# A MULTI-LEVEL AUTHENTICATION SCHEME FOR CONTROLLING ACCESS TO INFORMATION OF AN ENTERPRISE

**Mba O. Odim [1], Gbenga S. Fashoto [2], Victoria. I. Nsiamuna [1]**

**[1] Redeemer's University – Ede, Department of Computer Science**
**[2] University of Swaziland - Department of Computer Science**

Corresponding Author: Mba O. Odim, odimm@run.edu.ng

***ABSTRACT***: This study proposed a multilevel authentication security scheme for controlling access to private and sensitive information against unauthorised users. The scheme is composed of face recognition at the first level and username/password authentication, at the other level. The face recognition was modelled using principal component analysis, while the username and password employed VB.Net password tool. One hundred users were enrolled and their faces captured using a webcam; they were afterward used to access the performance of the proposed system. The results showed that access could only be granted by successful validation of the combined authentication levels. However, it was observed that the face recognition accuracy of the scheme could be impeded by the wrong positioning of the capturing device. Nevertheless, experiment showed that the scheme could provide a stronger protection of sensitive information than the single security level authentication scheme.

***KEYWORDS:*** Authentication, Access control, Information security, Principal Component Analysis, Face Recognition.

## 1. INTRODUCTION

Security of information will ever remain a major concern to organizations due to the ever-increasing sophistication of security breakers. There has been an increased frequency of unauthorized actions to information systems in recent years. This increase has been attributed mostly to internal users of information system, who account more than fifty percent of all violation ([BS17]). Managing access control to data/information in an authorized and authenticated way has therefore remained one of the key challenges in information security. In a complex environment, data owners and service providers need to continuously monitor all data access activities (who is accessing which data) in order to prevent unauthorized access ([H+16]). Information system security has evolved following the rapid technological progress and at the same time due the modern social contexts ([MG15]). Three most important considerations that require attention in information security architecture are: authentication, authorization, and access control. The user's authentication involves the verification of the provided credentials against those present in the database; authorization is the process of determining whether the user possesses substantial enough privileges to access the requested resources or not, and access control is the process by which access to those resources is restricted to a selected number of users.

Password authentication is one of the simplest and the most convenient authentication mechanisms. However, password authentication is an insecure network and is present in many application areas. Most password schemes are vulnerable to various attacks and are neither efficient, nor user friendly ([LLH06]). It easily could be forgotten. Biometric authentication systems have been recently gaining some popularity due to their ability to analyze the unique biological characteristics of human beings ([T+06]). The biometric characteristics are unique in nature which cannot be misplaced, stolen, forgotten, guessed, or easily forged. The face recognition technology is a branch of biometrics through which the humans are identified ([A+07]). Face recognition has become an essential identification scheme in modern age as the need for identification of individual has increased with the globalization of the world. Personal authentication through face has been under research since last two decades. The performance of the face recognition system has been enhanced using various algorithms. The Common algorithms used for face authentication, which are most traditional and extensively used algorithms in the research of face recognition are Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) ([NQA15]). PCA has been shown to be better than LDA with small dataset ([MK01]).

## 2. RELATED WORK

A numbers of research efforts to managing access control to data/information in an authorized and authenticated way was been ongoing. A dynamic access control system for cloud computing environment along with policy conflict resolution algorithm and several authorization validation processes was developed in ([H+16]). Four models:

access right, policy, access control management and authorization were considered in the proposal. The proposed system introduced a more efficient security scheme using an enhanced authorization scheme. The finding from the experimental analysis of the study showed that the proposed model could efficiently deal with the access control management in the cloud environment. In ([MG15]), a survey of the current security models with was carried out with a specific classification in term of their use: Access Control, Flow Control and Administration and presented a Flow Control and Administration models that allow the reinforcement of the security.

A basic introduction to Attribute Access Control (ABAC) and a comprehensive review of recent research efforts toward developing formal models of Attribute Access Control (ABAC) was provided in ([SO17]). The study presented a taxonomy of ABAC and used it to categorize and evaluate surveyed articles. Open problems were identified based on the shortcomings of the reviewed works and potential solutions discussed. An assessment of access control in cyber-physical system was conducted in ([LLK17]). It was discovered that existing solution neither satisfied the prioritization requirement efficiently nor worked well in cyber-physical system environment. Consequently, a new access control mechanism, named multi-factor access control, that employed a multi-factoring technique was developed. In the multi-factor access control, a user is granted multiple secret keys (that is factors) from independent authorities. When accessing a highly prioritized object, the user must present more than two factors, each of which is issued from different authorities. This decreases the probability of false evidence of qualification, increasing protection level. An identity-based cryptography (IBC) was employed in ([L+17]) to propose a Distributed Authentication and Authorization Scheme (DAAS), where an identity-based signature (IBS) was used to achieve distributed verifications of the identities of publishers and users. A new password authentication scheme was proposed in ([LLH06]). Users and the system could use the agreed session key to encrypt/decrypt their communicated messages using the symmetric cryptosystem. However, previous password schemes were vulnerable to various attacks and were neither efficient, nor user friendly.

Biometric authentication systems have been recently gaining some popularity due to their ability to analyze the biological characteristics of human beings ([T+06]). The face recognition technology is a branch of biometrics through which the humans are identified ([A+007]). Face recognition has become an essential identification scheme in modern age as the need for identification of individual has increased with the globalization of the world. In ([O+007]) humans and algorithms were merged using partial least square regression (PLSR). The study resulted in increased performance to near-perfect classification accuracy. In ([NQA15]) a survey of different approaches of face recognition was discussed. These were Holistic, Statistical, Artificial Intelligence, and Feature based. It was concluded that the hybrid approach was comparatively best approach as it uses two approaches. Further studies of some of the common and reliable approaches for facial recognition were explored in ([PS15]). These approaches include PCA, LDA, KDA, Neural Network etc. The paper discussed the basic model of facial recognition and explained each stage of this model. It also included different methods of feature extraction to describe the facial components. Priyanka and Singh ([PS15]) further observed that conducting a face recognition for one single face does not take a long time to process, but it takes a longer time to carry out face recognition on companies that have many faces. The paper implemented attendance/security system on companies that have many faces to be recognized. Cloud computing is a computing service that is done not on a local device, but on an internet connected to a data center infrastructure. The system of cloud computing also provides a scalability solution where cloud computing can increase the resources needed when doing larger data processing. The study was carried out by applying eigenface while collecting data as training data was done by using REST concept to provide resource.

This study proposed a multilevel authentication scheme for controlling access to private and sensitive information against unauthorised users. The scheme was composed of face recognition at the first level and username/password authentication at the other level. Users who want to access the private and sensitive information of the enterprise are required to enroll first. On successful enrollment, they are required to pass through authentication process by providing their credentials to access the required service or information. The process starts with face detection/recognition at the first level, if it succeeds, the user is then prompted to enter his username and password, otherwise, the authentication process is terminated and access denied. Full access is only granted by successful combination of face recognition, username and password authentication.

## 3. METHODOLOGY

The scheme provides a multilevel authentication scheme to access the private and sensitive (protected) information of the enterprise. Users are required to enroll first. Credentials required at enrolled include a facial template, username and password. On successful enrollment, they are required to pass through authentication process by providing their credentials to access the required service or information. The principal component analysis was employed for the facial recognition template, while the Visual Basic.NET username/password was used for the username/password credentials.

Figure 1 shows the block diagram of the proposed multilevel authentication scheme, composed of Facial recognition at the first level, Username name verification at the second level and Password verification at the third level.

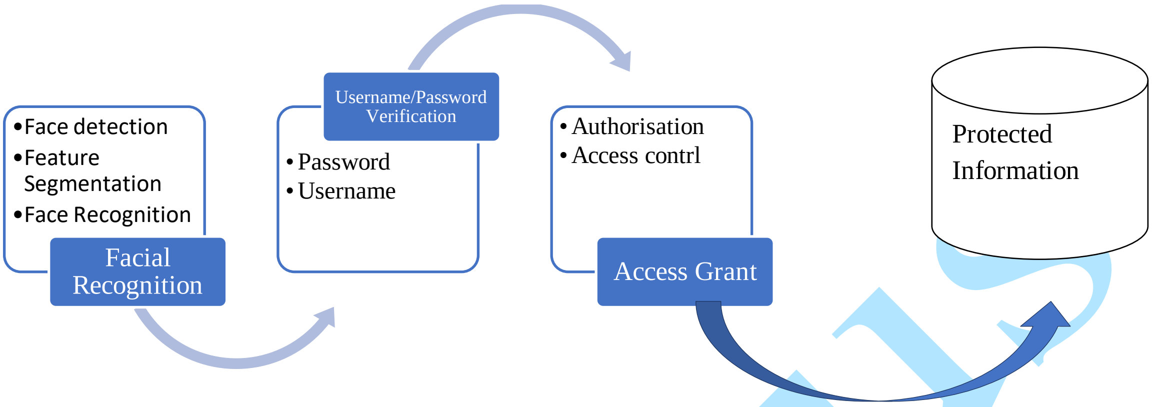


**Figure 1: A block diagram of the proposed multilevel authentication scheme**

The authentication process begins with facial recognition, whose success or otherwise determines whether or not the intended user will proceed to the next level of authentication (Surname and password verification). Access to the protective information is only possible is the entire authentication process succeeds.

### 3.1 Facial authentication method

A generic facial authentication method contains three major steps that is face detection, facial features segmentation and face recognition.

a. Face Detection
b. Features Segmentation.
c. Face Recognition

Face detection is one of the essentials and first step to all facial analysis. Feature segmentation is a simultaneous process, sometimes face detection suit comparatively difficult and require 3D head pose, facial expression, face relighting, gender, age and lots of other features ([M+13]). Face recognition is less reliable and its accuracy rate is still not up to the mark ([RCR13]). Figure 2 depicts a block diagram of general face recognition system.

The principal component analysis (PCA) was used to model the face recognition. PCA, as described in ([Mee13]) was utilized in compressing data sets of high dimensional vectors into lower dimensional ones. This procedure is useful, for instance, in representation and feature extraction. PCA is a procedure of distinguishing patterns in dataset and characterizing the information in such a way its similarities and contrasts can be highlighted.

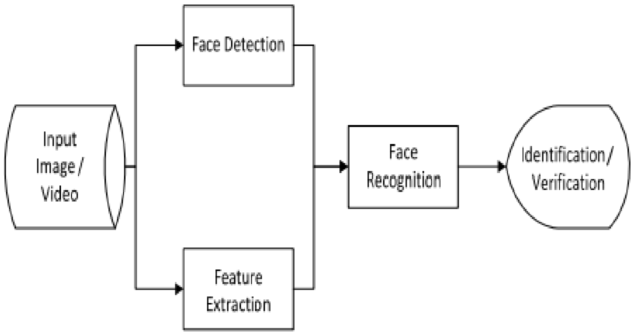


**Figure 2: Block diagram of general face recognition system ([NQA15])**

Patterns in dataset could be difficult to locate in information of high length, where the advantage of graphical outline is not accessible, PCA is a solid apparatus that can be utilized for breaking down the data. One other main advantage of PCA is the point at which these patterns are situated in the information, the data can be compacted, i.e. by decreasing the quantity of measurements, without much loss of data. The choice of this method was based on the algorithm being one of the most widely used algorithmic technique for face recognition. The PCA for the recognition process is divided into the training and testing phases. Figure 3 shows the training and testing phases respectively.

The training stage, involves the following procedure:

1. Convert the original images of the training set into a set of eigenfaces E
2. Compute the weights for each of the images in the training set and store in the set W
3. Obtain the unidentified image X, compute the weights for X and store the weights in the vector WX

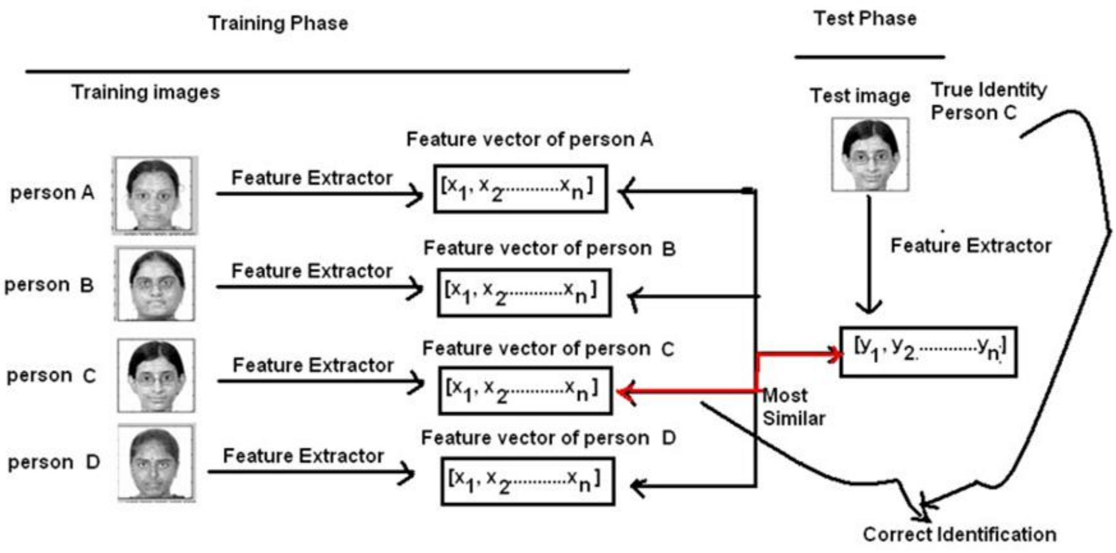

Training Phase
Test Phase
Training images
Test image
True Identity Person C
Feature vector of person A
person A
Feature Extractor
$[x_1, x_2 ........ x_n]$
Feature vector of person B
person B
Feature Extractor
$[x_1, x_2 ........ x_n]$
Feature Extractor
Feature vector of person C
person C
Feature Extractor
$[x_1, x_2 ........ x_n]$
$[y_1, y_2 ........ y_n]$
Most Similar
Feature vector of person D
person D
Feature Extractor
$[x_1, x_2 ........ x_n]$
Correct Identification

**Figure 3: Training and testing phases using PCA for face recognition ([Mee13])**

At the testing stage, we compare the weight WX of the test image X with the weights W of the training image as follows:

1. Compute the mean distance D between the weight vector W and the weight vector WX of the unidentified image.
2. Compare D with some threshold value.
3. If D goes beyond the threshold, θ,
   a. then show that the weight vector WX of the unidentified image is far apart from the weights of the faces. In such a scenario, the unidentified image X is not a face.
   b. Else, X is in fact a face, store its weight vector WX for later organization. Note that the optimal threshold value has to be determined factually.

The username-password was modelled using VB.Net, the following are the main code segments.

```
Private Sub btnUserLogin_Click (ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnUserLogin.Click
    If txtBxUserPassword.Text = "" Then
MsgBox("User Password Required", MsgBoxStyle.Critical,
"Missing Password")
    Else
      Dim SqlQuery As String
      Dim sqlCommand As New OleDbCommand
      Dim sqlAdapter As New OleDb.OleDbDataAdapter
      Dim table As New DataTable
      Dim noOfUsers As Integer
      Dim passwordExist As Integer = 0
      Dim i As Integer

      'to open connection
      Call ConnectionDB()

      Try
SqlQuery = "SELECT Password FROM
tblFaceRecognition WHERE Username= '"
&lblUsername.Text& "'" 'select all the fields in this table
        With sqlCommand
.CommandText = SqlQuery
```

## 4. RESULT AND DISCUSSION

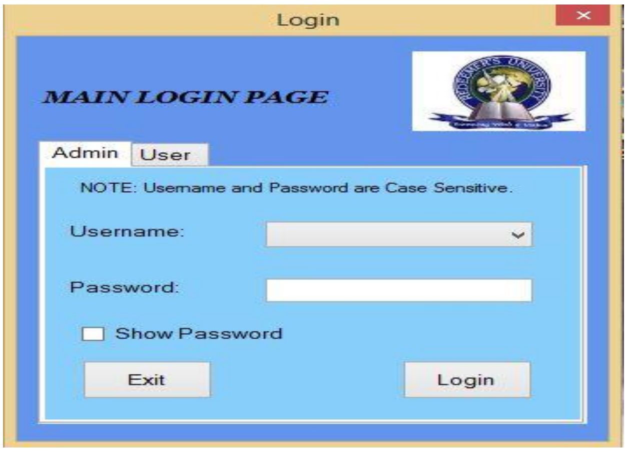
The implementation and the experimental result are presented and discussed in the following sections.

### 4. 1 Implementation

This subsection presents sample screenshots of User's Interfaces.

#### *4.1.1 Administrator's Module*

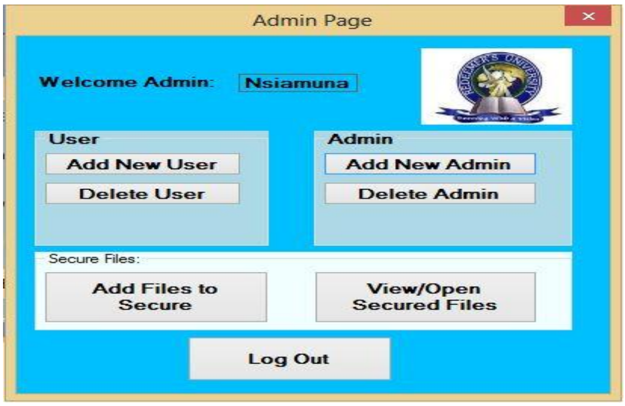
The main login consists of the Administrator's and the User's part as shown in Figure 4. This page provides a link to all parts of the face recognition system.



NOTE: Username and Password are Case Sensitive.

**Figure 4: Login page**

The Administrators can add, delete users and files (to be secured), view and access secured files (see figure 5).



Welcome Admin: Nsiamuna

**Figure 5: Administrative page**

The administrator is allowed to choose documents to be secured (see Figure 6) by clicking the Add Files to secure tab.

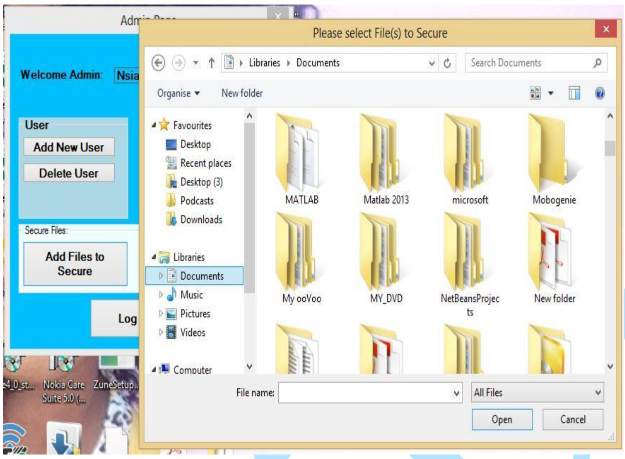
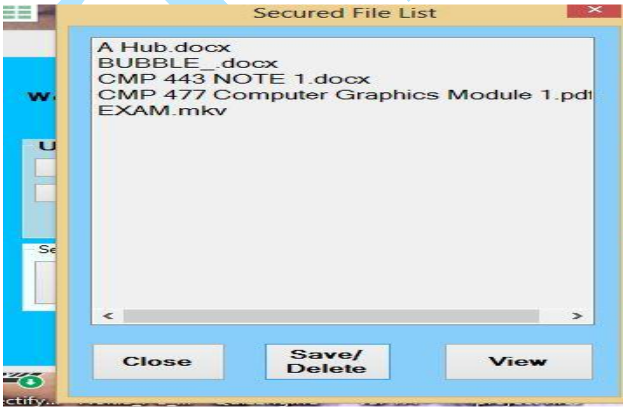


**Figure 6: Document repository**

Selected documents are displayed for verification, which could be deleted otherwise (sample documents are shown in Figure 7).



A Hub.docx
BUBBLE_.docx
CMP 443 NOTE 1.docx
CMP 477 Computer Graphics Module 1.pdf
EXAM.mkv

**Figure 7: Secured file list**

The administrator can delete a user if such user is no more required to access the private and sensitive information of the enterprise (see Figure 8).

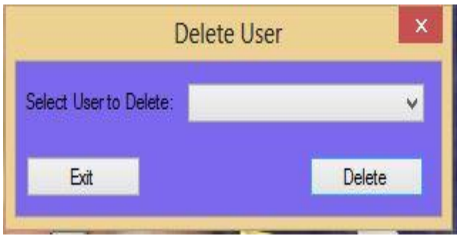
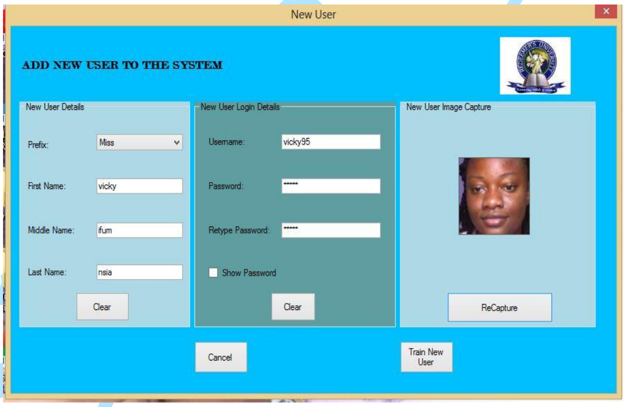


**Figure 8: The delete user interface**

### *4.1.2 User's Enrollment and Authentication*

**Users enrollment**: Users are required to be enrolled by the administrator before accessing the service/information. Figure 9 depicts the enrollment page.

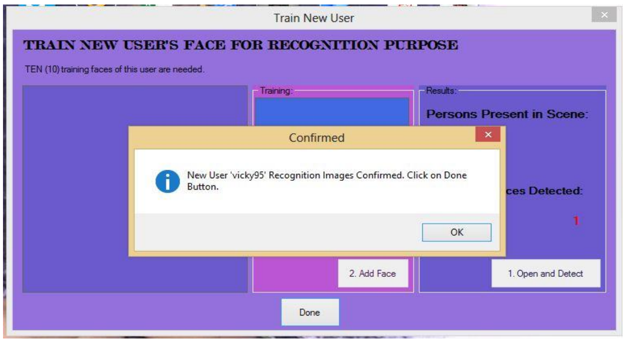


ADD NEW USER TO THE SYSTEM

Prefix: Miss
First Name: vicky
Middle Name: ifum
Last Name: nsia
Username: vicky95
Password: ******
Retype Password: ******

**Figure 9: Add New user interface**

Ten poses of the user's face are captured for the facial recognition training. If the training succeeds, a confirmation paged is displayed otherwise, the process is repeated until confirmation (see Figure 10).



TRAIN NEW USER'S FACE FOR RECOGNITION PURPOSE

TEN (10) training faces of this user are needed.

New User 'vicky95' Recognition Images Confirmed. Click on Done Button.

**Figure 10: Train new user**

**User's Authentication:** Successful enrolled users are required to go through some authentication process before access is granted to the protected documents. The authentication begins with facial recognition. The user's face is recaptured and match with enrolled captured faces in the database (see Figure 11).

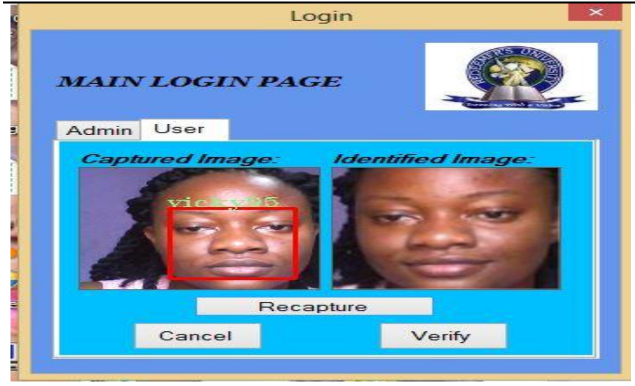
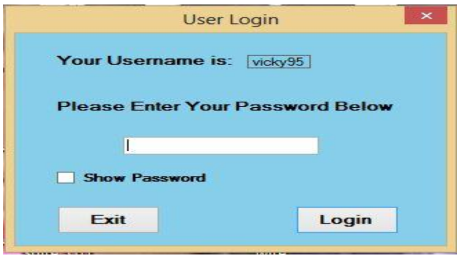


**Figure 11: User login page**

On successful verification of the face, the user enrolled username is displayed and he is prompted to enter his password (see Figure 12), otherwise, authentication fails.

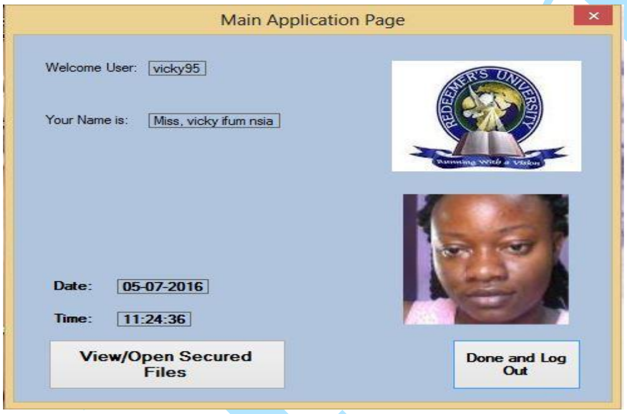


Your Username is: vicky95

□ Show Password

**Figure 12: User's login**

On successful login, the user is allowed to access the protected information (see Figure 13).



Welcome User: vicky95

Your Name is: Miss, vicky ifum nsia

Date: 05-07-2016

Time: 11:24:36

**Figure 13: Main application information access page**

## 4.2 Discussion of the Findings

### *4.2.1 Face Matching Ability of the System*

One hundred successful enrolled users were used to authentication and access control capability of the proposed scheme. The number of trials were carried out incrementally (10, 20, …, 100) The result is shown in Figure 14.

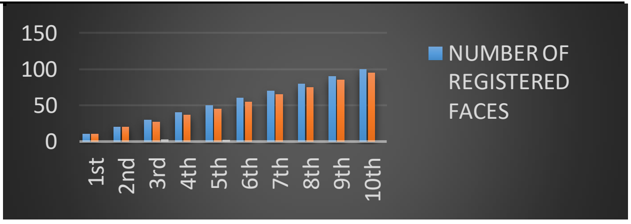


**Figure 14: Trials on identification of enrolled users**

The recognition ability of the 100 enrolled users was about 95%. The 5% error was due to some variations in the lighting conditions which affected the face capturing device. On adjusting the positions of the webcam of the computer system, this error was corrected (see figure 15) and recognition capability recorded 100%.

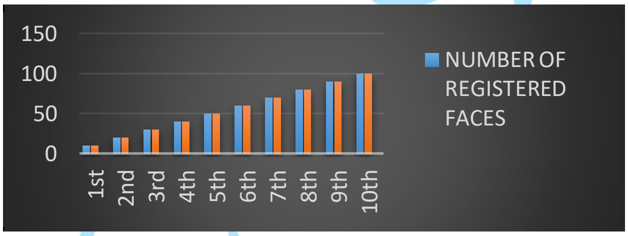


**Figure 15: Trials on authentication of registered faces after adjusting the system's webcam**

### *4.2.2 Assessment of the access control ability of the system*

A number of trials were conducted incrementally to examine the effectiveness of the system in granting access to authenticated/authenticated users. Figure 16 shows the result of this experiment.

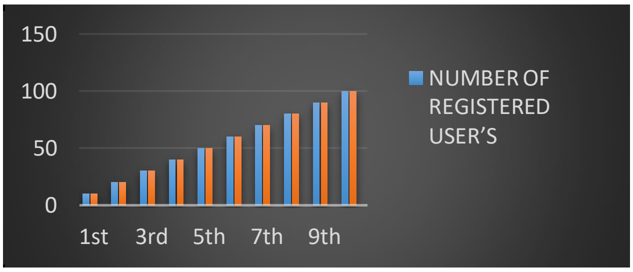


**Figure 16: Trials on access granting capability of the system**

The system recorded a 100% success in granting access to the secured information to the registered users.

## 5. CONCLUSION

The study proposed a multilevel authentication scheme for controlling access to private and sensitive information of an enterprise. The scheme consists of facial recognition, username and password authentication. The face recognition was modeled using the principal component analysis, while the username and password authentication were implemented using VB.Net tools. Empirical experiment showed that the scheme could provide a stronger protection of sensitive information than the single security level authentication scheme.

## REFERENCES

[A+07] **A. F. Abate, M. Nappi, D. Riccio, G. Sabatino** - *2D and 3D face recognition: A survey*, Pattern Recognition Letters, 28(14), 1885-1906. doi:10.1016/j.patrec.2006.12.018, 2007.

[BS17] **A. Boiko, V. Shendryk** - *System integration and security of information systems*. Procedia Computer Science, vol 104: 35 – 42, 2017.

[H+16] **M. Habiba, M. R. Islam, A. B. Ali, M. Z. Islam** - *A new approach to access control in cloud*, Arab J. Sci Eng., *41*, 1015-1030. doi:10.1007/s13369-015-1947-8, 2016.

[L+17] **R. Li, H. Asaeda, J. Li, X. Fu** - *A distributed authentication and authorization scheme for in network big data sharing*. Digital Communication and Networks, 3(4), 226-235, 2017.

[LLH06] **I. Liao, C. Lee, M. Hwang** - *A password authentication scheme over insecure networks*, Journal of Computer and System Sciences, 72 (4), 727-740. doi:10.1016/j.jcss.2005.10.001, 2006.

[LLK17] **E. Lee, J. Lim, J. Kim** - *Prioritized access control enabling weights, fine-grained protection in cyber-physical systems*. International Journal of Distributed Sensor Networks, 13 (12), 1-12, 2017.

[Mee13] **M. Meenakshi** - *Real-Time facial recognition system - design, implementation and validation*, Journal of Signal Processing Theory and Applications, 1, 1-18, 2013.

[MG15] **M. Mammass, F. Ghadi** - *An overview on access control models*, International Journal of Applied Evolutionary Computation (IJAEC), vol 6(4), 28-38. doi:10.4018/IJAEC.2015100103, 2015.

[MK01] **A. C. Martínez, A. Kak** - *Pca versus lda: Pattern Analysis and Machine Intelligence*, IEEE Transactions, 23(2), 228-233, 2001.

[M+13] **M. Murtaza, M. Sharif, M. Raza, J. H. Shah** - *Analysis of Face Recognition under Varying Facial Expression: A Survey*. The International Arab Journal of Information Technology (IAJIT), 10(4), (2013).

[NQA15] **M. Naeem, I. Qureshi, F. Azam** - *Face rcognition technique approaches: a survey*. Sci.Int. (Lahore), 27(1), 301-305, 2015.

[O+07] **A. J. O'Toole, H. Abdi, F. Jiang, P. J. Phillips** - *Fusing face-verification algorithms and humans*, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 37(5), 1149 - 1155. doi: 10.1109/TSMCB.2007.907034, 2007.

[PS15] **Priyanka, Y. Singh** - *A Study on Facial Feature Extraction and Facial Recognition Approaches*. International Journal of Computer Science and Mobile Computing, 4(5), 166-174, 2015.

[RCR13] **N. Rathore, D. Chaubey, N. Rajput** - *A survey on face detection and recognition*, International Journal of Computer Architecture and Mobility, 1(5), 2013.

[SO17] **D. Servos, S. L. Osborn** - *Current Research and Open Problems in Attribute Access Control*, ACM Computing Survey (CSUR), 49(4), doi:10.1145/3007204, 2017.

[T+06] **X. Tan, S. Chen, Z. Zhou, F. Zhang** - *Face recognition from a single image person: A survey*, Pattern Recognition, 3(1), 3-5, 2006.