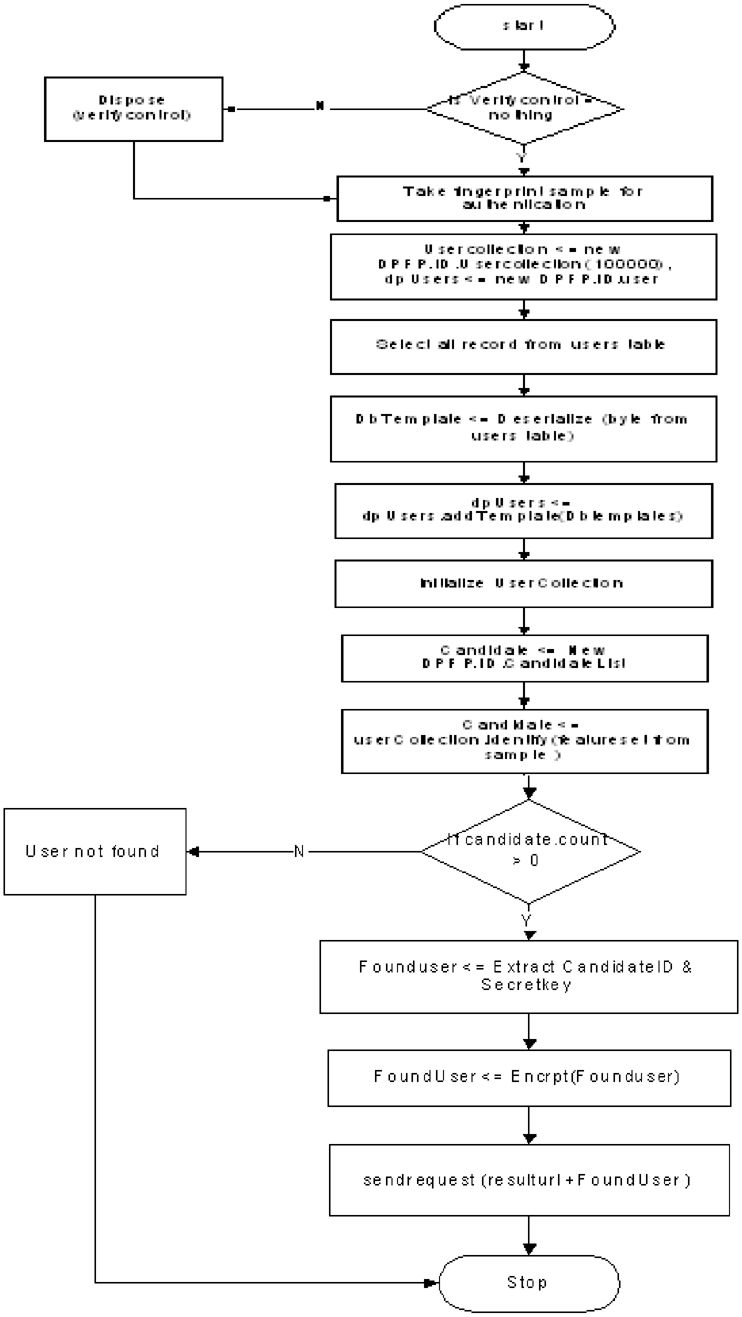

start
If Verify control = nothing
N
Dispose (verify control)
Y
Take fingerprint sample for authentication
Usercollection <= new DPFP.ID.Usercollection(100000), dpUsers <= new DPFP.ID.user
Select all record from users table
DbTemplate <= Deserialize (byte from users table)
dpUsers <= dpUsers.addTemplate(Dbtemplates)
Initialize UserCollection
Candidate <= New DPFP.ID.CandidateList
Candidate <= userCollection.Identify(featureset from sample)
If candidate.count > 0
N
User not found
Y
Founduser <= Extract CandidateID & Secretkey
FoundUser <= Encrpt(Founduser)
sendrequest (resulturl + FoundUser)
Stop

Fig. 2: Authentication module flow chart

The handshaking mechanism

The handshake mechanism is developed into the base class of the result processing software as a static function. The function fetches the secret key from the database and decrypts the query string sent to the browser from the verification module. After the decryption, the handshake module checks for the secret key if the matches the database current value. If it matches the module then check the user and pass the preconfigured access right to it and further determine the address to redirect the users request. For users with multiple access, available user's roles are displayed in a grid view for selection.

3.3 Database design and entity diagram

Three tables were synchronized to design an effective authentication protocol for the result processing software. The tables are the staffTable (i.e. Staff table which stores staff details), RoleTable (i.e. Designated roles table which stores roles assign to each user) and Users Table (i.e. all valid users table which stores fingerprint templates and usernames). The “staffTable” has a 1 to many relationship with the “roleTable” (1 x n). This implies that different users created in the staffTable are assign different role(s) (which describes the privilege level of the individual) in the roleTable. Some people have more than one roles assign to them. Example of such people are individuals who are class adviser for 3 classes (example class adviser for ND 1 and ND 2). The users table has the biometric fingerprint templates of valid users created during the enrollment process. The users table has an “Id” field (i.e. users identification number) has the primary key to ensure that the table can accept fingerprint of same users described by same username at different times in case of wrong identification of users. Such users are reenrolled into the system and the table keeps all the enrolled templates for the username. This is done to enhance recognition rate by increasing training samples for a particular user. Figure 3 describes the entitiy relationship of different tables used.

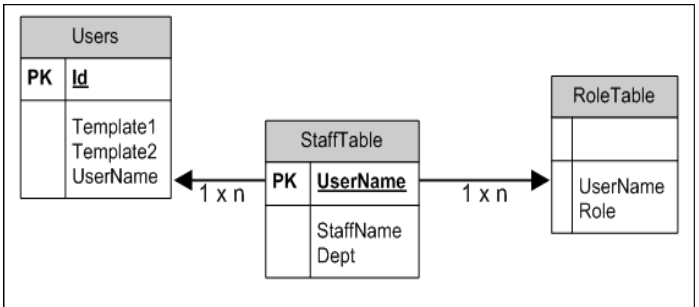


Fig. 3: Database entity relationship diagram.

3.4 Data flow diagram

A representation of the dataflow for both enrollment and authentication module is shown in figure 3 and 4 respectively. This shows where data emanates and are consequently stored after each decomposed process.

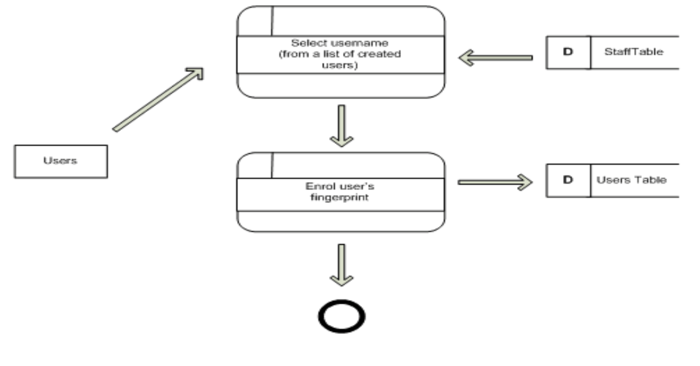


Fig. 4: Data flow diagram for the enrollment process

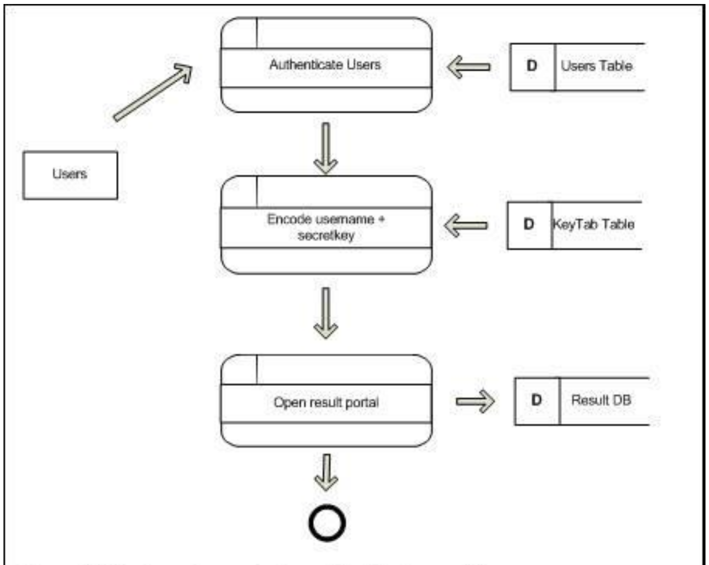
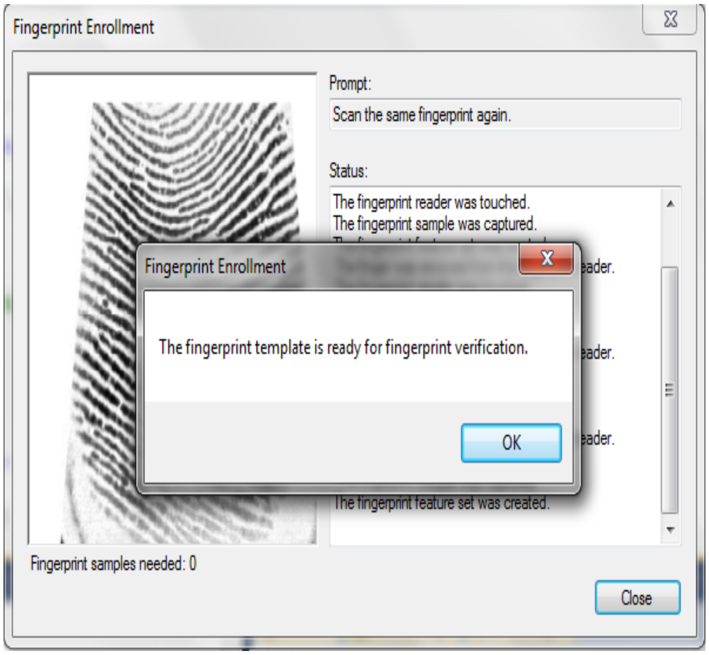


Figure 5: Data flow diagram for the authentication module

4.0 IMPLEMENTATION OUTPUT AND DISCUSSION

The system developed was of two parts namely the enrollment application and the authentication (i.e. identification module) application. The enrollment application was installed on designated systems. The systems were operated by data entry staffs in charge of capturing various users' fingerprint. Form output in figure 6 shows enrollment application after taken user's fingerprint sample and figure 7 shows a message box that indicated the end of a capturing session for user “wonder2”.


Fingerprint Enrollment

Prompt:
Scan the same fingerprint again.

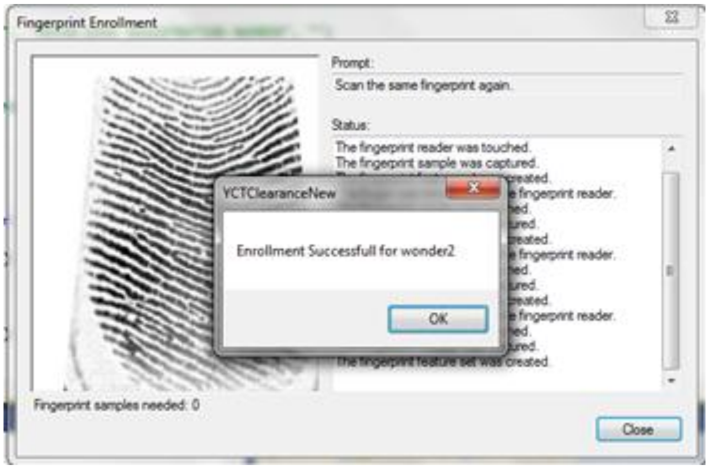
Status:
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.

Fingerprint Enrollment
The fingerprint template is ready for fingerprint verification.
OK

Fingerprint samples needed: 0

Close

Figure 6: *Form output after taking all the four fingerprint samples to form templates*



Scan the same fingerprint again.

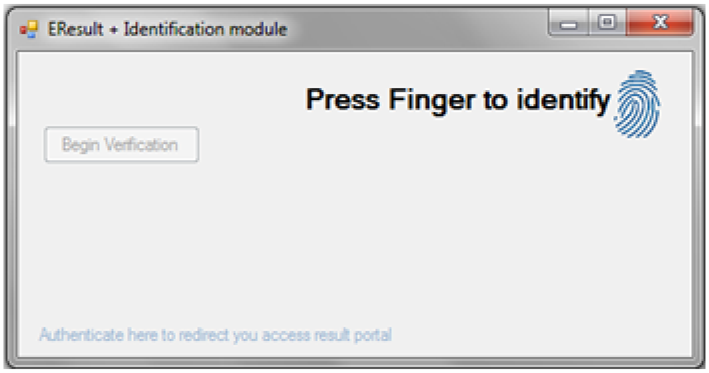
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.

Enrollment Successfull for wonder2

Fingerprint samples needed: 0

Fig. 7: *Form output showing the end of fingerprint capturing for user wonder2*

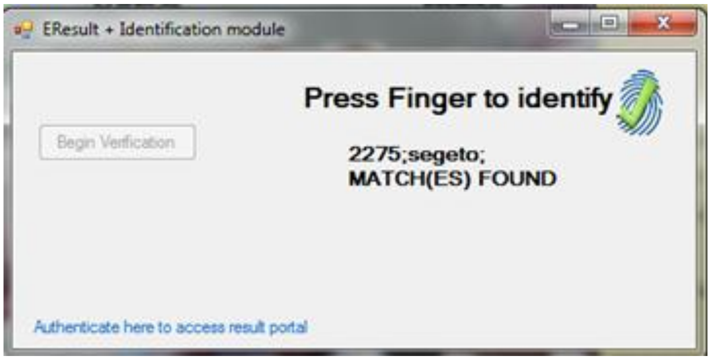
The authentication application was installed on every users' system. To gain access to the result portal, the user authenticates itself by placing any of the enrolled finger on the fingerprint scanner attached to the system after lauching the application. The interface shown in figure 8 and 9 is the form output of the authentication application before and after scanning a valid user's fingerprint. Figure 10 shows the web application triggerd after the user was identified. The address bar has the encoded string which was as a result of encrpting the username and the current secret key in the keytab table.



Press Finger to identify

Authenticate here to redirect you access result portal

Figure 8



Press Finger to identify

2275;segeto;
MATCH(ES) FOUND

Authenticate here to access result portal

Fig.9

SELECT CHOICE

○ Redirect to programmer's module
○ redirect to Vetting module

Fig. 10

5.0 Conclusion

This study showed the development of a window application based fingerprint authentication system to safeguard access to the result processing software. The enrollment and authentication application software were both developed using visual basic.net. The authentication application was installed on users system to redirect users to the result's portal website address without having to login using the conventional username and password. The request sent to the browser during the redirection also contains information that identifies the user to ensure that the individual was made to see what has been pre-configured to be seen based on its privilege level. This development ensures that no intruders were allowed to make malicious update or compromise the integrity of result without being well logged into the database showing the write transaction done by such individual. The system developed will ultimately help to eradicate cases of innocent users being punished for changes made to result by intruders and safeguard students' result data.

References

[1] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," Biometrics and Security Technologies International Symposium (ISBAST 2008), pp. 1-6, 2008.

[2] M. Akazue M. 1 and N.F. Efozia, "A review of biometric technique for securing corporate stored data," International Conference on Software Engineering and Intelligent Systems, pp. 329-342, 2010.

[3] J.K Ravi, B. Raja and K.R. Venugopal, "Fingerprint Recognition Using Minutia Score Matching," International Journal of Engineering Science and Technology, Vol .1, no. 2, pp. 35-42, 2009.

[4] A. Ashraf, A.E Kama, A.K Eman and A.E Ebeid, "Score Level Fusion for Fingerprint, Iris and Face Biometrics," International Journal of Computer Applications, Vol. 111, no. 4, Feb. 2015.

[5] A.K Jain, "Technology: Biometric recognition," nature international journal of science, Vol. 449, pp. 38-40, sept. 2007.

[6] O.O. Ayanuga, O.N Lawal, O. Oladipo and W.A Salau, "Multi-factor Authentication for Social Media," Nigeria Computer Society 12th international conference, Vol 26. pp. 168-175, July 2015.

[7] E. Zhu, J. Yin, C. Hu and G. Shang, "Quality estimation of fingerprint image based on neural network, " international conference of neutral computation, pp. 57-70, 2005.

[8] E. Zhu, J. Yin, C. Hu and G. Shang, "A Systemic method for fingerprint ridge orientation estimation and segmentation," pattern recognition, vol. 39, no 8, pp. 1492-1472, 2006.